ITI LIMITED
(A Govt. of India Undertaking)

Expression of Interest

FOR

Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center

Tender Notice No: ITI/MSPDelhi/2k22/SDC/02 Date: 24.05.2022

Addl. General Manager
ITI Limited, MSP-Delhi
201-202 Rohit House
3, Tolstoy Marg, New Delhi-110001
Phone: (011)-23317195
Email: namita_mspnz@itiltd.co.in
Website: www.itiltd.in

ITI LIMITED
(A Govt. of India Undertaking
Addl. General Manager ITI Limited,
MSP-Delhi 201-202 Rohit House 3,
Tolstoy Marg, New Delhi-110001
Phone: (011)-23317195
Email: namita_mspnz@itiltd.co.in

TENDER NOTICE

Tender Notice to: **ITI/MSPDelhi/2k22/SDC/02**
Date: 24.05.2022

ITI Limited invites ONLINE bid in TWO COVER SYSTEM (Technical & Financial) from eligible bidders which must be valid for a minimum period of 180 days from date of bid opening for following items:

Scope of Work	Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center

Interested parties may view and download the tender document containing the detailed terms & conditions at free of cost from the websites CPP Portal OR http://itiltd.in

The ONLINE bid is to be submitted over the tender wizard portal superscribing "Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center"**.**

Any queries may please be sent to etenderiti_mspdli@itiltd.co.in or you can contact below mentioned officers.

The helpdesk nos. **for bidding:**

a) **Shri Prashant Kumar: +91-99100-48364**
b) **Shri Abhay Sharma: +91-78274-50462**

M/s ITI Limited
AGM MSP Delhi

Subject: Expression of Interest (EoI) for Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center

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

This EOI/RFP/Tender is aimed at identifying suitable Commercial Organization as a 'System Integrator' having adequate strength in the above field.

The 'System Integrator' (SI) shall act as a OEM/System Integrator 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 EoI/RFP/Tender document.

Few important points & timelines are being furnished hereunder.

Sl. No.	Important Points / Timelines	Details
1	**EoI/RFP/Tender Enquiry Authority**	Addl. General Manager 201, 202 Rohit House, 3 Tolstoy Marg New Delhi- 110001 Ph: (011)- 23317195 namita_mspnz@itiltd.co.in
2	**Contact Person for the clarification of EoI/RFP/Tender Document**	Shri Prashant Kumar, Chief Manager Contact: +91-99100-48364 Shri Abhay Sharma, Marketing Executive Contact: +91-78274-50462
3	**Tender Type** **(Open/Limited)**	open
4	**No. of Cover/Packet**	Two Cover System
5	**Tender Category (Goods/Services/Works)**	Works
6	**Payment Mode (Online/Offline)**	Online RTGS/ NEFT Bank: Bank of Baroda, KG Marg MICR: 110012021 IFSC: BARB0CURZON Acc. No.: 06230500000010
7	**EoI/RFP/Tender Document Cost (inclusive of GST)**	10,000/-
8	**EMD Amount**	30,00,000/-
9	**Estimated Value of Enquiry**	-------
10	**Due Date, Time & Place for Sale of EoI/RFP/Tender Document**	31.05.2022; 12:00 p.m.
11	**Due Date, Time & Place for Submission of Bid**	31.05.2022; 02:00 p.m.

12	**Due Date, Time & Place for Opening of Technical Bid**	31.05.2022; 04:00 p.m.
13	**Due Date, Time & Place for Opening of Financial Bid**	Will be intimated
14	**Performance Security**	10% of contract value Or As asked by the customer

In order to get the clarity of the scope of work / terms & conditions, the bidders are requested to go through the whole EoI/RFP/Tender document and other project related requirements carefully. An explicit understanding of the requirement is rather essential for arriving at commercial assessment by the prospective bidders.

The selected bidder who is to play the role of a 'System Integration Associate (SIA)' has to enter in to a Contract with ITI Limited to forge a case-specific business alliance (under sole investment business modal) for arranging the requisite bidding inputs.

This EoI/RFP/Tender is being issued with no financial commitment and the response to this EoI/RFP/Tender shall not be assumed as mandatory for short listing of the vendor for giving the work.

Addl. General Manager
MSP-Delhi

Project Background:

ITI Limited (ITI) is a Public Sector Undertaking which functions under the aegis of The Ministry of Communications and IT, Government of India.

We at MSP-Delhi (which is part of the Corporate Marketing Department located at Bangalore) are engaged in the business of Telecom / ICT and e-Governance projects implementation, Supply of Hardware and Software and the services related with these items.

ITI is interested in addressing some of the prospected business opportunities where it is strongly positioned by virtue of its 'PSU Status', proven 'Project Management Capabilities' and rich Relevant- Experience. ITI is looking for business association from reputed System Integrators/ OEMs who can assist ITI to win the business and ultimately help ITI in the execution of the project.

The objective of this Invitation for submission of bid is to identify a System Integration Associate **(SIA)** to address a particular 'Business Opportunity' / a kind of 'Business Opportunity' which has emerged or under process to emerge from a client for the implementation of a project in Government Domain. The prospective customer has already published/disclosed its broad requirement through an Invitation for EoI/RFP/Tender/e-Mail/Discussions which is to be responded with the submission of Techno-commercial Proposal / Bid in due course of time.

The selected bidder who is to play the role of a 'System Integrator' has to enter in to a contract with ITI Limited to forge a case-specific business alliance for addressing the opportunity.

During the bidding process, the vendor is supposed to provide the requisite Techno-commercial inputs to ITI as per the Requirements/Specifications/Expectations/Scope of Work of the prospective customer to win a commercial-favour in terms of award of order to ITI. The name of the end-customer and other finer details of the Projects would be shared with the selected bidder prior to the actual bidding to be done by ITI.

In the event of the award of an order to ITI, the selected business associate would act as a SI/ Vendor to implement the project for which a separate 'Purchase Order' would be placed on the selected SI.

Eligibility Criteria of the Bidders:

The bidders are to fulfill the following eligibility criteria **and submit documentary proof in this regard:**

	Eligibility Criteria of Applicants	**Required Documents**
A	**Company Profile:** 1. The Bidder/ Consortium Partner shall be in operations for a period of at least three years prior to the date of bid submission. 2. The Bidder/ Consortium Partner should be a company registered in India for a period of at least three years prior to the date of bid submission.	Copy of certificate of Incorporation/Registration under Indian Companies Act1956/ 2013with roles & responsibilities of lead bidder and consortium partner.
B	Bidder's Undertaking for willingness to work with ITI as per customer tender terms and conditions.	Undertaking for the same.
C	**Company Financial Profile:** The Bidder/ Consortium Partner (singly or jointly) shall have an average annual turnover of INR 100 Crores over the last three (3) Financial Years i.e. for FY 2018-19, 2019-20, 2020-21.	Financial Audit Reports & CA Certificate.
D	The Bidder/ Consortium Partner (singly or jointly) should have a combined net worth of minimum INR 15 crore as on last date of latest audited financial year.	Bidder / consortium partner should produce a Certificate from the Chartered Accountant/Statutory Auditor confirming the net worth

E	**Key Certifications:** 1. The Bidder/ Consortium Partner shall have the following Certifications valid at the time of submission of bid. a. ISO 9001:2008 Or equivalent b. ISO 20000:2011 for IT Service Management or equivalent certification. c. ISO 27001:2013 for Information Security Management System or equivalent certification. d. CMMI- Level-3 for Analysis, Design, Application Development & Maintenance, Information Security & System Integration of Client Business Solutions, Data Centre Services, Cloud Implementation & Managed Services, Network Implementation Services.	ISO Certificates and CMMI Certificate confirming the desired requirements
F (1) (2) (3)	The Bidder/ Consortium Partner (singly or jointly) shall have an experience in Telecom Networks/ ICT/Cyber Security projects/ Data Centers/ DC Consulting/ DC Build during last 3 years from Government/PSU/ Statuary bodies, ending last day of month previous to the one in which applications are invited should be either of the following: - a. Three similar works costing not less than the amount equal to 60 Cr. OR b. Two similar works costing not less than the amount equal to 80 Cr. OR c. One similar work costing not less than the amount equal to 100 Cr. **AND** The Bidder/ Consortium Partner (singly or jointly) should also have consulted/ designed/ implemented at least two enterprise class Datacenters projects of value not less than 50 Cr. **AND** The Bidder/ Consortium Partner (singly or jointly) should have necessarily implemented at least three projects of Data Centre IT components including cyber security or cumulative value of INR 20Crores.	Copy of Purchase Order/s.

G	The Bidder/ Consortium Partner (singly or jointly) should have at least two Certified ITIL OR at least two certified ISO 20000:2018 LA employees on role.	Certificates of the resources to be submitted
H	**Company standings:** As on date of submission of the proposal, the Bidder as applicable shall not be blacklisted by any State / Central Government Department or Central/State PSUs.	Undertaking for non-blacklisted
I	The bidder should submit valid letter from the OEMs for the new hardware confirming following: a. Authorization for ITI Limited b. 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. c. Undertake that the support including spares, patches, and upgrades for the quoted products shall be available for 7 years from the signing of contract. . Bidder should submit valid letter from the OEMs for each product to be used in datacenter.	Relevant Document

General Terms and Conditions of EoI/RFP/Tender:

The prospective bidders are advised to study the EoI/RFP/Tender document carefully. Submission of your offer/bid shall be deemed to have been done after careful study and examination of the EoI/RFP/Tender with full understanding of its implications. Failure to furnish all information required in the EoI/RFP/Tender Document or submission of an offer/bid not substantially responsive to EoI/RFP/Tender 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**	Only ITI Empaneled Vendor (vendors who have signed the Empanelment Agreement **with ITI on or before the submission of the tender/bid/proposal)**
2	**Non-transferable Offer**	This EoI/RFP/Tender document is not transferable. Only those, who have purchased this offer document, 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 EoI/RFP/Tender document by issuing an addendum / corrigendum in writing or by standard electronic means. The addendum / corrigendum shall be sent to all contenders and will be binding on them. The Bidders shall acknowledge receipt of all amendments. To give bidders reasonable time in which to take an amendment into account in their Proposals ITI may, if the amendment is substantial, extend the deadline for the submission of Proposals.
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.
8	**Validity of Offer**	The offer should be valid for a minimum period of **6 Months** from the date of submission. The Bids valid for a period shorter than specified period Shall be rejected.
9	**Prices**	The prices quoted by the Bidder shall be FIRM during the performance of the contract and not subject to variation on any account. A bid submitted with an adjustable price quotation will be treated as non-responsive and

		rejected.
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.
11	**Taxes and duties**	The taxes and duties are to be clearly mentioned, if any.
12	**Payment Terms**	a) Payment shall be released to the vendor on back-to-back basis and on pro rata basis after ITI has received its payment after the submission of necessary document like Vendor Invoice, receipt acknowledgement of goods by end user etc. b) Other Direct Expenses will be deducted from the payment of the vendor. Expenses like cost incurred by ITI towards EMD/PBG/BG/SD processing. c) The payment shall be done on the basis of actual supply/installation of requirements as certified by the end customer. d) No advance payment will be made during the execution of the p r o j e c t . In case ITI receives any advance payment, the same may be released to the vendor after submission of equivalent amount of Additional BG valid till the completion of obligation for which payment has been released by the end customer.
13	**Warranty**	**1.** The Total duration of the O & M Services will be 5 years
14	**Liquidated Damages (LD)**	Liquidated Damages 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.
15	**Training**	Training of customer officers/representatives will be the responsibility of the selected Bidders.
16	**Acceptance Test Procedure (ATP)**	a) Vendor will conduct the Acceptance Test (AT) before handing over of the project(s) to ITI project executing division. .
17	**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.
18	**Contractual Period**	ITI's Delivery date provided to ITI by customer. Delivery extension will be on back-to-back basis. The successful Bidder shall so organize his resources and perform his work as to complete it not later than the date agreed to.

