CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

A Scientific Society of Ministry of Electronics & Information Technology, Government of India

Innovation Park, PANCHAVATI, Pashan Road, Pune - 411008
Tel: +91-20-25503671-676, e-Mail: mmg@cdac.in
www.cdac.in

Tender No: CDACP/AG22-IT/22-23/356

C-DAC invites ON-LINE bids for Supply, Installation, Integration, Testing & Commissioning of IT equipment at New Delhi and Bengaluru along with Training & Support.

Bidders are advised to go through instructions provided at 'Instructions for online Bid Submission' and submit duly filled bids online on the website https://eprocure.gov.in/eprocure/app as per the schedule given in the Tender Document.

TENDER SCHEDULE

Tender No: **CDACP/AG22-IT/22-23/356**

Name of the Institute	Centre for Development of Advanced Computing, Pune 411008.
Date of Release of Tender	01st November 2022
Date of Pre-bid Meeting	11th November 2022 at 11:00 hrs.
Place of Pre-bid meeting	C-DAC, Innovation Park, Panchavati, Pashan, Pune – 411008
Seek Clarification End Date	14th November 2022 till 1700 hrs
Bid Submission Start Date	23rd November 2022 from 0900 hrs
Last date of submission of bids	30th November 2022 till 1500 hrs
Date of opening of Technical bids	01st December 2022 at 1500 Hrs
Place of opening of technical bids	C-DAC, Innovation Park, Panchavati, Pashan, Pune – 411008
Bank Details	Bank Name : IDBI BANK A/c Name: C-DAC (Centre for Development of Advanced Computing) A/c No.: 60010010004258 Branch Address: 1st Floor, Plot No. 421/A, CTS No. – 1071, Gokhale Road, Near Symbiosis, Atur Centre, Pune – 411 016 IFSC/NEFT Code: IBKL0000600 SWIFT Code: IBKLINBB007

Section – I: Invitation For Bids (IFB)

1. *Introduction:*

   Centre for Development of Advanced Computing (C-DAC) - is a scientific society under the administrative control of Ministry of Electronics & Information Technology, Government of India. As a part of a project requirement, C-DAC invites 'ONLINE' bids from eligible bidders for supply, installation and commissioning peripheral equipment's as per schedule of requirements, terms and conditions stipulated in this document.

2. *Instructions for On-line Bid Submission*

   The bidders are required to submit soft copies of their bids electronically through the portal (www.eprocure.gov.in) using valid Digital Signature Certificates (DSC). The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal. More information useful for submitting online bids on the CPP Portal may be obtained at: https://eprocure.gov.in/eprocure/app.

3. *Assistance to Bidders:*

   Any query relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24*7 CPP Portal Helpdesk on :- 0120-4200 462, 0120-4001 002, 0120-4001 005, 0120-6277 787. e-mail for Technical - support-eproc@nic.in

4. *Contact information:*

   Material Management Group
   Centre for Development of Advanced Computing (C-DAC)
   Innovation Park, PANCHAVATI, Pashan Road,
   Pune 411008, Maharashtra, INDIA
   Tel No.: +91-20–25503671-676 Fax No.: +91-20–25694004
   E-mail: mmg@cdac.in

NOTE:

In case of any doubts, and/ or queries about the technical solution, specifications terms and conditions of the tender, the prospective bidder may send their queries in writing through email (mmg@cdac.in). The queries, requests for clarifications etc. must be sent within 7 days from the date of publication of the Tender. The bidders are requested to go through the entire tender document thoroughly, before raising any query. C-DAC, Pune shall address the queries raised by the bidders. The replies

to queries would be made available on the portal in due course of time. All the queries, doubts, clarifications etc. must be submitted in .xls format only as below.

Name of the bidder:				
Sl.No.	Section / Page No	Clause Reference	Query from bidder	C-DAC Response

5. *Two bid System:*

The two e-bid system will be followed for this tender. In this system, bidder must submit their offer - online in separate e-packets through https://www.eprocure.gov.in /eprocure/app, as explained below:

I: ONLINE – E-PACKET NO. 1: "TECHNICAL E-BID" SHALL CONTAIN FOLLOWING DOCUMENTS PERTAINING TO THE BIDDER: (PDF FORMAT ONLY)

a. Covering letter, as per **Annexure – A.**
b. Authority letter, as per **Annexure – B.**
c. Scanned copy of Demand Draft / Online Transfer (RTGS / NEFT etc.) towards tender fee of Rs. 5,000/- (Rupees Five Thousand Only). In case of Demand Draft, same should be drawn in favour of C-DAC payable at Pune. The original Demand Draft must be submitted at the place of Opening of the Tender on or before the Due Date & Time of the Tender Submission.
d. Scanned copy of Demand draft/Bank Guarantee / Online Transfer (RTGS / NEFT etc.) towards Earnest Money Deposit (EMD) valuing Rs. 1 (one) Crore.
    i. In case of DD, same should be drawn in favour of C-DAC payable at Pune.
    ii. The original Demand Draft/Bank Guarantee, towards EMD, must be submitted at the place of Opening of the Tender on or before the Due Date & Time of the Tender Submission.
    iii. Bank Guarantee needs to be submitted as per the format prescribed by any Commercial Bank in India valid for at least 120 days from the last date of bid submission.
    iv. Bidder availing EMD exemption has to mandatorily submit EMD Undertaking. Further, other bidder may also submit EMD Declaration in lieu of above-mentioned EMD amount as per **ANNEXURE G** of this tender document.

v. The EMD amount /BG will be returned to the Bidder (s) whose offer is not accepted, within 30 days from the date of opening of commercial bid(s).
vi. In case of the Bidder whose offer is accepted, the EMD will be returned on submission of Security Deposit (Refer Clause 4 of Section III). However, if the return of EMD is delayed for any reason, no interest/ penalty shall be payable to the Bidder.
vii. The successful Bidder, on award of contract / order, must send the contract/ order acceptance in writing, within 10 days of award of contract/ order, failing which the EMD will be forfeited and the order will be cancelled.

e. A copy of Certificate of Incorporation, Partnership Deed / Memorandum and Articles of Association / any other equivalent document showing date and place of incorporation, as applicable.
f. Copies of PAN and GST registration certificates.
g. Copies of at least two supply orders AND installation reports issued by the end user in the name of bidder in support of eligibility requirements stipulated at para 5, Section –II of this document.
h. The copies of Profit and Loss Accounts **OR** the certificate from a Chartered Accountant certifying the annual sales turnover of the bidder for the financial year 2019-2020, 2020-2021 and 2021-2022.
i. The undertakings from the Principal Manufacturer of respective items, as per **Annexure – C**
j. Declaration / Undertaking as per **Annexure E & F** needs to be submitted in compliance with the OMs & Orders (Public Procurement No.1) ref. F.No.6/18/2019-PPD dated 23.07.2020, Make In India Circular No. P-45021/2/2017-PP(BE-II) of DPIIT, Make in India contents F. No. W-43/4/2019- IPHW of MeitY along with amendments thereof.
k. The certificates of Origin of OEM & Manufacturing of product / item pertaining to all offered products from respective OEMs.
l. The duly filled technical bid containing detailed technical specifications, make, model, part numbers of the items offered, supported by the printed catalogue / leaflet published by the Principal Manufacturer.
m. A photo copy of the commercial bid without prices **(prices blocked)** and copy of commercial terms & conditions (in details) as included in the commercial bid. C-DAC reserves the right to reject the bid in case of discrepancy observed in the un-priced commercial bid and the actual commercial bid.
n. Other documents necessary in support of eligibility criteria, product catalogues, brochures etc.

o. **Note:** C-DAC reserves the right to reject the bid if any of the above listed document(s) is/are not submitted.

II: ONLINE – E-PACKET 2: "COMMERCIAL E-BID" SHALL CONTAIN:

The Commercial Bid complete in all respects must be uploaded in prescribed.xls format only.

6. *Last Date of submission/ uploading:*

The on-line bids, complete in all respect should be uploaded through www.eprocure.gov.in/eprocure/app on or before the last date of bid submission as given in tender schedule.

7. *Opening of Technical e-bids:*

The Technical e-bids will be opened - online on the date given in tender schedule, through www.eprocure.gov.in/eprocure/app portal at:

Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road, Pune 411008,
Maharashtra, INDIA.
Tel No.: +91-20–25694015 Fax No.: +91-20–25694004
E-mail: mmg@cdac.in

The bids must be submitted on-line. The Tender Fees & EMD/BG etc. (in case of DD/BG etc.) must be submitted in person or through post/ courier so as to reach on or before the due date and time. C-DAC shall not be responsible for any postal delays or any other reason for not submitting the tender fees/ EMD etc. in the specified time and resulting in disqualification / rejection of any bid. The representatives (maximum two) of bidders are welcome to attend the opening of the 'online' technical e-bids.

In case bidder requires any clarifications / information pertaining to the tender, they may contact C-DAC address given in Clause 4 of Section I.

Note: Please do not put "Commercial Bid" (prices quoted) in the "Technical Bid" envelope. If the price quoted is submitted/leaked with technical bid, the bidder/ tender will be rejected at the sole discretion of C-DAC.

8. *Opening of commercial e-bids – online through www.eprocure.gov.in/eprocure/app:*

Commerciale-bids of the qualified bidders only will be opened, in the presence of the bidders or their authorized representative of the bidders, who choose to

attend, at the time place and date to be informed later. The authorized representative of bidders, present at the time of opening of the bids shall be required to sign an attendance register as a proof of having attended the commercial bid opening.

The bidder's name, bid prices, discounts and other appropriate details will be displayed at the time of the opening of the commercial bids.

(End of Section - I)

Section II: Instructions to Bidders (ITB)

1. *Scope of Supply:*
   The total scope of supply is as given in '*Section – IV: Scope of Supply and Services*'. The bidders may quote for the same.

2. *Locations for the Supply, Installation & Warranty Services:*
   The entire products as described in 'Section -IV: Scope of Supply & Services' must be supplied, installed, commissioned & supported at the CDAC Customer premises in **New Delhi and Bengaluru.** The Item Wise Delivery Location is provided under 'Section-VII' of this RFP.

3. *Training:*
   Installation, Integration and hands-on training shall be carried out for all the items under the scope of supply as stated in 'Section-IV: Scope of Supply & Services' within 02 weeks from date of receipt for the components at respective sites.

4. *Delivery Period:*
   All the items covered in the Schedule of Requirements (Section – IV) must be supplied at site as per following:
   a) Category-I: within 120days from the date of placement of order.
   b) Category-II: within 180days from the date of placement of order.

5. *Eligibility Criteria:*

Sr. No	Qualification Criteria	Documents/Information to be provided in the submitted proposal
1.	The responding firm / agency shall submit the documents pertaining to a) Covering letter b) Authority letter	a) Covering Letter As per Annexure-A b) Authority letter As per Annexure-B
2.	The responding firm / agency a) Should have made a payment of **Rs. 5,000/- (Rupees Five Thousand only)** towards Bid submission Fee for the tender document b) Should have submitted a EMD of Rs. 1 crore only	a) DD for **Rs. << Enter the amount>>** b) The original bank EMD / DD / guarantee must be furnished in the format issued by Commercialised Bank.

Sr. No	Qualification Criteria	Documents/Information to be provided in the submitted proposal
		Bidder may also submit Undertaking as per **Annexure G** in lieu of EMD amount.
3.	Legal Entity • Company should be registered under Companies Act, 1956 • Registered with the Tax Authorities Should have been operating for the last three years (FY 21-22, FY 20-21 and FY 19-20) indicating that the turnover criteria is met.	a) Certificate of Incorporation / Partnership deed / Memorandum of understanding b) Registration Certificate c) Audited Balance Sheet d) PAN & GST Registration Certificates
4.	The Firm / Company should be in the business as a vendor for supply, installation, integration, commissioning and testing of Servers, Storages, Backup and Tape Libraries etc. for at least 3years as of 31st March 2022. Bidder shall share the details of previous experience in deployment and configuration of DC, Near DR and DR Storage replication during the last three years.	Work orders confirming year and Area of activity and Certificate from the client indicating the Satisfactory deployment of 3way storage replication across DC, NDR and DR.
5.	The responding firm shall not be under a declaration of ineligibility for corrupt or fraudulent practices and not Black listed by any of the Govt. / Public Sector / Govt. Societies.	A self-certified letter by the designated official of the responding firm as per **Annexure-A**
6.	The Net Worth of the responding firm must be positive for any one of the last three financial years.	Chartered Accountant Certificate for Net worth / Audited Balance Sheet
7.	The responding firm should be ISO 9001:2008certified.	Copy of certification which is valid on the date of submission.

Sr. No	Qualification Criteria	Documents/Information to be provided in the submitted proposal
8.	Established (existing) Support centre with more than 30 Professionals on roll (with at least 5 nos. of CCNA certified) at both Delhi and Bangalore together at the time of Bidding.	Need to submit the proofs (like Appointment letter, PF records etc.) with full address details with SPOC towards the same. C-DAC may cross-check the same.
9.	Declaration / Undertaking needs to be submitted in compliance with the OMs & Orders (Public Procurement No.1) ref. F.No.6/18/2019-PPD dated 23.07.2020, Make In India Circular No. P-45021/2/2017-PP(BE-II) of DPIIT, Make in India contents F. No. W- 43/4/2019- IPHW of MeitY along with amendments thereof.	Bidder need to submit as per **Annexure E & F**

Following conditions are in addition and the bidder must comply with each of the following eligibility requirements:

a. **The bidder must quote for all the items listed under each Category.**
b. Only the principal manufacturers or their authorised System Integrators are allowed to bid for the items as mentioned in the tender document, both are not allowed to bid simultaneously.
c. The specific authorisation letter from Principal/s, as per **Annexure - C** must be submitted along with the technical bid.
d. The Indian agent and the principal manufacturer / OEM cannot bid simultaneously.
e. Bidder should have minimum average annual sales turnover of Rs. 120 Crores for the last three financial years in the field of Information Technology.
f. Bidder need to submit the PO copies (during the last 5 years) as mentioned below showcasing the supply of IT Hardware and IT Software items as part of establishing of DC and DR. Bidder need to provide the successful completion certificate towards the same.
    i. Single Purchase order with value of 200 Crores. OR
    ii. Two Purchase orders with 125 Crores each OR
    iii. Three Purchase orders with 90 Crores each.
g. The bidders should upload the required documents as stipulated in Paragraph 5, Section – I.

h. Declaration as per **Annexure - E & F** (restrictions on procurement from a bidder of a country which shares a land border with India and compliance to GoI OM regarding Make in India).
i. Bidder shall submit the online links / documents and Data / specifications sheets pertaining to the quoted items.
j. The bidder has to mandatorily provide Certificate of Origin from OEM for each quoted component and also mention the same in the column 'Manufactured at (Place)' in the table of Section - V. For single quantity items, the bidder can declare the Country of Origin on OEM/ bidder's letterhead.
k. The bidder has to provide the un-priced BOM (Bill of Materials) for all quoted components.
l. The bidder must have service support center in New Delhi / NCR Delhi & Bangalore Region in order to comply with the necessary support and warranty terms (4hrs. response and NBD resolution). Bidder need to submit the declaration letter in this regard.
m. Bidder need to provide Single point of contact and also share the support and escalation matrix with details like eMail IDs and Phone nos.
n. OEM / Bidder shall declare that, the quoted products should not be under end of life and that the end of support should be available for the next 5 years from the date of supply.
o. OEM / Bidder shall declare that, the quoted products are brand new and not re-furbished and repaired products. The products so provided should be the latest available.
p. The bidder must agree to provide and execute the entire scope of work involved as per Section - IV.

Note:

a) The bidders should provide necessary and sufficient documentary evidence to support the eligibility criteria stipulated above. C-DAC reserves the right to reject any bid not fulfilling the eligibility criteria.
b) Bidders non-compliant to the above-mentioned eligibility criteria and / or not submitting the requisite documents shall be summarily rejected.

6. *Compliance to Make In India (Make in India Circular No. P-45021/2/2017-PP(BE-II) of DPIIT dated 16.09.2020) and Land Border sharing OM & Order (Public Procurement No.1) ref. F.No.6/18/2019-PPD dated 23.07.2020 and subsequent addendums/ amendments:*

a) The MII Declaration / Certificate (as per annexure F) to be provided by Statutory Auditor or Cost Auditor of the Company (in case of companies) or from a practicing Cost Accountant or practicing Chartered Accountant (in respect of suppliers other than companies).

b) Only “Class-I local supplier” having minimum 50% local content and “Class-II local supplier” having minimum 20% local content for the overall solution, shall be eligible to bid in this procurement.

c) The System Integrator (SI) / Bidder has to submit the consolidated MII (local content) % for the complete solution being offered as per Annexure F.

d) MII Purchase Preference shall be provided as per the provision of the said MII order.

e) The bidder and offered product should also comply with the provision of Land Border sharing OM & Order (Public Procurement No.1) ref. F.No.6/18/2019-PPD dated 23.07.2020 and subsequent addendums/ amendments.

7. *Order Placements:*

The Supply Order & Payments shall be released by:
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road,
Pune 411008, Maharashtra, INDIA.

8. *Pre-bid Meeting:*

Pre-bid meeting shall be done offline and the details are provided in the tender schedule.

9. *Exemptions:*

If in the view of bidder, any exemption / relaxation are applicable to them from any of the eligibility requirements, under any Rules / process/ Guidelines/ Directives of Government of India, bidder may submit their claim for the applicable exemption /relaxation, quoting the valid Rule/ process/ Guidelines/ Directives. In this case the bidder must submit necessary and sufficient documents along with the technical bid, in support of his claim. The decision about granting the exemption/ relaxation will be taken by the bid evaluation committee which is empowered to grant exemption/relaxation. The relevant and valid certificates in support of claim of exemption must be submitted.

The bidders should provide sufficient documentary evidence to support the eligibility criteria. C-DAC reserves the right to reject any bid not fulfilling the eligibility criteria.

10. Amendment to Bidding Documents

At any time prior to the deadline for submission of bids, C-DAC may, for any reason, whether on its own initiative or in response to the clarification request by a prospective bidder, modify the bid document.

The amendments to the tender documents, if any, will be notified by release of Corrigendum Notice on www.eprocure.gov.in/eprocure/app/, www.cdac.in/tender against this tender. The amendments/ modifications will be binding on the bidders.

C-DAC at its discretion may extend the deadline for the submission of bids if it thinks necessary to do so or if the bid document undergoes changes during the bidding period, in order to give prospective bidders time to take into consideration the amendments while preparing their bids.

11. Preparation of Bids

Bidder should avoid, as far as possible, corrections, overwriting, erasures or postscripts in the bid documents. In case however, any corrections, overwriting, erasures or postscripts have to be made in the bids, they should be supported by dated signatures of the same authorized person signing the bid documents. However, bidder shall not be entitled to amend/ add/ delete/ correct the clauses mentioned in the entire tender document.

12. Period of validity of bids

Bids shall be valid for minimum 365 (Bid Validity) days from the date of submission. A bid valid for a shorter period shall stand rejected.

C-DAC may ask for the bidder's consent to extend the period of validity. Such request and the response shall be made in writing only. The bidder is free not to accept such request without forfeiting the EMD/BG. A bidder agreeing to the request for extension will not be permitted to modify their bid.

13. Late Bids

C-DAC shall not be responsible and liable for the delay in receiving the bid for whatsoever reason.

14. Bid Opening & Evaluation of Bids

1. The duly constituted Tender Evaluation Committee (TEC) shall evaluate the bids. The TEC shall be empowered to take appropriate decisions on minor deviations, if any. The decisions of TEC shall be final and binding on all the bidders.

2. The technical bids will be evaluated in two steps.
   i. The bids will be examined based on eligibility criteria stipulated at Para 5 of Section – II to determine the eligible bidders.

   ii. The technical bids of only the eligible bidders shall be further evaluated based on the technical specifications of the required items and the proposal submitted by the bidder.

3. The eligible bidders would be required to present the proposed solution at date and place intimated for better understanding. The guidelines for presentation would be issued at a later date.

4. The commercial bids of only the technically qualified bidders shall be opened and the prices quoted by the bidders will be compared. The prices (including GST) will be compared.

5. Placement of Order(s)

i. **C-DAC shall award the contract to the eligible Bidder whose technical bid has been accepted and determined as the lowest evaluated commercial bid based on the Part (I-IV) respectively, along with taxes of the Commercial Bids. However, C-DAC reserves the right and has sole discretion to reject the bid quoting abnormally low prices, even if it is the lowest.**

ii. C-DAC reserves the right to place order on the sole bidder or the sole qualified bidder.

iii. C-DAC reserves the rights to release Purchase Order for partial or total quantity based on the requirement.

6. Offered Price Validity & Quantity Variation

i. **Bidders need to give an undertaking to supply the quoted items at the same price as quoted in the Tender without any price escalation till one year from the data of Bid submission. Taxes shall be paid as per the applicable rate of GST at the time of delivery.**

ii. **C-DAC reserves the right to increase the ordered quantity by up to 25% within the bid validity period.**

7. Purchaser's Right to amend / cancel

C-DAC reserves the right to amend the eligibility criteria, quantities, commercial terms & conditions, Scope of Supply, technical specifications etc, stipulated in this document.

C-DAC reserves the right to cancel the entire tender without assigning any reasons thereof.

8. *Corrupt or Fraudulent Practices*

a) It is expected that the bidders who wish to bid for this project have highest standards of ethics.
b) C-DAC will reject a bid if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices while competing for this contract.
c) C-DAC may declare a vendor ineligible, either indefinitely or for a stated duration, to be awarded a contract if it at any time determines that the vendor has engaged in corrupt and fraudulent practices during the award / execution of contract.

9. *Delivery of Project:*

All Individuals deployed/associated/interacting with the buyer pertaining to this procurement by the Seller will have to be Indian nationals. The individuals so associated would need to abide by The Official Secrets Act, 1923 and have to individually sign a Non-Disclosure Agreement (to be handed over to the buyer) at the time of delivery.

10. *Interpretation of the clauses in the Tender Document / Contract Document*

In case of any ambiguity/ dispute in the interpretation of any of the clauses in this Tender Document, the interpretation of the clauses by Director General, C-DAC shall be final and binding on all parties.

(End of Section - II)

Section- III: Special Conditions of Contract (SCC)

1. Award of Contract/LOI/Purchase order:

C-DAC reserves all the rights to procure full / partial list of components from the L1 bidder. In case of staggered procurement, C-DAC may place an order for minimum 50% of the quantity of any /all items. Bidder shall supply the same equipment (Make & Model) as per the cost mentioned in the bid.

2. Prices

i. Bidder must quote in INR only.
ii. The price quoted shall be considered firm and no price escalation will be permitted (except Govt. Statutory Levies).
iii. Bidder must indicate applicable GST separately. The bidder should exercise utmost care to quote the correct percentage of applicable GST on each item.
iv. In case, due to any error/ oversight, the GST rate quoted by the bidder is different than the actual GST rate as per the tariff, the bidder will not be permitted to rectify the error/oversight. The orders/ contract will be placed with the GST rate quoted by the bidder or actual tariff rate (as on placement of order), whichever is LOWER. The difference amount payable, if any, between the quoted GST rate and actual tariff rate shall be borne by the bidder.
v. Notwithstanding the paras mentioned above, if the GST is not quoted separately and the bid is silent whether GST is included or excluded in price, then for the purpose of evaluation of bids, the prices shall be taken as including GST. In this case, the GST applicable, if any will be borne by the bidder/contractor.
vi. The prices quoted must be inclusive of packing, forwarding, insurance, loading/un-loading and all incidental charges till destination and completion of total scope of work.
vii. The responsibility, cost and risk of the consignment shall rest with the bidder till receipt of goods is acknowledged by the end user at site in New Delhi & Bengaluru. However, such receipt/ acknowledgement shall not be treated as acceptance of goods.

NOTE: C-DAC is not eligible for any GST concession for this procurement and C-DAC shall not provide any GST Concessional Certificate against this order.

3. Software Licenses: (if applicable)

The software licenses, if any, are required to be and shall be provided in the name of C-DAC. The licenses shall contain paper licenses and at least one set of media

(CDs) – wherever applicable. All the Licenses quoted shall be perpetual. All the upgrades, latest Release and Revisions, signature updates shall be provisioned with-out any additional cost during the warranty period. These licenses should be transferable to C-DAC's Customer at a future date when C-DAC's contract with the Customer is concluded.

4. Security Deposit (SD):

The successful bidder will be required to furnish the Security Deposit in INR equivalent to 3% (Three) of the order value within 10 days of receipt of Supply Order. The Security Deposit should be submitted in the form of Demand Draft/Bank Guarantee drawn **(As per Annexure H)** in favour of C-DAC payable at Pune. The Security Deposit shall be for the period of 6 months initially (i.e. the delivery period), which shall be extended till the final installation, testing, commissioning, integration and acceptance by CDAC. The Security Deposit will be returned upon completion of installation, commissioning and acceptance by CDAC along with submission of Performance Bank Guarantee (PBG).

The Buyer also reserves the right to forfeit the Security Deposit of the seller during the delivery phase in the event the seller is unable to meet contractual obligations.

