National E-Governance Services Limited

5th Floor, 'The Estate',
121 Dickenson Road,
Bengaluru – 560 042

REQUEST FOR PROPOSAL

FOR

Providing Data Centre Managed Services

No: NESL/AO/RFP-DCMS/2023-24/1001

27th October 2023

Contents

1. Introduction

NeSL is India's first Information Utility and is registered with the Insolvency and Bankruptcy Board of India (IBBI) under the aegis of the Insolvency and Bankruptcy Code, 2016 (IBC). The company has been set up by leading banks and public institutions. The primary role of NeSL is to serve as a repository of legal evidence by way of contracts as well as the information pertaining to any debt/claim, as submitted by the financial or operational creditor, and verified and authenticated by the parties to the debt.

NeSL invites proposals from prospective Data Centre Operators (DCO), through this "Request for Proposal" (RFP), for "providing Data Centre Managed Services" to run their core IT activities. The objective of the RFP is to identify a managed services partner for providing Data Centre services (end-to-end dedicated infrastructure for network, computer, storage, and security) as envisaged in the subsequent sections. NeSL shall not have any contractual obligation whatsoever which should arise from this RFP process, till signing of Contract with any bidder. The bidders are advised to read the RFP document carefully and furnish the details and documents as sought in the RFP. Bids with shortage of proper solution/supporting documents shall be treated as non-responsive and shall be liable to be rejected.

2. Contact Information

National E-Governance Services Limited
5th Floor, 'The Estate',
121, Dickenson Road,
Bengaluru – 560 042
E-Mail: dcrfp@nesl.co.in

3. Key Events & Dates

Event	Target Date
Publishing of RFP	27th October-2023
Last date to send in requests for clarifications on the tender document (pre-bid queries)	2nd November 2023, 18:00 Thursday
Date of pre-bid meeting(on-line)	3rd November 2023, 11:00 Hrs. Friday
Response to Pre-Bid Clarifications / Corrigendum (if any, on the website)	10th November 2023 18:00 Hrs. Friday
Last date and time of submission of bids	27th November 2023, 15:00 Hrs. Monday

Date and time of opening of "Technical Bids"	27th November 2023, 15:30 Hrs. Monday
Place of opening of technical bids	Online (MS Teams meeting invite shall be sent to participated bidders)
Date and time for Technical Presentation and opening of Commercial bids	Will be intimated later to technically qualified bidders
Tender Fee	Rs. 1180/- via On-line transfer, UTR number to be shared along with the technical bid.
Bank Details	Beneficiary: National E-Governance Services Ltd Bank: Canara Bank Branch: Cantonment Branch, Bangalore Account number: 0404214000030 IFSC Code: CNRB0000404

4. Submission of Bids

a. The bidding process shall be based on 'Two Bid' system. The bid should be submitted through e-mail to dcrfp@nesl.co.in with "1001-BID" as part of the subject line within the specified date and time. The Technical and Commercial bids should be submitted as two separate files (Zip file) properly named as "1001-BID <Bidder Short Name> Technical Bid" and "1001-BID <Bidder Short Name> Commercial Bid" in the email attachment. **Both Technical and Commercials bid files (zip) must be password protected, with separate passwords for Technical and Commercial bids. The un-protected bids shall be rejected.** The bids received without required attachments (Technical bid and Commercial bid) or received after the last date and time of submission as specified in "Key Events & dates" shall be rejected. The bidders shall ensure timely submission and may please note that NeSL cannot be held responsible for any delay in email delivery within the stipulated time.

b. It may be noted that the size of a single email should not exceed 20 MB. In case the bid document size exceeds 20 MB, the bidder needs to send the bid documents using more than one e-mail, with proper naming convention 1001-BID <Bidder Short Name> Additional Technical Bid 01-03", "1001-BID_Additional_Technical Bid 02-03", "1001-BID_Additional_TechBid 03-03" etc.