19	**Extension of Contract**	On back-to-back basis.
20	**Inspection Authority**	All supplies will be subject to customer & ITI inspection.
21	**Tender Award Criteria**	Bidder offering the Highest Net Revenue Share to ITI i.e. lowest landing Cost of items to ITI shall be declared as the successful L1 bidder and the work shall be awarded to the successful declared (L1) bidder.
22	**Tender Document Cost** and **Earnest Money Deposit (EMD)**	**In case of bid submission:** Tender Document Cost and Earnest Money Deposit (EMD) must be remitted through NEFT/RTGS/Net Banking. No interest shall be payable on the EMD. **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 Note: Tender Document Fee will be non refundable
23	**Performance Security Deposit**	The value of performance security shall be 10 % of Contract Value (issued to Business Associate/SIA by ITI) or end-customer's performance security (as per order to ITI) whichever is lower. **The Security Deposit (SD) will be as below:** An amount equal to 10% of each invoice value shall be retained by ITI as Security deposit against Performance
24	**Consortium Bidding**	Consortium Bidding is allowed
25	**Signing of the Bids**	The Bid must contain the name, residence and place of business of the person or persons 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 furnished on 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 the person(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 or overwriting shall only be valid if they are initialed by the signatory (ies) to the bid.

26	**Submission of Tender**	The '**Technical Bid**' and **'Commercial Bids'** shall be uploaded on Tender Wizard Portal.
27	**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. Date and time of opening of price bids will be decided after technical bids have been evaluated by the committee and will be intimated to technically qualified bidders.
28	**Rejection of Bid**	ITI reserves the right to reject any or all tenders/quotations/bids received or 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. ITIalso reserves the right to cancel any order placed on basis of this tender in case of strike, accident or any other unforeseen contingencies causing stoppage of production at ITI or to modify the order without liability for any compensation.
29	**Termination For Default**	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 anymeans at the risk and cost 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 the contractor for completion of the work or part of the works or in case the works or part of works is not to be completed, the loss or damage suffered by ITI. In determining the amount, credit shall be given 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.
30	**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 invoking this 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 the ultimate 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 of the Company's obligations under this agreement; b) Mitigate the effect of any Force Majeure Event; and c) Comply with its obligations under this agreement.

		Further if the period of Force Majeure event extends beyond three months* the parties may consider the fore closure of the agreement. * Period of three months may vary at the discretion of ITI as per the validity period of the contract.
31	**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.
32	**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.
33	**Other Terms and Conditions**	
a		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.
b		The Bids/Offers of the Qualified bidders (who qualify the eligibility conditions) only would be subjected to the technical-evaluation.
c		The bidder is expected to go through the Scope of work and Specifications. The bidders are to quote only fully compliant solution.
d		The bidder may be required to study the existing system being used by the end-client to assess the exact requirements and the Quantum of work on "No-commitment" basis (no commercial compensation would be given to The bidder either by ITI or the end-client for doing this exercise).
e		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.
f		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.
g		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.
h		A clause-by-clause compliance statement to all Sections of the EoI/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 EoI/RFP/Tender document, shall not be considered for evaluation and shall be summarily Rejected.
i		The bidder should study carefully the document to assess the work and Risk factors associated with such type of Business opportunities.
j		The bidder has to consider the following major Cost Factors while arriving at a commercial decision: • Direct Cost (requisite IT Hardware and Application Software) • Taxes/ Duties • Services and Administrative Cost • Training and Documentation Cost

		• Contingencies
k		The bidder should enclose the documents in their '**Technical Bid**' & '**Commercial Bid**' as specified in the tender documents.
l		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.
m		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.
n		Due to any breach of any condition by the bidder, the Bid Security (EMD) submitted by the bidder may be forfeited at any stage whenever it is noticed and ITI 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.
o		All suppliers (including small scale units who are registered with the National Small Scale Industries Corporation under Single point registration scheme) shall furnish Bid Security to the purchaser as per the requirement. As such no bidder is exempted to furnish the EMD.
q		Suitable 'Training' would have to be imparted to ITI personnel at Bidder's cost in the areas of Installation, day to day Maintenance and Operation of entire system (in the event of placement of order by ITI). The training of the personnel shall be to ensure trouble free operations of the System/Equipment by the end customer.
r		The bidder is required to enclose Notarized Copy of the Power of Attorney from its 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.
s		The Power of Attorney given to the Authorized Signatory should be submitted and executed on the non-judicial stamp paper of appropriate value as prevailing in the respective states(s) and the same be attested by a Notary public or registered before Sub-Registrar of the states(s) concerned.
t		"DISCOUNT, if any, offered by the bidders shall not be considered unless specifically indicated in the price schedule.
u		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.
v		ITI shall not be responsible for any postal delay about non-receipt / non- delivery of the bid/documents. This EoI/RFP/Tender Document is absolutely not transferable.
w		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.
x		It is further stressed that synergies between ITI's competitors with the bidder or cartel Formation with other bidders would result in Disqualification of the Bidder.

Special Terms and Conditions of RFP/EoI/Tender:

1. The requirement is meant for addressing a business opportunity which has emerged from some Govt. body against their already published Tender-Notification / Invitation for the submission of Bids which envisages Implementation of Project.

2. The broad 'Scope of Work' would be as per the EoI/RFP/Tender Document. However, the exact Scope of Work will be intimated to the selected SI/Vendor in due course of time (once bidder is short-listed) for addressing the opportunity.

3. The bidder (in the capacity of a System Integrator) is supposed to address the business opportunity jointly with ITI under "Sole Investment Business Model". This may include arranging Bid Security and Performance Bank guarantee etc. All 'Terms and Conditions' as per ITI's customer with regard to Payment / Reward / Delivery/Penalty shall be applicable on the selected Business Associate /SI also (in the event of the award of the business to ITI by the end-customer).It may please be noted that ITI shall not open any 'Escrow Bank Account' with the consortium member/SI (in the event of the award of the order to ITI).

4. The bidder must be prepared to work with ITI limited on exclusive basis and will neither submit any direct proposal (to the end-client) nor submit any business proposal (to the end-client) through other business partner/PSU. In case of violation of the same, the EMD shall be forfeited and the bidder will be black-listed.

5. ITI reserves the right to quote & supply ITI manufacturing products if BOM of EoI/RFP/Tender Document contains ITI manufacturing products.

6. All activities like Proof of concept on "No Cost No Commitment" (NCNC) basis wherever applicable will be the responsibility of agencies.

7. Agencies should be willing to impart required training to ITI engineers for undertaking services & execution of project.

8. Agencies will be responsible for any short coming in the BOM and the same should be rectified free of cost.

9. Agencies should be willing to provide TOT for manufacturing of offered products in ITI if the bidder is an OEM.

10. Agencies should be willing to sign an exclusive agreement with ITI for smooth execution of the

project.

11. Earnest Money Deposit (EMD) / Bid security required for submitting the bid will be borne by the selected agency.

12. All CVC circulars/ Statutory guidelines as applicable needs to be followed.

13. Margin to ITI would be payable on Supply, I&C and AMC services undertaken by the selected agency for the project.

14. At least one of the consortium partner should be empaneled with ITI.

EoI/RFP/Tender Rejection Criteria:

The EoI/RFP/Tender/Bid will be rejected in case any one or more of the following conditions are observed**:**

1. Bids received without Proof of Purchase of EoI/RFP/Tender Document and EMD as per requirement.
2. Bids which are not substantially responsive to the Invitation for EoI/RFP/Tender.
3. Incomplete or conditional EoI/RFP/Tender that does not fulfill all or any of the conditions as specified in this document.
4. Inconsistencies in the information submitted.
5. Misrepresentations in the bid proposal or any supporting documentation.
6. Bid proposal received after the last date and time specified in this document.
7. Unsigned bids, bids signed by unauthorized person (without a valid Power of Attorney.
8. Bids containing erasures or overwriting except as necessary to correct errors made by the Bidder, in which case such corrections shall be authenticated by the person(s) signing the bid.
9. Bid shall remain valid for the specified period from the date of opening of EoI/RFP/Tender prescribed by the purchaser. A bid valid for a shorter period shall be rejected by the purchaser being non-responsive.
10. If Bidder will not submit any relevant documents as per documents to be submitted and Eligibility Criteria.

Please Note

The business associate submitting the bid against this EoI/RFP/Tender must not have an alliance with other bidders / competitors of ITI for the same business opportunity. The bidder if selected as vendor/SI will not be allowed to address the opportunity directly/ extend the help to any other competitor of ITI Limited for the subject project.

Lowest-Bid (Best Qualified Bid) Evaluation Methodology:

1. This EoI/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 EoI/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 EoI/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 generally taken as final, unless the aggrieved party establishes any Prima facie errors in the findings of the Committee. In such a situation, he may file a representation within 3 working days of receipt of decision from ITI Limited, duly listing the reasons / grounds. Such a representation would be considered at Senior Management Level of the Tendering Authority, whose decision would be final and binding on all the bidders.

7. The Bidders who have submitted the EoI/RFP/Tender Document cost & EMD 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 EoI/RFP/Tender Document.

10. The evaluation of technical and commercial marks will be normalized and then 50% weightage will be given to technical evaluation and 50% weightage will be given to financial evaluation in order to calculate a comprehensive mark.
11. Formulae for Evaluation is as mentioned below:
12. Bid Evaluation

    First and Second Stage Bid Evaluation

    All EoIs (bids) would be subjected to a process where the weightage of the technical part would be 60% and the weightage of the Commercial/Financial part would be 40%.

TECHNICAL RATING (**TR)** would be evaluated on the basis of the following formula:

$$\mathbf{TR} = \frac{\mathbf{60}}{\mathbf{100}} \mathbf{x\ Technical\ Score\ (TS)}$$

Where Technical Score **(TS)** would be calculated as per the committee marks.

Vendor should have at least 650 Technical Score out of 1000 to become eligible for opening of commercial bid.

COMMERCIAL RATING **(CR)** would be evaluated on the basis of the following formula:

$$\mathbf{CR} = \frac{\mathbf{40}}{\mathbf{100}} \mathbf{x\ Commercial\ Score\ (CS)}$$

COMMERCIAL SCORE (CS) will be worked out as formulae given below

A= Cost for Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center

B= Margin (in Percentage)

C= (A*B)/100

D= A-C

$$\mathbf{CS} = \frac{\mathbf{D}\text{ of the Lowest Bidder's Quote }\mathbf{(LQ)}}{\mathbf{D}\text{ of the Actual Bidder's Quote }\mathbf{(AQ)}} \mathbf{x\ 1000}$$

VR (Vendor Rating) = **TR** (Technical Rating) + **CR** (Commercial Rating)

The Bidder with highest VR will be treated as best bid.

13. ITI reserves the right to reject any or all bids without assigning any reasons thereof. ***It shall not be obligatory for ITI to award the work only to the lowest bidder.***

Matrix of Technical Bid Evaluation:

The technical evaluation for ascertaining the Technical Rating (**TR**) of the bids will be done strictly on the basis of Technical Score (TS) which would be computed as per the matrix shownbelow:

Sr. No	Parameters	Weightage in terms of Scoring		Max. Score
1.	Bidder/ Consortium Partner's combined net worth.	Eligibility Criterion (Minimum) to 1.2 times of the Eligibility Criterion	50	100
		More than 1. 2 times to 1.5 times of the Eligibility Criterion	75	
		More than 1. 5 times of the Eligibility Criterion	100	
2.	Bidder/ Consortium Partner should have certifications	ISO 9001:2008, 27001:2013	50	100
		ISO 9001:2008, 20000:2011, 27001:2013	75	
		ISO 9001:2008, 20000:2011, 27001:2013, CMMi V2.0	100	
3.	Bidder/ consortium partner's Average Annual Turnover duringlast 3 Financial Years	Eligibility Criterion (Minimum) to 1.2 times of the Eligibility Criterion	50	100
		More than 1. 2 times to 1.5 times of the Eligibility Criterion	75	
		More than 1. 5 times of the Eligibility Criterion	100	
4.	Bidder/ Consortium Partner shall have experience in Telecom Networks/ICT/Cybersecurity/DC	a. Three similar works costing not less than the amount equal to 60 Cr. OR b. Two similar works costing not less than the amount equal to 80 Cr. OR c. One similar work costing not less than the amount equal to 100 Cr.		50
5.	The Bidder/ Consortium Partner (singly or jointly) should also have consulted/ designed/ implemented of Data Center	At least two projects of value not less than 50 Cr.		50
6.	The Bidder/ Consortium Partner (singly or jointly) should have necessarily implemented Data Centre IT components including cyber security	At least three projects of INR 20Crores.		100