5. Completeness Responsibility:

Notwithstanding the scope of work, supply and or services stated in bid document, any equipment or material, engineering or technical services which might not be even specifically mentioned under the scope of supply of the bidder and which are not expressly excluded therefrom but which, in view of the bidder, are necessary for the performance / execution of work in accordance with the specifications are treated as to be included in the bid and has to be performed by bidder. The items which are over & above the scope of supply specified in the Schedule of Requirements may be marked as "Optional Items".

6. Performance Bank Guarantee (PBG):

The successful bidder will be required to furnish the Performance Guarantee towards the items supplied, in the form of a Bank Guarantee in INR equivalent to 3% amount of the order value, as per the format attached to this document **(Annexure – D)**.

This bank guarantee should be submitted within 15 days from the date of final installation, testing, commissioning, integration, training and acceptance by CDAC. The Bank Guarantee shall remain valid for the **consolidated warranty period (3 years) of complete solution plus 2 months (total 38 months).** The PBG

must be negotiable at a branch of issuing bank in Pune. In case of no warranty claims towards the items under warranty, the PBG will be returned on completion of warranty period.

C-DAC reserves the right to invoke the Performance Bank Guarantee submitted by bidder, in case of the following:

a. The items supplied by bidder fail to achieve the performance as stipulated in this document or
b. The bidder fails to provide the warranty and other services in scheduled time frame, as stipulated in this document or
c. The bidder delays to provide the warranty services as stipulated in this document.

7. Warranty:

i. The Supplier warrants that all the Goods are new, unused, and of the most recent or current models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.
ii. The supplier further warrants that all Goods supplied under this contract shall have no defect arising from design, materials or workmanship (except when the design and/or material is required by the Purchaser's specifications) or from any act or omission of the supplier.
iii. The supplier should ensure that all features of the proposed solution are functional without requirement of any additional procurement of Hardware, Software, Subscriptions and Licenses from day one.
iv. The warranty should be comprehensive on site, basis. In case of any defect, fault occurring in the items supplied, during warranty period, the supplier shall arrange to repair /replace same free of cost.
v. The warranty period shall start from the date of demonstration of final solution and acceptance by CDAC.
vi. **All items including both Hardware and Software, respective subscriptions, supply shall include 3 (Three) years onsite comprehensive warranty with NBD support and call logging (single point of contact) mechanism based on telephonic, e-mail/chat support. The bidder should also provide escalation matrix for warranty support.**
vii. Bidder and OEM should ensure 4 hours' response time and resolution time of within 48 hrs. from the time of call logging covering all parts & labour starting from the date after the successful installation, during the warranty period covering all parts & labour.
viii. During the warranty period, bidder will have to undertake preventive and comprehensive maintenance of the entire hardware components, firmware,

equipment, support and accessories supplied by the bidder at the place of installation of the equipment.

ix. Collecting of faulty Hardware from the site and provisioning the replacement of Hardware under warranty at onsite shall be the responsibility of the supplier.

x. In case of fault arising in any hardware containing in-built memory, hard disk, or similar storage media, the said faulty hardware will not be allowed to be taken back from the C-DAC Customer premises. New hardware in place of faulty hardware will have to be provided by the supplier, without taking away the faulty hardware.

8. Acceptance Criteria:

The acceptance criteria shall be as stipulated in **Section-IV** of this document.

9. Payments:

a. No advance payment will be made.

b. 50% payment shall be released only after supply and acceptance of all the items by CDAC, under respective category. No part payment shall be released in case of short shipment from the respective category.

c. 40% of the Payment will be released upon installation / commissioning, integration, training, testing, demonstration of DC, Near DR, DR replication & failover etc. as stipulated in Section – IV: Scope of Supply and Services

d. Balance 10% payment shall be released after submission of PBG (valuing 3% of order value) covering the warranty period of 38 months from the date of final installation, testing, commissioning, integration, training and acceptance by CDAC.

e. C-DAC reserves the rights to confiscate PBG amount if the bidder is not adhering to the support matrix of 4 hrs. response time and Next Business Day (NBD) complaint resolution.

10. Timely servicing /rectification of defects during warranty period

After having been notified of the defects/service requirement during the warranty period, seller has to complete the required service/rectification within the next business day (NBD). If the seller fails to complete the service/rectification within the defined time limit, a penalty of 0.5% of the unit price of the product shall be charged as penalty for each week of delay by the seller. Seller can deposit the penalty with the buyer directly else the buyer shall have the right to recover all

such penalty amount from the PBG. Cumulative penalty cannot exceed more than 10% of the contract value after which the buyer shall have the right to get the service/rectification done from alternate sources at the risk and cost of the seller besides the forfeiture of the PBG. Seller shall be liable to reimburse the cost of such service/rectification to the Buyer.

11. Shipping Documents:

The invoice shall be raised in the name of:
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, PANCHAVATI, Pashan Road, PUNE 411008
Maharashtra, INDIA

The name, address and details of contact person of C-DAC's Customer will be informed to the successful bidder.

12. Penalty for delayed delivery /Services

C-DAC reserves the right to levy penalty @ of 0.5% of order value per week of delay beyond the scheduled deliveries / execution of the order successfully (which includes installation, configuration, DC-DR replication), subject to maximum of 5% of the order value.

C-DAC reserves the right to cancel the order in case the delay is more than 10 weeks.

The delay in delivery and/or installation not attributed to supplier viz. delay in site preparation, delay in submission of required documents (by C-DAC) etc. and the conditions arising out of Force Majeure will not be considered for the purpose of calculating penalties.

13. Jurisdiction:

The disputes, legal matters, court matters, if any shall be subject to Pune jurisdiction only.

14. Force Majeure:

C-DAC may consider relaxing the penalty and delivery requirements, as specified in this document, if and to the extent that, the delay in performance or other failure to perform its obligations under the contract is the result of an Force Majeure. Force Majeure is defined as an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, floods, storms etc.), acts of states / state agencies, the direct and indirect consequences of wars (declared or

undeclared), hostilities, national emergencies, civil commotion and strikes at successful Bidder's premises or any other act beyond control of the bidder.

15. Arbitration:

In case any dispute arises between the C-DAC and successful bidder with respect to this RFP, including its interpretation, implementation or alleged material breach of any of its provisions both the Parties hereto shall endeavour to settle such dispute amicably. If the Parties fail to bring about an amicable settlement within a period of 30 (thirty) days, dispute shall be referred to the sole arbitrator mutually appointed by both parties. If the sole arbitrator is not appointed mutually by both the parties then the District Court Pune shall have exclusive jurisdiction for appointment of sole arbitrator through court. Arbitration proceedings shall be conducted in accordance with the provisions of the Arbitration and Conciliation Act, 1996 and Rules made there under, or any legislative amendment or modification made thereto. The venue of the arbitration shall be Pune. The award given by the arbitrator shall be final and binding on the Parties. The language of arbitration shall be English. The common cost of the arbitration proceedings shall initially be borne equally by the Parties and finally by the Party against whom the award is passed. Any other costs or expenses incurred by a Party in relation to the arbitration proceedings shall ultimately be borne by the Party as the arbitrator may decide. Courts in Pune only shall have the exclusive jurisdiction to try, entertain and decide the matters which are not covered under the Arbitration and conciliation Act.

16. Risk and Ownership:

All risks, responsibilities; liabilities pertaining to goods in transit and/or delivered at site shall remain with selected bidder till they are accepted by C-DAC.

The successful bidder will make own arrangements to secure and safeguard the goods delivered at site, at their own cost. C-DAC may coordinate with the client for getting help for these arrangements.

Upon 90% of payment and post successful acceptance testing, C-DAC shall become owners of goods ordered but all risks, responsibilities; liabilities thereof in all goods shall remain with selected OEM/bidder till installation, commissioning, integration, and training of all goods to the end user. Part deliveries shall not be treated as deliveries. Only full deliveries of all items ordered will be considered as delivery.

17. *Limitation of Liability:*

The liability of the Bidder / Contractor arising out of breach of any terms/conditions of the tender / contract/work order and addendums/amendments thereto, misconduct, wilful default will be limited to the total order value. However, liability of the bidder in case of breach of any relevant Law/ Act, injury, damage caused to the personnel/property for any reasons attributed to the bidder, will be at actuals.

18. *Termination:*

Validity of purchase order will remain till fulfilment of all obligations (Including but not limited to providing comprehensive warranty / support till Completion of three years from acceptance of the entire integrated solution as a whole) by the successful bidder. In case of the delays in providing the stipulated services, and /or defect/delay/under or non- Performance pertaining to the services / products supplied by the bidder, C-DAC will give written notice to the bidder directing to set the things right within 30 days of notice. If bidder fails to comply with the requirements, C-DAC shall have the right to terminate the contract and / or cancel the order/s. The successful bidder agrees and accepts that he shall be liable to pay damages claimed by C-DAC, in the event of termination of contract / cancellation of order, as detailed in this RFP. The successful bidder may terminate the contract by at least 30 days' written notice, only in the event of non-payment of undisputed invoices for 90 days from the due date. Except this situation, the successful bidder shall have no right of termination. C-DAC reserves the right to terminate the contract / cancel order with or without cause/ reason, by giving 90 days' notice to the successful bidder.

C-DAC will release the due amount payable to successful bidder towards the material and / or services provided till the date of termination, those are accepted by C-DAC/ end user. However, the amount towards penalty, if any will be deducted from the payable amounts.

19. *Indemnity:*

The successful bidder shall indemnify, protect and save C-DAC from/against all claims, losses, costs, damages, expenses, action suits and other proceeding, resulting from/arising out of:

a. infringement of any law pertaining to intellectual property, patent, trademarks, copyrights, safety and security etc. by the bidder or
b. such other statutory infringements in respect of any item supplied by successful bidder, or
c. any act/omission/performance/under or non or part performance/failure of the bidder.

20. Assignment:

Selected bidder/ Party shall not assign, delegate or otherwise deal with any of its rights or obligation under this Contract without prior written permission of C-DAC.

21. Severability:

If any provision of this Contract is determined to be invalid or unenforceable, it will be deemed to be modified to the minimum extent necessary to be valid and enforceable. If it cannot be so modified, it will be deleted and the deletion will not affect the validity or enforceability of any other provision.

(End of Section - III)

Section – IV: Scope of Supply and Services

1. Enterprise Architecture to be Supported:

a. C-DAC is undertaking a greenfield and turnkey project to build a suite of Big Data enterprise Applications, each of which is to be built over a secure, flexible, configurable through network that has multiple attributes of support for the latest networking protocols, continuous visibility and monitoring, policy driven centralized orchestration and management, and the ability to fully abstract the networking capabilities from the platform services and applications overlaid on top. The software configurable network should have a IPv4 / IPv6 Underlay and should provide a rich networking Overlay (both L2 and L3 protocols and tunneling) supporting the platform services and applications built on top.

b. The complete solution is to be spread over two geographical locations, one hosting both the DC and the Business Continuity Near DC (BCP), and the other hosting the Disaster Recovery (DR) site. The DC and Near DC (BCP) are located in a single Campus within the understanding of a "campus" in enterprise networks. The WAN connectivity is provided by external Communication Service Providers (CSPs) using dedicated MPLS links and SDWAN links while the LAN at all locations is to be designed, engineered, and operated by C-DAC. The entire technology and solution stack is intended to be created as a Private Enterprise Cloud built entirely on-premise at the locations specified. None of the capabilities of the network, the virtualized Compute and Storage, and associated services can be connected to or managed from OEM or System Integrator resources or services deployed on any public cloud or an OEM specific remote site. DC and BCP sites are approx. 100Mtr apart and existing Dark Fibre cable (OM4) will be used to connect the two sites directly with multiple 400G links.

c. Apart from the locations mentioned above, the solution will connect to a number of Data Nodes at various locations as the source of data for the big data applications. At least one application will connect to such data nodes deployed on the public Internet. The solutions deployed at the DC, BCP and DR sites, and the remote data nodes specified above, will constitute the federated data layer backend for the applications. The applications are to be delivered to a number of Consumption Nodes in diverse configurations, ranging from small Branch Office type configurations having their own LAN and gateways using centrally managed user endpoints at secured premises over secure links, to single user endpoints connecting to a Virtual Desktop Infrastructure (VDI) deployed in the DC, BCP and DR sites. The Underlay and Overlay networks should be able to provide a single view of the DC, BCP, DR

and all the Points of Presence (PsOP) (comprising of the Data Nodes and Consumption Nodes) to support the Platform Services, Applications, and Data Layers of the full stack solutions.

d. The network should support the Applications to have full Data Isolation and a high degree of Data Autonomy. The applications will utilize a virtualized layer of compute and storage using the hypervisor and container and storage virtualization architectures from all leading OEMs, specifically VMWare, Microsoft, Citrix, Red Hat, and Oracle. Containerization using Docker, Kubernetes, and equivalent technologies should be fully supported. The Overlay networks should provide the capabilities for segmentation required to ensure Service Isolation and Service Autonomy of each of the common platform services like Authentication, Authorization, Certificate Management, Secrets Management, API Management, etc.

e. The entire network and platform services with their associated data should have an Observability capability, with network observability in the Underlay and Overlay network. The routing, bandwidth management, and other network configuration aspects for both the Underlay and Overlay should fully flexible based on the evolving needs. A dedicated Fabric Management cluster, preferably using appliances, should be provided for orchestration and maintenance of Overlay and Underlay configurations. Granular control of network flows in both the Underlay and Overlay should be ensured supporting Security requirements.

f. The totality of the Compute and Storage resources, except specific components deliberately operated in bare metal configurations, are to be virtualized using a variety of virtualization software from prominent OEMS like Microsoft, VMWare, Red Hat, Oracle etc. and to be managed centrally for creation of VMs, Containers and related virtualized computing objects. It should be possible to use the underlying hardware and firmware in a manner that is agnostic of the virtualization software that may be used.

g. The totality of the Compute and Storage resources will be deployed using an Overlay Network connecting all the sites, including the DC, BCP, and DR and also extending to a set of remote nodes. The networking interfaces of the compute and storage resources should be standards based and it should be possible to provide the required connectivity without specific networking equipment dependencies.

h. The totality of the Compute and Storage resources will be monitored, configured and updated from a centralized NOC and SOC. It will be necessary for hardware and software assets being procured to have standards-based interfaces for such functionality. In case of any specific communication and reporting mechanisms specific to the hardware and software being supplied, the Bidder will be expected to provide the necessary software and hardware to make these assets ready for integration.

i. **Important Note for OEMs and Bidders**:
The purpose of providing a detailed articulation of the Enterprise Architecture, and the Network and Network Security Architecture in the subsequent sections, is to ensure that OEMs and Bidders are able to examine the detailed BoM and BoQ and map the choice of hardware and software that they propose to support the desired business outcomes. Suitability of the actual Bidder proposal, to be certified by the OEM, for the Enterprise Architecture requirements given above will be evaluated as part of the Technical Evaluation. It will be the responsibility of the Bidders to point out any gaps in the RFP and propose additional hardware and software components beyond those already listed in the RFP to meet the architecture requirements given in Section IV.

2. Network Architecture:

a. The networking layer of the full stack enterprise solution comprising of multiple applications built using multi-tenancy approach is proposed to be designed and engineered as a unified multi-site Spine-Leaf Fabric.

b. The inter-site communications may be engineered as inter-Spine traffic or via Border Leafs. All traffic to the remote Data Nodes (except Data Nodes in the public Internet) and Consumption Nodes will pass through and be controlled by a Systems Gateway using firewall appliances with the ability for deep packet inspection, WAFs, VDI Gateway, VPN terminations and the creation of DMZs. The Data Nodes in the public Internet will be connected through a separate Internet Gateway.

c. All networking nodes/appliances will be required to operate with Active-Active HA configurations. The design should support 100G uplinks from Compute leaf to Spine Switches with equal number of links forming full mesh from leaf to each spine. The design will support Out of Band network management across all data center sites. Seamless movement of workloads between the data

center sites is to be ensured. 400G connectivity will be designed and engineered between Spines in the same campus.

3. *Network Security Architecture:*

a. The solution will have two NGFW deployed in HA in DC, BCP and DR for each of the MPLS and Internet segments. These two clusters (Cluster-1 and Cluster-2) of NGFW will form single cluster between DC and BCP and state will be in sync across them for load balancing, and asymmetric routing between DC and BCP.

b. Redundancy must be achieved with dedicated session sync between each peer set. Each pair of NGFW will have a bi-directional integration with a pair (HA) / Cluster of SANDBOX. Virtual context / domains in the NGFW will hand-off the respective VRF from the respective switch and used for segmentation between different application zones, NOC, SOC, and Platform Services. BGP session to be established with the Border, Service and L3 Perimeter switches respectively for dynamic routing.

c. NGFW to have active integration with VMWARE ESXI, SIEM and SOAR platform.

d. An NGFW Manager will be used for flexible centralized deployment of firewall policies.

e. The WAF solution has two devices deployed in HA in DC, BCP and DR for each of the MPLS and Internet segments. It shall be used for load balancing and web application inspection of the VDI traffic and shall be placed before the user and internet facing applications with SSL offload enabled. WAF will be logically segmented (virtual application delivery control) to provide isolation for the respective application. WAF shall integrate with SANDBOX for file sanitization.

4. *Technical Specifications:*

Subject to the stipulations given in **Paragraph 1-3** of Section-IV above, the bidder should supply, install, program, and configure, test, commission the items as detailed in **'Section-V: Technical Specification'.**

5. *Acceptance Criteria:*

a. Hardware should be from original manufacturers and should be shipped in original packing with OEM part numbers.

b. All supplied Hardware should go through POST for at least 24 hrs.

c. The Bidder will be required to obtain a successful installation and commissioning certificate from C-DAC, after the activities covering installation, initial programming and configuration, and testing are completed. This will cover all internal and external integrations. This also included demonstration of features, capability of the products listed in the specifications of the product in RFP.

d. Bidder shall showcase the appropriate licenses (on the respective OEM site) mentioned in the RFP.

e. Bidder shall share the workorder placed on the OEM for back-to-back support of 3 years for the quoted items after the date of commissioning.

f. Bidder shall showcase the Work Order placed on the OEM for delivery of services earmarked for the OEM as per Paragraph 7 of Section IV. This will clearly indicate the scope of work apportioned to the OEM and the corresponding manhours of effort applied.

g. The Bidder, duly supported by the OEM, shall provide appropriate training on the supplied hardware and software, including the demonstrated initial configurations at the time of commissioning, to the C-DAC teams comprising the L1, L2, and L3 Operations and Maintenance (OAM) staff to be deployed at each of the sites, in the manner described in Paragraph 7 of Section IV.

h. Server configuration (BIOS, Firmware, Hyperthreading, IPMI etc.)

i. Storage configuration (Creation of RAID groups, volumes, assigning of Hot spares, Volume mgmt., Licenses, Remote Replication options (Block level), snapshots and showcase remote replication of test data etc.

j. Backup Software configuration for client and server, backup policies and integration with Tape Libraries. Tape Library volume creations, partitioning, drive allocation, showcasing of parallel threads and parallel streaming through the supplied Backup Software etc.

k. Bidder shall execute all the points mentioned under Scope of Work as given at **Paragraphs 6 to 12 of Section-IV**.

6. General Scope of Work:

a. General Scope will be applicable to all the quoted items (software, hardware, and services).

b. The Bidder will ensure that all stages covering installation, initial programming and configuration, and testing are fully documented and endorsed by the OEM. The Bidder will also be required to provide the Work Order placed on the OEM as documented proof of the involvement of the OEM within the scope of Paragraph 7 of Section IV. Bidders should link this with the Acceptance Criteria given at **Paragraph3e, 3f and 3g of Section IV**.

c. Bidder shall ensure that the items supplied are as per the Tender specifications, combined with changes stipulated in Corrigenda issued (if any).

d. Bidder shall ensure that the items are received in good condition at the respective delivery location in presence of C-DAC official and record the same.

e. Bidder shall maintain the inventory of the supplied items and maintain the associated Barcodes, Licenses, Software etc.

f. Bidder shall ensure the deployment, configuration of all items as per the requirement submitted by C-DAC.

g. Bidder is responsible to showcase the integration of all software and hardware supplied towards the Tender.

h. Bidder shall complete the entire installation, configuration and integration of all hardware and software supplied at DC, BCP, DR, and any remote sites (as applicable) within one month.

i. Bidder shall participate and demonstrate DC, BCP and DR functionality with failover from the perspective of network, security components, Storage replication and other components supplied as per RFP.

j. Periodic upgradation of all software and firmware as advised by the OEM or by the Government of India Cybersecurity agencies. For this purpose, the Bidder should provide all patches and upgrades in removable media and apply them from within the premises controlled by C-DAC and/or its Customer. This will include updating of signatures and threat feeds etc. of the relevant hardware and software components.

k. To maintain all supplied items in a good state of health and operations.

l. To provide the necessary interfacing and orchestration of OEM involvement in the provision of services earmarked for the OEM and as part of the support contract.

7. OEM Scope of Work:

a. Considering the complexity and importance of the solution, sensitivities of C-DAC's Customer, as well as the tight schedules, active engagement of the concerned OEMs is expected. The Bidder will provide full visibility into the actual scope of work written down to the OEM, including the effort in man months in the Technical bid document. The cost for this should be captured separately in the Commercial Bid.

b. The Bidder has to ensure that OEM engages its Professional Services (PS) team for planning, design, implementation, integration, validation, handover, and training of the respective hardware and software components across all three sites - DC, BCP and DR. The engaged PS Team members should be OEM's employees and the OEM should not further outsource these obligations to another vendor. These commitments will be a part of the Technical Evaluation and will be tracked at all stages after the issue of the PO.

c. The OEM is required to provide an Authorization as per Appendix C to this RFP that the OEM "undertakes to provide, within the Scope of Work defined in the tender, technical and other support towards fulfilling the requirements of installation, commissioning, benchmarking, acceptance criteria and product warranty services of the components to be supplied and installed at the C-DAC Customer sites". The following paragraphs provide a brief, though not necessarily complete, interpretation of these commitments.

d. The OEM concerned (where there is more than one in the equipment included in the Bid) will assign a designated technical expert to oversee all installation, configuration, and integration activities as given within the Overall Scope of Work given at **Paragraph 6 & 12 of Section IV** and segment specific Scope of Work as given at **Paragraphs 8 to 12 of Section IV**.

e. The OEM assigned expert will be required to guide and validate all documentation supporting the installation, configuration, and integration as per the defined scope.

f. The OEM will support the Bidder in providing appropriate training on the supplied hardware and software, including the demonstrated initial configurations at the time of commissioning, to the C-DAC teams comprising the L1, L2, and L3 Operations and Maintenance (OAM) staff to be deployed at each of the sites. Product specific training should be delivered by the OEM representatives ONLY.

g. OEM participation, guidance, and validation of all activities within the scope of this paragraph will be provided on-premise at New Delhi and Bangalore.

8. Scope of Work – Network Fabric

a. Supply, Installation, Configuration, Commissioning, Integration, Testing and Maintenance Support of complete hardware including all necessary software licenses as per the BOM and Technical specifications mentioned in tender for DC, BCP, DR and any remote site. This will be done in consultation with the OEM as per Paragraph – of Section --.

b. The solution should be planned to keep a holistic view of the network requirement spanned across the three sites connected with MPLS cloud and the Internet segment. Dedicated leaf-spine fabric to be deployed for Internet facing setup and MPLS facing setup.

c. Network should be designed to support applications running in active-active mode from both DC and BCP. The DR will remain in passive mode until a failover to the DR site is done.

d. Multiple physically separate Leaf-Spine fabrics will exist in each site catering to the requirement of OOB Management, user applications and Internet facing applications. All the fabrics in all 3 sites (DC, BCP and DR) need to be provisioned.

e. Leaf-Spine Fabric should be built with L3 Underlay and open standards (VXLAN, EVPN) Overlay. Proposed fabric technology should support multiple OEM switches to be part of a single leaf-spine fabric.

f. Leaf switches are to be configured for VXLAN tunneling with distributed Anycast gateway supporting symmetric integrated routing and bridging with EVPN control plane.

g. The fabric should be configured with EVPN multihoming for active-active redundancy to server and other appliances connected to the EVPN fabric.

h. Fabric should be configured with ARP suppression.

i. Fabric to be configured for Multicast requirement in VXLAN overlay network.

j. Fabric to be configured with QoS as per requirement.

k. The fabric to be designed with virtual output queue based architecture to avoid head of line blocking issues in the fabric.

l. The design should leverage VXLAN and VRFs within the fabric for network segmentation as per requirement.

m. Fabric must be designed to provide packet buffering for low latency(<=50ms) when receiving traffic at line rate on all uplink ports simultaneously.

n. The network fabrics are required to be stretched across DC, BCP and DR for layer-2 and Layer-3 services using VXLAN+EVPN.

o. DC and BCP sites are approx. 100Mtr apart and existing Dark Fibre cable (OM4) need to be lighted to connect the Spines at the two sites directly with multiple 400G links for 1:1 oversubscription.

p. Dark Fibre lighting shall include supply of rack mounted LIUs and Single mode duplex Fibre LC connectors to light-up 32 cores on each side.

q. The DCI between DC-BCP and DR sites to be configured with multi-domain VXLAN+EVPN to maximize data plane and control plane isolation with DR site.

r. MPLS/SD-WAN cloud to provide only Underlay. DCI should be transparent to MPLS/SD-WAN underlay. There should not be any routing dependency for Overlay networks on MPLS/SD-WAN cloud other than Underlay IP reachability between DCI nodes.

s. Network monitoring and management system to be set up to centrally monitor and manage all the network switches across 3 sites and in remote provider location, from a central dashboard. HA/Backup of the system to be configured in another site for continued day-2 operation in case of primary system/site failure.

t. All day-0 switch provisioning and day-2 fabric operations across sites should be done centrally from the Fabric Manager to minimize human errors.

u. Network wide monitoring based on real-time state streaming should be configured for all switches for in depth visibility with ability to quickly troubleshoot and correlate historical metrics over a timeline.

v. Role based access control to be configured for network fabric with change controls for approval and execution in place.

w. Fabric to be configured to show physical and logical fabric topology on a central dashboard with ability to show path of a flow over network topology.

x. Fabric to be configured for flow generation, collection, and analytics.

y. Dedicated device(s) with minimum 4GB of packet buffer to be configured in each site to aggregate mirrored traffic from all the leaf-spine switches over 100G links, to further use the traffic for security and performance analytics purposes.