c. The bidder is advised to submit the duly protected editable (Word or Excel) files of the solution documents of technical bid as well, along with the pdf files of the same. The editable files of annexures and documents in support of eligibility criteria need not be submitted. In case of any anomalies between editable document and pdf document, content of pdf document shall prevail.
d. The commercial bid with the password protected zip file should be shared in both pdf and excel formats. Bidders shall only use the excel file format (**Section-V.xlsx**) provided by NeSL to fill in the details. In case of any anomalies between editable document and pdf document, content of pdf document shall prevail.
e. Bidder shall provide detailed split-up BoM of all components with make and model, compliance statement with respect to technical requirements along with reference pages to the supporting technical documents, diagrams of proposed architecture along with technical bid.
f. Successful bidder shall further submit a detailed LLD (Low level design) along with schematic, IP addressing, security policies, capabilities of the proposed solutions etc. within 15 days from the date of issuance of PO.

5. Pre-Bid Meeting/Clarification on RFP

Any clarification sought on the RFP shall be sent through e-mail to dcrfp@nesl.co.in with "**1001-QUERY**" as part of the subject line, latest by the date and time specified in "Key Events & Dates". Any query received post last date specified shall not be entertained and NeSL reserves the right to respond to such queries.

6. Bid submission checklist.

The Bidder shall provide a filled checklist as per the template given below, to ensure that minimum required documents are placed in the bid.

Sl. No	**Documents to be submitted**	Submitted (Yes/No)	Remarks, if Any
A. Technical Bid (Eligibility Criteria)			
1	Demand Draft /On-line transfer receipt for Rs. 1180/- towards document processing fee		
2	Covering letter for "Technical Bid" as per **Annexure -1**		Signed by authorized signatory.
3	Authority Letter **(Annexure – 2)**		
4	Earnest Money Deposit (EMD) 2% of Bid Value		As per format given in **Annexure – 3**
5	The registration certificate as per Companies Act 1956 / 2013 or Limited Liability Partnership Act, 2008 issued by competent authority, along with the		Certificate of Registration issued by Registrar of companies/competitive authority, along with copy of memorandum and

	copies of Memorandum and Articles of Association.		articles of association to be attached.
6	The Bidder to provide an undertaking on his letter head that all the technical requirements highlighted as part of Technical Scope are covered in totality in the proposal submitted by the bidder.		Letter of confirmation from the authorized representative of the bidder (self-certified letter)
7	GST registration certificate.		Self-certified copy
8	Audited Financial statements for the financial years 2020-21, 2021-22 and 2022-23 as applicable.		In support of eligibility requirement stipulated at para 1(3), Section – II.
9	The bidder should have a positive net-worth in the last three financial years.		The document should support eligibility requirement stipulated at para 1(4), Section – II.
10	The Bidder shall submit valid certifications for the following: a) ISO 27001:2013/2022 b) ISO 20000:2018 All the above certificates are mandatory.		ISO Certificates.
11	Copies of at least 03 Purchase Orders / Customer certificates for providing managed Data Centre services to Government/PSU/Scheduled Banks received in past 3 years along with Name and contact details of customer representative.		The documents should support eligibility requirement stipulated at para 1(6), Section – II. The customer who has issued the PO should be visible. A letter from authorized representative of the company in terms of status of execution of the PO should be enclosed (Not yet started/ Completed / Progress and billed)
12	a) Copy of valid certification towards Rating 3/ Tier-3 or above (TIA-942/Uptime as the case may be) of the DC Facility. b) Undertaking to renew the certifications whenever due, during the entire duration of the contract.		a) The documents should support eligibility requirement stipulated at para 1(7), Section – II. b) Free format undertaking