7.	Bidder/ Consortium Partner should have minimum 2 ITIL OR 2 ISO 20000:2018 LA certified employees	2 ITIL or 2 ISO 20000:2018 LA certified employees		100
8.	ITI's past Experience with the Bidder/ Consortium Partner.	No Experience	00	50
		Past Experience	50	
9.	Availability of Technical Man-Power with theBidder/ Consortium to Manage the Project Activities.	Eligibility Criterion (Minimum) to 1.2 times of the Eligibility Criterion	25	50
		More than 1. 2 times to 1.5 times of the Eligibility Criterion	50	
10.	Understanding of the Requirement, Technical Solution, Project Implementation Plan, Availability and OEM's Backing for Warranty Note: Submit a copy of technical presentation along with technical bid			100
11.	Technical Presentation	Average (demonstrates an ambiguous Solution	50	200
		Fairly Good (demonstrates an Ordinary Solution)	100	
		Very Good Solution	150	
		Excellent Solution	200	

Documents to be submitted along with the "Technical Bid":

The Bidder/System Integrator (SI) must submit the following documents along with their Technical Bid:

1. Bid covering Letter on the Letter-Head of the Bidder Company indicating Name and Address of the Authorized Signatory (with Contact telephone numbers and email ID)as per Annexure-A.
2. Bidder's Profile as per Annexure-B.
3. Proof of Empanelment with ITI.
4. Power of Attorney authorizing the bidder to submit the Bid/EoI on behalf of the Bidder/Consortium.
5. Tender-Document Cost of required amount.
6. Bid Security (EMD) of required amount.
7. Copy of PAN Card.
8. GST Registration Certificate.
9. Turnover Certificate(s)/Audited Balance-sheet(s) & Profit-Loss Account(s) of the Bidder /All consortium members for last three years.
10. Declaration on the Letter-Head of the Bidder Company for Non-Black Listing as per Annexure-C.
11. Declaration / Undertaking on the Letter-Head of the Bidder Company as per Annexure-D.
12. Compliance Statement of '**Eligibility Criteria of the Bidder'** along with supporting documents (credentials, experience certificates, declarations & others)
13. Integrity Pact /Non-Disclosure Agreement as per
14. Tender Documents duly signed & accepted by the bidder
15. All MAF and other technical documents should be submitted by vendor along with technical bid

In case, the bidders do not submit any of the above mentioned papers/information along with Expression of Interest, his bid will be rejected and bid will not be considered for further evaluation.

It is reiterated that any bid not fulfilling any of the essential requirements mentioned in this EoI/RFP/Tender document would be classified as "Technically Non-Qualified/Non-Responsive" and Commercial bids of such bidders will not be opened and subsequently returned to the bidder. ***No relaxation would be given to any bidder on any of these conditions.***

Documents to be submitted along with the "Commercial Bid":

The Bidder/System Integrator (SI) must submit the following documents along with their Commercial Bid:

1. Price Bid as per EoI/RFP/Tender Document format only. No other format will be accepted.

Brief Scope of Work:

Section IV- Scope of Work
The selected bidder shall operate, and maintain the SDC for a period of 5 years from the date signing of contract. The selected bidder shall undertake expansion of the CUSTOMER'S DATA CENTER as and when required by SITEG during the currency of the agreement at the rates quoted for add-on components in the financial bid.

Operations and Maintenance

The selected bidder will provide 24x7 operating and maintaining services for a period of 5 years from the date of signing of contract. The scope of the services for overall Physical and IT infrastructure management as per ITIL framework during this period shall include 365x24x7 Monitoring, Maintenance and Management of the entire Data Centre, along with providing Helpdesk services. The scope of work during the operations phase is divided into the following areas:
System Administration, Maintenance & Management Services
Network Management Services
Backend Services (Mail, messaging etc.)
Storage Administration & Management Services
Security Administration Services
Backup & Restore Services
Physical Infrastructure Management and Maintenance Services
Help Desk Services
BMS Services
Services for ISO 27001 and ISO 20000 compliance
Coordination with respective department for application Hosting and provide necessary support for hosting.
Facilitate required support infrastructure for hosted application
Bandwidth Management Services
Desktop/Workstation: DCO has to bring necessary equipment (Desktop, Laptop, Intercom, Printer, scanner, Fax etc) required for day to day functioning of the data centre.
MIS Reports: The bidder shall provide the MIS reports for all the devices installed in the Data Centre in a prescribed format and media as mutually agreed with the SITEG on a periodic basis. Whenever required by Govt. of HP, DCO should be able to provide additional reports in a pre-specified format. Any other report as desired by the SIA/CT/TPA will also be provided by the DCO as and when required.

Creating of VPN for access over the internet and Intranet (Suitable description should be provided)
All Patch cords for LAN connectivity either CAT-6 or FC would be the responsibility of DCO. All the patch cord should be from the same OEM as off Network.

System Administration, Maintenance & Management services

The objective of this service is to support and maintain all the Systems and Servers that will get hosted in SDC for the project period from the Final Acceptance Test:
365x24x7 monitoring and management of the servers in the Data Centre.
Regular monitoring of all the applications hosted at CUSTOMER'S DATA CENTER.
Facilitate application migration in coordination with application owners / departments.
Operating System and database administration, including but not limited to management of users, processes, preventive maintenance and management of servers including updates, upgrades and patches to ensure that the system is properly updated. Bidder should include the Cost for 5 years upgrades, updates, and patches for the components covered under this RFP.
Adoption of data centre related policies related to patch management, backup as defined by the Government of

Customer Site/SIA.
Installation and Re-installation of the server hardware in the event of system crash/failures.
Regular analysis of events and logs generated in all the sub-systems including but not limited to servers, operating systems, security devices, etc. to identify vulnerabilities. Action shall be taken in accordance with the results of the log analysis.
Adoption of policies as defined by the Customer Site
Provide integration and user support on all supported servers and data storage systems.
Problems shall be logged in at the Help Desk and resolved as per the SLAs defined in this RFP document.
Manage and monitor server configuration, performance, and activity of all servers.
Document all server configurations.
Hardening servers, in line with security policies.
Vendor Management: The DCO is required to provide vendor management support to the departments. It must be noted that the user departments would not like to avail any services which overlaps with their existing service contract and lead to multiple ownerships. However, in case the departments require this service then as per the severity level / escalation mechanism agreed with the user department the DCO shall provide vendor management services

Network Management

The objective of this service is to ensure continuous operation and upkeep of the LAN & WAN infrastructure at the SDC including all active and passive components. The scope excludes maintenance of WAN links, which shall be the responsibility of HIMSWAN Implementation Agency. However, for overall functioning of the data center, the selected bidder shall be responsible to coordinate with HIMSWAN team for WAN link related issues.
The services to be provided for Network Management include:

Ensuring that the network is available 365x24x7 as per the prescribed SLAs
Attending to and resolving network failures and snags
Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
Configuration and backup of network devices including documentation of all configurations.
365x24x7 monitoring of the network which should include (hardware component –processor cards, fans, power supplies, cables, latency, bandwidth, packet loss, errors, collisions, security) to spot the problems immediately.
Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.
DCO shall monitor and administer the network within the SDC up to the integration points with HPSWAN and Internet.
DCO shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
DCO shall carry out break fix maintenance of the LAN cabling or maintenance work

Application Monitoring

It should include monitoring of:
Web Services
Application Server
Database Server
Middleware
Others

Backend Services

The selected bidder is required to maintain and support all the Backend Services implemented at the SDC Customer Site, The services includes:

Directory Services
Database Service
Directory Services
It should include the following services:
Domain management;
Group management;
User management;
Implementation of policies and standards

Directory services are to be used within SDC only.
Database Services
Management of database on an ongoing basis to ensure smooth functioning of the same.
Management of changes to database schema, disk space, storage, user roles.
Performance monitoring of the databases on a regular basis including, preventive maintenance of the database as required.
Management of database update or patch update as and when required with minimal downtime.
Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.

Storage Administration and Management Services

The bidder shall be responsible for the management of the storage solution and shall provide the following services:
Identify key resources in the Storage solution
Identify interconnects between key resources in the Storage solution
Receive asynchronous notification that the configuration of the Storage solution has changed
Identify the health of key resources (Fabrics-Fabric errors, zoning errors, Ports-failed GBIC, Device- status/ attributes change Hardware components-processor, memory, Fans, power supplies, utilization of ports) in the Storage solution
Identify the available performance of link failures, loss of signal, loss of synchronization, link utilization, bandwidth GB/s or MB/s or frames/s, statistics of all ports interconnects in the Storage solution
Receive asynchronous notification that the performance of the Storage interconnect solution has changed
Identify the zones being enforced in the Storage solution
Create/delete and enable/disable zones in the Storage solution
Identify the storage volumes in the Storage solution
Create/delete/modify storage volumes in the Storage solution
Identify the connectivity and access rights to Storage Volumes in the Storage solution
Create/delete and enable/disable connectivity and access rights to Storage Volumes in the Storage solution
Storage administration –facilitate the states in connecting to the Storage later and give them access rights as required
Monitoring security:
Administrative task:
Restrict administrative tasks to a select set of users
Enforce strict passwords
Installation and configuration of the storage system at SDC

Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.
Configuration of SAN whenever a new application is hosted on the SDC. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.
These are indicative requirements; DCO needs to fulfill all the requirements mentioned in the SLA.

ISO 27001 ISMS Standards

Bidders are required to submit the ISO 27001 (ISMS) implementation cum certification plan as part of their technical proposal. This plan should be comprehensive enough and will include the milestones, description, timelines etc.

DCO have to ensure to establish PDCA model for the ISMS, DCO would be responsible for establishing, operating, monitoring, reviewing, maintaining and improving the Information Security Management System (ISMS) at the CUSTOMER'S DATA CENTER. For the purpose DCO shall implement ISO/IEC 27001 standard and get certification from the certification body empanelled by CERT-In such as STQC, as well as DCO would be responsible for successfully carrying out surveillance Audit and closer of Non conformities as per requirement of the Certification body. However, DCO have to take consent of SITEG / Client in case of any changes required in policy manual or documentation or in forming of Information security organization or as required. Maintenance activity after getting the certificate is the responsibility of DCO. Also, the DCO has to submit a report within a week of completion of the maintenance activity as defined in the certification, failing which the subsequent QGRs will be deferred.

DC operator (DCO) has to operate the data centre as per ISO/IEC 27001 Standard.

o The CUSTOMER'S DATA CENTER operator i.e. DCO should be made responsible to apply, obtain and maintain the ISO 27001 certification for CUSTOMER'S DATA CENTER project duration and all expenses for obtaining the same must be borne by the DCO. In case of default, please refer the Service Level Agreement, Section 5.8.

ISO 20000 ITSM Standard

Bidders are required to submit the ISO 20000 (ITSM) implementation cum certification plan as part of their technical proposal. This plan should be comprehensive enough and will include the milestones, description, timelines etc.

ISO/IEC 20000 adoption in a CUSTOMER'S DATA CENTER infrastructure helps in ascertaining that the Services delivered to the Client / SIA / User Departments (of the State) by the DCO are:

As per the agreed Service levels

Professionally managed with domain expertise

Project Risks are well understood and managed

DCO shall be responsible to implement ISO/IEC 20000 standard which shall promote the adoption of an integrated process approach to effectively deliver managed services to meet the SDC, Client and User Departments".

Following methodologies are proposed for ITSM standard.

PDCA (Plan-Do-Check-Act) methodology shall be adopted to implement ISO 20000 standard to establish the objectives and processes necessary to deliver results in accordance with customer requirements as well as the SDC's policies and to Implement the processes accordingly. DCO shall Monitor and measure processes and services against policies' objectives and requirements and report the results and take actions on the differences and continually improve process performance.

Alignment of information technology services and strategy.

To create a formal framework for current service improvement projects.

To improve relationship between different departments via better definitions and more clarity in terms of responsibility and goals.

To create stable framework for both resource training and service management automation.

The SDC operator i.e. DCO shall be responsible for applying, obtaining and maintaining the ISO 20000 certification for the entire SDC project duration. DCO shall also be responsible for preparation of Operational Manual for HP SDC along with the certification.DCO must obtain ISO 20000 certification for the CUSTOMER'S DATA CENTER and all expenses obtaining the same must be borne by the DCO.