9. Scope of Work - WIPS

a. The Bidder would need to perform site visit to understand the coverage and placement of WIPS devices. The dual controllers in HA need to be housed in DC and BCP, DR to ensure high availability and continuation of WIPS Services.

b. Bidder/OEM need to configure and deploy the WIPS sensors and Controllers as per the security requirement.

10. Scope of Work – Firewall & WAF

a. Supply, Installation, Configuration, Commissioning, Integration, Testing and Maintenance Support of complete hardware including all necessary software licenses as per the BOM and Technical specifications mentioned in tender for DC, BCP and DR site.

b. Integration with Network Fabric Manager, VMWARE hypervisor components, SANBOX, SIEM and SOAR, endpoint security as per the requirement.

c. Establishing BGP with the respective switches, full mesh connectivity, HA setup with stateful session, testing of both symmetric and asymmetric routing.

d. Advanced and Custom - filters, signatures, and API integrations as per the requirement

e. Fine tuning of WAF rules after analyzing the application behaviour.

f. Vulnerability assessment of the application and writing required policies/configurations to do virtual patching.

11. Scope of Work – NAC

a. Supply, Installation, Configuration, Commissioning, Integration, Testing and Maintenance Support of complete hardware including all necessary software licenses as per the BOM and Technical specifications mentioned in tender for DC, BCP and DR site.

b. Enforce 802.1x and device profiling with access controls on end-point systems.

c. Granular access controls for all the network devices with TACACS+.

d. Enforce dynamic policy controls on switches and Firewall.

12. Detailed Scope of Work:

a. Bidder is responsible to showcase the integration of all Software and Hardware supplied as part of this RFP.

b. Bidder shall demonstrate DC, BCP and DR functionality with failover for various components like Storage, Database clusters, Backup activities etc.

c. Meeting DC, BCP and DR deployment and functionality includes the following:

1) Shall submit the detailed plan about the project execution.
2) Shall meet Zero RPO.
3) Shall meet 45 Minutes of RTO.
4) Storage based (Block / Change Block) & Snapshot Replication.
5) VM level Replication.
6) Replication of Cluster of VMs / Site Recovery Tools or equivalent as per the RTO and RPO.

d. Implementation of Stretch Cluster / Seamless integration of DC and BCP to form a single cluster w.r.to Compute & Storage.

e. Deployment and configuration of VMs with the supplied Hypervisor.

f. Integration of Cluster Mgmt. Tools for smooth migration, scaling-up/down of Virtual Systems based on the load.

g. Shall perform Logical Partitioning of Storage and Tape Library as per the customer needs.

h. Integration of Backup/Restore Tools (with encryption) towards snapshots, incremental, differential, Full dumps.

i. Configuration of Storage for various RAID Groups, Volumes with hot spares and Snapshots.

j. Understanding of underlaying Network details (details will be shared with the L1 bidder)

k. Deployment of SOC: Configuration of SIEM , SOAR and associated tools to provide the deep analysis and automation of repeated tasks. Required APIs shall be provided and bidder need to factor appropriate manpower to write the scripts towards integration of various logs, devices for analysis and mitigation.

l. Deployment of EDR across all VMs and physical systems.

m. All the equipment Firmware and patches shall be applied in offline mode (no internet connectivity to the devices is allowed).

n. All the licenses shall be supplied and applied in offline mode.

o. Deployment of VM level Security and integration of VM level Firewall controllers with East-West Firewall.

p. Need to route the cables from the supplied devices to the respective rack level switches (both Copper and Fibre)

q. Perform the cabling and rack dressing.

r. Providing necessary support during the Warranty period towards replacement of faculty Hardware, Configuration of devices and supplied Software's.

s. Bidder need to appoint a single point of contact and provide the details for raising of tickets. Please note that support and services offered shall be confined to DC, BCP and DR and there is "NO" provision of online access to any system, device and software.

t. Bidder need to provide call registration model like ticketing system with escalation matrix. Shall provide an url /portal to track the status of the raised tickets.

u. During the warranty support period, the bidder shall have tie up with the respective OEM for Backend support for the entire set of ICT Infrastructure listed in schedule of requirements (Section V, Annexure-1).

v. The bidder shall furnish documentary proof of backend support including software upgrades, availability of spares, availability of hardware/ software modules required for scalability for a period of 03 years from the respective OEMs of the products offered (As per format given in Annexure F).

w. The tie up with OEM of the Hardware equipment installed in the Data centre should cover:
   1) 24 x 7 x 365 Onsite Support for all supplied hardware equipment with 4 hours response and NBD resolution.
   2) Provision to log complaints/ open support cases directly with OEM. For this purpose the required details should be shared with C-DAC along with component IDs for all components covered under warranty/maintenance.
   3) Root Cause Analysis of all failures – a preliminary report shall be submitted within 24 hours of the failure and a detailed technical analysis report on the root cause from OEM shall be submitted within one week from the date of failure.

x. On-site support of OEM for Troubleshooting in case of critical failures, especially for the failures extending beyond the permissible downtime.

y. Bidder shall provide an onsite dedicated RE (Residence Engineer) at DC on 9/6 basis. RE is responsible towards:
   1) Proactive monitoring of supplied equipment / devices.
   2) Tracking of all tickets / incidents raised and co-ordinate with the Bidder & OEM to rectify / replace the faulty component.
   3) Performance finetuning.
   4) Co-ordinate with the DC, BCP and DR Operations team.
   5) Responsible to perform DC-DR drills as per the schedule.

z. Submit daily report on health of the systems.

aa. Shall obtain permission from the Operations Head towards any changes in the configuration, updates, replacement of parts, devices, software etc.

bb. Shall inform the new Serial number, License and other details to the Operations Head to update inventory.

cc. Change of RE shall be taken-up only with the permission of C-DAC.

(End of Section - IV)

Section-V: Technical Specifications

Category-I

1. DEGAUSS01

Sr. No.	Features & Specifications
1.	Should have minimum 2Tesla magnetic field to degauss Hard disks, CDs etc.
2.	Shall Track and record media serial/asset number, user ID, witness ID, date, time, and location in a password-protected system for Auditing.
3.	Shall provide proof by capturing a JPG image of the media immediately after degaussing.
4.	Records the crush depth of the physical destroyer.
5.	Shall Document destruction of solid-state media when using the solid-state destroyer.
6.	Automatically generates exportable Certificates of Erasure and Destruction for audit and archival purposes
7.	Provides searchable, verified database of sanitized drives to satisfy auditors
8.	Shall be able to physically destroy solid-state media, flash drives, USB thumb drives, mobile phones and SSHD controller boards, CDs, Access cards etc.
9.	Should generate a detailed report and certificate towards De-gaussing and destroying.
10.	Should meet safety standards of UL/IEC/CE or equivalent.

2. HSM01

Sr. No.	Parameter	Specifications
1.	Physical Characteristics	19 Inch Rack Mount with a maximum size of 2U along with rack mounting kit, Input Voltage – 230 V AC 50 Hz, Operating Temperature range must include 15 degrees Centigrade to 35 degree centigrade, Operating humidity range must be better than 30 to 70 (RH) Non condensing at 35 degree centigrade, Protection against physical attacks such as use

Sr. No.	Parameter	Specifications
		of potting of critical components, tamper evident security labels etc.
2.	Supported operating Systems	Programming APIs must be available for Windows and Linux, Should be configurable to communicate only with authenticated servers.
3.	Host connectivity	TCP/IP Network based appliance- Dual 1 Gigabit interfaces, dual fiber 10 Gigabit Ethernet interfaces
4.	Safety, security and environmental compliance	Comply to standards like RoHS, UL, CE, FCC
5.	Hash/message digest	Minimum SHA-1, SHA-2 (224, 256 and 384)
6.	Cryptography Symmetric	Symmetric Algorithm : AES, 3DES (2 Key and 3 Key)
7.	Cryptography Asymmetric	Cryptographic algorithms: Diffie-Hellman , RSA (2048, 4096 bit), DSA
8.	Cryptography ECC	Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC), ECDSA and ECDH
9.	Cryptographic module security and certification	Compliance to FIPS 140-2 Level 3 , Password and Multi-Factor (PED)
10.	Min. Memory within HSM (MB)	16 MB
11.	Number of Partitions within HSM	5
12.	Number of Partitions Expandable upto within HSM	20
13.	Key Storage Area	Inside the HSMs FIPS 140-2 Level3 cryptography boundary
14.	Application Interfaces (APIs)	Compatibility: PKCS#11, OpenSSL, Java (JCE) ,C and C++, Compatible to interface with opensource based CA software like OpenCA and EJBCA
15.	Key Generation and Storage	Ability to generate and store ECC P256 minimum 90 keys on board on demand

Sr. No.	Parameter	Specifications
16.	Signing Performance	Minimum ECC-P256 10000 and RSA-2048 5000
17.	Speed	• Signing speed: RSA 2048 bit – at least 5000 Signatures/seconds, ECC (256 Bit) 10000 Signautres/Seconds • Key generation speed RSA (2048bit) 14 keys/sec ECC (256 bit) 90 keys/sec
18.	Access control	Authenticated multi-level access control, Protection for configurability using secure devices such as smart card and USB token, Roles - Support for role based access control (minimum 2 roles)
19.	Load Balancing	Clustering, load-balancing
20.	Key back up	Secure key backup and recovery
21.	Key Processes	Onboard key generation and Digital Signing
22.	Support for multiple HSMs	Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover
23.	Power source	Dual hot-swap power supplies, field serviceable
24.	Monitoring	Storing of event based audit logs and standard mechanisms for viewing logs
25.	CLI / GUI	Command line interface (CLI)/graphical user interface (GUI)
26.	Backup device	Provide one no. of backup device to take backup of HSM stored keys.
27.	Reliability	MTBF: Minimum 40000 hrs
28.	Warranty	3-year onsite comprehensive warranty with "No" additional cost for change/ replacement of parts, charges towards labour, consumables, shipment, insurance etc. 24x7 support with 4 hours of response time with NBD resolution. Hard Disk should be covered under warranty on non-returnable basis
29.	Licenses	Supply should include all the necessary licenses required for meeting the above specifications.
30.	Rack mounting	HSM should mountable and fit in standard 42 U, 19" rack

Sr. No.	Parameter	Specifications
		Mounting sliding rail Kit and with cable manager
31.	Packaging contents	1. Supply with User manual or links 2. Server Rail Kit with screws 3. IEC type power cables
32.	Additional Requirements	The HSM should be provided with 1) 1 Nos. of PED device, 2) 1 Nos. of compatible keys/card set of 10 keys, 3) 1 Nos. of Backup HSM 4) The quoted Backup HSM and HSM should compatible with "Safenet Luna SA 7000" HSM and it's backup device

3. HSM02

Sr. No.	Parameter	Specifications
1.	Physical Characteristics	PCI-Express CEM 3.0, PCI, PCI Express Base 2.0 Low Profile PCIe card Input Voltage – 230 V AC 50 Hz, Operating Temperature range must include 15 degrees Centigrade to 35 degree centigrade, Operating humidity range must be better than 30 to 70 (RH) Non condensing at 35 degree centigrade, Protection against physical attacks such as use of potting of critical components, tamper evident security labels etc.
2.	Supported operating Systems	Programming APIs must be available for Windows and Linux, should be configurable to communicate only with authenticated servers.
3.	Host connectivity	TCP/IP Network based appliance- dual 1 Gigabit interfaces dual 10 Gigabit Ethernet interfaces
4.	Safety, security and environmental compliance	Comply to standards like RoHS, UL, CE, FCC
5.	Hash/message digest	Minimum SHA-1, SHA-2 (224, 256 and 384)
6.	Cryptography Symmetric	Symmetric Algorithm: AES, 3DES (2 Key and 3 Key)
7.	Cryptography Asymmetric	Cryptographic algorithms: Diffie-Hellman, RSA (2048, 4096 bit), DSA

Sr. No.	Parameter	Specifications
8.	Cryptography ECC	Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC), ECDSA and ECDH
9.	Cryptographic module security and certification	Compliance to FIPS 140-2 Level 3 , Password and Multi-Factor (PED)
10.	Min. Memory within HSM (MB)	16 MB
11.	Number of Partitions within HSM	5
12.	Number of Partitions Expandable upto within HSM	20
13.	Key Storage Area	Inside the HSMs FIPS 140-2 Level3 cryptography boundary
14.	Application Interfaces (APIs)	Compatibility: PKCS#11, OpenSSL, Java (JCE) ,C and C++, Compatible to interface with opensource based CA software like OpenCA and EJBCA
15.	Key Generation and Storage	Ability to generate and store ECC P256 minimum 90 keys on board on demand
16.	Signing Performance	Minimum ECC-P256 2000 and RSA-2048 1000
17.	Access control	Authenticated multi-level access control, Protection for configurability using secure devices such as smart card and USB token, Roles - Support for role based access control (minimum 2 roles)
18.	Load Balancing	Clustering, load-balancing
19.	Key back up	Secure key backup and recovery
20.	Key Processes	Onboard key generation and Digital Signing
21.	Power consumption	18W maximum
22.	Monitoring	Storing of event based audit logs and standard mechanisms for viewing logs
23.	CLI / GUI	Command line interface (CLI)/graphical user interface (GUI)
24.	Backup device	One no. of backup device to take backup of HSM stored keys.
25.	Reliability	MTBF: Minimum 40000 hrs

Sr. No.	Parameter	Specifications
26.	Warranty	3-year onsite comprehensive warranty with "No" additional cost for change/ replacement of parts, charges towards labour, consumables, shipment, insurance etc. 24x7 support with 4 hours of response time with NBD resolution. Hard Disk should be covered under warranty on non-returnable basis
27.	Licenses	Supply should include all the necessary licenses required for meeting the above specifications.
28.	Rack mounting	HSM should mountable and fit in standard 42 U, 19" rack Mounting sliding rail Kit and with cable manager
29.	Packaging contents	1. Supply with User manual or links 2. Server Rail Kit with screws 3. IEC type power cables

4. KM01

Sr. No.	Features & Specifications
1.	The proposed solution should be a appliance based solution integrated with Hardware Security Module (HSM), standard 19" rack mountable with sliding rails, max. 2U size
2.	Minimum 1 TB of internal storage, mini. 16GB RAM, 8 Core processor.
3.	Minimum 1x1GB 1x10Gb fibre ethernet ports with SFPs
4.	Should provide a centralized management console to control the lifecycle and permission of the keys using REST API, Command Line Interface
5.	Should support REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG API for application integration
6.	Support for SNMP v1, v2c, v3, NTP, Syslog UDP/TCP and integration with SIEM solution for logging, analysis & monitoring purpose
7.	Integration with Local User , AD, LDAPS, certificate authentication for clients
8.	Dual hot swappable power supplies
9.	1 Million encryption key management capability
10.	Should maintain Audit trail of User, Time, Date, Use etc.
11.	Should support Hypervisors like VMWare ESXi, KVM, Microsoft Hyper-V etc
12.	Should support Cloud Platforms like vSphere
13.	Shall be provided in High Availability (HA) with Active-Active cluster
14.	Supply should include FIPS 140-2 Level3 certified embedded or network attached HSM with multi-factor authentication support

5. PIM-PAM01

Sr.No.	Features & Specifications
1.	Proposed solution must be an Appliance & should provide self-managed vault & not rely on external RDBMS for any data storage.
2.	The Appliance shall support concurrent user sessions of 200 users. The Appliance shall have 50TB of Hard disk space after configuring the RAID 6 or better protection. Appliance shall have min. Four ports of 10G SFP+ SR and

Sr.No.	Features & Specifications
	4 Ports of 1G Copper ethernet to connect to the switches. One Mgmt. port is also required. Supply shall include both 4 no. CAT 6 Ethernet patch cables of 3 mts. length and 4 nos. of FC LC to LC OM3 MM patch cables of 3 mts. length.
3.	Proposed solution must support browser-based RDP & SSH without additional server resource requirement. Capability must be supported in multi-site architecture.
4.	Proposed solution must support integration with LDAP and AD seamlessly without requirement of additional S/W and H/W.
5.	Proposed solution must allow restrictive, controlled & secure sharing & collaboration of privileged session among support teams working across multiple locations without requiring agents
6.	Proposed solution must support connections from endpoints, HTML5 browser and Microsoft Remote Desktop Service Terminal Server technology. Solution must not rely on OS dependent SSH Tunnelling and third party terminal services technology.
7.	Proposed solution must provide break glass functionality to retrieve password securely from an encrypted satellite vault. This vault must use same encryption as used in the PAM vault.
8.	Proposed solution must support provisioning, de-provisioning & operations of privileged accounts from PAM interface
9.	The solution supports discovery of Servers, Workstations, Desktops & Laptops.
10.	The solutions allows discovery of privileged accounts in Windows Server, Desktops, Laptops including Services accounts, IIS Pools, scheduled tasks and enforce password policy.
11.	Solution allows provisioning of local privileged accounts for platforms including Windows, Unix, SQL & PostgreSQL Database and Microsoft Active Directory
12.	Solution supports cross-platform access (using any OS or browser) for operating system, databases, hypervisors, web applications, management consoles and network devices
13.	Solution should not rely on Active-X/Java components or third party licensed components for accessing target devices
14.	Solution support wide variety protocols and clients for initiating privileged sessions including Unix, Linux, Windows RDP, web based applications, network device, databases, hypervisors and virtualization management utilities.
15.	Solution must support inbuilt proxy for supporting secure session management across distributed environments.
16.	Solution should support session isolation between potential malicious desktops and target server via hardened jump server

Sr.No.	Features & Specifications
17.	Solution must allow to access target system using SSH Keys without revealing private key.
18.	Solution supports video like playback in a web browser with ability to search based on metadata
19.	Session recordings must be tamper proof and encrypted
20.	Solution support web based interface for transferring files using ftp/sftp from user machine to target server and server to server
21.	Solution provides deep & granular visibility into privileged account activities with logging & video playback capabilities of privileged account activities
22.	Solution provides session logs with correlated meta data that are linked to commands and textual information for easy reviewing
23.	Solution allows real-time viewing of privileged sessions from centralized web console
24.	Solution should track abnormal and suspicious user activity and provide notifications like long session duration, outside work hour access etc.
25.	Solution should support behavior based detection of anomalous privileged activities
26.	Solution support password changes for variety of platforms including Operating System (Windows & Unix), Databases, Routers, Switches, Firewalls, Storage Devices, Cloud Portals & Hypervisors)
27.	Solution should support storage and management of SSH Keys
28.	Solution can reset or change passwords of individual accounts on-demand or based on automated schedule and criteria.
29.	Solution can reconcile password status periodically based on a schedule and provide list of out-of-sync passwords
30.	Solution should allow to set randomized password based on multiple option including dictionary characters, length, complexity
31.	Solution should allow password checkout for a specified period of time
32.	Solution should control multiple people checking out same password in same duration
33.	Solution enable administrators to login with normal accounts to PAM Console and perform a transparent login with privileged accounts & control administrator triggered application execution by enforcing simple application control policies applied from a user context
34.	Solution allows enforcement of least privilege policies by controlling commands execution profiles by users on Unix based machines
35.	Solution allows enforcement of least privilege policies by controlling application execution profiles based on user logon on windows based machines
36.	Solution allows users to logon to Windows Server with normal accounts and elevate privileges based on pre-approved policies
37.	Solution allows implementation of additional security control for re-authorization of administrators to highly critical application usage

Sr.No.	Features & Specifications
38.	Solution should control & manage 'Su' commands based on user policies & Manage SUDO with ease and full proof audit capabilities
39.	Solution restrict Commands based on a user profile and capture complete video and command logs for review and audit purposes
40.	Solution allows provisioning of Linux local users accounts without manual intervention
41.	Solution must provide automatic execution and management of privileged tasks with pre-packaged commands for easy automation of routine backup jobs, routine file movement activities, service execution based on application job schedules, data gathering from multiple systems, configuration checks & configuration change based on SSH, telnet and PowerShell interfaces.
42.	Solution must allow users to publish pre-packaged tasks and also delegate to other team members without any session login
43.	Solution must capture complete log of execution activities for later review
44.	Proposed solution must govern privileged entitlements, access to privileged access platform, account inventory for improved compliance
45.	Access: Solution supports solution administration from any HTML5 compliant browser without installing any utilities or agents.
46.	Administration: Solution supports defining flexible attribute based rules for configuring user & account groups
47.	Encryption: The solution should provide include AES encryption, a FIPS 140-2 software encryption module, support for Hardware Security Modules (HSMs)
48.	Multifactor Authentication (MFA): Solution supports integrated Multifactor including soft token via SMS, Email, time tokens via mobile application or mobile push authentication
49.	Workflow: Solution supports approval workflow with complete audit capabilities & notification support via email supporting multiple levels and multiple approvers at each level.
50.	Solution provides out of the box reports and customized reports for Account Inventory, User Inventory, Asset Inventory, System Performance, Password Activity etc.
51.	Solution provides mechanism for distribution of reports by email
52.	Solution should provide actionable dashboard for solution administrations
53.	Vault must be secured and hardened without allowing DBA or PAM administrators to tamper system or password data
54.	All subscriptions , software updates , Firmware updates and Hardware Appliance shall cover 3 yrs. warranty.
55.	All licenses shall be perpetual.

6. SHREDDER01

Sr. No.	Features & Specifications
1.	Should support Cross Cut and Microcut
2.	Should have provision for cutting of Papers, CDs and Access cards
3.	Should support seperate feed for Paper, CD & Access cards
4.	Should support Automatic paper feed for paper size of A4
5.	Should comply to Security Levels as per DIN66399
6.	Should support shredding of min. 10 nos. of A4 sheets of 70GSM at a single instance.
7.	Noise Level at one meter distance at the time of shredding shall be less than 70dB
8.	Shall support Single Phase Power Supply
9.	Shall have Automatic stacking and Feed Facility
10.	Shall cover 3 yrs. onsite warranty
11.	Capacity of Waste Bin shall be >= 11 litres
12.	Material of Cutting Blade shall be made of Steel Alloy
13.	Shall have LED Indication (Power, standby and Processing)
14.	Shall have overheat and overload protection
15.	Supply shall include 3 mts. power cable.