13	An undertaking on the stabilized operations of the proposed datacentre facility for at least 24 months prior to date of submission along with supporting documents (Customer certificate, DC reports etc.)		Undertaking in own format
14	The geographical location of the proposed Data Centre facility should be within 100 kms of Mumbai zero point.		Self-certification supported by reliable map data like Google Earth
15	Undertaking on availability of server farm/s (currently being in operation) in more than one floor in the proposed datacentre facility along with copy of the civil layout of the proposed Data Centre facility, clearly depicting the floors and room segregation details (Server farm, Network, SOC, Monitoring, BMS, Meet-Me, Telco/WAN etc.), to show facility for two operating server farms.		Undertaking in own format
16	Supporting document to prove that the premises where the proposed datacentre is located is either be owned by the bidder or is having a lease/rent agreement for use of said premises for said purpose, valid for at least ten years from date of submission of bid.		Copy of ownership document or relevant pages of registered Lease agreement
17	A self-certificate confirming an uptime of at least 99.982% for the past 3 years, for the datacentre facility.		Self-certificate confirming in own format.
18	The existing MSP company or its subsidiaries are not eligible to participate in this bid		Self-certification
B. Technical Bid (Technical Solution)			
1	Technical proposal shall be prepared and submitted in reference to the technical details of the solution stipulated at para 2(4), para 2(5) and para 2(6) of Section – II.		Statement of confirmation in own format.
2	Compliance statement as per format given in **Annexure – 4.**		Signed by authorized signatory.
3	Submission of relevant documentation for each of the items at serial number 1 to 6 of "***Table: Evaluation Matrix of section-II (General conditions of contract)***"		Confirmation by authorized signatory in free format that information submitted is complete, accurate and validated by relevant authorities/ subject matter experts.

4	Commercial Bid with value/price information masked		
C: Experience & Support Infrastructure			
1	The Bidder or Bidder's Parent Company (In case bidder is a majority owned subsidiary of parent company) must have provided DC or DR to at least 10 Companies in India.		Copy of the credential Letter or Copy of Purchase order from Companies hosting DC/DR sites at the Service Provider's data centre facility.
D: Commercial Bid			
1	**As per format given in Section – V**		

7. Withdrawal or modification of Bids

The bids submitted can be withdrawn at any time prior to the last date and time of submission of bids. The bidder must submit a request in writing in case they wish to withdraw their bid. NeSL reserves the right to permit such a withdrawal of bid. Bidder may re-submit their bid if required, on or before the last date of submission of bids. However, the bidders can use this facility not more than two times. Bids cannot be modified or withdrawn after the Closing Time as indicated in Key Events & dates section above.

8. Opening of Bids

❖ Technical Bid opening

NeSL shall send invite to all participants in the RFP to participate in the Online Technical bid opening. The bidder shall share the password for the "Technical Bid" submitted as attachment to the email in Zip file, through online chat or in person during "Technical Bid" opening session. The response shall be briefly captured and displayed to the participating bidders. Representatives of the participating bidder, with prior intimation shall only be allowed to participate in the "Technical Bid" opening session. It may be noted that, if for any reason, the password protected file of a bidder could not be opened, the bid will be disqualified. All the participant bidders/representatives shall mandatorily participate in the "Technical Bid" opening session (Online) during the stipulated time. The bid of a non-participating bidder during the opening meeting shall be treated as a non-responsive bid and hence will not be processed further.

❖ Commercial Bid Opening

The invitation for participating in the Commercial bid opening (Online) session shall be shared only to those bidders who are qualified in the evaluation of their technical bids submitted. The date and time of "Commercial Bid" opening shall be finalized, after the "Technical Bid" evaluation. The bidder shall share the password for the "Commercial Bid" submitted as attachment to the email in Zip file, through online chat or in person during "Commercial Bid" opening session. The response shall be captured in brief and displayed to the participating bidders. Representatives of the

participating bidder, with prior intimation shall only be allowed to participate in the Commercial bid opening session. All the technically qualified bidders/representatives shall mandatorily participate in the Commercial bid opening session (Online) during the stipulated time. The bid of a non-participating bidder during the opening meeting shall be treated as a non-responsive bid and hence will not be processed further.