Maintenance activity after getting the certificate is the responsibility of DCO. Also, the DCO has to submit a report within a week of completion of the maintenance activity as defined in the certification, failing which the

subsequent QGRs will be deferred.

IT Security Administration Services

The objective of this service is to provide a secure environment through the implementation of the ISO 27001 ISMS Standard and finally the DCO must obtain ISO 27001 certification for the CUSTOMER'S DATA CENTER and all expenses obtaining the same must be borne by the DCO. This service includes:
Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked.
Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
Provide a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery etc.
Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, protecting email gateways, firewalls, servers, from viruses.
Ensuring that the security policy maintained and draft various relevant , procedures , guidelines and other ISMS documents as per ISO 27001 standard and implement these procedure accordingly , these documents shall be, maintain and updates as per the ISMS ISO 27001 requirement.

A process must ensure the continuous improvement of all elements of the information and security management system. (The ISO/IEC 27001 standard adopts the Plan-Do-Check-Act [PDCA] model as its basis and expects the model will be followed in an ISMS implementation.
Suitable mechanism should be adopted for maintaining the ISMS, forensic logs or other required government compliance by the DCO time to time. Bidders are advised to refer the CERT-In guidelines for the security alerts and act accordingly.

Backup / Restore Services

Backup of storage as per the defined policies.
Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies as defined by the state
Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.
Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
365x24x7 support for file and volume restoration requests at the Data Centre.
Prompt problem resolution in case of failures in the backup processes.
Media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite). The SIA/State will provide a suitable site/place for offsite storage of media and provide security personal for transportation of media as well as at offsite location. The DCO will be responsible for all backup of the data stored on the SAN as well as servers, brought under this RFP. For any other backup activity related to user department, only the media management is the responsibility of the user department, backup activity will be facilitated by DCO as defined in this section.
DCO shall assure that backup of operating system, database and application is performed as per the Client agreed policies. This is done by monitoring and enhancing the performance of scheduled backups, DCO should ensure schedule regular testing of backups and ensure adherence to related retention policies. DCO would also ensure that 24 x 7 support for file and volume restoration requests is available at the data centre.

Physical Infrastructure Management and Maintenance Services

The bidder shall select the appropriate equipment which are available in industry for infrastructure management solution, the BMS should be deployed to facilitate monitoring and management of the Data Centre Non-IT Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

Proactive and reactive maintenance, repair and replacement of defective components (IT and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the selected bidder.
The selected bidder shall have to stock and provide adequate onsite or offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.
The selected bidder shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by SITEG at any time.
Monitoring physical access (biometric scan, video camera etc.).
DG set performance should be monitored continuously to achieve similar performance (as recorded during FAT) throughout the project period.

Help Desk Services

The help desk service will serve as a single point of contact for all ICT related incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also resolution of incidents. The scope of work includes:
24x7x365 Help Desk facility for reporting issues / problems with the IT infrastructure.
To provide a service desk facility and the set up all necessary channels for reporting issues to help desk. The incident reporting channels will be the following:
Specific E-Mail account
Dedicated Phone Numbers
Web based
To implement a call logging system in line with the severity levels as mentioned in the SLA.
Help Desk shall undertake the following activities:
Log issues / complaints related to IT infrastructure at the Data Centre under the scope of work and issue an ID number against the issue / complaint.
Assign severity level to each issue / complaint.
Track each issue / complaint to resolution
Escalate the issues / complaints if necessary as per the escalation matrix defined in discussion with SITEG.
Provide feedback to the callers.
Analyze the issue / complaint statistics and provide monthly reports including but not limited to:
Type of incidents / calls logged
Incidents / calls resolved
Incidents / calls open
Creation of knowledge base on frequently asked questions to aid the users of the IT infrastructure.
Provisioning of requisite number of Help Desk software licenses for operating the Helpdesk facilities.
The Helpdesk solution should have in built work flow for helpdesk automation.

Preventive Maintenance
DCO has to carry out the Preventive & reactive maintenance of CUSTOMER'S DATA CENTER infrastructure / components. This includes carrying out inspection, testing, satisfactory execution of diagnostics and the necessary repairs and replacement of parts wherever needed to keep the service & operation levels of the IT & non-IT equipment of CUSTOMER'S DATA CENTER in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during the normal office Hours (i.e. 9am to 6pm on weekdays) of

CUSTOMER'S DATA CENTER operations. DCO needs to maintain the Log Book for such preventive and reactive maintenance activities. For Scheduled and Preventive Maintenance by DCO for the Hardware /or Software /or Active /or Passive shall be done with written prior intimation to client at least 72 hours in advance. Preventive Maintenance should be carried out at least once in every quarter, which includes:
Checking for any loose contacts in the cables & connections for the respective infrastructure and equipment.
Run diagnostics tests on respective infrastructure and equipment.
Cleaning and removal of dust and dirt from the interior and exterior of the equipment.
Ensuring that wiring is done as per the standard.
Ensuring that wiring diagrams are updated, whenever there are modifications.
Ensuring the management of rack space equipment as needed.
Ensuring that all Software, Tools (CD / DVD), OEM Documentation (Knowledge base), CUSTOMER'S DATA CENTER documentation (with Manuals), other or backup tapes, disks and other media are kept properly labeled and organized in Catalogue.
Carrying out and verifying back-ups consistency on regular interval.
Checking and listing all wear and tear of the equipment and site environment.
Ensuring no flammable material is present.
Clearing up of any unnecessary items or Spares. CUSTOMER'S DATA CENTER operator needs to ensure cleanliness within CUSTOMER'S DATA CENTER
Preventive Maintenance Activities of components as per the OEM's recommendation/ advice.

Disaster Recovery (DR) Activities
Disaster Recovery (DR) is very important in the context of SDC. The major objective of having DR facility for SDC is to ensure reliable Data Backup and Periodic Replication based on the Replication solution for the State.

The DCO will be responsible for taking the actual backup and providing technical resources and controls for implementing and operating the DR Plan and Strategy as framed by the State Government. DCO shall be responsible for performing all DR activities and creation of related documents as per guidelines of MEITY, GOI, the high level scope of work but not limited is mentioned below:
Preparing DR Strategy and DR Plan based on MEITY, GOI & NIC guidelines and States' individual studies.
Criteria for Disaster declaration
Identification of various risks involved
Preparation of Fault Tolerance mechanisms to follow in case of outages
Stakeholder Analysis containing information on the various Stakeholders and their Roles & Responsibilities in the entire DR Process
Identification of additional Infrastructure on DR Site, apart from the DR infrastructure provisioned under the scheme
Coordinate for provisioning of bandwidth for connectivity from SDC to DR Site.

Enabling Dept users' connectivity to DR Site for infrastructure access & monitoring
Coordinate for Procurement and installation of SAN Storage for consolidation of DR Storage requirements for mapped SDCs in the DR Site
Responsibility of bringing the application live and required setup from DR site
Coordinate for Operations & Maintenance (O&M) of infrastructure owned by State at the DR site
DR Training, conduction of Mock Drills, and updation in DR Plan
Infrastructure & Operations Tracking from SDC to –DR Site (Patch Management, Remote Replication cycle management, Storage availability, Reporting, etc)
Identification of all critical data required for Disaster Recovery
DR Implementation methodology of the State
For the purposes of disaster recovery (DR), DCO shall facilitate and undertake DR drill in accordance with DR Operator, and SITEG.

DR services for CUSTOMER'S DATA CENTER are being provided by M/s Nextra Ltd.

Expansion of CUSTOMER'S DATA CENTER

The broad scope of work during this phase will include the following, but is not limited to:
Design of the Data Centre expansion
Physical Infrastructure comprising of Civil, Electrical & Mechanical works required to build the extension of Data Centre.
Multi-layer physical security infrastructure to prevent unauthorized access to the extended Data Centre
Networking & Security Infrastructure and other associated IT Components in the extended Data Centre
Help desk and other monitoring and management services.
Supply/ Installation
All active and passive components.
Physical infrastructure components such as UPS and Air-Conditioning System, Fire Detection and Control System, Diesel Generator Units, Lighting system, Power, CCTV Surveillance systems, and Network Cabling etc.
IT Infrastructure components such as Servers, Databases, Networking & Security components, Storage media, Software and other IT components required at the extended Data Centre.
Commissioning & Acceptance Testing shall involve the completion of the supply and installation of the required components and making the extended Data Centre available to SITEG for carrying out live Operations and getting the acceptance of the same from the SITEG.
All applications hosted in the SDC will be under the management of Application Owner, the Data Center Operator will only monitor all the applications.

Application migration would be responsibility of the user department, However DCO would facilitate the department to migrate the application.
Acceptance testing shall be carried out before the commencement of Live Operations. The extended Data Centre would be tested for the following parameters:
Electrical Requirements
Cooling & Environmental Control
Fire Detection, Prevention & Suppression requirements
Surveillance & Physical Security
LAN Passive Components
IT Security
All documentation generated during design, installation and commissioning phase shall always be made available to the SITEG on request.
All the hardware and software provided by the DCO under this RFP should have all the relevant supports required for the entire period of the project.
Detailed scope of work for each of the above mentioned components is given below:

Design

The selected bidder shall design the extension of Data Centre in line with minimum requirements as laid out in TIA 942 specifications for Tier II Data center wherever possible. The design should ensure an uptime of 99.749% on a quarterly basis.Some of the key considerations for designing the extended SDC are given below:
Scalability
All components of the data centre must support scalability to provide continuous growth to meet the requirements and demand of various departments. A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system. The Data Centre should support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work together on a common problem in parallel). Modular design of the Data Centre is an excellent strategy to address growth without major disruptions. A scalable SDC shall easily be

expanded or upgraded on demand. Scalability is important because new computing component are constantly being deployed, either to replace legacy component or to support new missions.
In future if any new additional hardware or software procure by the State that will be hosted in the State Data Centre which is under warranty and if the DCO need a specialized skill set to Operate and Manage this hardware and Software O&M charges will be 1.5% per Qtr of respective hardware and Software. Accordingly the SLA for the respective hardware or software will be the responsibility of the DCO.

In future if any new additional hardware or software procure by the State that will be hosted in the State Data Centre which is not under warranty, O&M charges will be 3.0 % per Qtr of respective hardware and Software. Accordingly the SLA for the respective hardware or software will be the responsibility of the DCO.
It is the responsibility of the DCO to provide all the Monitoring Solutions such as EMS, Antivirus, HIPS etc with required hardware, OS, Database and required CAL licenses for their monitoring for implementation of Monitoring Solutions.
It is also the responsibility of the DCO to take care for any kind of scalability that is required in these solution during the project period.
Availability
All the components of the extended data centre must provide adequate redundancy to ensure high availability of the e-Governance applications and other Data Centre services. Designing for availability assumes that systems will never fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage. The bidder shall make the provision for high availability for all the services of the extended data center.
Interoperability
The entire system/subsystem should be interoperable, in order to support information flow and integration. Operating systems and storage technologies from several vendors must interact well with each other. These systems should support the open architecture solutions such as XML, LDAP, SOAP, etc. where information/data can be ported to any system, whenever desired. Open standards compatibility should be a measure for software to ensure its interoperability.

Security
The extended SDC must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from malicious attacks or theft from external (through internet) and internal (through intranet) hackers. Using Firewalls and Intrusion detection systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worms attacks should be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. SDC should also endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired.
The SDC layout should be divided into domains such as:
Inside Zone –is the secure zone which has a restricted access. This zone mainly consists of storage and database servers which are not directly accessible to the outside zone. The inside zone is separated using strong access control and a firewall, which provides an additional level of security to the infrastructure.
Outside Zone – includes the intranet and internet zones. The intranet users and internet users connect to the extended SDC to avail various active services. The outside zone is bifurcated by placing a firewall which strengthens the security of the servers by restricting unauthorized access.
De-militarized Zone – (DMZ) would be a "neutral zone" between extended SDC's internal network and the outside extranet network. It would prevent extranet users from getting direct access to the

servers. In other words, this is a small network that lies between a trusted internal network (SDC LAN), and an un-trusted external network (such as the public Internet). Mostly the DMZ contains devices accessible to Internet traffic, such as Web, FTP, SMTP and DNS servers.
Manageability
The extended CUSTOMER'S DATA CENTER must be designed in an efficient way to ensure an easy maintenance. It must facilitate ease of configuration, ongoing health monitoring, and failure detection that are vital to the goals of scalability, availability, and security. The design must be able to match the growth of the

environment of the Data Center.