7. SAFE01

Sr. No.	Parameters	Specifications
1.	Fire-resistant safe	up-to 1000c outer and maintaining 52c inside
2.	dust resistant	yes
3.	pilferage	yes
4.	humidity	yes
5.	magnetic field	yes
6.	customize	adjustable shelves, lockers, drawers and pull-out trays
7.	accidental damage	yes
8.	electrostatic	resistance to electrical interference

Sr. No.	Parameters	Specifications
9.	security	2 – high precision 10 -lever cylinder
10.	locking options	combination lock, biometric lock ,electronic lock
11.	emergency evacuation	Snap-shut mechanism to quickly lock cabinet in crisis
12.	Dimension	Height =1875 cm width=850 cm depth=800 cm Weight=856 kg volume=372 litres
13.	Capacity	DLT/LTD tapes =672 Data Cartridge=432 ALT data Cartridge=1696 CD/DVD(r,rw)&RAM =1344 Zip disk=1812
14.	Testing	ERTL and CBRI = endurance upto 60 min
15.	Warranty	3 years of comprehensive warranty

8. SAFE02

Sr. No.	Parameters	Specifications
1.	Dimension in cms	Height =42 width=35 depth=35
2.	Weight	16 kgs
3.	Capacity	40 L
4.	Lock Type	Biometric and Electronic
5.	Intelligence	Basic
6.	Strength	10X(pro)
7.	Fire Resistance	Yes
8.	Double wall	Yes
9.	Internal Shelves	Yes
10.	Internal Lighting	Yes
11.	Low Battery Indicator	Yes
12.	Non Volatile Memory	Yes
13.	Master Password	No

Sr. No.	Parameters	Specifications
14.	Motorised Shooting Bolts	Yes
15.	Mechanical Override Key	Yes
16.	Automatic Freeze	Yes
17.	Warranty	3 years comprehensive warranty
18.	Fingerprint Storage Capacity	30 fingerprints

9. SERVER02

Sr. No	Parameter	Specifications
1.	**Server Height**	1. 2U rack mounted with sliding rails
2.	**Processors**	1. Two Intel® Xeon® Scalable or AMD 2nd Gen processors, configured 2. 24 cores/processor @ 2.1 GHz base freq. or better. 3. Processor launch date should not be earlier than 2021).
3.	**Memory**	1. 512 GB ECC RAM expandable to 1TB, @ 2933 MT/s, should have min. 12 DIMM slots 2. Memory should be supplied in balanced configuration.
4.	**Hard Drives**	1. 2 x 900GB SSDs in RAID1 2. 8 x 10TB SSDs in RAID 6.
5.	**GPUs**	1. Should be installed with 2 nos. of NVIDIA H100 80GB GPUs 2. System should be NVIDIA certified for aforementioned GPUs
6.	**RAID Controller**	1. 12Gbps PCIe 4.0 with RAID 1, 5, 6 2. 2GB or higher Cache Memory.
7.	**1G Networking features**	1. 2 nos. of 1 Gbps Copper Ethernet with Additional Dedicated management ethernet interface port. 2. 3 mts. length factory crimped copper ethernet patch cords for each port including 1 management port.
8.	**10G Networking features**	1. 4 x 10G Fibre Ethernet ports along with transceivers SFP+ SR 2. 5 mts. length 10G factory crimped LC to LC OM3 fibre

Sr. No	Parameter	Specifications
		Ethernet patch cords, for each port
9.	Redundant Power Supply	1. Hot-plug, Redundant Power Supply 2. Power supplies should be Gold or Platinum certified.
10.	Embedded Remote Management	1. 1 Gbps dedicated management ethernet interface 2. Capabilities should include KVM over IP, power on, off & reset, virtual media with appropriate perpetual licenses. 3. Support for serial over IP. Support for SNMPv2 or higher gets and alerts. 4. System remote management should support browser based graphical remote console along with Virtual Power button, remote media management using USB/CD/DVD Drive. 5. It should be capable of upgrade of software and patches from a remote client using Media/image/folder 6. ILO/ILOM/IDRAC/IPMI/RSA or equivalent with support for virtual media management, Remote KVM. 7. License for perpetual use for all supported features 8. Server should support power on password and Bios Password.
11.	OS Support and Certification	1. Windows Server 2016 or latest, Ubuntu, Red Hat Enterprise Linux, Red Hat
12.	Warranty	1. 03 Years onsite comprehensive with NBD warranty
13.	Security & Encryption	1. System should Support Secure Firmware Updates, Support of Trusted Platform Module enabled within the BIOS for secure cryptographic key generation, secure storage of keys
14.	OS License	1. Supply shall include latest release of RHEL Operating System with support for mentioned no. of sockets and cores. 2. The subscription / Licenses shall be valid for 03 Years with support for Un-Limited Virtual hosts with-in the physical server.
15.	Virtualization Support	1. VMWare VCentre, Citrix XenServer, Hyper V
16.	Power cables & Rack mounting kits	1. Required power cables and rack mounting kit should be provided.

Sr. No	Parameter	Specifications
17.	Location of Network ports	1. All network ports should be at the back-side of the server
18.	PCIe	1. All slots should be PCIe Gen 4 2. PCIe – 2 nos. of PCIe Gen4 x8 and 1 nos. of PCIe Gen4 x16 should be made available for use by C-DAC after meeting technical requirements stipulated 3. Risers to be provided if required

10. SERVER03

Sr. No	Parameter	Specifications
1.	Server Height	1. 2U rack mounted with sliding rails
2.	Processors	1. One Intel® Xeon® Scalable or AMD 2nd Gen processors, configured 2. 24 cores/processor @ 2.1 GHz base freq. or better. 3. Processor launch date should not be earlier than 2021).
3.	Memory	1. 192 GB ECC RAM expandable to 512GB, @ 2933 MT/s, should have min. 12 DIMM slots 2. Memory should be supplied in balanced configuration.
4.	Hard Drives	3. 2 x 900GB SSDs in RAID1 4. 8 x 12 TB NL-SAS in RAID 6.
5.	RAID Controller	1. 12Gbps PCIe 4.0 with RAID 1, 5, 6 2. 2GB or higher Cache Memory.
6.	1G Networking features	1. 2 nos. of 1 Gbps Copper Ethernet with Additional Dedicated management ethernet interface port. 2. 3 mts. length factory crimped copper ethernet patch cords for each port including 1 management port.
7.	10G Networking features	1. 4 x 10G Fibre Ethernet ports along with transceivers SFP+ SR 2. 5 mts. length 10G factory crimped LC to LC OM3 fibre Ethernet patch cords, for each port
8.	Redundant Power Supply	1. Hot-plug, Redundant Power Supply 2. Power supplies should be Gold or Platinum certified.

Sr. No	Parameter	Specifications
9.	**Embedded Remote Management**	1. 1 Gbps dedicated management ethernet interface 2. Capabilities should include KVM over IP, power on, off & reset, virtual media with appropriate perpetual licenses. 3. Support for serial over IP. Support for SNMPv2 or higher gets and alerts. 4. System remote management should support browser based graphical remote console along with Virtual Power button, remote media management using USB/CD/DVD Drive. 5. It should be capable of upgrade of software and patches from a remote client using Media/image/folder 6. ILO/ILOM/IDRAC/IPMI/RSA or equivalent with support for virtual media management, Remote KVM. 7. License for perpetual use for all supported features 8. Server should support power-on password and Bios Password.
10.	**OS Support and Certification**	1. Windows Server 2016 or latest, Ubuntu, Red Hat Enterprise Linux, Red Hat
11.	**Warranty**	1. 03 Years onsite comprehensive with NBD warranty
12.	**Security & Encryption**	1. System should Support Secure Firmware Updates, Support of Trusted Platform Module enabled within the BIOS for secure cryptographic key generation, secure storage of keys
13.	**OS License**	1. Supply shall include latest release of RHEL Operating System with support for mentioned no. of sockets and cores. 2. The subscription / Licenses shall be valid for 03 Years with support for Un-Limited Virtual hosts with-in the physical server.
14.	**Virtualization Support**	1. VMWare VCentre, Citrix XenServer, Hyper V
15.	**Power cables & Rack mounting kits**	1. Required power cables and rack mounting kit should be provided.

Sr. No	Parameter	Specifications
16.	Location of Network ports	2. All network ports should be at the back-side of the server
17.	PCIe	1. All slots should be PCIe Gen 4 2. PCIe – 2 nos. of PCIe Gen4 x8 and 1 nos. of PCIe Gen4 x16 should be made available for use by C-DAC after meeting technical requirements stipulated 3. Risers to be provided if required

11. SERVER04

Sr. No	Parameter	Specifications
1.	Server Height	2. 2U rack mounted with sliding rails
2.	Processors	4. Two Intel® Xeon® Scalable or AMD 2nd Gen processors, configured 5. 24 cores/processor @ 2.1 GHz base freq. or better. 6. Processor launch date should not be earlier than 2021).
3.	Memory	3. 576 GB ECC RAM expandable to 1TB, @ 2933 MT/s, should have min. 12 DIMM slots 4. Memory should be supplied in balanced configuration.
4.	Hard Drives	5. 2 x 900GB SSDs in RAID1 6. 8 x 10TB SSDs in RAID 6.
5.	RAID Controller	3. 12Gbps PCIe 4.0 with RAID 1, 5, 6 4. 2GB or higher Cache Memory.
6.	1G Networking features	3. 2 nos. of 1 Gbps Copper Ethernet with Additional Dedicated management ethernet interface port. 4. 3 mts. length factory crimped copper ethernet patch cords for each port including 1 management port.
7.	10G Networking features	3. 4 x 10G Fibre Ethernet ports along with transceivers SFP+ SR 4. 5 mts. length 10G factory crimped LC to LC OM3 fibre Ethernet patch cords, for each port
8.	Redundant Power Supply	3. Hot-plug, Redundant Power Supply 4. Power supplies should be Gold or Platinum certified.

Sr. No	Parameter	Specifications
9.	**Embedded Remote Management**	9. 1 Gbps dedicated management ethernet interface 10. Capabilities should include KVM over IP, power on, off & reset, virtual media with appropriate perpetual licenses. 11. Support for serial over IP. Support for SNMPv2 or higher gets and alerts. 12. System remote management should support browser based graphical remote console along with Virtual Power button, remote media management using USB/CD/DVD Drive. 13. It should be capable of upgrade of software and patches from a remote client using Media/image/folder 14. ILO/ILOM/IDRAC/IPMI/RSA or equivalent with support for virtual media management, Remote KVM. 15. License for perpetual use for all supported features 16. Server should support power on password and Bios Password.
10.	**OS Support and Certification**	2. Windows Server 2016 or latest, Ubuntu, Red Hat Enterprise Linux, Red Hat
11.	**Warranty**	2. 03 Years onsite comprehensive with NBD warranty
12.	**Security & Encryption**	2. System should Support Secure Firmware Updates, Support of Trusted Platform Module enabled within the BIOS for secure cryptographic key generation, secure storage of keys
13.	**OS License**	3. Supply shall include latest release of RHEL Operating System with support for mentioned no. of sockets and cores. 4. The subscription / Licenses shall be valid for 03 Years with support for Un-Limited Virtual hosts with-in the physical server.
14.	**Virtualization Support**	2. VMWare VCentre, Citrix XenServer, Hyper V
15.	**Power cables & Rack mounting kits**	2. Required power cables and rack mounting kit should be provided.

Sr. No	Parameter	Specifications
16.	Location of Network ports	3. All network ports should be at the back-side of the server
17.	PCIe	1. All slots should be PCIe Gen 4 2. PCIe – 2 nos. of PCIe Gen4 x8 and 1 nos. of PCIe Gen4 x16 should be made available for use by C-DAC after meeting technical requirements stipulated 3. Risers to be provided if required

12. SERVER06

Sr. No	Parameter	Specifications
1.	Server Height	1. 2U rack mounted with sliding rails
2.	Processors	1. Two Intel® Xeon® Scalable or AMD 2nd Gen processors, configured 2. 24 cores/processor @ 2.1 GHz base freq. or better. 3. Processor launch date should not be earlier than 2021).
3.	Memory	1. 768 GB ECC RAM expandable to 2TB, @ 2933 MT/s, should have min. 12 DIMM slots 2. Memory should be supplied in balanced configuration.
4.	Hard Drives	1. 2 x 900GB SSDs in RAID1 2. 8 x 10TB SSDs in RAID 6.
5.	RAID Controller	1. 12Gbps PCIe 4.0 with RAID 1, 5, 6 2. 2GB or higher Cache Memory.
6.	1G Networking features	1. 2 nos. of 1 Gbps Copper Ethernet with Additional Dedicated management ethernet interface port. 2. 3 mts. length factory crimped copper ethernet patch cords for each port including 1 management port.
7.	10G Networking features	1. 4 x 10G Fibre Ethernet ports along with transceivers SFP+ SR 2. 5 mts. length 10G factory crimped LC to LC OM3 fibre Ethernet patch cords, for each port
8.	Redundant Power Supply	1. Hot-plug, Redundant Power Supply 2. Power supplies should be Gold or Platinum

Sr. No	Parameter	Specifications
		certified.
9.	**Embedded Remote Management**	1. 1 Gbps dedicated management ethernet interface 2. Capabilities should include KVM over IP, power on, off & reset, virtual media with appropriate perpetual licenses. 3. Support for serial over IP. Support for SNMPv2 or higher gets and alerts. 4. System remote management should support browser based graphical remote console along with Virtual Power button, remote media management using USB/CD/DVD Drive. 5. It should be capable of upgrade of software and patches from a remote client using Media/image/folder 6. ILO/ILOM/IDRAC/IPMI/RSA or equivalent with support for virtual media management, Remote KVM. 7. License for perpetual use for all supported features 8. Server should support power on password and Bios Password.
10.	**OS Support and Certification**	1. Windows Server 2016 or latest, Ubuntu, Red Hat Enterprise Linux, Red Hat
11.	**Warranty**	1. 03 Years onsite comprehensive with NBD warranty
12.	**Security & Encryption**	1. System should Support Secure Firmware Updates, Support of Trusted Platform Module enabled within the BIOS for secure cryptographic key generation, secure storage of keys
13.	**OS License**	1. Supply shall include latest release of RHEL Operating System with support for mentioned no. of sockets and cores. 2. The subscription / Licenses shall be valid for 03 Years with support for Un-Limited Virtual hosts with-in the physical server.
14.	**Virtualization Support**	1. VMWare VCentre, Citrix XenServer, Hyper V
15.	**Power cables & Rack mounting kits**	1. Required power cables and rack mounting kit should be provided.

Sr. No	Parameter	Specifications
16.	Location of Network ports	1. All network ports should be at the back-side of the server
17.	PCIe	1. All slots should be PCIe Gen 4 2. PCIe – 2 nos. of PCIe Gen4 x8 and 1 nos. of PCIe Gen4 x16 should be made available for use by C-DAC after meeting technical requirements stipulated 3. Risers to be provided if required

13. STGSANNAS01 (Unified Storage with NAS & SAN delivery methods)

Sr. No	Parameters	Specifications
1.	Storage Type	1. Unified storage appliance must be quoted with support for SAN (FC and iSCSI) and NAS (NFSv3, v4 and v4.1, pNFS, CIFS, SMB 2, 3,3.02 and 3.1.1; FTP and SFTP). 2. Access with hybrid capability to operate with NVMe Solid State Drives (NVMe SSDs) and Hard Disks Drives (HDDs) with auto-tiering between all of them
2.	Storage Architecture	1. Offered storage must have minimum dual active-active controllers for NVMe & NL-SAS tiers with: a. Minimum 256GB DRAM cache on each controller. b. The cache should be Globally coherent. Data should be protected against loss or unavailability in case of failure of 1 controller outage, for NVMe c. Battery/capacitor backup for cache. Data in cache should be protected, in the event of a power failure, via battery backup for more than 72 hours, or written to NVMe/NL-SAS disks d. NVMe and NL-SAS/SATA disk pools should use separate controllers to ensure different failure domains 2. Ability to support up to 100 HDDs/SSDs in same system by adding disk enclosures and scalability to 2PB in the same solution 3. No single point of failure 4. Non-disruptive firmware upgrade Entire storage solution must be from a single OEM with dedicated firmware/OS optimized for data processing.

Sr. No	Parameters	Specifications
		5. The architecture should support high read and write performance by aggressively prefetching 6. It should support ability to sustain minimum 2 controller and 4 drive failures without loss of data and impact on performance
3.	**Storage Capacity**	1. Storage solution should be offered with total **500TB** usable capacity with 1DWPD on dual port NVMe SSDs. 2. Additional 10% usable space (or equivalent number of drives) should be offered as hot spare, for NVMe
4.	**SSDs and HDDs**	1. Unified storage must be supplied with self-encrypting dual-ported 1DWPD NVMe SSDs 2. Storage should support both in-line and post process data reduction via compression/deduplication 3. NVMe SSDs must be configured in RAID6 dual parity protection with one hot spare per pool.
5.	**Data Integrity**	1. The Storage System should support detecting and correcting data integrity issues due to any bit rot or phantom writes, misdirected reads/writes operations.
6.	**GUI Based management**	1. Storage must have a single web GUI based administration interface for configuration, storage management and performance analysis. 2. The proposed storage should provide proactive monitoring of the health of the system and proactive support when any hardware failure occurs. The provision to provide (health / stats) reports 3. System Management software should have capability to monitor performance for IOPS, throughput, latency and should be able to monitor controllers, disk pools, NFS shares, drives.
7.	**Network Interface**	1. Offered storage should have minimum **4x 100Gbps** QSFP28 ethernet ports with required optical modules for connectivity to client. 2. Additionally, storage should have 2x 1Gbps ethernet ports for management. 3. Each storage controller should have at least 2 x 100 GbE ports.
8.	**Protocol Support**	1. Should support iSCSI, SMB2 and SMB3,NFSv2,NFSv3,NFSv4 and NFSV4.1,SNMP,SMT.

Sr. No	Parameters	Specifications
		2. Authentication integration should support Windows Domain, LDAP, Local password file. It should be possible to join the storage to multiple AD domains, LDAP realms. 3. Should support Multi-protocol for simultaneous file & folder access to all files/folders in the entire system via ANY of the protocols supported
9.	**Rack Space**	1. Offered solution must fit in standard 42U 19" RACK 2. Storage solution should fit in max 10U 3. Max. rated power for the storage solution should not be more than 5KW
10.	**Virtualization Support**	1. Should be able to manage storage through Vcenter Datastore 2. Should able to support balance number of controllers with Datastore 3. Should have plugin to manage storage array from vCenter and should allow to create Datastore within vCenter 4. Should be able to monitor VMs storage through vCentre 5. Support offload cloning to the storage array instead of consuming host resources 6. The storage array should support industry-leading hypervisors like VMware ESXi, Microsoft Hyper-V, Red Hat KVM/ Virtualization, Oracle VM, XenServer 7. The proposed storage shall support CSI (Container Storage interface) driver (minimum version 1.0) to provision persistent (block) storage for database workloads running as containers 8. It should have capability to create a snapshot of the provisioned volumes. 9. Support for VMware vSphere and Hyper-V 10. Should support VMWare VAAI and VASA 11. VMware certified storage

Sr. No	Parameters	Specifications
11.	**Mandatory Software Features (must include all licenses in perpetual mode)**	1. Point in time snapshot and clones 2. Thin Provisioning 3. Inline Deduplication, Inline Compression 4. Remote replication, Synchronous and Asynchronous (File and Block) for disaster recovery functions 5. Web based GUI or CLI based Management 6. Alerts (SMTP email, SNMP) and syslog for logging 7. Quota based storage allocation for users, groups and directory/project
12.	**Security Certifications**	1. FIPS140-2 certification
13.	**Performance**	1. The storage solution must support 1000,000 100% random read IOPS with 8KB block size and with DIRECTIO (to bypass client cache) on iSCSI interface with less than 3ms latency. 2. Additionally, storage solution must support 5GB/s sequential read performance from single NFS share with 32KB blocksize. 3. A benchmarking report on storage OEM letterhead signed by authorized signatory must be submitted along with tender response showing required performance numbers.
14.	**OS Support**	1. The storage shall support connectivity to multiple host operating systems such as Windows, Unix, Enterprise Linux, Solaris etc.
15.	**Support and Maintenance**	1. 3 Years of standard NBD support. 2. All the support details including escalation matrix, e-mail ids and contact numbers have to be provided on OEM letterhead.
16.	**Data Replication**	1. Storage should support at least 3-way replication over WAN across three sites with sync and async mode of operation. 2. Should support both block and file-based replication 3. All licenses for for replication support should be quoted for entire capacity and 3 nos. of destination. 4. Replication should support comprehensive file and directory selection criteria for replication. Selection criteria shall include: filename, include/exclude directories, file size, file creation, access and modified times.
17.	**Installation**	1. The installation, configuration and integration with VMWare setup has to be done by OEM engineer

Sr. No	Parameters	Specifications
18.	Training	1. Installation and configuration training to be provided by OEM to at least 5 participants 2. On-premise Operations and Management training has to be provided to at least 20 participants
19.	Configuration Scalability/ Upgrades	1. Storage cluster configuration should be independent of hardware configuration to support upgrade the storage cluster non-disruptively 2. Shares & exports should not be impacted when hardware is added or removed 3. It should be possible to add new generation controller/node of the quoted OEM to the existing storage cluster without an impact on allocated volumes/LUNs/file-shares parent and the clients accessing them

14. STGBKPTP01

Sr. No	Parameter	Specifications
1.	Tape library functionality	1. Offered Tape drive should be native FC LTO-9 drives of minimum 4 nos. 2. Offered drive should have native speed of minimum 400MB/sec and a compressed speed of 1000 MB/sec. 3. Tape Library should be supplied with eight no. of FC based I/O interfaces (two for each drive). 4. Quoted Tape library, Tape drives should support WORM functionality and WORM tapes 5. The Tape Library should support barcode reading. 6. The Tape Library should have support for partitioning of tape library (at least 4). The necessary software and associated perpetual licenses must be supplied with library. 7. Tape Library should have GUI panel. 8. The Tape Library should be capable of auto cleaning of drives.
2.	Storage capacity of Tape library	1. Enterprise Class Tape library of minimum 8 PB native storage capacity.

Sr. No	Parameter	Specifications
3.	**Management**	1. Tape Library should provide remote monitoring capability (Ethernet based management port). 2. The Tape Library should be SMI-S/ (SNMP& SMTP) complaint. 3. Tape Library should have a mechanism to hold Persistent history and analysis of events and logs for easy troubleshooting.
4.	**Cables**	1. Supply should include 8 no. of FC (multimode) patch cables compatible with the quoted Tape drives and SAN switch. 2. Bidder should supply all the required cables required for installation, configuration and integration of tape library with backup server. 3. All power cables should be of IEC male type for rack side connectivity
5.	**Backup Software**	1. Supply should include Backup software which will support the quoted library. 2. Backup Software should work with Linux as a backup server and support various clients installed under various operating systems. 3. Backup software should support backup clients (mix and match of Windows, Linux and Database clients).
6.	**Backup / Client Agents**	1. Capacity based Licenses which shall include unlimited Client Licenses for Windows OS, Linux* OS and Databases
7.	**Rack compatibility**	1. Should be compatible with 19 inch standard rack and supply should include rack mounting kit.
8.	**Encryption**	1. Tape Library should support encryption so as to write the media in an encrypted format and to restrict the access of the Tape media from other Tape library. 2. Supply should include required Software, Hardware and associated licenses to provide the encryption and decryption of the data.
9.	**LTO Tape cartridge**	1. Supply should include fully populated LTO-9 WORM tape media along with Barcode labels. 2. Additional barcode labels of 2 sets (total 200 labels) are to be supplied.

Sr. No	Parameter	Specifications
		3. The Tape Library should be quoted with 4 no of LTO-9 cleaning cartridges.
10	**Power supply**	1. Should support hot swappable power supplies. 2. Supply should include redundant hot swappable Power supplies.
11	**License and support**	1. Supply should include perpetual licenses for the Tape library, logical partitioning, monitoring, backup software etc.
12	**Cables**	Supply should include: 1. IEC type power cables for the quoted power supplies 2. 1 no. of factory crimped (moulded) ethernet cable of length 5 mts. for mgmt. 3. 8 nos. of FC cables for redundant connectivity of SAN switches and Tape Drives.
13	**SAN Switches**	1. Supply shall include 2 nos. of 16 Port 32Gbps FC switch with interfaces fully populated with transceivers
14	**Warranty**	1. Tape Library and both the SAN Switches should have 3 yrs. NBD warranty along with upgrades for Firmware and upgrades of backup Software which shall include both minor and major releases without any additional cost.

15. STGBKPTP02

Sr No.	Parameter	Specifications
1	**Auto Tape Library**	Tape Library of min. 400TB Native capacity expandable to 1 PB and Backup Software - Qty-01. Max. 4U size
2	**Functionality**	Offered Tape drive should be native FC LTO-9 drive, minimum 2 nos., with 8Gbps FC interface
		Offered drive should have native speed of minimum 300MB/sec
		Tape Library should be supplied with two no. of FC based I/O interfaces (one for each drive)

Sr No.	Parameter	Specifications
		Quoted Tape library, Tape drives should support WORM functionality and WORM tapes
		The Tape Library should support barcode reading
		The Tape Library should have support for partitioning of tape library (at least 2)
		The necessary software and associated perpetual licenses must be supplied with library
		Tape Library should have GUI panel
		The Tape Library should be capable of auto cleaning of drives. The Tape Library should be supplied with 2 nos. of Cleaning Cartridges
3	Capacity	All power cables should be of IEC male type for rack side connectivity
		Management: Tape Library should provide remote monitoring capability (Ethernet based management port)
		The Tape Library should be SMI-S/ (SNMP& SMTP) complaint.
		Refer cables under point no. 9
		Bidder should supply all the required cables required for installation, configuration and integration of tape library with backup server
		Backup Software Supply should include Backup software which will support the quoted library
		Backup Software should work with Linux as a backup server and support various clients installed under various operating systems
4	Backup / Client Agents	10 no. of Linux agents / client
		2 no. of Windows agents / clients
		2 no. of Database clients (Shall support MySQL / PostGreSQL
5	Encryption	Tape Library should support encryption so as to write the media in an encrypted format and to restrict the access of the Tape media from other Tape library
		Supply should include required Software, Hardware and associated licenses to provide the encryption and decryption of the data
6	Rack compatibility	Should be compatible with 19 inch standard rack and supply should include rack mounting kit
7	Power Supply	Power supply Should support hot swap power supplies, Supply should include redundant hot swappable Power supplies and cooling fans

Sr No.	Parameter	Specifications
8	Additional Requirements	LTO Tape cartridge Supply should include fully populated LTO-9 WORM tape media along with Barcode labels to meet 400TB Native storage
		Additional barcode labels of 4 sets (total 400 labels) are to be supplied
		The Tape Library should be quoted with 2 no of LTO-9 cleaning cartridges
		License and support, supply should include perpetual licenses for the Tape library, minimum 2nos logical partitioning, monitoring, backup server and client software etc
9	Cables	Supply should include IEC type power cables for the quoted power supplies and 1 no. of factory crimped (moulded) ethernet cable of length 5 mts.
		Cables: Supply should include 4 no. of FC (multimode) patch cables compatible with the quoted Tape drives
10	Warranty	3 years NBD warranty and with upgrades for Firmware, Backup Software, Client-Agent/Backup-Client

16. TERMINAL01

Sr. No	Parameter	Specifications
1.	CPU	10th Generation Intel® Core™ i7-10700 (8-Core, 2.9GHz to 4.8GHz, 65W) or equivalent AMD ryzen or higher processor
2.	BIOS	OEM BIOS
3.	Graphics	Integrated Graphics
4.	Memory	16GB DDR4 non ECC memory
5.	Hard Drive	256GB SSD Hard Disk Drive
6.	Ethernet	Integrated 10/100/1000 Mbps Ethernet controller
7.	I/O ports	6 USB Port combination of: 3.0 and 2.0; 1 RJ-45; 1 HDMI Port; 1Line-out (front);
8.	Monitor	Minimum 21.5-inch FHD (1920 x 1080 @ 60 Hz) 16:9 Aspect Ratio Tilt and Height-adjustable stand, pivot (rotation) Display port/HDMI TCO Certified 250 cd/m² Brightness, Windows Hello compatible Webcam or Built in camera.
9.	Keyboard	104Keys USB Keyboard (same OEM)
10.	Mouse	2 Button USB Optical Mouse (same OEM) with Scroll wheel
11.	Operating System	Microsoft Windows 11 (or higher) Professional 64 Bit version pre-loaded
12.	Security	Antivirus, DLP.