9. Bid Validity

Bids shall be valid for a minimum of 180 days from the date of submission. A bid valid for a shorter period shall be rejected. NeSL may ask for the bidder's consent to extend the period of validity keeping the prices and terms & conditions unchanged. Such request and the response shall be made in writing only.

10. Amendment and Cancellation of RFP

a. At any time prior to the last date/time for submission of bids, National E-Governance Services Limited for any reason, whether on its own initiative or in response to the clarification/request by a prospective bidder during pre-bid meeting, may amend the Eligibility criteria, Commercial terms and conditions, Scope of Supply, Technical specifications etc. stipulated in this document.

b. The amendments to the RFP documents, if any, will be notified by release of Corrigendum Notice on the website of NeSL. The amendments/ modifications will be binding on the bidders.

c. National E-Governance Services Limited at its discretion may extend the deadline for the submission of bids if it is necessary to do so or if the bid document undergoes changes during the bidding period.

National E-Governance Services Limited reserves the right to cancel the entire RFP without assigning any reasons thereof.

(End of Section – I)

1. Bidder Eligibility Criteria

The bidder must possess the requisite experience, strength, and capabilities in providing the services necessary to meet the requirements, as described in the RFP document. The bidder must submit the documents as listed at **para 6, section – I** and the bids must be complete in all respect covering the entire scope of work as stipulated in the RFP document. The invitation to bid is open to all bidders who qualify the eligibility criteria as given below:

Sl. No	Clause	Documents required
1	The Bidder should be registered under Companies Act, 1956/2013 or Limited Liability Partnership Act, 2008 and should be in existence for minimum 5 years in India.	Copy of the Certificate of incorporation or registration issued by the competent authority.
2	The bidder should have valid GST registration for the services offered.	Copy of valid GST registration certificate.
3	The bidder's average turnover for the last 3 years shall be at least Rs 50 Crores from datacentre services. Last three (3) financial years means, FY 2020-2021, 2021–2022, 2022-2023.	The copies of audited financial documents for the last three financial years.
4	The bidder should have a positive net-worth in the last three financial years.	A certificate from a Chartered Accountant certifying positive net-worth of the bidder for last three financial years.
5	The bidder firm should be ISO 27001:2013/2022 and ISO 20000:2018 certified.	Copy of the valid certifications to be submitted along with the technical bid.
6	The bidder should have (i) received a minimum of 3 orders in the past 3 years for providing services similar to the services asked for in this RFP. (ii) and should have provided service for at least 2 years for at least one such order	Relevant documents such as PO copy/Customer certificate shall be submitted along with technical bid. The names and contact details of these three clients shall be provided.

7	The offered datacentre should have either Uptime Institute Tier III (minimum) Certification of Constructed Facility OR TIA 942 certification with rating 3 (minimum) for the constructed facility valid over the entire contract period. The said certificates must have been issued in the name of the bidder.	Copy of Valid certificate (Uptime/ TIA-942). In case of validity getting expired during the envisaged project duration, the Bidder shall submit an undertaking to renew the same in due course.
8	The DC infrastructure from which the services are offered should be in stabilized operations for at least 24 months prior to date of submission.	An undertaking from the bidder along with supporting documents.
9	The geographical location of the proposed Data Centre facility should be within 100 kms of Mumbai zero point.	Self-certification supported by reliable map data like Google Earth.
10	The proposed Data Centre facility should have server farm/s (currently in operation) on more than one floor.	Undertaking by the bidder along with copy of the civil layout of the proposed Data Centre facility, clearly depicting the floors and room segregation details (Server farm, Network, SOC, Monitoring, BMS, Meet-Me, Telco/WAN etc.)
11	The premises where the proposed data center is located should either be owned by the bidder or must have a lease/rent agreement for the use of said premises for said purpose, valid for at least ten years from date of submission of bid.	Supporting document for the same.
12	The proposed DC infrastructure from which the services are offered should have uptime of at least 99.982% for the past 3 years.	A self-certificate to this effect issued by authorized signatory should be submitted.