Integration of SDC with SWAN

Another most important aspect which should be taken care while designing the extended SDC is about seamless integration with SWAN. Bandwidth requirement between SWAN and extended SDC needs to be taken into consideration; so that there should not be any bottleneck for accessing the extended SDC services. CUSTOMER'S DATA CENTER is connected to SWAN Core Switch through 1 gigabit connectivity in redundant mode.

Internet bandwidth at SDC

State has provisioned internet bandwidth in HP SDC. DCO will liaison with the ISP's. Furthermore, DCO shall be responsible to ensure its availability, and need to co-ordinate & liaison with ISP (selected by state) for internet links.

IPv6 ready Data Centre

All the hardware and software (including but not limited to all the routers, switches, firewall, servers, and operating systems) supplied under this tender shall be IPv6 ready from day one. The performance as specified in the specification of each component in the RFP is for IPv6. These components should also be ready to work on IPv4 whenever required.

Storage

Last but not the least, an assessment of the storage requirement for the entire SDC environment should also be taken into consideration. This would be based on the number of applications, their database structure, users and transactions volume. DCO should design the storage solution (SAN / NAS) keeping in mind the relevant requirement and its usage in line with SDC's objective. The storage system should be scalable enough to handle future requirements. The DCO should also adopt detailed System and Data back-up processes and methodologies, using industry standard tools to provide long term storage and archival solution.

Storage should support controller based or host based zero bit data reclaim (in case it is not controller based it would be the responsibility of DCO to ensure zero bit data reclaim feature with proper storage management policies).

Site Preparation

SITEG shall provide the necessary minimum constructed space for the expansion of the SDC. Selected bidder shall arrange for necessary clearances which shall enable them to undertake civil, electrical, and mechanical works including false ceiling, partitioning, installation of electrical component, cable laying etc at the extended SDC.

Supply/ Installation

The Selected bidder shall procure and supply all IT (active and passive) and Non-IT components. The selected bidder would be required to undertake all the necessary civil, electrical, plumbing and mechanical works including false ceiling/flooring, partitioning, installation of electrical component, cable laying etc and other necessary services to create the Non- IT/Physical infrastructure.

Installation shall mean to install and configure / integrate every component and subsystem component, required for functioning of the extended Data center.

DCO has to bring necessary equipment, as part of facility management services, (Such as desktop, workstation, Printers, Large Display screens (for Incident display and monitoring), , Handsets etc…) required for day to day functioning of the extended data centre.

4.4 Resource Requirement

Indicative Manpower Resources

S. No	Description	Min Qualification, Relevant Expérience & Certifications
1	Project In-Charge/Project Manager	BE/MCA overall 15 Years experience with 10 years in Government Domain, ITIL/ITSM/ISO 20000 Certified
2	Technical Consultant - Data Centre Physical Infrastructure	B.E./B.Tech, 5 Years
3	Technical Specialist - Server / Storage	B. E/B. Tech/MCA, 5 Years, MCSE/RHCE,/MCP
4	Technical Specialist – Network	B. E/B. Tech/MCA, 5 Years, CCNA/CCNP
5	Security Expert	B.E./B.Tech/MCA /preferably Master's Degree in Information Security, 5 Years, Security Certifications, ISMS LA
6	Database Administrator	B.E./B.Tech/MCA, 5 Years, Oracle / MS / relevant Certifications
7	EMS Administrator	B.E./B.Tech/MCA, 3 Years
8	Storage Administrator	B.E./B.Tech/MCA, 5 Years
9	System Engineer	B.E./B.Tech/MCA, 3 Years
10	Electrical Engineer	B.E./B.Tech/3 year Polytechnic Diploma in Electrical, 3 years experience
11	Infrastructure Support Staff	ITI with 3 Years experience in Civil/ Electrical Infrastructure Support
12	Helpdesk Staff	Graduate, 2 Years, Relevant, ITIL Knowledge
13	Support Staff / Back office Staff	Relevant House Keeping Experience
14	Security Guard	Minimum 3 years of relevant experience, 10th pass

PRICE BID

Price Bids will be uploaded in the format available at Tender Wizard Portal

(Bid Covering Letter / Annexure-A)

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

Subject: Bid Covering Letter against Expression of Interest (EoI) for Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data Center

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 **2021**

Authorized Signatory

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

(Annexure-B)

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)	2017-18	2018-19	2019-20
5.	IT Turnover in last 3 financial years (Rs in Crore)	2017-18	2018-19	2019-20
6.	Profit / Loss in last 3 financial years (Rs in Crore)	2017-18	2018-19	2019-20
7.	Net-worth in last 3 financial years (Rs in Crore)	2017-18	2018-19	2019-20
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 **2021**

Authorized Signatory

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

(Annexure-C)

To
ITI Limited, MSP-
Delhi
Rohit House, 3
Tolstoy Marg New
Delhi- 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 **2021**

Authorized Signatory

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

(Declarations / Annexure-D)

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

Subject: Declarations against Expression of Interest (EoI) for Operation and Maintenance, and expansion of physical and IT infrastructure for State Government Data CenterDevelopment Programs
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) for getting 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 / Security submitted 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 upon question under any circumstances

Dated this Day of **2021**

Authorized Signatory

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

(Annexure-E)

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 **2021**

Authorized Signatory

Name:
Designation:
(Company Seal)

(Annexure-G)

INTEGRITY PACT

PURCHASE ORDER No.

THIS Integrity Pact is made on……day of..... 21 .

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

1.1 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.

1.2 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

2.1 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

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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

4.1 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.

4.2 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

5.1 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.

5.2 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

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

6.2 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.

6.3 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)

8.1 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.

8.2 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.

8.3 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.

8.5 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.

8.6 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.

8.7 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

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

10.2 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

11.1 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.

11.2 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).

11.3 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

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

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

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

12.4 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.

12.5 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 not be subject to any Arbitration.

12.5 The action stipulates in this Integrity 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.

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

For PRINCIPAL For CONTRACTOR(S)

…… ……

(Name & Designation) (Name & Designation)

Witness Witness

1) ……1)……...

11. Annexure 4 - Inventory & Expansion BOM

Existing BoM

6.1 Exiting Hardware Inventory – IT (HPSDC)

SN	Component	Make	Model	Specifications	Count
1	Firewall	Cisco	cisco_asa_5585_ssp20	ASA 5585-X Chassis with SSP20 8GE 2 SFP2 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 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	6

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	6

				series chipset USB2 Enhanced Host Controller 2 * Emulex LPe 12002 Dual Port 8Gb Fibre Channel HBA 2 * Broadcom 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), 2.70 GHz	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	1

				10Gb SFP+ Adapter-2 Nos) 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 module MMF 850nm DOM 4 * 1000BASE-T SFP (NEBS 3 ESD) Cisco ASR1002-X 4GB DRAM	2
7	SAN Switch	Cisco	cisco_mds_9513	Cisco MDS 9506 Base	2

				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	
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 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	2

				UP/ 8p LIC KVM local IO cable for UCS servers console port	
9	Storage	Hitachi	Hitachi HUS VM	HUS / HUS VM File Module SMU 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	1

				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 LAN ports,4 PIM slots, and 2 EPIM/PIM slots 1 GB DRAM, expandable to 2 GB	1

				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 Engine - 2U - RoHS. Includes Signature Protections, BehavioralProtections and BWM. With signature Update	2
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	6

				Platinum PS Forward airflow, 16 * 1000BASE-T SFP 32 * 10GBASE-SR SFP Module, Promo Layer 3 License for Nexus 6001	
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 airflow, 2 * Nexus 1100W Platinum PS Forward airflow, 12 * 1000BASE-T SFP 12 * 10GBASE-SR SFP Module, Promo Layer 3 License for Nexus 6001	3
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,	6

				4 * Blade slot blanking panel for UCS 5108/single slot	
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 * 128GB 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 Nexus 7K USB Flash Memory - 8GB (Log Flash) Nexus 7000 - Supervisor 2 Enhanced	2

				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-Series48 Port 1/10G (SFP+) Enhanced 24 * 1000BASE-SX SFP transceiver module MMF 850nm DOM Nexus 7000 F2-Series48 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	

6.2 Existing Software Inventory (HPSDC)

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
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 (HPSDC)

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	Civil	NA	lumpsum

	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			
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 HPSDC 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
9	Antivirus License	Symantec	Symantec Endpoint	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	Number Licence(s) for for SAN Management	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

6.5 Existing CCTNS Project Hardware

Sr. No	Device	Make	Model Name	Count
1	Juniper Firewall	Juniper	SRX 650/Juniper	1
2	Core Switch	Juniper	Ex2200/Juniper	1
3	Safenet HSM	Safenet	Safenet HSM	2
4	Load Balancer	Array	Array APV 5600	2
5	DB Server	IBM	X3850X5	2
6	IBM Blade Chassis	IBM	Blade Center H/IBM	1
7	Blade Server1	IBM	X440	8
8	Primary 10 G Switch	IBM	IBM Flex Fabric 10Gb Switch	2

9	Primary 10 G Switch	IBM	ibm Flex 8GB San Pass-thru	2
10	HP Tape Library	HP	MSL8096	1
11	KVM Console	APC	APC Schneider Electric	1

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

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

Expansion BOM

6.7 New BOM for extended HPSDC 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.	FC Module for existing SAN Switch (Cisco 9513), fully populated 8/16 Gbps ports with SFP's	IT	4
7.	Servers (including chassis, controllers, cables and all accessories & modules etc)	IT	1000 Cores, & 6TB RAM
8.	Database Server	IT	3
9.	500 TB Usable space for Existing Storage (Hitachi VSP1000)	IT	500 TB usable space
10.	Security Incident and Event Management	IT	1
11.	Advance Persistence Threat Solution (Anti - APT)	IT	1
12.	DDoS solution	IT	2
13.	Tape Cartridge LTO6 with Barcode label (6.2 TB)	IT	500 qty
14.	Desktops	IT	4 set
15.	Data cabling for complete DC including NOC, BMS, Non-IT etc.	Non-IT	As required
16.	Fibre Cables (5 Meters, 10 Meters, 30 Meters)	Non-IT	210 (70 qty each)
17.	Access Control Solution (for DC area, UPS & Electrical room)	NonIT	1 Set
18.	Air-condition for 300 sqft except DC area 2 Tr (2+1) including accessories, intelligent timer & Stabilizer	NonIT	3
19.	Building Management System (BMS Solution) along with necessary hardware & software including Temp & RH sensors, cabling, perpetual full use processor licenses	NonIT	1 set
20.	CCTV Solution (with min 9 Dome Cameras, 2 bullet (outdoor) cameras)	NonIT	1 set
21.	LED Display	Non-IT	4 set
22.	Civil & Interior Work Including:	NonIT	Lump sum As

	• 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 • Hot aisle containment • 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		Required
23.	Electric Work including: • Electrical cabling (HPSDC 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 HPSDC Electrical panel • Cabling upgradation/additional cabling from DG Sets to HPSDC Electrical panel • Any other components required	NonIT	Lump sum As Required
24.	Fire Extinguishers (C type)	NonIT	7
25.	Floor PDU (180 KVA) with isolation transformer - shall be used for power distribution inside the data centre	NonIT	2
26.	GAS Suppression & Fire Detection System (min 4 NOVEC 1230 cylinders - 3 Server farm area & 1 UPS room)	NonIT	1 set
27.	Glow Signage-Exit (Server Farm Area -3, UPS room - 1, Exit (with light) - 1)	NonIT	5
28.	HSSD Solution (VESDA)	NonIT	1
29.	IPDU for New Racks	NonIT	52
30.	IPKVM with LCD Monitor	NonIT	4
31.	Phase sequencer (3 Phase)-600KVA	NonIT	1
32.	Lighting (4 Nos) & CAC (3 Nos of 1.8Tr) including stabilizers for Transformer room	NonIT	1 Set
33.	Precision AC with accessories N+1 set (Working Unit - 7 Nos. of 6.8 Tr and Standby Unit - 1 Nos. of 6.8Tr) including one water purifier for water inlet supply for PAC	NonIT	8
34.	Rodent Repellent System (DC Area & UPS Room)	NonIT	2
35.	Network Racks (including blankers) Floor Standing 19" 42U 800(mm) (W)X 800(mm)	NonIT	2
36.	Server Racks (including blankers) Floor Standing 19" 42U 600(mm) (W) X 1000 (mm)	NonIT	11
37.	UPS for BMS (5 KVA) (N=1) N+1 including battery bank	NonIT	2