Sr. No	Parameter	Specifications
13.	**Authentication**	Supply shall include Biometric Finger print reader along with drivers compatible to the quoted windows Version.
14.	**Warranty**	03 years onsite comprehensive with NBD warranty for all hardware & software

17. SIEM01

Sr. No.	Parameters	Specifications
1.	**Performance and Architecture**	1. SIEM solution must be an on premise scalable dedicated appliance / purpose built OEM Solution. It should be a physically segregated three tier architecture and support both agent-based and agent-less for information collection. 2. It should have minimum 50K sustained and peak events per second (EPS) across all tier (Collection, Correlation and Management). Collectors should be able to buffer events and should be able to deploy multiple collectors for scalability. 3. Solution should integrate with all IP devices. Should have no limitation on number of devices. Should support all standard log formats (like Syslog, JSON, Windows events, W3C, ELF, and NCSA etc.), SNMP, JDBC, ODBC, CDR/CMR, WMI, JMX and flows (like sFlow, NetFlow, IPFIX etc.). 4. Solution should have User Entity Behavior Analytics (UEBA) to detect advanced attacks, support API like REST and SOAP for integration. Support remediation trigger when a specified incident occurs. 5. Should have minimum built-in storage (with RAID 5 or better) of retaining minimum 180 days of data (Raw and Normalized Logs in regards to the asked EPS requirement). 6. Should maintain Raw and Normalized logs for 1 year through (built-in / SAN / NAS) storage. Both raw logs and normalized logs should be made available. Real-time logs should be available for non-repudiation and

Sr. No.	Parameters	Specifications
		integrity verification and log archiving based of rules/policies. 7. SIEM solution should maintain minimum 180 days of logs (both Raw and normalized) in an uncompressed format to allow for fast searching, threat hunting and investigation. 8. SIEM solution must have components like Collectors, Log management, Correlation engine, Threat intelligence feeds (like Malicious – domains, IPs, URLs, hashes, software, Tor nodes etc.), Log forensics and Analysis, IT compliance and Reporting. 9. Should support forensic analysis in case on any incident, dynamically link incidents to hosts / IP and users. Detect unauthorized devices, applications, changes with respect to configuration, software, registry, files and folder all in real time. 10. Option to deploy in HA mode. 11. The proposed appliance / Hardware must have at least 2x10GE (SFP+, 10GBase-SR) / 2x25G (SFP28, 25GBase-SR) and 2x1GE (1000Base-F, 1000 Base–SX) / Copper fully populated from day one. Supply must include required Transceivers.
2.	**Integration**	1. Solution should integrate with SOAR and must have flexibility to deploy / enable (SOAR) as and when desired with no additional licenses cost (for hardware, software, feature/function). SIEM alerts should be able to be ingested into SOAR and SOAR enrich intelligence from SIEM as when required to take remediation action. It should utilize an alarm received as an event to trigger IR playbooks that initiate enforcement actions on target enforcement network and security systems such as firewalls, and network fabric / SDN controllers, Workload protection, End point security etc. 2. SIEM solution must support information in the context of network and security devices(like Switches, Routers, Firewall, WAF, DDoS, Server and Network Load balancer,

Sr. No.	Parameters	Specifications
		Anti-APT), SDN controllers, Virtualization and Container environments (VMWare, VMWare NSX, Hyper-V, Redhat, Docker etc.) custom applications, end point security (EDR / XDR) and their centralized controller, DLP software, Incident and ticketing Management tool, Syslog, ELK Stack, Physical security devices (biometric readers, smart card etc.), Storage (EMC, NetApp, Isilon, Nutanix etc.), Databases, VOIP, AAA & NAC, 3. Should integrate with threat detection tools like Network Traffic Analyzer / NBAD (Network behavior anomaly detection) and Vulnerability Application and Penetration Testing (VAPT) tools, Kafka, Tableau, and Hadoop, Jira, Centralized Management Database(CMDB), ITSM tools, IP address lookup, Workflow automation platforms, Cloud infrastructure (like Openstack). 4. SIEM solution should integrate the logs collected from 18 Branch offices of NIA. Logs will be collected over MPLS network. 5. Threat Intelligence feeds (MISP, MITRE, SANS, ThreatConnect, CyberARK, etc.) with support of STIX/TAXII/Open API.
3.	**Management**	1. The solution should provide reports for IT Compliances like PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, and SANS critical security controls. 2. Secure Web-based / GUI, secure inter module communication. 3. The solution should have the ability to export and import reports and rules. Also, solution should be able to create custom reports and dashboard with role-based access control. 4. Correlation in real time, historical correlation and correlation based on rule, risk, location and vulnerability.

Sr. No.	Parameters	Specifications
		5. Support advanced syslog parser, User context in real-time with audit trails of IP addresses, user identity changes, physical and geo-mapped location and security event collections. 6. SIEM solution should support Local, SAML 2.0, OpenLDAP, and Microsoft Active Directory for enterprise authentication. 7. Solution should have single pane of glass window to detect, prevent, respond, view reports, alarms & alerts, Incident Analysis (entire security incident lifecycle) with security orchestration capabilities in real-time. 8. Pre-defined and Analyst-centric dashboards. Service portal should be intelligent, which automates ticketing management system and other process. Service desk should integrate SIEM and SOAR, where alerts from SIEM ingested into SOAR can auto trigger new service incident. And the service incident status updates from SIEM and SOAR should be in sync with service desk. 9. The solution provided must have access to at least 6 analyst / administrator concurrent session 24x7 with no limitation on user creation.
4.	**SOAR Features**	1. SOAR solution should integrate with SIEM solution as mentioned in above section and all the IP devices. It should detect, prevent and respond with security orchestration capabilities natively available with solution. 2. The solution must provide at least 20 out of the box playbooks & out of the box content to create playbooks which can be customized as well as used from day 1 to reduce day to day operational tasks. 3. SOAR solution should collect real time global threat Intel data, de-dupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner. 4. Proposed Solution must allow to add IOC sources in platform such as TOR Project official exit nodes, Ransomware Tracker, Cyber Crime tracker etc. based on IP Address, URLs, Domain, Files hashes (MD5) etc.

Sr. No.	Parameters	Specifications
		5. Proposed SOAR technology should have Threat Intel platform inbuilt with OEM threat Intel feeds and support for both commercial and open source threat Intel feeds. 6. SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources. 7. Proposed solution should support searching of Data/artifacts associated with historical incidents. 8. Proposed solution should support assigning of incident to a user or a group. 9. The solution should provide option to manually invoke selected playbook based on any selected or set of selected events. 10. Proposed solution should have playbooks and workflow for automation and orchestration. 11. Proposed solution must provide ability to run playbooks on-demand through REST API calls. 12. Proposed solution should have out of the box built in playbooks visible in the GUI. 13. Proposed solution should allow creating new playbooks in a visual workflow manner. 14. Proposed solution should allow creation of Manual Tasks and Automated Tasks in Playbooks. 15. Proposed solution should support standard languages such as python, JavaScript etc. for extending playbooks and integrations. Should support Open APIs. 16. Proposed solution should have integration with Forensic tools, Communication tools, SIEM tools, Endpoint Security solution EDR / XDR etc.), Network Security solution, Web Proxy, Threat Intelligence, Dynamic malware analysis, SDN Controller, Wi-Fi Controller etc.

Sr. No.	Parameters	Specifications
		17. Proposed solution should support adding of new product integrations from GUI without any interaction with command line. 18. Proposed solution must provide MITRE ATT&CK mapping out of the box. The threat Intel must map with MITRE TTP's to create a prioritized threat detection dashboard. 19. Leveraging on threat intelligence analysis and learning solution must provide capabilities to develop case studies for use internal incident response training exercises, input to red teaming, threat hunting and other relevant activities Provide security-related input into architecture and technology solution changes etc. 20. Proposed solution should support SSO, AD, LDAP etc. for managing authentication centrally in an enterprise environment. 21. Proposed solution should support user's definition and user role management. 22. Proposed solution should support at least six analysts/administrators.
5.	**License, Support and Warranty**	1. 24X7 support with 4 hrs response time. For Hardware replacement (RMA) / Resolution time must be within 48 hrs. 2. Telephonic, e-mail/chat support with call logging (single point of Contact) mechanism must be provided on 24x7x365 basis by OEM. Also must provide escalation matrix. 3. The bidder must provide 3 yrs comprehensive warranty with the following: a. Subscription of all software, Firmware and associated Licenses (of all features) and effective from day one. b. Warranty for all the supplied Hardware and software. c. Bidder must ensure that all features of the proposed solution is functional without requirement of any additional procurements of Hardware, Software, Subscriptions and Licenses from day one. d. All hardware, software replacements and delivery must be taken care by the bidder with no financial implications to NIA.

Sr. No.	Parameters	Specifications
		e. Online upgradation of firmware/software/patches as and when required.

18. SMARTRACK

Sr. No	Parameter	Specifications
1.	Cabinet Size	(HxWxD) 2000 x 600 x 1200 (mm)
2.	Usable U space	29 U
3.	Air Flow Management Panel	5U x 3, 2U x 3, 1U x 2
4.	Vertical Cable Management Panel	2
5.	Area (incl. service space)	1.5 m2
6.	Color	RAL7021 Black
7.	IP Marking	IP5X
8.	Display panel	9" Touch Panel LCD
9.	Display Languages	English
10.	LED Lighting	2, Front & Rear
11.	System Luminance	88lux/1M
12.	UPS Capacity	5 kVA / 5 kW
13.	UPS Backup time	10 minutes @ 3 kW
14.	System Capacity	3 kW
15.	System Input Requirement	50A, Single Phase 220/230/240
16.	Outdoor Unit for Air conditioner	Yes (Split)
17.	System Frequency	50Hz or 60Hz
18.	Power Distribution Units (PDU)	16A input , 12 x C13 + 4 x C19, 2 pcs/ 32A input , 18 x C13 + 6 x C19, 2 pcs
19.	Lightning Protection Device	Level 3, 20KA
20.	UPS Maintenance Bypass	Included
21.	Cooling Capacity	1,800W ~ 3,500W, variable speed
22.	Refrigerant	R410A
23.	Emergency fan	Two, one at front bottom and one at rear top
24.	System Management (UPS/Cooling/PDU)	Yes
25.	Temperature Sensor	2
26.	Water Leak Detection	1 piece, 5 meters long
27.	Door Access Sensor	2
28.	Safety Standards	EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
29.	EMC Standards	EMC Standards EN 55022:2010 EN 61000-3-11:2000 EN 55024:2010 EN 61000-3-12:2011
30.	Noise Level	< 58 dB[1]

19. STGBKP01

S.No	Enterprise Backup Appliance Solution – 1PB (2 Qty DC & DR) with Backup Software
1	Proposed solution should be compatible to various OS platforms and should be capable of supporting backup/ restores from various OS platforms including Windows and Linux. Both Backup Management Server, Media Server and Client software should be capable of running on all these platforms.
2	The supply shall include Media Server, VTL Appliance, Backup Software and associated Licenses. Media Server shall have at least 4 nos. of 10G and two nos. of 100G ethernet FC (LC-LC) interfaces, 1 mgmt. interface per controller.
3	The licenses shall be based on capacity basis (min. 300TB) and shall support unlimited clients for Windows, Linux, Databases etc.
4	Backup Solution should support various level of backups including full, incremental, synthetic, optimized synthetic and user driven backup along with various retention period.
5	The solution shall include Backup Software, Backup Clients, Media Server and associated Licenses.
6	The solution shall support Data deduplication, Data encryption at Rest and Data Encryption in transit.
7	The proposed backup solution must include Agent/Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, MySQL, No-SQL, Exchange, distributed databases, filesystems, NFS, Hypervisors, Bigdata and Hadoop.
8	Proposed solution must provide Bare Metal Recovery, deduplication, encryption, database online backup, deduplication, backup data replication etc. with installation of single agent on clients. Multiple Agents/Binaries should not be installed on the production Servers to achieve all above features.
9	Backup Solutions should have capabilities to tape/disk-out backup catalogue and deduplication catalogue separately. Also should be able to replicate all catalogue information along with replication of backup images to DR site.
10	Backup Solution must be proposed along with integrated Disk-Based Purpose Build Backup Appliance (PBBA) each with minimum 300TB usable capacity and scalable to more than 1PB usable.
11	Proposed Backup solution should be integrated purpose build backup appliance (PBBA) with dedicated hardware, network, OS, security and storage. Solution should be plug & play and should be capable to scale out.
12	Proposed Backup solution must provide a “turnkey” fully integrated backup solution (Backup Appliance and Backup Software) from a single OEM for better supportability, performance and to avoid multi-vendor ownership which results in to daily challenges in later stage.

S.No	Enterprise Backup Appliance Solution - 1PB (2 Qty DC & DR) with Backup Software
13	The proposed disk appliance should be offered with dual controller and each controller shall support minimum 4 x 10Gbps Ethernet and 2x100G Fibre Channel.
14	The proposed device shall support intelligence to understand Source based and target based (at client application level, backup server level and media server level) de-duplication so that only unique – non duplicated data is copied to the proposed device.
15	The proposed Backup Appliance should have integration with Physical Tape devices and offer mechanism for taking the backup on a physical tape library from the appliance seamlessly.
16	The proposed disk based backup appliance shall have flexibility to enable or disable the de-duplication feature for a given disk pool in Appliance for Faster Backup and Restoration.
17	The proposed device shall support rated write performance of minimum 12 TB per hour and when enabled with source level de-duplication, shall have rated performance of at least 40 TB/hr.
18	The Proposed Backup solution must provide Management of the backup software and backup disk dedupe appliance from the same console for better manageability.
19	The proposed Purpose Build Backup Disk Appliance must be capable to act as a Backup Controller/Backup Server and Data Mover/Media Server simultaneously.
20	Proposed Backup Appliance solution must be able to perform agentless backup RHEV and VMWare environment without the need of any additional proxy host.
21	Proposed Backup appliance solution should support database incremental backup and should support instant recovery for database.
22	Proposed Solution Should include Single patch upgrade for backup software, backup appliance, file system and security updates.
23	Proposed backup appliance solution should support agentless data movement in parallel stream to optimized data movement for big data workloads.
24	The Proposed backup software license should not be tied to the storage device. This means if another Backup Appliance is installed at the DR site, then the appliance will not need separate dedupe license or any other backup software license.
25	The proposed device should have inbuilt WAN optimization capabilities and also be tolerant to complete or intermittent network failures or TCP packet drops.
26	The proposed Backup Appliance have built-in data security component against malicious threats and attacks.
27	Solution should be proposed along with OEM professional services for one-time installation direct by OEM Vendor.

S.No	Enterprise Backup Appliance Solution - 1PB (2 Qty DC & DR) with Backup Software
28	Proposed solution shall have separate dedicated drives for Operating System of Appliance and shall not participate in data backup. It should have Operating System disk in mirroring and data disk on Raid 6 with Hot spare.
29	Proposed appliance must have expandable option by adding head & disk unit to 500 TB usable space without the need of any Deduplication license if front end data size is not changed. Additional disk space will be utilized for multiple copy with long retention.
30	License with respect to no. of hosts and replication licenses should be provisioned from DC to DR and vice versa.
31	Backup Software shall be compatible to take backups on to D2D as VTL, backup on to ISCSI targets (Ref. Backup Software and Tape Library)
32	Backup Software shall be compatible to take backups on to D2D as VTL, backup on to ISCSI targets
33	The solution provider should provide detail plan for action and should supply, install all required hardware and software
34	The solution provider should provide support details and escalation matrix along with the OEM authorization certificate for supply and support the solution.
35	Comprehensive Warranty for 3 years
36	Installation and configuration, OnSite Support for Maintenance and Management for 3 years

Category-II

1. Network switch specifications

All the network switches (Types) should be from the same OEM and compatible with the Fabric Manager.

a. SWITCH Type-06

Sr. No	Parameter	Specifications
1.	**Performance and Architecture**	1. Device should have modular hardware architecture to support 100G and 400G line cards. Should be capable to support scale of a minimum of 72 nos. of 100G QSFP28 ports and 16 nos. of 400G OSFP/QSFP-DD ports. 48 nos. of QSFP28 ports all populated with 100G single mode Duplex fiber LC connector transceiver and 10 nos of 400G OSFP/QSFP-DD ports all populated with single mode transceiver from day-1. 2. Device should support wire rate L2 and L3 forwarding. 3. Device should be based on industry standard virtual output queue based architecture to avoid head-of-line blocking issues. 4. Device should support custom profiling/carving of TCAM hardware resource to support varying use cases. 5. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 6. Support open standard based protocol VXLAN + EVPN to build Leaf-spine fabric. 7. The Leaf-spine fabric should support distributed gateway based architecture with support for symmetric integrated routing and bridging. 8. Device should have deep packet buffers of 8GB or more to handle congestion scenarios arising out of TCP incast and varying in-out link speed. 9. Device should be able to support up to 200K MAC address. 10. Device should support 4K VLANs, 9200 bytes Jumbo frame. 11. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. 12. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. 13. Device should support minimum 128-way ECMP.

Sr. No	Parameter	Specifications
		14. Device should be able to support 256K IPv4 routes. 15. Device should support ISIS (IPv4 & IPv6), OSPF (IPv4 & IPv6), BGP, BGP monitoring protocol. 16. Device should support graceful restart for ISIS, OSPF and BGP. 17. Device should support policy based routing (IPv4 & v6), VRRP (IPv4 & v6) and multi-hop BFD. 18. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP. 19. Device should support VPC/MLAG for active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 20. Device should support symmetric Integrated Routed & Bridging (for both Type-2 and Type-5) and distributed anycast gateway functionality in VXLAN+EVPN fabric. 21. Support VRF. 22. Device should support routed-multicast/OISM with EVPN for multicast support in VXLAN overlay. 23. Device should support Role based access control, AAA with TACACS+ and RADIUS. 24. Device should support ACL with Layer-2, L3 and L4 parameters. 25. Device should have support 20K or more ingress/egress hardware ACL entries. 26. Device should support control plane policing to safeguard system from DOS attacks. 27. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 28. Device should support priority queuing. 29. Device should support PFC/DCBX. 30. Device should have virtual output queuing based architecture, such that every input port will have a virtual output queue for every output port on the switch. 31. Should advance automation with support for onboard python and bash, API. 32. Should support custom application installation with RPM install and docker containers. 33. Device should support streaming telemetry that is not dependent on SNMP, for example device should be able to

Sr. No	Parameter	Specifications
		stream CPU process information, LLDP information and much more. 34. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 35. Device should support onboard tcpdump/wireshark for troubleshooting purpose and should support mirroring to L3 destination using GRE encapsulation. 36. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 37. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. Device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with time-series database view, traffic flow analytics, PSIRT/Bug visibility, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, change management, notification through email & msg, 3rd party integration. 2. Minimum one Out-Of-Band Management port 1x 1G RJ45. 3. **Refer Annexure – II for Management features**
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 OR equivalent, IEC or equivalent. 5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status

b. SWITCH Type-09 (Management Core)

Sr. No	Parameter	Specifications
1.	**Performance and Architecture**	1. Device should be capable to support scale of a minimum of 72 nos 10G native SFP+ ports. Populated with 26x10G SFP+ multimode LC transceiver from Day-1. 2. Device should have minimum 06 x 100G QSFP ports populated with 100G SM LC transceiver from Day-1. 3. Device should support wire rate L2 and L3 forwarding. 4. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 5. Device should be able to support up to 128K MAC address. 6. Device should support 4K VLANs, 9200 bytes Jumbo frame. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. Device should support minimum 128-way ECMP. 10. Device should be able to support 256K IPv4 routes. 11. Device should support ISIS(IPv4 & IPv6), OSPF(IPv4 & IPv6), BGP, BGP monitoring protocol. 12. Device should support graceful restart for ISIS, OSPF and BGP. 13. Device should support policy based routing(IPv4 & v6), VRRP (IPv4 & v6) and multi-hop BFD. 14. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP. 15. Device should support VPC/MLAG for active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 16. Device should support symmetric Integrated Routed & Bridging(for both Type-2 and Type- and distributed anycast gateway functionality in VXLAN+EVPN fabric. 17. Support VRF. 18. Device should support Role based access control, AAA with TACACS+ and RADIUS.

Sr. No	Parameter	Specifications
		19. Device should support ACL with Layer-2, L3 and L4 parameters. 20. Device should support control plane policing to safeguard system from DOS attacks. 21. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 22. Device should support priority queuing. 23. Device should support PFC/DCBX. 24. Should support advance automation with support for onboard python, bash and API. Should support custom application installation with RPM install and docker containers. 26. Device should support streaming telemetry that is not dependent on SNMP, for example device should be able to stream CPU process information, LLDP information and much more. 27. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 28. Device should support onboard tcpdump/wireshark for troubleshooting purpose. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 30. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with time-series database view, traffic flow analytics, PSIRT/Bug visibility, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change management, notification through email & msg, 3rd party integration. 2. Minimum one Out-Of-Band Management port 1x 1G RJ45.

Sr. No	Parameter	Specifications
		3. **Refer Annexure – II for Management features.**
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent. 5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status

c. SWITCH Type-03 (Compute LEAF)

Sr. No	Parameter	Specifications
1.	**Performance and Architecture**	1. 24 nos. of 10G SFP+ ports all populated with multimode LC transceiver, 6 nos. of 40/100G QSFP28 ports populated with 100G single mode (duplex fiber LC connector) transceiver from day-1 2. Device should support wire rate L2 and L3 forwarding (for asked port configuration). 3. Device should be based on industry standard virtual output queue based architecture to avoid head-of-line blocking issues. 4. Device should support custom profiling/carving of TCAM hardware resource to support varying use cases. 5. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 6. Device should have deep packet buffers of 2GB or more to handle congestion scenarios arising out of TCP incast and varying in-out link speed. 7. Device should be able to support up to 128K MAC address. 8. Device should support 4K VLANs, 9200 bytes Jumbo frame.

Sr. No	Parameter	Specifications
		9. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. 10. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. 11. Device should support minimum 128-way ECMP. 12. Device should be able to support 256K IPv4 LPM routes. 13. Device should support ISIS (IPv4 & IPv6), OSPF (IPv4 & IPv6), BGP, BGP monitoring protocol. 14. Device should support graceful restart for ISIS, OSPF and BGP. 15. Device should support policy based routing (IPv4 & v6), VRRP (IPv4 & v6) and multi-hop BFD. 16. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP. 17. Device should support VPC/MLAG for active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 18. Device should support symmetric Integrated Routed & Bridging (for both Type-2 and Type-5) and distributed anycast gateway functionality in VXLAN+EVPN fabric. 19. Support VRF. 20. Device should support routed-multicast/OISM with EVPN for multicast support in VXLAN overlay. 21. Device should support Role based access control, AAA with TACACS+ and RADIUS. 22. Device should support ACL with Layer-2, L3 and L4 parameters. 23. Device should have support 12K or more ingress/egress hardware ACL entries. 24. Device should support control plane policing to safeguard system from DOS attacks. 25. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 26. Device should support priority queuing. 27. Device should support PFC/ECN/DCBX. 28. Device should have virtual output queuing based architecture, such that every input port will have a virtual output queue for every output port on the switch.

Sr. No	Parameter	Specifications
		29. Should advance automation with support for onboard python and bash, API. 30. Should support custom application installation with RPM install and docker containers. 31. Device should support streaming telemetry that is not dependent on SNMP, for example device should be able to stream CPU process information, LLDP information and much more. 32. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 33. Device should support onboard tcpdump/wireshark for troubleshooting purpose and should support mirroring to L3 destination using GRE encapsulation. 34. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 35. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. Device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with time-series database view, traffic flow analytics, PSIRT/Bug visibility, Zero touch provisioning, resource utilization monitoring, Change Management, event notification, auto topology view, notification through email & msg, 3rd party integration. 2. Minimum one Out-Of–Band Management port 1x 1G RJ45. 3. **Refer Annexure – II for Management features.**
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent.