13	The bidder must not be blacklisted/banned/debarred due to non-performance, by any Department/Office of the Government of India or of any State Government, Public Sector Undertaking, Autonomous Organization of Government of India, as on the date of submission of the bids and that there must not be any regulatory action initiated /pending against them as on the date submission of the bids.	Undertaking by the bidder given in the covering letter.
14	The bidder must quote for all the line items given in the price schedule. Failure to do so shall lead to disqualification of the bid.	Commercial Bid with value/price information masked **(Bidders who reveal price in technical bid will be disqualified)**
15	The existing MSP company or its subsidiaries are not eligible to participate in this bid	Self-certification

2. Technical Bid evaluation

The technical bids will be evaluated by the Technical (TEC) Evaluation Committee duly constituted by the competent authority. The technical bids will be evaluated in two steps.

i. The bids will be examined based on eligibility criteria stipulated in **Section- II –** Bidder Eligibility criteria, to determine the eligible bidders.
ii. The technical bids of only the eligible bidders shall be further evaluated based on evaluation. The method is given below.
iii. The bidders must use the format included in the RFP document. Tender documents submitted in different formats may lead to outright rejection of the bid.

Bidders to note: The minimum cutoff for further consideration of your bid for commercial evaluation is a score of 70% across each of the following evaluation parameters, as well as an overall score of 75%.

Table : Evaluation matrix:

Sno:	Parameter	Supporting Document	Maximum Marks	Marking Criteria
01	Business Turnover: The bidder's average turnover for the last 3 years shall be at least Rs 50 crores from datacentre services. Last three (3) financial years means, FY 2020-2021, 2021–2022, 2022-2023.	The copies of audited financial documents for the last three financial years.	15 Marks	Annual turnover for prescribed 3 years will be taken into account and marks will be given as follows: a) Rs. 50 – Rs. 500 Crore: 12 marks. b) >Rs. 500 crores: 15 marks
02	Business Operation: The DC infrastructure from which the services are offered should be in stabilized operations for at least 24 months prior to date of submission.	An undertaking from the bidder along with supporting documents.	15 Marks	a) 24 months to 60 months: 12 marks. b) > 60 months: 15 marks.
03	The bidder should have received a minimum of 3 similar orders in the past 3 years for providing managed Data Centre service, each of such orders should be from a distinct customer.	Relevant documents such as PO copy/ customer satisfaction certificate shall be submitted along with technical bid. The names and contact details of customers shall be provided.	15 Marks	a) Similar projects (3 to 7 Orders): 12 marks. b) Similar projects (8 Orders & above): 15 marks.
04	Technical solutioning for this RFP requirement: a) Compute infrastructure including network and storage	Bidder to provide the following: High level design	10 Marks	Based on assessment

	b) Security infrastructure	document BoQ, Make, Model, split-up part no		
05	Approach and methodology for Compute infrastructure including network and storage. a) Implementation b) Configuration, integration with existing DC c) Acceptance testing (AT) d) Commissioning	Bidder to describe in detail the following but not limited to: Project implementation plan, High level network design, service management procedures, data replication plan, DR drill, switch back plan, solution for replication of MySQL and NFS. Any other dependencies anticipated from existing MSP provider.	10 Marks	Based on assessment
06	Approach and methodology for security a) implementation b) configuration c) acceptance testing (AT) d) commissioning	Bidder to describe in detail the following but not limited to: Approach to entire security framework, vulnerability management, Threat intelligence feeds, handling of security events and response, dashboards and	10 Marks	Based on assessment

		reporting mechanism, plans for replicating network and security configurations from existing DC including but not limited to firewall, WAF, PAM, AD, SIEM etc. Any other dependencies anticipated from existing MSP provider.		
07	Technical Presentation on overall understanding of Scope of Work.		25 Marks	As recommended by the Technical Evaluation Committee as per the Evaluating criteria of areas specified in Scope of Work and Technical Bid

Note: All experience calculations will be in reference to the date of release of RFP.