38.	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
39.	Water leak detection system (DC Area & UPS Room)	NonIT	2
40.	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

6.8 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
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

6.9 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	___x_____KVA modules for modular UPS (for a total capacity of 80 KVA(Scalable capacity)) along with battery bank for 30 min backup	to be specified by bidder
2	**IT Infrastructure**	
2.1	Blade Server as per specification given in RFP vol II	5
2.2	App, Web and other blade Servers	
a.	RAM (256 GB per blade)	5
b.	CPU (Ten Core CPU for blades)	5
2.3	DB Server	
a.	RAM (256 GB)	2
b.	RAM (512 GB)	2
c.	CPU (for DB server as per specification given in RFP Vol II)	5
2.3	Storage	
a.	8 Front end ports per controller	2
b.	Additional back-end ports to achieve 128 Gbps more bandwidth	1
c.	SATA Drives (for 50 TB usable capacity. Per drive cost x number of drives to be provided)	1
d.	FC/SAS Drive (for 50 TB usable capacity. Per drive cost x numberof drives to be provided)	1
e.	SLC SSD Drive (for 10 TB usable capacity. Per drive cost xnumber of drives to be provided)	1
f	Enclosure for Drives (for additional 150 TB Capacity)	As required
g.	SAN Switch ports (4/8/16G)	96
h.	Licensing per port	96
i.	Cascading License (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	10
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
j	~~Oracle Analytics Server - Named User Plus~~	100
k	ODI enterprise edition - processor perpetual	10
l	~~Oracle Database enterprise - processor perpetual~~	10
m	~~Oracle Advance Security option - processor perpetual~~	10

n	~~Oracle Database tuning pack - processor perpetual~~	10
o	~~Oracle Database Diagnostic pack - processor perpetual~~	10
p	~~Oracle Partitioning - processor perpetual~~	10
q	~~Oracle Real Application Cluster - processor perpetual~~	10
r	~~Oracle Golden Gate - processor perpetual~~	10
s	~~Oracle Golden Gate for non oracle - processor perpetual~~	50
t	Weblogic Server Enterprise Edition - processor perpetual	4
u	~~IBM MasterData Master Data Management Extension for IBM Cloud Pak for Data Virtual Processor for Core License- VPC~~	47
2.6	FC Module for existing SAN Switch, fully populated 8/16 Gbps ports with SFP's	2
2.7	Any other Suggested Equipment	

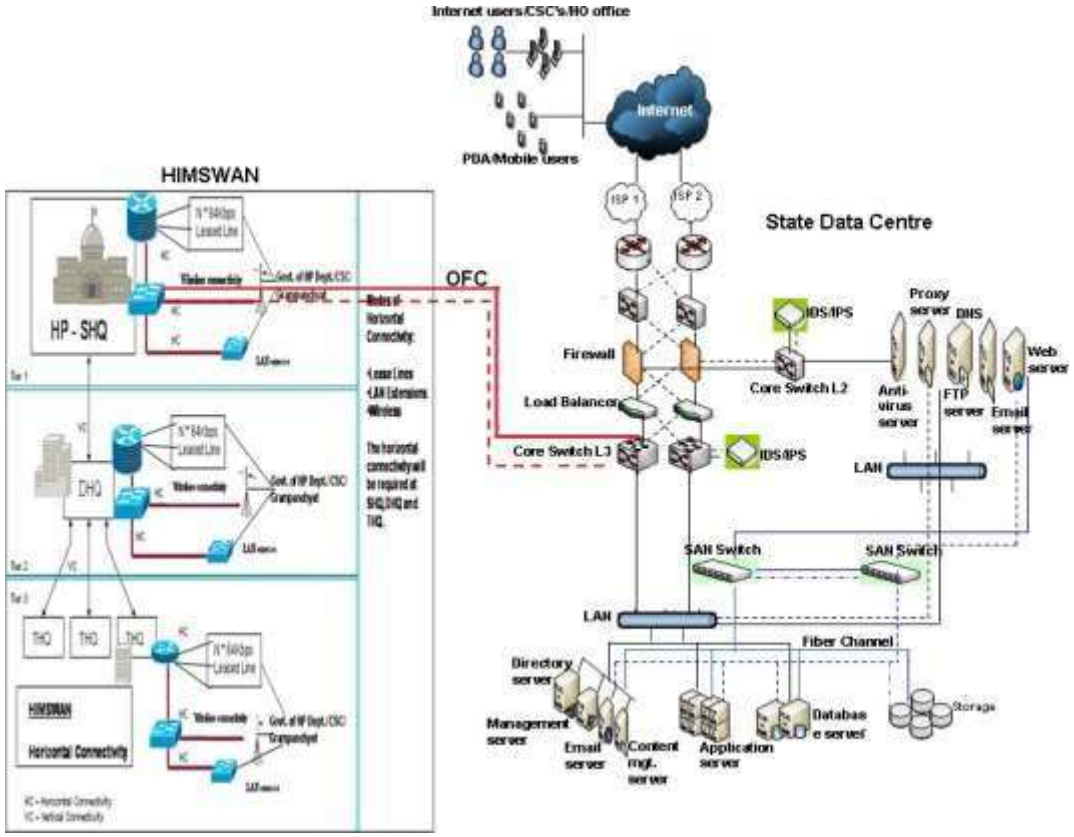
Technical Requirement

1 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.

2.1 SDC Architecture – IT

SDC architecture is being depicted in the schematic as:



2.1.1 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:

2.1.1.1 Web Servers

Web based applications are easily accessible from any sort of the network, Intranet, internetor 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.

2.1.1.2 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.

2.1.1.3 Database Server

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

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

2.1.1.4 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.

2.1.1.5 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 basic task is to regulate some of the flow of traffic between computer networks of different trust levels. There is a perimeter / external firewall as well as internal firewall in redundant mode which acts as different layer of security for SDC IT infrastructure. Furthermore both the firewalls i.e. perimeter firewall & internal firewall should be of different OEMs and DCO should ensure that there should not be any interoperability & functional issues in terms of security & network infrastructure. Hence firewalls 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.

2.1.1.6 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 their monitoring 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.

2.1.1.7 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 ofthe 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.

2.1.1.8 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.

2.2 Technical Specifications - IT Components

2.2.1 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.
1.1.5	Switch should have for modular stacking, in addition to asked uplinkports.
1.2	**Performance:**
1.2.1	Switch shall have minimum 3.6 Tbps of switching fabric and minimum 1.5 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 or more
1.2.4	Switch shall have 8K or more multicast routes.
1.2.5	Switch should support atleast 64K flow entries
1.2.6	Switch should support 128 or more STP 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.
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, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.

1.3.7	Switch should support 802.1x authentication and accounting, IPv4 and IPv6ACLs and Dynamic VLAN assignment and MACSec-256 on hardware*
1.3.8	Switch must have the capabilities to enable automatic configuration of switchports as devices connect to the switch for the device type.
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 no's of SFP+ ports, atleast 48*10/25 G SFP+, 6*40/100 G uplinkPort. 24* 1G UTP ports Uplink port should be modular. 40 MB Buffer.
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's Operating System should be tested for EAL 2/NDPP orabove under Common Criteria Certification.

2.2.2 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 of forwarding 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 4GB 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 code point (DSCP) and cross stack 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.
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 trace route for ease of troubleshooting by identifyingthe 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), AggressiveUDLD, Link Aggregation Control Protocol (LACP), and Dynamic Trunking Protocol (DTP) or equivalent.
5.11	Switch should be Software Defined Networking Ready with Open flow or similar protocol support
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.

2.2.3 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* 10 Gbps ports across two or more cards
6	Hard Disk	Two numbers of minimum 480 GB SSD drives or higher capacity
7	RAID controller	SSD drives compatible RAID Controller to enable RAID 10
8	Redundancy	The blade server to be provided with port level and card level redundancy for I/O connectivity.
9	Form Factor	Half Height/ Width Blade
10	Virtualisation	Heterogeneous support for guest Operating systemslike 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 in server 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.

2.2.4 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+1power 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 based 2 CPU and 4 CPU server. Should support built-in management software in redundancy
		Should provide single management console for all theblade 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 20Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure) for a fully populated chassis for converged Traffic.
		All Network and management modules should be populatedfrom day 1 to ensure redundancy

2.2.5 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 Cloud DDoS Scrubbing Centre in INDIA
4	DDoS OEM should be present in the "LEADER" quadrant in the Latest published Forrester wave Report AND IDC Report for DDoS.
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 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port. The above mentioned parameters should be publically available on OEM Website.
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 5000 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 behavior based technology. The device should generate Automatic Real Time Signature within 20 seconds, without any manual intervention for protection against Zero Day DDoS Attacks.
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. All the learned baseline information should be in sync between physical appliance and cloud scrubbing centre in case of traffic diversion OEM Should have Cloud DDoS Scrubbing Centre in INDIA.
20	The Signaling should include Attack footprint intelligence to ensure effective and fast mitigation
21	Cloud Scrubbing OEM should have 8 Tbps + of Scrubbing capacity. The proposed DDoS Solution OEM should be able to offer On-Demand & Always-On services.
22	Cloud Scrubbing should provide unlimited attack mitigation (no restriction based on attack traffic volume)
23	OEM DDoS Cloud Scrubbing Centres should have the feature to integrate with Public Cloud environments and offer On-Demand & Hybrid Cloud DDoS service from Day-1. It should collect Log/telemetries/data from Cloud environments in order to detect DDoS Attacks.
24	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1.

2.2.6 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 40Gbps on same appliance.
- Should be a standalone independent hardware-based NIPS appliance andshould be other than Router, Internet Firewall, Intranet Firewall, DDoS andLoad balancer based vendors to avoid any single point of failure.

- Should support VA scanners (Qualys, Rapid 7, and Nessus) to fine tune theIPS 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 bypasstraffic even with the power on, in event of un-recoverable internal software error such as firmware corruption and memory errors
- Should intercept and inspect SSL traffic for any malicious content without performance degradation
- Should have 100 million legitimate concurrent Sessions/Concurrent connections and 650,000 new Connections per second from day one.
- 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
- Proposed solution should have at least security effectiveness rate 99 % as per2017 NSS Labs NGIPS report
- 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)
- IPS solution should have machine learning to detect exploit kit landing page.
- 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, exploittype and the reputation score
- 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 securitypolicies 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 privatekey from the network flow in order to help restore encrypted files to the victimwhile 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
- OEM should be leader in vulnerability discovery as per latest Frost and Sullivanreport discovering Microsoft & Adobe vulnerabilities worldwide.

- 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 six year support for complete NIPS including update, upgrade, licenses, patches etc.

Physical Requirements

- 19” Rack Mountable
- All necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, wire managers, etc. should be provided to install NIPS inthe Data Centre

2.2.7 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).	
4	OEM should have Cloud WAF PoP in India.	
5	OEM should be present in Gartner's Leader Quadrant as per last published report for ADC.	
	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	
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 Propsed 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 recommeded, ICSA Certified and 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)	
25	**The proposed WAF should support the Activity Tracking, which should include the following:**	
	Mimicking user behavior	
	Dynamic IP	
	Anonymity	
	Scraping	
	Clickjacking	
26	**Device Fingerprint-based tracking**	
	The Proposed WAF should support Device Fingerprint technology 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 funtionality 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.	
30	**Centalized Management**	
	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.	

2.2.8 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 featurefor 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 and upgrades during the complete tenure of the project.

2.2.9 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 andDomains 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, Windows Registry entries, File hashes, Malware detections and Malware families through adashboard
5. The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations whereapplicable.
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. Proposed solution should have >99% breach detection rate as per NSS 2017 test Labreport
9. The proposed solution should have a built-in document vulnerabilities detection engine toassure analysis precision and analysis efficiency.
10. The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session.
11. 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.