Sr. No	Parameter	Specifications
		5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status

d. SWITCH Type-05 (L3 Perimeter)

Sr. No	Parameter	Specifications
1.	**Performance and Architecture**	1. 48 nos. of 1/10G ports and 6 nos. of 40/100G QSFP28 ports, provided with 8x 1G-T, 8x 1G-SX, 16x 10G-SR, 4x 10G-LR, 2x 40G-SR4, 2x 40G-LR4 (all LC connector), 2x100G Single mode (duplex fiber LC connector)transceiver from day-1. 2. Device should support wire rate L2 and L3 forwarding. 3. Device should be based on industry standard virtual output queue based architecture to avoid head-of-line blocking issues. 4. Device should support custom profiling/carving of TCAM hardware resource to support varying use cases. 5. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 6. Support open standard based protocol VXLAN + EVPN to build Leaf-spine fabric. 7. The Leaf-spine fabric should support distributed gateway based architecture with support for symmetric integrated routing and bridging. 8. Device should have deep packet buffers of 4GB or more to handle congestion scenarios arising out of TCP incast and varying in-out link speed. 9. Device should be able to support up to 200K MAC address. 10. Device should support 4K VLANs, 9200 bytes Jumbo frame. 11. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. 12. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. 13. Device should support minimum 128-way ECMP. 14. Device should be able to support 256K IPv4 routes.

Sr. No	Parameter	Specifications
		15. Device should support ISIS (IPv4 & IPv6), OSPF (IPv4 & IPv6), BGP, BGP monitoring protocol. 16. Device should support graceful restart for ISIS, OSPF and BGP. 17. Device should support policy based routing (IPv4 & v6), VRRP (IPv4 & v6) and multi-hop BFD. 18. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP. 19. Device should support VPC/MLAG for active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 20. Device should support symmetric Integrated Routed & Bridging (for both Type-2 and Type-5) and distributed anycast gateway functionality in VXLAN+EVPN fabric. 21. Support VRF. 22. Device should support routed-multicast/OISM with EVPN for multicast support in VXLAN overlay. 23. Device should support Role based access control, AAA with TACACS+ and RADIUS. 24. Device should support ACL with Layer-2, L3 and L4 parameters. 25. Device should have support 20K or more ingress/egress hardware ACL entries. 26. Device should support control plane policing to safeguard system from DOS attacks. 27. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 28. Device should support priority queuing. 29. Device should support PFC/DCBX. 30. Device should have virtual output queuing based architecture, such that every input port will have a virtual output queue for every output port on the switch. 31. Should advance automation with support for onboard python and bash, API. 32. Should support custom application installation with RPM install and docker containers. 33. Device should support streaming telemetry that is not dependent on SNMP, for example device should be able

Sr. No	Parameter	Specifications
		to stream CPU process information, LLDP information and much more. 34. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 35. Device should support onboard tcpdump/wireshark for troubleshooting purpose and should support mirroring to L3 destination using GRE encapsulation. 36. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 37. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. Device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with time-series database view, traffic flow analytics, flow path identification, PSIRT/Bug visibility, Zero touch provisioning, resource utilization monitoring, Change Management, event notification, auto topology view, notification through email & msg, 3rd party integration. 2. Minimum one Out-Of-Band Management port 1x 1G RJ45. 3. **Refer Annexure – II for Management features.**
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent. 5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status

e. SWITCH Type-01 (Management TOR)

Sr. No	Parameter	Specifications
1.	**Performance and Architecture**	1. Device should support minimum 48x 1G RJ45 ports. 2. Device should have minimum 4 x 10G SFP+ ports populated with multimode transceiver LC from day-1. 3. Device should support wire rate L2 and L3 forwarding. 4. Device should support custom profiling of TCAM hardware resource to support varying use cases. 5. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 6. Device should be able to support up to 64K MAC address. 7. Device should support 4K VLANs, 9200 bytes Jumbo frame. 8. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. 9. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. 10. Device should support minimum 32-way ECMP. 11. Device should be able to support 128K IPv4 LPM routes. 12. Device should support ISIS(IPv4 & IPv6), OSPF(IPv4 & IPv6), BGP, BGP monitoring Protocol. 13. Device should support graceful restart for ISIS, OSPF and BGP. 14. Device should support policy based routing(IPv4 & v6), VRRP (IPv4 & v6) and multi-hop BFD. 15. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP. 16. Device should support VPC/MLAG for active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 17. Device should support symmetric Integrated Routed & Bridging(for both Type-2 and Type-5) and distributed anycast gateway functionality in VXLAN+EVPN fabric. 18. Support VRF. 19. Device should support routed-multicast/OISM with EVPN for multicast support in VXLAN overlay. 20. Device should support Role based access control, AAA with TACACS+ and RADIUS. 21. Device should support ACL with Layer-2, L3 and L4 parameters.

Sr. No	Parameter	Specifications
		22. Device should support control plane policing to safeguard system from DOS attacks. 23. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 24. Device should support priority queuing. 25. Device should support PFC/DCBX. 26. Should support advance automation with support for onboard python and bash, API. 27. Should support custom application installation with RPM install and docker containers 28. Device should support streaming telemetry that is not dependent on SNMP, for example device should be able to stream CPU process information, LLDP information and much more. 29. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 30. Device should support onboard tcpdump/wireshark for troubleshooting purpose and should support mirroring to L3 destination using GRE encapsulation. 31. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 32. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with time-series database view, traffic flow analytics, PSIRT/Bug visibility, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change management, notification through email & msg, 3rd party integration. 2. Minimum one Out-Of–Band Management port 1x 1G RJ45. 3. **Refer Annexure – II for Management features.**

Sr. No	Parameter	Specifications
3.	General	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent. 5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status.

f. SWITCH Type-04 (Management POE)

Sr. No	Parameter	Specifications
1.	Performance and Architecture	1. Device should support minimum 48x 1G RJ45 POE+ ports. 2. Device should have minimum 4 x 10G SFP+ ports populated with multimode LC transceivers from day-1. 3. Device should support wire rate L2 and L3 forwarding. 4. Device should support redundant hot-swappable fans and redundant hot-swappable power supplies. 5. Device should be able to support up to 32K MAC address. 6. Device should support 4K VLANs, 9200 bytes Jumbo frame. 7. Device should support MST, per-vlan RSTP, BPDU Guard, Loop Guard. 8. Device should support LLDP and LACP to bundle links and detect mis-cabling issues. 9. Device should be able to support 64K IPv4 LPM routes. 10. Device should support routing protocols ISIS, OSPF (IPv4 and v6), BGP. 11. Device should support graceful restart for, OSPF, BGP. 12. Device should support policy based routing, VRRP. 13. Device should support Multicast with PIM-SM, PIM-SSM, MSDP and anycast-RP.

Sr. No	Parameter	Specifications
		14. Device should support active-active layer-2 and layer-3 forwarding while running in VXLAN+EVPN based fabric. 15. Device should support symmetric Integrated Routed & Bridging(for both Type-2 and Type-5) and distributed anycast gateway functionality in VXLAN+EVPN fabric. 16. Device should support routed-multicast/OISM with EVPN for multicast support in VXLAN overlay. 17. Device should support Role based access control, AAA with TACACS+ and RADIUS. 18. Device should support ACL with Layer-2, L3 and L4 parameters. 19. Device should support control plane policing to safeguard system from DOS attacks. 20. Device should support policing, shaping, Marking, DHCP/COS classification and ACL based classification. 21. Device should support priority queuing. 22. Should support advance automation with support for onboard python and bash, API. 23. Should support custom application installation docker containers. 24. Device Should support streaming/model-driven telemetry. 25. Device should support IEEE 1588 PTP boundary clock, SNMP v3, IPFIX/Netflow/SFlow and logging. 26. Device should support onboard tcpdump/wireshark for troubleshooting purpose and should support mirroring to L3 destination using GRE encapsulation. 27. Should support measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using IP SLA or Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357. 28. All proposed switches in the network should be able to run on same OS image and managed from single dashboard for simplified operations with minimal security exposure.
2.	**Management**	1. The device should be provided with monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with timeline view,

Sr. No	Parameter	Specifications
		traffic flow analytics, Zero touch deployment, topology view, Workflow management, 3rd party integration. Dedicated management solution should be provided with the device. 2. Minimum one Out-Of-Band Management port 1x 1G RJ45.
3.	General	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Device hardware, software should be from the same OEM. 3. Should operate at AC ~50Hz, 220-240V. 4. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC CFR 47 Part 15 OR equivalent, IEC or equivalent. 5. 0°C to 40°C operating temperature and 10% to 90% relative humidity. 6. Should have LED indicator for per port status.

Annexure-II Fabric Management Capabilities for Switches

Sr. No	Parameter	Specifications
1.	Features	1. The Fabric Management capabilities are to be provided as a unified cluster covering all the networking devices in scope. Based on availability of APIs and associated interfaces of other security and virtualization components, integration and interaction with Overlay traffic and fabric components has to be provided. The Bidder should specify the native and third party integration capabilities of the solution. 2. Management and monitoring of all the proposed hardware switches deployed across sites (DC, BCP and DR) (except POE Switches) must be provided through single pane of glass. 3. Should provide zero touch provisioning natively for quick deployment and provisioning of network devices minimising human effort and errors. 4. Should support automated workflow based deployment and provisioning of leaf-spine fabric from a single dashboard for all sites.

Sr. No	Parameter	Specifications
		5. Should provide real-time monitoring and historical time-series database view of various parameters of the network devices using streaming telemetry that is not dependent on SNMP. Should be capable of collecting traffic flow data (netflow/ sflow) for detailed traffic insight. 6. Should be able to show network wide devices resources utilization and their historical trends. Detect components exceeding capacity thresholds ahead of time. 7. Should be able to automatically discover and show fabric topology for Underlay and Overlay visualization. 8. The Overlay network is to be designed for a multi-tenancy Applications suite running with a set of Common Platform Services and deployed over a unified virtualised compute and storage platform. The Fabric Manager, with its API integrations with third parties should be capable to integrate with private cloud enterprise solutions. 9. Should support change management to carry out multiple network-wide changes in one go. Should support network wide rollback for device configuration and device image to a previous state. Should support workflow based change management for all devices under management. 10. All the proposed hardware switches should be able to run on OEM standard OS and it should be possible to centrally apply upgrades and patches while the fabric remain in service, minimising down time of the entire solution. 11. Should have capability to provide instant visibility into any applicable bugs and PSIRTs that can impact the proposed devices helping in regular network audits and compliances. 12. In terms of the stipulations given at Paragraph 1f of Section IV, the Bidders should necessarily articulate the need and impact of adding additional hardware and software components to the BoM and BoQ specified in the RFP. As an indicative guideline, the following should be considered for provisioning of the Fabric Management capability: a. The Fabric Manager must be physical appliance based. Fabric management infrastructure should be provisioned in HA mode at each of the sites and should

Sr. No	Parameter	Specifications
		cover all fabrics; the necessary software licenses should be bundled with the appliances. b. The management solution for Internet and MPLS facing fabric should be isolated. c. Fabric Manager appliances should be quoted with direct OEM TAC support. d. Should be able to support a minimum of 350 Switches from day-1. e. Should support alert notification via email. f. The Fabric Manager and the Switches should be of the same OEM.

2. Firewall specifications

Firewall Type having SANDBOX, Log Analyzer & the Firewall Manager solution must be from the same OEM

a. Firewall Type-FW01 (EAST-WEST Firewall in HA Pair)

Sr. No	Parameter	Specifications
1.	**Features**	1. Certified FIPS 140-2, EAL 4+ / Common Criteria. 2. Should be Next-Generation Firewall (NGFW) with separate Data and control/Management plane. 3. Must have 6x 100GE/40GE QSFP28 (single mode LC), 16x 10 GE SFP+ multimode LC, 2x RJ45 Management ports from Day1. All required transceivers should be populated from day one and compatible with the quoted switches. 4. The solution should have sufficient Physical RAM and CPU to cater the requested performance throughput. 5. Threat prevention throughput of 50 Gbps(per unit of HA) in real world/production/enterprise mix environment with all the security engines like IPS, Application control, web filtering, anti-malware etc, enabled. 6. SSL VPN throughput of at least 10 Gbps. Should support client based VPN and at least 3000 concurrent SSL VPN users.

Sr. No	Parameter	Specifications
		7. Concurrent sessions of 2 million or above and new sessions / Sec of 1 Million or above. 8. The proposed solution should support HA in Active/Active and Active/Passive mode. The Firewall in HA should support stateful clustering across sites. HA should be supported on both IPV4 and IPV6. Feature like IPS, Anti malware, Web filtering, DDOS prevention and Traffic Shaping should be available in Active-Active. 9. Should be a hardware appliance based. Firewall. IPSEC and SSL VPN, Anti-Malware, IPS, Web and Application control, DDOS prevention, Traffic-Shaping/Bandwidth Management and Routing functionalities must be integrated in a single appliance. 10. Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6) , DNS64 & DHCPv6 functionality. 11. Support unlimited IP/User Devices. 12. Firewall appliance must have at least 20 virtual firewall domains/instants (active from day-1) scalable to 25(with additional license) with each firewall domains/instances having a separate administrative control OR equivalent, Security zones and VLAN. 13. The following features must be available in each virtual firewall domain/instant context environment: Firewall, IPSEC and SSL VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy based routing, DDOS, User and Group management, Logging and Reporting. 14. Solution must inherit all the standard RFC's with respect to the firewall functionalities. 15. Must support REST API. 16. Firewall must have a hardened OEM operating system. 17. The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection. 18. Should support bi-directional integration with Anti-APT/SANDBOX for sharing threat intelligence and automated mitigation of zero day attacks.

Sr. No	Parameter	Specifications
		19. Automatic failover (condition based on ICMP, TCP or UDP protocol) as well as load sharing for outbound traffic. 20. Must support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation up to layer 7 traffic (including application type and SSL/TLS). 21. Firewall policy must facilitate IP, Network, Port, Protocol, User, Application and Zone. And must facilitate to apply features like IPS, Web & application Content filtering, Anti-Malware, IPS, DDOS prevention, Traffic Shaping (define - guaranteed, burstable/maximum bandwidth, set different level of priority) on any firewall policy for a specific time/Date/Period. Firewall policy must also have an option of configuring exceptions to any specific features. 22. The proposed system shall be able to operate on either Transparent (bridge) mode or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. 23. Must support DNS client and NTP client. 24. Must support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability. Also, must support Ethernet bonding functionality for full mesh deployment architecture. 25. Support all SNMP versions support v3. 26. Must support various form of user Authentication methods simultaneously, like: Local Database, LDAP server, RADIUS server, TACACS+ server and PKI methods (PKI authentication with PCKS#7, PCKS # 10 standards). 27. Two-factor authentication without any external Hardware. 28. Windows Active Directory single sign-on by means of agent/clientless/Captive portal which broker between users when they log on to the AD domain and the end-device.

Sr. No	Parameter	Specifications
		29. Second factor authentication through email, Certificate, SMS, RSA token for remote users. 30. The proposed firewall shall be able to create custom application signatures and profile. 31. The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application based on the content. 32. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections. 33. Should support TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection etc.) 34. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network. 35. The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc. 36. The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports. 37. Should be able to perform Anti-malware scans for HTTP, SMTP, IMAP, POP3, and FTP traffic. 38. Should detect and prevent malicious DNS request from inside hosts to outside bad domains, sinkhole the DNS request and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs.

Sr. No	Parameter	Specifications
		39. Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data. 40. All the proposed threat functions like IPS, Anti-Malware, web and application control etc. should work in isolated air gapped environments without any need to connect with the Internet. 41. The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time). 42. Dedicated on premise anti-APT/sandbox solution in HA to be provided. The SANDBOX should be able to support the following- i) dynamic threat analysis on such as EXEs, DLLs, ZIP /RAR/7ZIP/TNEF files, PDF documents, Office Documents, Java, Android APKs/JAR, Adobe Flash applets, JPEG/GIF/BMP/WMF, on APT & SSL based APT attacks. ii) detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database iii) Analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications. iv) pre-populated Licensed copies of Operating systems (like Windows 7, Windows 8.1, Windows 10, Linux and Android etc.) and applications/softwares (like Microsoft Office). v) file sizes up to 100 MB or more vi) ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack. vii) capture and store packet captures of traffic relevant to the analysis of detected threats.

Sr. No	Parameter	Specifications
		viii) to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST). ix) deployment in out-of-band mode (also SPAN/TAP) & inline mode and block malicious traffic. x) SMB / CIFS / NFS protocol for sharing and transferring files xi) visibility into scan histories of each file scanned that are aborted, completed, or in progress xii) provide reports in (but not limited to) PDF/CSV formats xiii) anti-evasion capabilities to prevent malwares detection of being run/executed in the virtualized environment. xiv) to analyze email attachments and malicious links for static and dynamic analysis xv) SIEM log integration. xvi) to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc. xvii) number of Interfaces - 4x GE RJ45 ports, 2x 10 GE SFP+ slots xviii) VM's of at least 50 xix) process minimum of 5000 files/day xx) The solution should have redundant AC power supply fully populated (within box) from day one. xxi) 2 TB in RAID 1 from day one 43. Should protect against phishing and JavaScript 44. The proposed solution should support the ability to create QoS policy on a per rule basis- by source address, by destination address, by application (such as Skype, Bittorrent, YouTube, azureus, webex), by static or dynamic application groups (such as Instant Messaging or P2P groups), by port and services. 45. Should support the following authentication protocols: LDAP, Radius (vendor specific attributes), and Token-based solutions.

Sr. No	Parameter	Specifications
		46. Firewall appliance must have at least 2TB local hard-disk in order to keep log/statistics information.
2.	**Management**	1. Hardware appliance based centralized complete management (of all proposed NGFW appliances) solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access. 2. Provide separate appliance / VM / Software for collection and Analysis of firewall Logs and reporting. If VM / Software based then, the OEM/MSI should provide the necessary hardware(rack mountable system with required resources CPU, RAM, Storage, Network Interfaces to connect to the switching fabric as mentioned in the RFP) and licensed software(hypervisor, Operating System and any supporting software) along with OEM support for the mentioned warranty period in the RFP. 3. The provided log reporting and analysis appliance (Hardware / VM / Software) must have storage capacity of at least 32TB. 4. Real time logging based on all Traffic and correlated log view based on other logging activities. 5. Management access control using Profile/Role based for granular control. Local access to appliance/s modules must support role based access. 6. Support configurable option for E-mail or SMS alerts (Via SMS gateway) in case of any event trigger. Provision to send mail or SNMP traps to EMS in response to system failures or threshold violations of the Health attributes. 7. Firewall configuration changes / commands issued must be logged. Also provision for exporting. 8. Must provide the real time health status of NGFW on dashboard for CPU memory utilization, state table, total No. of concurrent connections and the connections/second counter, real time data transfer/bandwidth utilization of individual IP/Application/protocol/port/Interface/Zone.

Sr. No	Parameter	Specifications
		9. Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc. 10. Support standard report templates an dashboards with option to schedule reports. 11. Support reports to be send by email at scheduled intervals. Must support logs to be forwarded to a syslog server (Multiple for redundancy) in open standard log format. 12. Must support for SIEM log integration. The solution must be capable of sending logs to a SIEM system via syslog. 13. Must support future expansion. Same centralized management must support if number of appliances are increased. 14. Configuration backup and restore on to/from a remote system via GUI/CLI over HTTPS/SSH or equivalent secure mechanism. 15. Firmware, OS, Software updates via Centralized Manager/Controller and must support version roll back functionality. Also, must support multiple OS, firmware image for booting options. 16. Must have Hardware Sensor Monitoring capabilities for reporting hardware health. 17. Option for scheduled updates so that it can be scheduled for specific days and time. 18. Total of two pairs (in HA) of management and log analyzer must be provided, where each pair of management and log analyzer should have license for atleast 06 firewalls from day-1.
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Should operate at AC ~50Hz, 220-240V. 3. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent. 4. The proposed Firewall must have redundant Hot-swappable Power supply from day one. Appliances/s must be rack mountable (supply support sides rails if required).

Sr. No	Parameter	Specifications
		5. Supply should include necessary console and power cables, 20 nos. of 3 Meters multimode LC Fiber patch Cables and 10 nos. of 3 Meters single mode LC patch cable.

b. Firewall Type-FW02 (North-south in HA Pair)

Sr. No	Parameter	Specifications
1.	**Features**	1. Certified FIPS 140-2, EAL 4+ / Common Criteria. 2. Should be Next-Generation Firewall (NGFW) with separate Data and control/Management plane. 3. Must have 6x 100GE/40GE QSFP28 single mode LC, 16x 10 GE SFP+ multimode LC, 2x RJ45 Management ports from Day1. All required transceivers should be populated from day one and compatible with the quoted switches. 4. The solution should have sufficient Physical RAM and CPU to cater the requested performance throughput. 5. Threat prevention throughput of 10 Gbps (Per Unit of HA) in real world/production/enterprise mix environment with all the security engines like IPS, Application control, web filtering, anti-malware etc, enabled. 6. SSL VPN throughput of at least 10 Gbps. Should support client based VPN and at least 3000 concurrent SSL VPN users. 7. Concurrent sessions of 2 million or above and new sessions / Sec of 1 Million or above. 8. The proposed solution should support HA in Active/Active and Active/Passive mode. The Firewall in HA should support stateful clustering across sites. HA should be supported on both IPV4 and IPV6. Feature like IPS, Anti malware, Web filtering, DDOS prevention and Traffic Shaping should be available in Active-Active. 9. Should be a hardware appliance based. Firewall. IPSEC and SSL VPN, Anti-Malware, IPS, Web and Application control, DDOS prevention, Traffic-Shaping/Bandwidth Management and Routing functionalities must be integrated in a single appliance.

Sr. No	Parameter	Specifications
		10. Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6) , DNS64 & DHCPv6 functionality. 11. Support unlimited IP/User Devices. 12. Firewall appliance must have at least 20 virtual firewall domains /instants active from day-1 scalable to 50(with additional license) with each firewall domains/instances having a separate administrative control OR equivalent, Security zones and VLAN. 13. The following features must be available in each virtual firewall domain/instant context environment: Firewall, IPSEC and SSL VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy based routing, DDOS, User and Group management, Logging and Reporting. 14. Solution must inherit all the standard RFC's with respect to the firewall functionalities. 15. Must support REST API. 16. Firewall must have a hardened OEM operating system. 17. The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection. 18. Should support bi-directional integration with Anti-APT/SANDBOX for sharing threat intelligence and automated mitigation of zero day attacks. 19. Automatic failover (condition based on ICMP, TCP or UDP protocol) as well as load sharing for outbound traffic. 20. Must support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation up to layer 7 traffic (including application type and SSL/TLS). 21. Firewall policy must facilitate IP, Network, Port, Protocol, User, Application and Zone. And must facilitate to apply features like IPS, Web & application Content filtering, Anti-Malware, IPS, DDOS prevention, Traffic Shaping (define - guaranteed, burstable/maximum bandwidth, set different level of priority) on any firewall policy for a specific time/Date/Period. Firewall policy

Sr. No	Parameter	Specifications
		must also have an option of configuring exceptions to any specific features. 22. The proposed system shall be able to operate on either Transparent (bridge) mode or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. 23. Must support DNS client and NTP client. 24. Must support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability. Also, must support Ethernet bonding functionality for full mesh deployment architecture. 25. Support all SNMP versions support v3. 26. Must support various form of user Authentication methods simultaneously, like: Local Database, LDAP server, RADIUS server, TACACS+ server and PKI methods (PKI authentication with PCKS#7, PCKS # 10 standards). 27. Two-factor authentication without any external Hardware. 28. Windows Active Directory single sign-on by means of agent/clientless/Captive portal which broker between users when they log on to the AD domain and the end-device. 29. Second factor authentication through email, Certificate, SMS, RSA token for remote users. 30. The proposed firewall shall be able to create custom application signatures and profile. 31. The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application based on the content. 32. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections. 33. Should support TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection etc.)

Sr. No	Parameter	Specifications
		34. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network. 35. The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc. 36. The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports. 37. Should be able to perform Anti-malware scans for HTTP, SMTP, IMAP, POP3, and FTP traffic. 38. Should detect and prevent malicious DNS request from inside hosts to outside bad domains, sinkhole the DNS request and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs. 39. Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data. 40. All the proposed threat functions like IPS, Anti-Malware, web and application control etc. should work in isolated air gapped environments without any need to connect with the Internet. 41. The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time). 42. Dedicated on premise anti-APT/sandbox solution in HA to be provided. The SANDBOX should be able to support the following- i) dynamic threat analysis on such as EXEs, DLLs, ZIP /RAR/7ZIP/TNEF files, PDF documents, Office

Sr. No	Parameter	Specifications
		Documents, Java, Android APKs/JAR, Adobe Flash applets, JPEG/GIF/BMP/WMF, on APT & SSL based APT attacks. ii) detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database iii) Analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications. iv) pre-populated Licensed copies of Operating systems (like Windows 7, Windows 8.1, Windows 10, Linux and Android etc.) and applications/softwares (like Microsoft Office). v) file sizes up to 100 MB or more vi) ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack. vii) capture and store packet captures of traffic relevant to the analysis of detected threats. viii) to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST). ix) deployment in out-of-band mode (also SPAN/TAP) & inline mode and block malicious traffic. x) SMB / CIFS / NFS protocol for sharing and transferring files xi) visibility into scan histories of each file scanned that are aborted, completed, or in progress xii) provide reports in (but not limited to) PDF/CSV formats xiii) anti-evasion capabilities to prevent malwares detection of being run/executed in the virtualized environment. xiv) to analyze email attachments and malicious links for static and dynamic analysis xv) SIEM log integration.

Sr. No	Parameter	Specifications
		xvi) to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc. xvii) number of Interfaces - 4x GE RJ45 ports, 2x 10 GE SFP+ slots xviii) VM's of at least 50 xix) process minimum of 5000 files/day xx) The solution should have redundant AC power supply fully populated (within box) from day one xxi) 2 TB in RAID 1 from day one 43. Should protect against phishing and JavaScript 44. The proposed solution should support the ability to create QoS policy on a per rule basis- by source address, by destination address, by application (such as Skype, Bittorrent, YouTube, azureus, webex), by static or dynamic application groups (such as Instant Messaging or P2P groups), by port and services. 45. Should support the following authentication protocols: LDAP, Radius (vendor specific attributes), and Token-based solutions. 46. Firewall appliance must have at least 2TB local hard-disk in order to keep log/statistics information.
2.	**Management**	1. Hardware appliance based centralized complete management (of all proposed NGFW appliances) solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access. 2. Provide separate appliance / VM / Software for collection and Analysis of firewall Logs and reporting. If VM / Software based then, the OEM/MSI should provide the necessary hardware(rack mountable system with required resources CPU, RAM, Storage, Network Interfaces to connect to the switching fabric as mentioned in the RFP) and licensed software(hypervisor, Operating System and any supporting software) along with OEM support for the mentioned warranty period in the RFP.

Sr. No	Parameter	Specifications
		3. The provided log reporting and analysis appliance (Hardware / VM / Software) must have storage capacity of at least 32TB. 4. Real time logging based on all Traffic and correlated log view based on other logging activities. 5. Management access control using Profile/Role based for granular control. Local access to appliance/s modules must support role based access. 6. Support configurable option for E-mail or SMS alerts (Via SMS gateway) in case of any event trigger. Provision to send mail or SNMP traps to EMS in response to system failures or threshold violations of the Health attributes. 7. Firewall configuration changes / commands issued must be logged. Also provision for exporting. 8. Must provide the real time health status of NGFW on dashboard for CPU memory utilization, state table, total No. of concurrent connections and the connections/second counter, real time data transfer/bandwidth utilization of individual IP/Application/protocol/port/Interface/Zone. 9. Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc. 10. Support standard report templates an dashboards with option to schedule reports. 11. Support reports to be send by email at scheduled intervals. Must support logs to be forwarded to a syslog server (Multiple for redundancy) in open standard log format. 12. Must support for SIEM log integration. The solution must be capable of sending logs to a SIEM system via syslog. 13. Must support future expansion. Same centralized management must support if number of appliances are increased. 14. Configuration backup and restore on to/from a remote system via GUI/CLI over HTTPS/SSH or equivalent secure mechanism. 15. Firmware, OS, Software updates via Centralized Manager/Controller and must support version roll back

Sr. No	Parameter	Specifications
		functionality. Also, must support multiple OS, firmware image for booting options. 16. Must have Hardware Sensor Monitoring capabilities for reporting hardware health. 17. Option for scheduled updates so that it can be scheduled for specific days and time. 18. Total of two pairs (in HA) of management and log analyzer must be provided, where each pair of management and log analyzer should have license for atleast 06 firewalls from day-1.
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Should operate at AC ~50Hz, 220-240V. 3. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent. 4. The proposed Firewall must have redundant Hot-swappable Power supply from day one. Appliances/s must be rack mountable (supply support sides rails if required). 5. Supply should include necessary console and power cables. 20 nos. of 3 Meters multimode LC Fiber patch Cables and 10 nos. of 3 Meters single mode LC patch cables.

c. Firewall Type-NGFW02

Sr. No	Parameter	Specifications
1.	**Features**	1. Certified FIPS 140-2, EAL 4+ / Common Criteria. 2. Should be Next-Generation Firewall (NGFW) with separate Data and control/Management plane. 3. Must have 8x 1 GE RJ45, 2x 1 GE SFP multimode LC, 1x RJ45 Management ports from Day1. All required transceivers should be populated from day one and compatible with the quoted switch. 4. The solution should have sufficient Physical RAM and CPU to cater the requested performance throughput. 5. Threat prevention throughput of 1 Gbps in real world/production/enterprise mix environment with all the security engines like IPS, Application control, web filtering, anti-malware etc, enabled.

Sr. No	Parameter	Specifications
		6. Should support client based VPN and at least 10 concurrent SSL VPN users. 7. Should be a hardware appliance based. Firewall. IPSEC and SSL VPN, Anti-Malware, IPS, Web and Application control, DDOS prevention, Traffic-Shaping/Bandwidth Management and Routing functionalities must be integrated in a single appliance. 8. Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6) , DNS64 & DHCPv6 functionality. 9. Support unlimited IP/User Devices. 10. Firewall appliance must support at least 2 virtual firewall domains/instants. 11. The following features must be available in each virtual firewall domain/instant context environment: Firewall, IPSEC and SSL VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy based routing, DDOS, User and Group management, Logging and Reporting. 12. Solution must inherit all the standard RFC's with respect to the firewall functionalities. 13. Must support REST API. 14. Firewall must have a hardened OEM operating system. 15. The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection. 16. Should support bi-directional integration with Anti-APT/SANDBOX for sharing threat intelligence and automated mitigation of zero day attacks. 17. Automatic failover (condition based on ICMP, TCP or UDP protocol) as well as load sharing for outbound traffic. 18. Must support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation up to layer 7 traffic (including application type and SSL/TLS). 19. Firewall policy must facilitate IP, Network, Port, Protocol, User, Application and Zone. And must facilitate to apply features like IPS, Web & application Content filtering, Anti-Malware, IPS, DDOS prevention,

Sr. No	Parameter	Specifications
		Traffic Shaping (define - guaranteed, burstable/maximum bandwidth, set different level of priority) on any firewall policy for a specific time/Date/Period. Firewall policy must also have an option of configuring exceptions to any specific features. 20. The proposed system shall be able to operate on either Transparent (bridge) mode or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. 21. Must support DNS client and NTP client. 22. Must support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability. Also, must support Ethernet bonding functionality for full mesh deployment architecture. 23. Support all SNMP versions support v3. 24. Must support various form of user Authentication methods simultaneously, like: Local Database, LDAP server, RADIUS server, TACACS+ server and PKI methods (PKI authentication with PCKS#7, PCKS # 10 standards). 25. Two-factor authentication without any external Hardware. 26. Windows Active Directory single sign-on by means of agent/clientless/Captive portal which broker between users when they log on to the AD domain and the end-device. 27. Second factor authentication through email, Certificate, SMS, RSA token for remote users. 28. The proposed firewall shall be able to create custom application signatures and profile. 29. The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application based on the content. 30. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate

Sr. No	Parameter	Specifications
		SSH Tunnel traffic in an inbound and outbound connections. 31. Should support TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection etc.) 32. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network. 33. The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc. 34. The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports. 35. Should be able to perform Anti-malware scans for HTTP, SMTP, IMAP, POP3, and FTP traffic. 36. Should detect and prevent malicious DNS request from inside hosts to outside bad domains, sinkhole the DNS request and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs. 37. Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data. 38. All the proposed threat functions like IPS, Anti-Malware, web and application control etc. should work in isolated air gapped environments without any need to connect with the Internet. 39. The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time). 40. Should protect against phishing and JavaScript

Sr. No	Parameter	Specifications
		41. The proposed solution should support the ability to create QoS policy on a per rule basis- by source address, by destination address, by application (such as Skype, Bittorrent, YouTube, azureus, webex), by static or dynamic application groups (such as Instant Messaging or P2P groups), by port and services. 42. Should support the following authentication protocols: LDAP, Radius (vendor specific attributes), and Token-based solutions. 43. Firewall appliance must have at least 100GB local hard-disk in order to keep log/statistics information.
2.	**Management**	1. Solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access. 2. Real time logging based on all Traffic and correlated log view based on other logging activities. 3. Management access control using Profile/Role based for granular control. Local access to appliance/s modules must support role-based access. 4. Support configurable option for E-mail or SMS alerts (Via SMS gateway) in case of any event trigger. Provision to send mail or SNMP traps to EMS in response to system failures or threshold violations of the health attributes. 5. Must provide the real time health status of NGFW on dashboard for CPU memory utilization, state table, total No. of concurrent connections and the connections/second counter, real time data transfer/bandwidth utilization of individual IP/Application/protocol/port/Interface/Zone. 6. Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc. 7. Support standard report templates an dashboards with option to schedule reports. 8. Support reports to be send by email at scheduled intervals. Must support logs to be forwarded to a syslog server (Multiple for redundancy) in open standard log format.

Sr. No	Parameter	Specifications
		9. Configuration backup and restore on to/from a remote system via GUI/CLI over HTTPS/SSH or equivalent secure mechanism. 10. Firmware, OS, Software updates provision and must support version roll back functionality. Also, must support multiple OS, firmware image for booting options. 11. Must have Hardware Sensor Monitoring capabilities for reporting hardware health. 12. Option for scheduled updates so that it can be scheduled for specific days and time.
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Should operate at AC ~50Hz, 220-240V. 3. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent. 4. Supply should include necessary console and power cables. 4 nos. of 3 Meters multimode LC Fiber patch Cables and 10 nos. of 3 meters CAT6 patch cables.

d. Web Application Firewall Type-01

Sr. No	Parameter	Specifications
1.	**Features**	1. Provide comprehensive and reliable support for high availability on Stateful session failover with Active-active & active standby unit redundancy mode. 2. Should support a local user database 3. Should have built-in tcpdump-like tool and log collecting functionality 4. Should support REST API for integration. 5. Should support one arm, reverse and transparent proxy mode deployment scenarios 6. The server load balancer should deliver 50 Gbps of L4 throughput and 50 Gbps of Layer 7 throughput. 7. The server load balancer should deliver 1 million concurrent sessions 8. The sever load balancer should be proposed with 4x 40GbE QSFP single mode LC and 8x 10G SFP+ multimode LC. All

Sr. No	Parameter	Specifications
		the transceivers should be populated from day one and compatible with the quoted switch. 9. The appliance MUST support layer 2 to layer 7 load balancing 10. The appliance MUST support server load balancing methods- Round-Robin, Weighted Round-Robin, Least Connections, Fastest Response, URI, Host, Host Domain, and Destination IP Hash. 11. The solution must maintain server persistency with - Source-IP, Source-IP Hash, Source-IP/Port Hash, Hash Header, Hash Request, Persistent Cookie, Rewrite Cookie, Insert Cookie, Hash Cookie, Embedded Cookie, RADIUS Attribute, and SSL Session ID. 12. The solution must provide application & server health checks for well-known protocols –ICMP, TCP, TCP Echo, HTTP, HTTPS, DNS, RADIUS RADIUS Accounting, SMTP, POP3, IMAP4, FTP, TCP Half Open, SNMP, SSH, UDP, L2 Detection 13. Support layer4 and layer 7 load balancing for well-known protocols like - HTTP, HTTPS, TCP, UDP, FTP, RADIUS 14. Support content routing 15. Support scripting 16. Support outbound multi-homing Link Load Balancing 17. Support load balancing of servers between different data centres 18. Support dynamic proximity is based on round-trip time using ICMP or ICMP and TCP. 19. Support dynamic proximity based on round-trip time using ICMP or TCP 20. Support inbound Link Load Balancing. 21. Hardware based SSL acceleration. 22. Support Certificate/Private Key backup/restore to/from local disk or remote TFTP server, and through WebUI 23. Support all common certificate formats, self-generated CSR (Certificate Signing Request), self-signed Certificate and private key for specified host. 24. Support HTTP to HTTPS header rewrite for enhanced application delivery support for Host Request URL Referrer Scripting allows manipulation (insert, remove, replace) of any HTTP header.

Sr. No	Parameter	Specifications
		25. Must have end to end SSL support to act as a SSL Server and/or as SSL Client. 26. Support client certificate verification, CRL's (HTTP, FTP, LDAP) and OSCP protocol. 27. Support Elliptic Curve Diffie-Helman ciphers ECDHE-RSA-AES256, ECDHE-RSA-AES128, ECDHE-RSA-RC4, ECDHE-RSA-DES. 28. Support customizable SSL/TLS versions 29. Support malware scanning from day one and integration (open API / ICAP) with the proposed Sandbox. 30. Should have support of integration with Web application Vulnerability assessment tools to virtually patch web application vulnerabilities. 31. Provide performance optimization using TCP connection multiplexing, TCP buffering. 32. Support IEEE 802.3ad link aggregation 33. Provide selective compression for Text, HTML, XML, Java Scripts, CSS, Mime types and pictures 34. Support WAF Features – i) Protection from the OWASP Top 10 application attacks ii) Support API Protection, API Gateway, captcha, Virtual patching, Data Leak Prevention iii) SQLi/XSS Injection Detection, Cookie Poisoning, Session Hijacking, Buffer Overflow Attacks, Brute Force Attacks, Path (directory) Traversal, Malicious file upload, XML/JSON/SOAP Validation, HTTPS Header security iv) The proposed appliance should provide minimum 50Gbps WAF (SSL) throughput. v) The server load balancer should cater up to 50,000 SSL TPS on RSA 2K key and 40,000 ECC CPS on (EC-P256). vi) Zero Day Attack Blocking 35. SYN flood protection 36. Support HTTP authentication 37. Support policy-based Connection limiting at L4 or L7 at virtual server or real server level.

Sr. No	Parameter	Specifications
		38. Support Virtualization. Minimum 10 Virtual ADC license should be provided from day one 39. Certified for EAL2 / Common Criteria Program for Security related functions / Indian Common Criteria certification Scheme (IC3S) by STQC.
2.	**Management**	1. Should support backup of the full system configuration via the GUI 2. Support centralized management through Web / GUI. Four pairs (each pair in HA) of manager/controller is required with each pair having license to manage at least 06 WAF from day-1. 3. Should support multiple log formats such as CSV/ Syslog/ TXT, etc and multiple syslog servers. 4. Support reporting and sending the report via E-Mail. 5. Should support report formats in PDF/HTML/WORD/RTF, etc.
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Should operate at AC ~50Hz, 220-240V. 3. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent. 4. Should have internal redundant power supply 5. Supply should include necessary console and power cables. 12 nos. of 3 Meters multimode LC Fiber patch Cables and 4 nos. of 3 Meters single mode LC patch cables.

3. WIPS (WIPS Controller Type-01 & WIPS Scanner Type 02)

Sr. No	Parameter	Specifications
1.	**Features**	1. Proposed Radio solution shall provide No-WIFI zone 2. Proposed solution shall not implement No-WIFI zone by jamming the signal or creating the noise in entire Wireless unlicensed spectrum. 3. Proposed radio solution shall continue to provide wireless intrusion detection and prevention 24x7 even if the sensors/radios disconnect from its cloud or on-prem Management /control system.

Sr. No	Parameter	Specifications
		4. Proposed hardware/sensors shall provide dedicated scanning and prevention radio for 2.4 and 5 Ghz band 5. Proposed hardware/sensors shall provide WIPS and WIDS function for WIFI 6 Clients/Protocol. 6. Entire WIPS and WIDS policies should be manged from single management plane. 7. The solution must auto-classify APs (BSSID) precisely in different categories as managed / authorized (ie. managed device connected to the networks), external (i.e. un-managed APs not connected to the networks, e.g. neighbours), and rogue APs (un-managed AP connected to the networks) 8. The solution must be able to detect and automatically prevent all types of Rogue (unauthorized APs connected to the network) APs, such as: a) APs such as Bridge and NAT b) MAC-adjacent Open/Encrypted Wi-Fi routers c) Non-MAC-adjacent OPEN Wi-Fi routers 9. The solution must be able to detect and automatically prevent all Wi-Fi enabled devices such as laptops bridging or involved in ICS when connected to the network 10. The solution shall provide RSSI based fencing to implement the NO-WIFI zone. 11. The solution must be able to detect and automatically prevent all Wi-Fi enabled devices such as laptops, Smart devices bridging or involved in ICS when connected to the network. 12. The solution must detect mis-configured authorized APs (APs which are not configured as Security compliance) and automatically prevent them. 13. The solution must detect Honey Pot attacks. It should be able to prevent the authorized client from connecting to a honeypot AP while operating in No WIFI zone. 14. "The WIPS solution should NOT affect the operation of an external (i.e. neighbours) or a managed access point while preventing a rogue AP on the same channel. 15. The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-

Sr. No	Parameter	Specifications
		Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, No-WIFI operations. 16. The Solution must provide reports of all the clients with WIFI turned ON in NON-WIFI zone.
2.	**Management**	1. The controller/ Management server should be able to rollback all sensors/group of sensors to previous version. 2. Controllers (in HA) must be provided from day-1, where each pair of controller should be able to control atleast 15 WIPS units from day-1. 3. The Controller/ Management server Upgrade should not disrupt WIPS , WIDS . 4. The sensor upgrade to controller version should be flexible and be scheduled on per AP group or site basis as required. 5. For management and monitoring operations, the controller /Management server must provide a web interface, command-line interface, and APIs. 6. The solution must allow automatic schedules for report generation and distribution of reports to Specific users via email. 7. The Controller/Management server must provide centralized WIPS , WIDS in Location tracking management system 8. The controller/Management server should support open API's for integration with 3rd party configuration management, inventory management, performance management, process automation, reporting, WLAN monitoring tools etc. 9. Controller should support v2c, v3 10. The Controller / solution should locate wireless devices (APs and Clients) on floor maps. 11. The Controller/Management server should support manual and scheduled automatic system backup. 12. The solution should maintain controller user action logs which should include all activities performed by the user like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 30 days. Bidder / OEM must provide all the necessary hardware and Software (include OS, Hypervisor etc. if any) with respective licenses for the management/Controller.

Sr. No	Parameter	Specifications
2.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. WIPS unit should have POE+ One Gigabit RJ45 Port. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent.

4. Network Access Control-01

Sr. No	Parameter	Specifications
1.	**Features**	1. The solution should provide an easy-to-use BYOD ready granular secure access control solution that is context aware, identity enabled, location and device based. The proposed solution must combine Authentication, Authorization, and Accounting (AAA), Posture, Profiling and Guest Access management services on to a single platform and support the ability to be managed from a single management console. 2. The solution should be deployed in out-of-band mode. 3. The solution should support centralized deployment and High Availability. 4. Support Captive Portal. 5. Solution must be provided with perpetual Licenses, supporting minimum 500 device for TACACS+ and 1000 devices for NAC and 100 for device Profiling, Posturing and Guest Access from Day 1. License should be splitable across (DC, BCP and DR) 6. The solution must be deployed with 802.1x authentication for managed endpoints to provide Zero Trust Security with Pre- and Post-Admissions Control. The solution should not be dependent on ARP or SNMP enforcement approach. 7. The NAC solution be able to integrate with wireless and wired network devices. 8. The solution should be able to evaluate and on-board endpoints connected behind an unmanaged switch thorough agent. 9. If a system is connected to the IP Phone, NAC should authenticate both IP phone and computer before granting network access. 10. The proposed NAC solution should be able to detect endpoints and categorizes them based upon the type of

Sr. No	Parameter	Specifications
		endpoint (Ex: Windows, Printer, Network Device, IP Camera, Android, iPad,etc). 11. The solution should have a capability to detect and profile IoT and IIoT devices. 12. The proposed NAC solution must support profiling by targeting specific endpoints for specific observable attribute. 13. The proposed solution should support profiling devices automatically based on their Category, OS, MAC address, etc. 14. The proposed NAC solution should provide support for discovery, policy-based placement, and monitoring of endpoint devices on the network all within the same appliance 15. The proposed NAC solution must support profiling via passive and active collectors using various methods like SNMP, DHCP fingerprinting, HTTP-agent, NMAP, WMI, SSH, etc. 16. The proposed NAC solution must support a solution for device management for network access. For example; if a new system is introduced in the network (For Eg. System without a 802.1x supplicant), an email alert should be sent by NAC to the IT admin for approving the network access from that device. 17. The proposed NAC solution must provide the ability to create custom profiling rules into groups and enforce policy. 18. The proposed NAC solution should produce a real-time endpoint discovery with detailed information including which switch port the device is connected. 19. The NAC solution should to have built-in / via integration capability to analyse behaviour of device/user (not limited to detect and prevent MAC address spoofing) such as client location / posture change, and enforce adaptive authentication by challenging a device/user for MFA authentication/ restrict device/user. 20. The proposed NAC solution shall include the following in-built components a) Local RADIUS server for wireless and wired network and devices

Sr. No	Parameter	Specifications
		b) TACACS+ server for securing access to network infrastructure devices with AAA capabilities c) NAC client agents e) Enforcement Manager f) Integration Interfaces g) One Time Password for 2FA/MFA 21. The proposed NAC solution must be capable of supporting 802.1X authentication and shall work with endpoint devices (supplicant) and network devices (authenticator) that are enabled for IEEE 802.1X authentication. 22. The proposed NAC solution must be capable of supporting SNMP v2 and v3 enforcement and shall work with endpoint devices (without 802.1x supplicants) and network devices that are enabled SNMP to send traps to NAC device. 23. The proposed NAC solution must make use of alternate authentication methods such as MAC address authentication or web authentication to authenticate endpoint devices that do not support 802.1X authentication 24. The proposed solution NAC must support following credentials for authentication a) User ID and password b) Digital certificates only c) Combination of User ID and password and digital certificates or d) Combination of User ID and password and hardware token. 25. The proposed NAC solution should integrate with multivendor switches and Wireless Controllers to support enforcement actions such as switch port block, assign dynamic VLAN and dynamic ACL via 8021x and SNMP. 26. The proposed NAC solution must enforce security policies by blocking, isolating, and remediation of noncompliant machines in a quarantine area without needing administrator attention. Once the user's machine is remediated, the user's machine shall be redirected automatically to the assigned network segment. 27. The proposed NAC solution should be able to perform endpoint posture verification with agentless,

Sr. No	Parameter	Specifications
		temporary/dissolvable agent and persistent agent on corporate, contractor and guest endpoints. 28. The proposed NAC solution must be able to remotely install agents/components to corporate hosts without end-user interaction. 29. The proposed NAC solution must support pre- and post-admission control Zero Trust capabilities for network access through 802.1x. 30. The proposed NAC solution must support all of the following authenticating protocols: PAP, MS-CHAP, MS-CHAP-V2, EAP-MD5-Challenge, EAP-MS-CHAP-V2, (EAP)-MD5, Protected EAP (PEAP), EAP-Transport Layer Security (TLS), EAP Tunnelled Transport Layer Security (EAP-TTLS), EAP Generic Token Card (EAP-GTC). 31. The proposed solution should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: Local Databased on the NAC device, External RADIUS, Active Directory, LDAP, OTP, SAML 2.0, and SQL through agent. 32. The proposed NAC solution should support multifactor Authentication for better security. The solution should include Token based authentication. 33. The proposed solution should support password management by integrating with LDAP server and allow users to receive notification about password expire. The solution should also allow users to reset their password through the NAC agent. 34. The proposed NAC solution should support installation of a browser based agent to perform compliance checks (AV, Patches etc.,) on Guest endpoints 35. Must have granular compliance check options which includes the following: Hard drive encryption detection, Detection of Pre-defined Anti-malware with latest signature and updated, Personal Firewall, OS Check, CVE Check (known vulnerability detection), Processes, Registry Check, Files, TCP or UDP Ports Check, NetBIOS, MAC address Check, Patch Check by integration with Patch

Sr. No	Parameter	Specifications
		Management Solution, Machine Certificate check, OS Updated. 36. The solution should support posture assessment capabilities on Windows, Linux and Mac endpoints. 37. The NAC solution shall be configurable to enable or disable the performance of a re-authentication process upon detection of a posture change in the endpoint devices during post admission. 38. The solution should be able to check system process and also kill the process, detect and modify Registry keys, detect and delete malicious files, through auto remediation. This capability should be supported with persistent and browser based temporal/dissolvable agent. 39. Solution should support integration with patch management solution with auto remediation capabilities. 40. The agent should support credential provider capabilities to allow new users to successfully authentication with the AD server through NAC before windows logon in 802.1x secure environment. 41. The built-in local RADIUS server should support 802.1x for user and device authentication. 42. TACACS+ device administration should support granular control of access to network devices - a) Role-based access control b) Per Command level authorization with detailed logs for auditing c) The solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive,? (any character), * (matches any), etc 43. The proposed NAC solution must provide complete guest lifecycle management by allowing non-IT employees to provide controlled access to guests and consultant reducing the IT workload including via captive portal. 44. The proposed solution should be able to integrate with Next Generation firewall and perform Layer 3 enforcement from unauthorized access.(Eg: Any

Sr. No	Parameter	Specifications
		device/user connection to firewall bypassing NAC should be blocked). 45. The solution should allow adding levels of security to detect threats coming from users who are authenticated through the system by integrating NAC with a SIEM and Firewall solutions. 46. The solution should be able to integrate with other security solutions using REST API, IF-MAP, Syslog and other methods to detect and enforce threat prevention policies and provides a collaborative and comprehensive approach toward complete network security. 47. The proposed NAC solution should integrate with Identity providers (Duo, RSA, etc.) 48. Proposed appliance must have minimum RAM to cater to the requested client/user capacity. 49. Proposed hardware appliance must have at least 2x 10G SFP+ SR multimode LC and 2x 1G copper ports populated from Day-1 compatible with proposed the switch. 50. The proposed solution must comply to the following industries recognized certifications: PCI-DSS, FIPS-2, NDcPP.
2.	**Management**	1. Centralize single dashboard for management of all the NAC appliances. 2. Should have flexible filtering capabilities to sort out device information based on different attributes (e.g MAC address, Manufacturer name, hostname, IP address, etc.) 3. Should provide device inventory in both CSV and PDF exportable format. 4. Should provide information on how many devices are not profiled, how many devices are newly seen in day/week/month, etc. 5. Guest management portal shall support customizable pages, registration with multiple credential notification methods (SMS, Email, webpage, etc.), self-on-boarding for Guest/Contractor or Employees BYOD devices. 6. Support built-in monitoring, reporting, and troubleshooting console. 7. NAC GUI should support Dashboard with contextual information (compliance, number of users, devices, etc.)