12. The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox.
13. Solution should be deployed on premise along with on premise sandboxing capability andno data should be allowed to go on public cloud.
14. 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.
15. Proposed solution should be able to provide customizable sandbox to match customer'sendpoint environments
16. The solution should allow administrator to categorize files as safe based on Hash values(MD5)
17. 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.
18. Proposed solution should have 2 TB in RAID 1 of on box storage from day one with ascalability of 8 TB
19. The proposed solution should be able to run at least 20 parallel sandboxes imagesscalable up to 60 for analysis of payload
20. Customized sandbox solution should support following operating systems (Windows XP,Win7, Win8/8.1, Win 10, Windows Server 2008, 2012, 2016 and CentOS)
21. 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
22. The destination website in both intranet (in corporation network) and internet (typicalinternet website) shall be supported as patient zero functionality
23. 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.
24. 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
25. Solution shall be capable to perform threats inspection over 40,000 con-current HTTPSsessions
26. 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.
27. 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
28. Solution must support up to 800,000 emails/day on single appliance having have at least4 TB of Storage on the box.
29. The proposed solution and must have an integrated solution that provides enterprise message transfer agent (MTA) capabilities SMTP/SMTP-TLS, Antivirus, Content Filtering,

multi-tiered SPAM prevention ,BEC/CEO fraud attack prevention, ransomware, Unknown malware threats - Sandboxing and anti-phishing

30. The Proposed Solution should support authentication mechanisms like DKIM, DMARC &SPF checks to detect & fight against techniques used in mail phishing & spoofing.
31. 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)
32. The Proposed Solution should support End-User Quarantine feature
33. Solution should be able to centrally manage and deploy sandbox image update tomanaged products.
34. Solution should be able to centrally manage and deploy product updates includingpatches, hotfixes, and firmware upgrade
35. The proposed solution should have advanced detection technology that discovers targeted threats in email messages, including spear-phishing and social engineeringattacks.
    - Reputation and heuristic technologies catch unknown threats and documentexploits
    - File hash analysis blocks unsafe files and applications
    - Detects threats hidden in password-protected files and shortened URLs
    - Predictive machine learning technology detects emerging unknown security risks
    - Blocks malicious URLs in email messages at the time of mouse clicks
    - Engines -Static/Dynamic Analysis
    - Anti-security and self-preservation
    - Autostart or other system configuration, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change, Rootkit, cloaking, Suspicious network or messaging activity, patternbased, reputation, Heuristics & Machine learning.
36. The proposed solution should have bi - directional seamless integration with Endpoint Security, HIPS and NIPS for detecting and mitigating zero day threats leveraging sandboxanalysis.

2.2.10 Perimeter/external Firewall

Feature	Technical Specification
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 should bescalable to additional 8 * 40G in future.
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 64 GB of RAM or more
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale againstdynamic latest security threats.

	The proposed solution shouldn't use a proprietary ASIC hardware for anykind of performance Improvement.
Performance & Scalability	Should support 10 Gbps of NGFW (FW, AVC, and IPS) real-world / production performance from day one
	Firewall should support atleast 20,000,000 concurrent sessions
	Firewall should support atleast 70,000 connections per second
	Firewall should have integrated redundant hot-swappable power supply
	Firewall should have integrated redundant hot-swappable fan tray / modules
Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
	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
	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., selectingrules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should support more than 25,000 (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 inspectionsand 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 withother security solution like Network Admission Control
	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor 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 againstthreats
	The Appliance OEM must have its own threat intelligence analysis centerand should use the global footprint of security deployments for more comprehensive network protection.
	The detection engine should support capability of detecting and preventinga 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 policyto 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 andspecific 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 260 million of URLs in more than 70 categories.
Distributed Denial of Services	Should support automatic Real Time Signature generation based on RateVariant, Rate Invariant algorithms & Challenge Response Mechanisms; within few seconds, without human intervention
	Should support DDoS flood attack prevention rate of 1.5 M Packet persecond
	Should support behavioral analysis using behavioral algorithms and automation to defend against threats, including Mirai DNS Water Torture, Burst and Randomized attack

	Should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying thefootprint of the anomalous traffic. Real time Attack footprint should be visible to the administrator for forensics purpose. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood
	The DDoS solution can be either an integrated module in the proposed Solution or offered as separate appliance. However functionality shall be required from day 1.
	POSITIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic
	ZERO DAY ATTACK PROTECTION should be provided by behavior-based protection with automatic signature creation against within few seconds of unknown, zero-day DDoS attacks without any manual intervention. The DDoS detection methodology should not be limited to Rate based detection and mitigation.
	Zero day DNS flood protection with (Challenge Response mechanism likeRFC check, Active Challenge, Passive challenge) and Automatic real time signature creation.
	The Proposed DDOS solution should support 1Gbps DDOS mitigation fromDay#1 and scalable up to 5Gbps DDOS mitigation in the same device.
Management	The management platform must be accessible via a web-based interfaceand ideally with no need for additional client software
	The management platform must be a dedicated OEM appliance with 2 x10G port and integrated redundant power supply from day one
	The management platform must provide a highly customizable dashboardand multi-domain management
	The management platform must provide centralized logging and reporting functionality
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
	Should support troubleshooting techniques like Packet tracer and capture
	Should support REST API for monitoring and config programmability
	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 issuingalerts (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 fromday one
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability forcomplete 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 enableevents 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

2.2.11 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) Intellatest generation Xeon Scalable Processors with minimum 2.9 GHz &minimum 16 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* 960 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) and memory mirroring.
11	Network	Should have 2 * 10 GbE (embedded) LAN ports, 4*25 GbE network portsfor LAN connectivity, 2*100G Ethernet IB ports for connectivity
13	PCIe Slots	Up to 6 PCIe Generation 3.0 slots
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 with existing fabric interconnect switch for single management and to retain existing network & compute Design. Incase proposed Rack servers are not compatible with existing switch then Bidder should include equivalentconfiguration of Switch for server's connectivity.

2.2.12 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 threepublished 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 asingle 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 numbervisibility and accordingly create rule for virtual patch against vulnerability
8. Behavior monitoring along with ransom ware protection engine, ransom ware engineshould have feature to take backup of ransom ware encrypted files and restoring thesame.
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 inemail, 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 datacorrelated 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 fromapplication 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 youinstant 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 andcontrol.

2.2.13 Security Incident Management Solution

S.No	Description
1	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.
2	The solution should be a physical appliance form factor with following components:
	a. Management & Reporting
	b. Normalization and Indexing
	c. Correlation Engine
	d. Data Management
3	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.
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.
5	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.
6	Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc
7	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs. SIEM for logs and deep packet inspection should be from same OEM
8	A single log appliance should support minimum 30,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.
9	The solution should be storing both raw logs as well as normalized logs. Thesame should be made available for analysis and reporting. Solution should have built in storage of 12TB.

10	The solution should incorporate and correlate information that enables theInformation Security Team to quickly prioritize it's response to help ensure effective incident handling.
11	The monitoring should be cross device and cross vendor and be both out of thebox and scalable to cover additional devices and applications as required
12	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration
13	Should store RAW packet DATA for 7 days and normalized packet data for 120 days for forensics.
14	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, imageviews, artefact & raw packet and object extractions.

2.3 SDC Architecture – Physical Infrastructure

2.3.1 Layout of Data Centre

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**

2.3.2 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 securityarchitecture 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.

2.3.3 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.

2.3.4 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 areas 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 conditioner on 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.

2.3.5 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 uniformair distribution over the entire face of the server racks. Positions of Indoor units shallbe 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/ requirementsfor Data Centre. All the design parameters and head-load estimation calculations indetail 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 ± 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% ± 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. Thehigh 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 sensibleand 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. anindividual faulty fan can be replaced without having to stop the entire unit, thus reducing 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 andfans, PCB, and safety devices.
14.2	The unit shall have inbuilt 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

2.3.6 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 sourceand 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.

2.3.6.1 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 inparallel redundant mode (1+1) configuration without any modification.
2	Each 180 KVA redundant UPS shall be with modular architecture with appropriate nos. of 20~30KW Hot Swappable Power Modules of double conversion configuration, i.e. 6 nos modules in case of 20 KW Modules, 5 nos modules in caseof 25 KW Modules and 4 nos modules in case of 30KW. The 180 KW UPS shall be scalable upto 240 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 switch for high-speed transfers along with RS232 port, USB port, SNMP Slot, Dry contactports	
	b) Switch Unit comprising of Main Breaker, Maintenance Bypass and OutputBreaker	
6	The control panel comprising of a graphical LCD DISPLAY, touch screen based, with LED status indicators for monitoring of all measured parameters, UPS andbattery 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 30 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 inputcurrent	< 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

2.3.7 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-linear loads
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**

2.3.8 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 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 therunning of the Data Center.

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 than or 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, 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, 50 Hz 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 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 for mounting 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 Fuel Tank with mounting brackets to run for minimum 24 hours complete 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 exhaustpipe & 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.

2.3.9 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-operator component 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

2.3.10 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

2.3.11 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 and built-in surge protection
9	It should support multi-user access and collaboration

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

2.3.13 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.

2.4 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 630 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 630 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 keeping in 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 available in case of failure of any connection. Two separate connections to the rack should be provisioned for the Rack power distribution, one from PDU-1 (SourceUPS 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

2.4.1 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 outto 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/ breakerwithout 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 colouron 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 3 phases 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 insulated copper 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 copperconductor crimped with lugs and terminated on a terminal block of proper rating.

2.4.2 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 beextendable.

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.

2.4.3 Circuit Breakers

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

2.4.3.1 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

2.4.3.2 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.

2.4.3.3 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.

2.4.4 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 beby application of powder coated paint of approved shade and stoved.

2.4.5 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 entirewiring 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 notenter 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 beprovided 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

2.4.6 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 can remain 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.

2.4.7 Wiring

- PVC insulated copper conductor (FRLS) cable shall be used for sub circuitruns 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 reduction of 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, allshall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.Bs shall not be bunched in one conduit. In large areas and othersituations 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 excepting at 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 fromDB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required maximum number of PVC insulated 650 / 1100 grade copper conductors cable which can be drawn in a conduit.

2.4.8 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 systemand provisioning should be there to earth UPS systems, Power distribution units, 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 respectiveprotective 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.

2.4.9 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 as per 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.

2.4.10 Electrical Lights

The electrical lights proposed in the Server Room and UPS & Electrical Room should be 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

2.5 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.

2.5.1 Data Cabling

2.5.1.1 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 IEEEEthernet 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.

2.5.1.2 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.

2.5.1.3 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.

2.5.1.4 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 standards ISO/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.

2.5.1.5 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

2.5.1.6 6 CORES - INDOOR OM4 FIBER CABLE

S. No.	**PARAMETER**	**SPECIFICATIONS**
1	**Type of Cable**	6F 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	6 Core
d)	Jacket Color	Aqua
4	**DIMENSIONS**	
a)	Diameter Over Jacket	5.1 mm
5	**PHYSICAL SPECIFCATIONS**	
a)	Cladding Diameter	125.0 µm
b)	Minimum Bend Radius, Loaded	76 mm
c)	Minimum Bend Radius, Unloaded	51 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

2.5.1.7 1 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

2.5.1.8 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

2.5.1.9 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

2.6 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:

2.6.1 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 mm with 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 and joints should be finished properly as per manufacturer's specification.

2.6.2 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.

2.6.3 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 rate shall Include for preparing the surface smoothly and all as per manufacture's specification etc. Finally finishing with One coat of approved brand of fireresistant 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.

2.6.4 Painting

- Providing and applying fire retardant paint of approved make and shade to givean even shade over a primer coat as per manufacturers recommendationsafter applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Basecoating shall be as per manufacturer‘s recommendation for 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.

2.6.5 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.

2.6.6 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.

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

Sr.	Description

	Building Management System (BMS)
	Bidder to visit the HPSDC Site, check and study the existing installed BMS for Phase1 HPSDC. 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 HPSDC 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 zone. The entire system shall be backed by maintenance free battery. The system shall be totally tamper proof andactivate an alarm if the control panel is opened, the sensors tampered with or if the system cable is cut even in the disarming state. The Panel shall provide volt free contacts to connect to BMS System.
2	**Water leak detection Module:**
	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 HPSDC Site, check and study the existing installed PA System for Phase 1 HPSDC. 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 to announcement from the designated location within the Facility.
§	To play light music if required.
1	**Speakers**
§	Input Power required is 16W RMS / 24W Max.
§	Rated voltage should be 100V
§	Low Impedance must be 8
§	Frequency response should range between 85-20,000Hz.
§	Speaker must have a woofer & tweeter.

Sr.	Description
	Fire Detection and Control Mechanism
	Bidder to visit the HPSDC Site, check and study the existing installed Fire Panel for Phase 1 HPSDC. 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 1 ton (e.g. 24) zone single loop addressable fire detection and alarm system, utilizing addressable detection and alarmsounders.
·	Detection shall be by means of automatic heat or smoke detectors located throughoutthe 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 stroagedevice.
·	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 theremaining devices on the loop inoperable.

.	The system status shall be made available via panel mounted LEDs and a backlit 8 linex 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 / Stopsounders and Cancel fault buzzer, etc. will be clearly marked.
.	Cancel fault and display test functions shall be configurable to be accessed from level 1or level 2.
.	All system controls and programming will be accessed via an alphanumeric keypad. Thecontrol 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 referenceand 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 systemshall 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 theoption 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 in compliance 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 with the manufacturer, but in no case less than five (5) years from the date of systemacceptance
.	Additionally, Portable Extinguishers (CO2 or Halon based Extinguishers are not acceptable) 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 no more than 4 feet to ensure the stability of the piping and reduce the possibility ofcracks 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 shop drawings.
.	The design program for the air sampling pipe network shall provide a balanced engineered 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 takeninto 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 HPSDC Site, check and study the existing installed Access ControlSystem for Phase 1 HPSDC. 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
·	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 in communication 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 file server:
	(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 ofusers.
·	Should have Global and local anti-pass back/anti-tailgate capability.
·	System must have provision of creation of data bank, easy retrieval of informationand validity expiry warning.
·	The software shall seamlessly support and integrate with the smart cards and otheraccess 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 withISO standard
·	All RF data transmission between the card and the reader shall be encrypted, usinga 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 visualindication to indicate successful/unsuccessful authentication.
·	The reader should provide the following audiovisual indications:-
o	An audio transducer should provide various tone sequences to signify: accessgranted, access denied, power up and diagnostics.
o	A high-intensity light bar shall provide clear visual status (red/green/amber) that isvisible even in bright sunlight.
.	Should be compact but rugged to withstand handling by multiple users. Verificationtime should be less than 10 sec.
.	May have separate fingerprint enrolment/programming facility to transfer fingerprintto 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 flexiblesolution
·	Input- H.265/ H.265+/H.264/ H.264+/MPEG4 video formats, supports audio compressions Recording, Playback, Back-up, Network recording, and Network playback
·	Supports live view, storage, and playback of the connected camera
·	Storage capacity to store more than 120 days backup

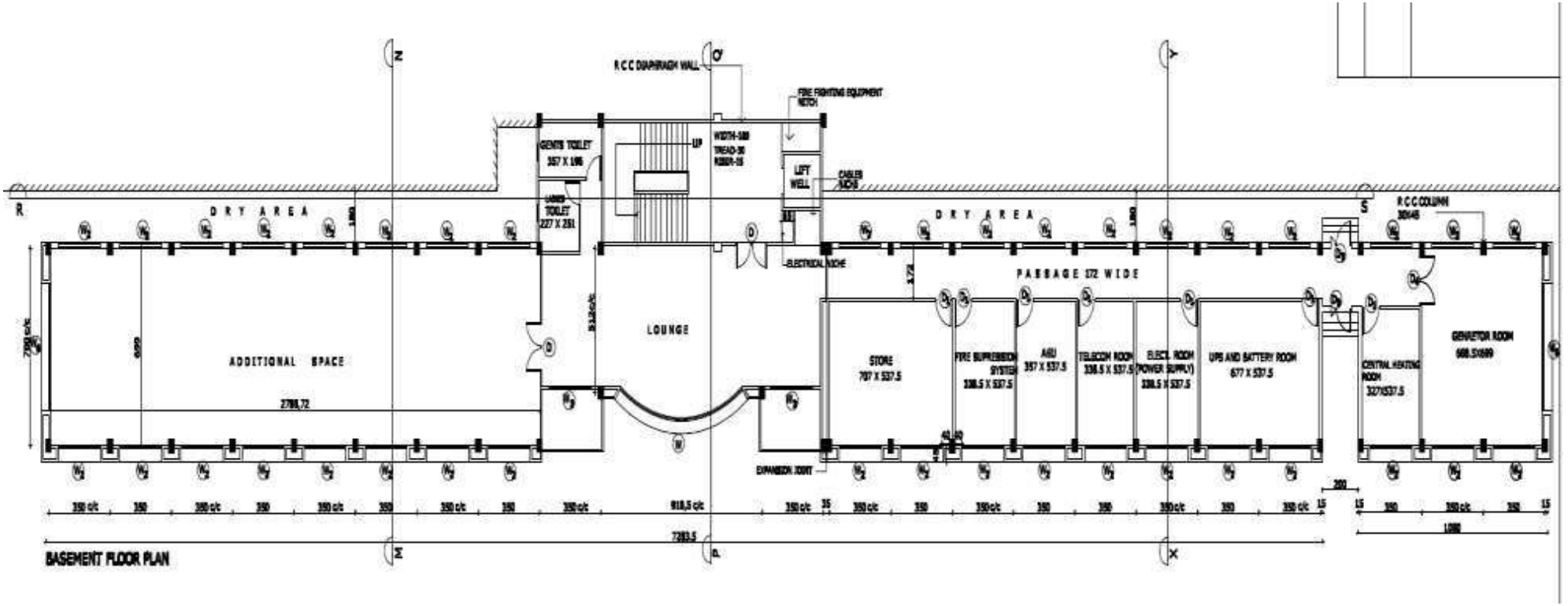
·	HDMI and VGA independent outputs provided
·	Rated voltage: 220-240 VAC 50/60Hz.

2.8 Rodent Repellent

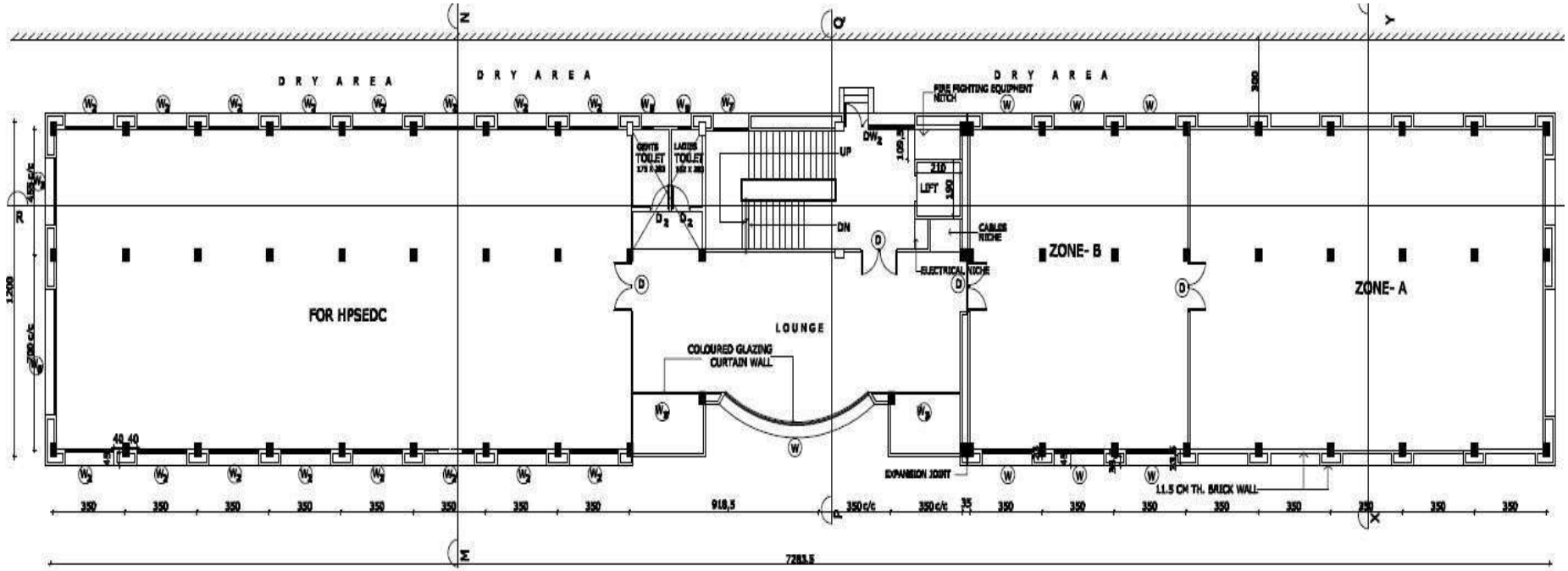
Sr.	Specification
The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non- toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be 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.

3 Annexure

3.1 Basement floor Plan for the SDC building



3.2 Ground floor Plan for the SDC building



GROUND FLOOR PLAN

3.3 Server Farm Area

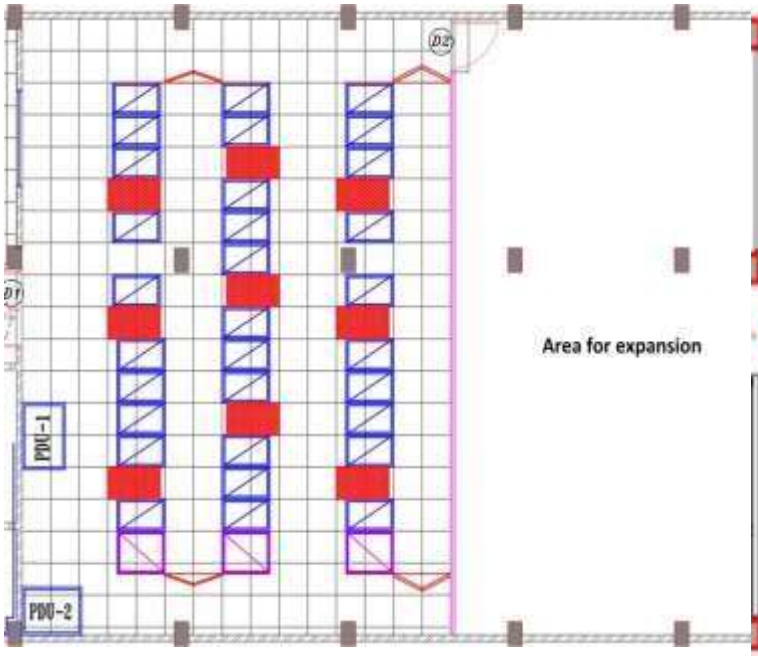


Figure1

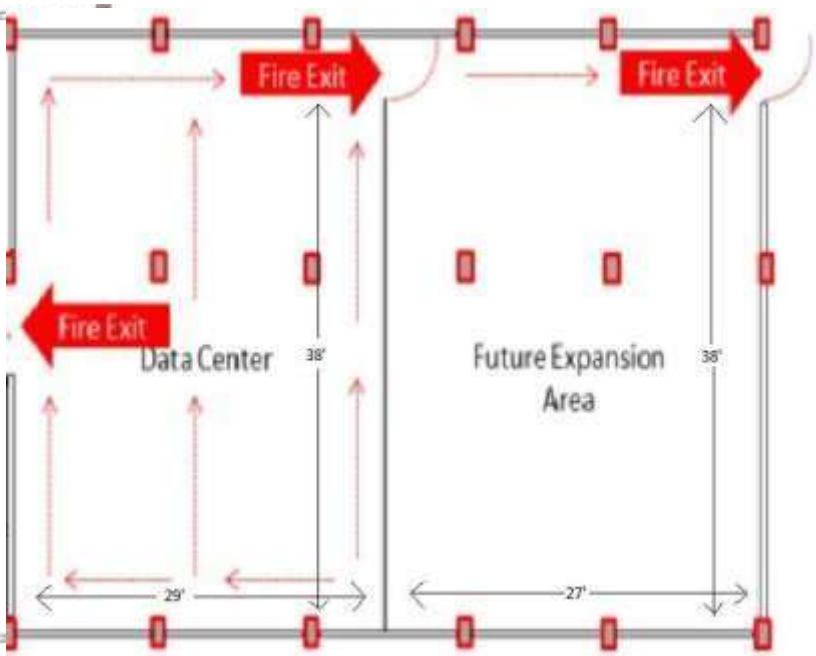


figure2