Sr. No	Parameter	Specifications
		8. NAC GUI should support historical data on contextual information. 9. The proposed NAC solution should allow administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network.
3.	**General**	1. TAC should be directly from the OEM with 24x7 support. Should be provided with NBD replacement. 2. Should have safety and standards certifications as below: ROHS, UL or Equivalent and FCC OR equivalent. 3. Supply should include required power cables and 4 nos. 3 Meters multimode LC Fiber patch Cable and 4 nos. of 3 Meters CAT6 patch cables.

(End of Section - V)

Section – VI: BOQ / Commercial-Bid Format

1. Category-I

S.NO.	ITEM DESCRIPTION	QUANTITY	ITEM PRICE (W/O Tax)	TAX (GST)%	ITEM PRICE (With TAX)	TOTAL PRICE (With TAX)
1	HSM01	6				
2	HSM02	2				
3	KM01	10				
4	STGBKP01	4				
5	STGBKPTP01	4				
6	STGBKPTP02	2				
7	DEGAUSS01	2				
8	SIEM01	3				
9	PIM-PAM01	3				
10	SAFE01	2				
11	SAFE02	2				
12	SERVER02	12				
13	SERVER03	62				
14	SERVER04	141				
15	SERVER06	30				
16	SHREDDER01	2				
17	STGSANNAS01	6				
18	TERMINAL01	38				
19	SMARTRACK	2				

2. Category-II

S.NO.	ITEM DESCRIPTION	QUANTITY	ITEM PRICE (W/O Tax)	TAX (GST)%	ITEM PRICE (With TAX)	TOTAL PRICE (With TAX)
1	Firewall Type-FW01in HA Pair (EAST-WEST) bundled along with SANDBOX, Analyser and Manager for each Pair	6				
2	Firewall Type-FW02 in HA Pair (North-south) bundled along with SANDBOX, Analyser and Manager for each Pair	6				
3	Firewall Type-NGFW02 (CA)	2				
4	SWITCH Type-01 (Management TOR)	68				
5	SWITCH Type-03 (Compute LEAF)	132				
6	SWITCH Type-04 (Management POE)	6				
7	SWITCH Type-05 (L3 Perimeter)	12				
8	SWITCH Type-06 (SPINE)	12				
9	SWITCH Type-09 (Management Core)	12				
10	Web Application Firewall Type-01	18				
11	Network Access Control in HA Pair-01	3				
12	WIPS (WIPS Controllers in HA & WIPS Scanners-30)	01				

Prices: All-inclusive (Applicable GST Extra) and must be quoted in Indian Rupees only.
Delivery: FOB Delhi & Bangalore within 120 days for Category I and 180 days for Category II items, from the date of issuing of PO.

Validity: The commercial bid shall be valid for a period of 365 days.

Note: Please note that, Bidder need to submit the Price masked Commercial Bid (Un-Priced Commercial Bid).

(End of Section – VI)

Section – VII: Item Wise Delivery Location

1. Category-I

S.NO.	ITEM CODE	DELHI	BANGALORE	Total No.
1	DEGAUSS01	1	1	2
2	HSM01	4	2	6
3	HSM02	1	1	2
4	KM01	6	4	10
5	PIM-PAM01	2	1	3
6	SAFE01	1	1	2
7	SAFE02	1	1	2
8	SERVER02	7	5	12
9	SERVER03	37	25	62
10	SERVER04	83	58	141
11	SERVER06	19	11	30
12	SHREDDER01	1	1	2
13	SIEM01	2	1	3
14	SMARTRACK	1	1	2
15	STGBKP01	2	2	4
16	STGBKPTP01	2	2	4
17	STGBKPTP02	1	1	2
18	STGSANNAS01	4	2	6
19	TERMINAL01	25	13	38

2. Category-II

S.NO.	ITEM CODE	Delhi	Bangalore
1	Firewall Type-FW01	**4**	**2**
2	SWITCH Type-06	**8**	**4**
3	SWITCH Type-03	**76**	**56**
4	SWITCH Type-09	**8**	**4**
5	SWITCH Type-01	**42**	**26**
6	WIPS Scanner Type 02	**20**	**10**
7	WIPS Controller Type-01	**1**	**1**
8	SWITCH Type-04	**4**	**2**
9	Web Application Firewall Type-01	**12**	**6**
10	Network Access Control-01	**2**	**1**
11	SWITCH Type-05	**8**	**4**
12	Firewall Type-FW02	**4**	**2**
13	Firewall Type-NGFW02	**1**	**1**

(End of Section - VII)

ANNEXURE – A: COVERING LETTER

Date:
To:

Director General
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road,
Pune - 411008 Maharashtra, INDIA

Subject: Tender for submission ……..

Dear Sir,

We, the undersigned, offer to supply Computer Hardware and Software items, in response to your Tender No **CDACP/AG22-IT/22-23/356.**

We are hereby submitting our proposal for same, which includes Technical Bid and the Price Bid on www.eprocure.gov.in

We undertake, if our proposal is accepted, to submit a Security Deposit & Performance Bank Guarantee of 3% of the contract/ order value, as per terms stipulated in the tender.

We hereby certify that my/ our firm has not been disqualified and/ or blacklisted by any Office/ Department/ Undertaking of the State Government/ Central Govt. of India, PSU/ Autonomous Body of Government of India, at the time of submission of this bid.

We agree to abide by all the terms and conditions of the tender document, including corrigenda. We would hold the terms of our bid valid for 90 days as stipulated in the tender document.

We understand you are not bound to accept any Proposal you receive.

The undersigned is authorized to sign this bid document. The authority letter to this effect is enclosed.

Yours sincerely,
Authorized Signatory:
Name and Title of Signatory:
e-mail:

Mobile No:

ANNEXURE – B: AUTHORITY LETTER

Date:

To:

Director General,
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road,
Pune - 411008 Maharashtra, INDIA

Subject: Authority Letter

Reference: Tender for supply of …….. No **CDACP/xxxxxxxxxxxxx**

Dear Sir,

We, M/s _____ (Name of the bidder) having registered office at _____ (address of the bidder) herewith submit our bid against the said tender document.

Mr./Ms. _____ (Name and designation of the signatory), whose signature is appended below, is authorized to sign and submit the bid documents on our behalf against said RFP

Specimen Signature:

The undersigned is authorised to issue such authorisation on behalf of us.

For M/s _____ (Name of the bidder)

Signature and company seal
Name
Designation
Email
Mobile No.

ANNEXURE C – UNDERTAKING BY PRINCIPAL MANUFACTURER(S)

(To be submitted in Original on Letterhead-Separately for items in each Category)

Date:
Director General,
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road,
Pune - 411008 Maharashtra, INDIA

Subject: Undertaking by Principal Manufacturer against tender no. CDACP/XXXXXXXXXX for ……..

Dear Sir,

We, M/s _____ (Name of the manufacturer) having registered office at _____ (address of the manufacturer) by virtue of being manufacturer for _____ (Name of the product/s), hereby certify that M/s _____ (Name of the bidder) having their office at _____ (Address of bidder) are our Authorised Distributors/ Dealers for our range of products quoted by them, as listed below:

1
2

Within the scope of requirement as per the tender mentioned above, we undertake to provide technical & other support towards fulfilling the requirements of installation, commissioning, benchmarking, acceptance criteria and product warranty services of the components to be supplied and installed at the C-DAC Customer sites by M/s. (Name of bidder) against said tender.

We also certify that the products offered are not nearing end-of-life / end-of-support five years down the line from the date of bidding.

The undersigned is authorised to issue this certificate on behalf of M/s _____ (Name of the manufacturer).

For M/s _____ (Name of the manufacturer)

Signature & company seal
Name
Designation
Email
Mobile No.

ANEXURE D - PROFORMA OF BANK GUARANTEE

(To be submitted by the vendor for claiming payment)

To,

Centre for Development of Advanced Computing
Innovation Park, PANCHAVATI,
Pashan Road, Pune – 411 008

BANK GUARANTEE NO:
DATE:

Dear Sir(S)

This has reference to the Purchase Order No. _____ Dated _____ been placed by Centre for Development of Advanced Computing(C-DAC), Pune on M/s_____ (Name & Address of vendor) for supply, installation, commissioning and warranty of _____ (description of items) at the C-DAC Customer sites.

The conditions of this order provide that the vendor shall,

Arrange to deliver the items listed in the said order to the consignee, as per details given in said order, and

Arrange to install and commission the items listed in said order at client's site, to the entire satisfaction of C-DAC and

Arrange for the comprehensive warranty service support towards the items supplied by vendor on site as per the warranty clause in said purchase order.

M/s (Name of Vendor) has accepted the said purchase order with the terms and conditions stipulated therein and have agreed to issue the performance bank guarantee on their part, towards promises and assurance of their contractual obligations vide the Supply Order No. _____ M/s. _____ (name of vendor) holds an account with us and has approached us and at their request and in consideration of the promises, we hereby furnish such guarantees as mentioned hereinafter.

C-DAC shall be at liberty without reference to the Bank and without affecting the full liability of the Bank hereunder to take any other undertaking of security in respect of the suppliers obligations and / or liabilities under or in connection with the said contract or to vary the terms vis-a – vis the supplier or the said contract or to grant time and or indulgence to the supplier or to reduce or to increase or otherwise vary the prices or the total contract value or to forebear from enforcement of all or any of the obligations of the supplier under the said contract and/or the remedies of C-DAC under any security now, or hereafter held by C-DAC and no such dealing(s) with the supplier or release or forbearance whatsoever

shall have the effect of releasing the bank from its full liability of C-DAC hereunder or of prejudicing right of C-DAC against the bank.
This undertaking guarantee shall be a continuing undertaking guarantee and shall remain valid and irrevocable for all claims of C-DAC and liabilities of the supplier arising up to and until _____ (date)
This undertaking guarantee shall be in addition to any other undertaking or guarantee or security whatsoever the that C-DAC may now or at any time have in relation to its claims or the supplier's obligations/liabilities under and / or in connection with the said contract and C-DAC shall have the full authority to take recourse to or enforce this undertaking guarantee in preference to the other undertaking or security (ies) at its sole discretion and no failure on the part of C-DAC in enforcing or requiring enforcement of any other undertaking or security shall have the effect of releasing the bank from its full liability hereunder.

We _____ (Name of Bank) hereby agree and irrevocably undertake and promise that if in your (C-DAC's) opinion any default is made by M/s _____ (Name of Vendor) in performing any of the terms and /or conditions of the agreement or if in your opinion they commit any breach of the contract or there is any demand by you against M/s _____ (Name of Vendor), then on notice to us by you, we shall on demand and without demur and without reference to M/s _____ (Name of Vendor), pay you, in any manner in which you may direct, the amount of Rs. _____/- (Rupees _____ Only) or such portion thereof as may be demanded by you not exceeding the said sum and as you may from time to time require. Our liability to pay is not dependent or conditional on your proceeding against M/s _____ (Name of Vendor) and we shall be liable & obligated to pay the aforesaid amount as and when demanded by you merely on an intimation being given by you and even before any legal proceedings, if any, are taken against M/s _____ (Name of Vendor)
The Bank hereby waives all rights at any time inconsistent with the terms of this undertaking guarantee and the obligations of the bank in terms hereof shall not be anywise affected or suspended by reason of any dispute or disputes having been raised by the supplier (whether or not pending before any arbitrator, Tribunal or Court) or any denial of liability by the supplier or any order or any order or communication whatsoever by the supplier stopping or preventing or purporting to stop or prevent payment by the Bank to C-DAC hereunder.

The amount stated in any notice of demand addressed by C-DAC to the Bank as claimed by C-DAC from the supplier or as suffered or incurred by C-DAC on the account of any losses or damages or costs, charges and/or expenses shall as between the Bank and C-DAC be conclusive of the amount so claimed or liable to

be paid to C-DAC or suffered or incurred by C-DAC, as the case may be and payable by the Bank to C-DAC in terms hereof.
You (C-DAC) shall have full liberty without reference to us and without affecting this guarantee, to postpone for any time or from time to time the exercise of any of the powers and rights conferred on you under the contact with the said M/s _____ (Name of Vendor) and to enforce or to forbear from endorsing any power or rights or by reason of time being given to the said M/s _____ (name of Vendor) which under law relating to the sureties would but for the provisions have the effect of releasing us.

You will have full liberty without reference to us and without affecting this guarantee, to postpone for any time or from time to time the exercise of any of the powers and rights conferred on you under the contract with the said M/s _____ (Name of Vendor) and to enforce or to forbear from endorsing any power or rights or by reason of time being given to the said M/s _____ (Name of Vendor) which under law relating to the sureties would but for the provisions have the effect of releasing us.

Your right to recover the said sum of Rs. _____/- (Rupees _____ only) from us in manner aforesaid will not be affected/ or suspended by reason of the fact that any dispute or disputes have been raised by the said M/s _____ (Name of Vendor) and/ or that any dispute or disputes are pending before any officer, tribunal or court or Arbitrator.

The guarantee herein contained shall not be determined or affected by the liquidation or winding up, dissolution or change of constitution or insolvency of the said M/s _____ (Name of Vendor) but shall in all respects and for all purposes be binding and operative until payment of all dues to C-DAC in respect of such liability or liabilities.

Our liability under this guarantee is restricted to Rs._____/- (Rupees _____Only). Our guarantee shall remain in force until unless a suit action to enforce a claim under guarantee is filed against us within six months from (which is date of expiry of guarantee) all your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.
We have power to issue this guarantee in your favour under Memorandum and Articles of Association of our Bank and the undersigned has full power to do under the power of Attorney dated.

Notwithstanding anything contained herein:

Our liability under this guarantee shall not exceed Rs_____ (in words)
This bank guarantee shall be valid up to _____ & unless a suit for action to enforce a claim under guarantee is filed against us within six months from the date of expiry of guarantee. All your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there after i.e., after six months from the date of expiry of this Bank guarantee.
We are liable to pay the guaranteed amount or any parts thereof under this bank guarantee only and only if you serve upon us a written claim or demand or before _____.
The Bank guarantee will expire on (Min 37 months from the date of successful installations of the items in the order) _____.

Granted by the Bank

Yours faithfully,

For (Name of Bank)

SEAL OF THE BANK
Authorised Signatory

ANNEXURE E CERTIFICATE/UNDERTAKING FROM BIDDER

(ON COMPANY'S LETTERHEAD)

To: Director General,
C-DAC, Pune – 411008

Ref: Tender / Enquiry No. XXX dt. XXXX

We have read the clause mentioned in Order (Public Procurement No. 1) No. F.No.6/18/2019-PPD of Public Procurement Division, Department of Expenditure, Ministry of Finance dated 23rd July 2020 and further Order/OMs regarding restrictions on procurement from a bidder of a country which shares a land border with India.

In view of this, we certify that,

a. We are not from a country sharing land border with India and any registration as mentioned in said OM is not applicable to us.

OR

b. We are registered with the competent authority as mentioned in said OM. The copy of registration No.xxxdt.xxx is enclosed.

(Delete whatever is not applicable)

For (Name of Bidder)

Authorised Signatory
(Name & Signature)
(Company's Seal)

ANNEXURE F

Declaration / Certificate to be provided by Statutory Auditor or Cost Auditor of the Company (in case of companies) or from a practicing Cost Accountant or practicing Chartered Accountant (in respect of suppliers other than companies)

Please submit the certificate as per format given below:

To:

Director General,
Centre for Development of Advance Computing,Pune – 411008

Sub: Tender for …….
Ref: Tender No. CDACP/AG22-IT/22-23/356

We hereby certify that the goods / software being offered by us vide our proposal, comply with the provisions of Make In India Order No P-45021/2/2017-PP (BE-II), dated 16th Sept 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI, read with order number W-43/4/2019-IPHW- MeitY, dated 7th September, 2020 issued by IPWH division of MeitY, GoI for respective items.

We also certify that, we are not from a country sharing land border with India as defined in order No. F/No/6/18/2019-PPD dated 23 July 2020 issued by public procurement Division, Dept. of Expenditure, Ministry of Finance, GoI and the goods offered by us comply with the provisions of said order (details provided below).

We hereby certify the details pertaining to goods / software offered by us, against the tender requirement is given below:

Sr No	Item Description, Make, Model	Country of origin of OEM	Country of Manufac tureof item	Percentage of local contents as defined by order number W-43/4/2019-IPHW-MeitY, dated 7th September, 2020issued by IPWH division of MeitY,GoI *	Details of the location(s) at which the local value addition is made
1	Category I & II Items with description			Consolidated MII / Local Content for the complete solution declared by System Integrator (SI)/ Bidder	

Note 1: The Country of origin / manufacturing, should be declared for individual items being offered for both Category I & II items.

Note 2: CDAC reserves the right to Accept / Reject / Cancel the bid / bidder, at its sole discretion, based on the responses received against the MII and Land border sharing declarations submitted by the bidders / vendors.

Note 3: The System Integrator / Bidder, needs to provide the MII / Local content declaration as a consolidated figure for the complete solution. However, location of value addition should be declared for each item.

For (Name of bidder)

Authorized Signatory Name & Designation:
Mobile No:

ANNEXURE G

(ON COMPANY'S LETTERHEAD)

Date:

To:
Director General,
Centre for Development of Advanced Computing (C-DAC)
Innovation Park, Panchavati, Pashan Road,
Pune - 411008 Maharashtra, INDIA

Subject: EMD Undertaking as per GFR – 2017, Rule 170(iii)
Ref: Tender Ref. No. ……. & Tender ID

Dear Sir,

We, the undersigned, offer to Supply the ----------
as per tender at C-DAC Pune, in response to your Tender No CDACP/AG22-IT/22-23/356.

We are hereby submitting our proposal for same, which includes technical bid and the financial bid. As a part of eligibility requirement stipulated in said tender document, we hereby submit a declaration in lieu of Earnest Money Deposit (EMD), as given below:

1. Our bid shall remain valid for 365-days from the date of submission and that we will not withdraw or modify our bid during the validity period,
2. In case, we are declared as successful bidder and an order is placed on us, we will submit the acceptance in writing within 7 days of placement of order on us.
3. In case, we are declared as successful bidder and an order is placed on us, we undertake, to submit a Security Deposit of 3% of the order value, as per terms stipulated in the tender.
4. In case of failure on our part to comply with any of the above said requirements, we are aware that we shall be declared as un-eligible for said tender and /or debarred from any future bidding process of C-DAC for a period of minimum two years.
5. The undersigned is authorized to sign this undertaking.

Yours sincerely,

Authorized Signatory:
Name and Title of Signatory:
e-mail:
Mobile No:

ANNEXURE H

(PERFORMA OF BANK GUARANTEE TOWARDS Security Deposit)

ABank Guarantee No. ----------

Ref:
To
Centre for Development of Advanced Computing,
S.P. Pune University Campus
Pune - 411007

Dear Sir(s),

Whereas the Centre for Development of Advanced Computing having its office at S.P. Pune University Campus, Pune - 411007(hereinafter called the CDAC) which expression shall, unless repugnant to the context or the meaning thereof, include all its successors, administrators, executors and assignees has invited tender No.---------- and M/s ---------- having Registered/ Head Office at ---------- ---------- ---------- (Hereinafter called the "Contractor" which expression shall, unless repugnant to the context or the meaning thereof, mean and include alt its successors, administrators executors and assignees) have submitted a quotation Reference No. ---------- and Bidder having agree to furnish as a conditions precedent for participation in tender as unconditional and irrevocable bank guarantee of Rs---------- (Rupees ---------- Only) for the due performance of Bidder's obligations as contained in the terms of the Notice inviting tender and other terms and conditions contained in the tender Documents supplied by the CDAC specially the conditions that (a) bidder shall keep his bid open for a period of day i.e. from ---------- to ---------- or any extension thereof, and shall not withdraw or modify it in a manner not acceptable to the CDAC (b) the Bidder will execute the contract, if awarded, and shall furnish performance guarantee in the format prescribed by the CDAC within the required time. The Bidder has absolutely and unconditionally accepted these conditions. The CDAC and the Bidder have agreed that tender document is an offer made on the condition that the bids, if submitted would be kept open in its original form without variation or modification in a manner not acceptable to the CDAC for a period of ---------- days i.e. from ---------- to ---------- or any, extension thereof and that submission of the bid itself shall be regarded as an unconditional and absolute acceptance of the conditions, contained in the tender documents. They have further agreed that the contract consisting of tender documents as the OFFER and submission of the bids as the ACCEPTANCE shall be a separate contract distinct from the contract which will come into existence when the bid is finally accepted by the CDAC. The consideration for this separate initial contract preceding the main contract is that the CDAC is not agreeable to sell the tender documents to the Bidder and to consider the tender to be made except on the condition that the bids shall be kept open for the period indicated above and the Bidder desires to submit bid on this condition after entering into this separate initial contract with the CDAC promises to consider the tender on this condition and Bidder agrees to keep this bid

open for the required period. These reciprocal promises form the CONSIDERATION for this separate initial contract between the parties.

2. Therefore, we ---------- registered (indicate the name of Bank) under the laws of ---------- having Head/ Registered Office at (hereinafter referred to as the "Bank") which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators and executors hereby issue irrevocable and unconditional bank guarantee and undertake to pay immediately on first demand in writing Rupees all money to the extent of Rs ---------- (Rupees---------- ---------- only) at any time immediately on such demand without any demur, reservations, recourse, contest or protest and/ or without any reference to the Bidder and any such demand made by the CDAC on the bank shall be conclusive and binding notwithstanding any difference between the CDAC and the Bidder or any dispute pending before any court/arbitrator or any other matter whatsoever. We also agree to give that Guarantee herein the CDAC in writing. This guarantee shall not be determined/discharged/affected by the liquidation, winding up, dissolution or insolvency of the Bidder and will remain valid, binding and operative against the bank.

3. The bank also undertakes that the CDAC at the option shall be entitled to enforce this guarantee, against the Bank as a principal debtor, in the first instance, without proceeding against the Bidder.

4. The bank further agree that as between the bank and the CDAC, purpose of the guarantee, any notice of the breach of the terms and conditions contained in the bid Documents as referred above given to the bank by the CDAC shall be conclusive and binding on Bank, without any proof, notwithstanding any other matter or difference or dispute whatsoever. We further agree that this guarantee shall not be *affected* by any change in our constitution, in the constitution of the CDAC or that of the Bidder. We also undertake not to revoke, in any case, this Guarantee during its currency.

5. The bank agree with the CDAC that the CDAC shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms of the tender or get extension of the validity period from time to time. We shall not be relieved from our liability by reason of any such variation or extension of the validity period or for any forbearance, act of omission and commission on the part of the CDAC or any indulgence shown by the CDAC to the said Bidder or by any such matter or thing whatsoever which under the law relating to sureties, would, but for this provision, have the effect of so relieving us.

6. Notwithstanding anything contained here in above our liability under his Guarantee is limited to Rs. ---------- (Rupees ---------- ---------- only) in aggregate and it shall remain in full force upto ----------(225 days from the date of bid opening) unless extended further from time to time, for such period as may be instructed in writing by M/s ---------- ---------- on whose behalf this guarantee has been given, in which case, it shall remain in full force upto the expiry of extended period. Any claim under this guarantee must be received by us before ----------

- (date of expiry of validity period) or before the expiry of extended period, if any. If no such claim is received by us within the said date/extended date, the rights of the CDAC under this guarantee will cease. However, if such a claim has been received by us within and upto the said date/extended date, all right of the CDAC under this guarantee shall be valid and shall not cease until we have satisfied that claim.

7. In case contract is awarded to the Bidder here in after referred to as "Contractor" the validity of this Bank Guarantee will stand automatically extended until the Bidder furnished to the CDAC a bank guarantee for requisite amount towards performance guarantee for satisfactory performance of the contract. In case of failure to furnish performance bank Guarantee in the format prescribed by the CDAC by the required date the claim must be submitted to us within validity period or extended period, if any. If no such claim has been received by us within the said date /extended date, rights, of the CDAC under this guarantee will cease. However if such a claim has been received by us within the said date/extended date all rights of the CDAC under this guarantee shall be valid and shall not cease until we have satisfied that claim,

In witness where of the Bank, through its authorised officer, has sent its hand & stamp on this ---------- day of ---------- (month & year).

Signature
(Full name in capital Letters)
Designation with bank stamp

Witness No.1

Signature
(Full name and address in capital letters)

Witness No.2

Attorney as per power of attorney
No ----------
Date ----------

Signature
(Full name and address in capital letters)

***** END OF DOCUMENT ******