Technical Presentation:

Sr. No	Particulars	Marks
1	Understanding of the project requirements	5
2	Project Implementation Plan with Manpower deployment	5
3	Overall Technical solution, approach, and methodology	15

As part of the evaluation process, bidders are required to provide a presentation to the Technical Evaluation Committee (TEC) to explain their proposed solution highlighting key aspects, covering the scope, technical requirements and specifications detailed out in Section IV. The TEC may request additional documents or information from bidders during the evaluation process if needed. The TEC is authorized to address any deviations as necessary.

The commercial bids of only technically qualified bidders will be opened, and they will be duly informed in writing about the schedule.

3. Evaluation of Commercial Bids:

The "Price Schedule: - **Section-V** stipulates the base configuration requirements of Virtual Machines/Servers, network components/bandwidth and storage capacity.

This is based on the initial requirement during the first year of the contract. Over the years, the requirement is expected to increase. However, the prices quoted will be computed and compared for numbers and configurations as given in "Price Schedule". This price will be taken for deriving and evaluating the Lowest Quoted (L1) bidder. NeSL is under no obligation to grant the contract only based on pricing as a criterion to the lowest bidder. NeSL reserves the right to make the final decision regarding the final declaration of the successful Bidder. If more than one technically qualified bidder quotes the same lowest price, the bidder having the highest technical score among these shall be the successful bidder. If more than one bidder happens to achieve the same technical score and quote the same lowest price, NeSL reserves the right to declare the successful bidder by application of its discretion by a team of experts.

NeSL reserves the right to award the contract for appropriate numbers and configurations for any particular year, depending upon the requirement.

The bidders are required to quote the prices strictly as per the Price Schedule given, enabling NeSL to arrive at an appropriate price for required configurations and/or requirements.

The bidders must also ensure that the Commercial Bid does not contradict the Technical Bid in any manner.

4. Award of Contract and Release of Payment:

The contract will be awarded, and payments will be released by

National E-Governance Services Ltd.
5th Floor, 'The Estate', 121,
Dickenson Road, Bengaluru – 560 042
e-mail - dcrfp@nesl.co.in www. nesl.co.in

(End of Section – II)

1. Contract:

   a. Formal contract shall be executed with the successful bidder based on this RFP.
   b. The initial period of contract for providing the Datacentre Services will be for five (5) years. The complete IT set up as desired under this RFP must be made fully operational and ready to commence NeSL's services within eight weeks from the date of the award of the contract, failing which NeSL reserves the right to levy penalty as stipulated under SLA & Penalty section below.
   b. The period of contract can be further extended with mutually agreed terms and conditions subject to satisfactory performance of the entire contract.
   c. The selected bidder shall also extend the same terms and conditions, prices, service level agreement to existing and future subsidiaries of NeSL if and when desired by NeSL. Suitable amendments to the contract shall be made to the contract as and when required.

2. Prices:

   a. The prices for the services to be rendered must be quoted in INR only.
   b. The bidder must quote for all the items listed in Price Schedule, **Section – V,** failing which the bid will be rejected.
   c. Prices must be quoted in the **excel attachment only as per format given in Section-V.** PDF of the same to be shared part of the secured zip commercial bid file.
   d. The prices quoted must include all the costs/charges including - but not limited to, manpower costs, fuel and energy charges, repairs and maintenance charges of the facility, communication charges, license fees (if applicable), back-to-back support arrangements with OEM/Software publisher, royalties, rent (if any), insurance, handling charges, incidental charges etc.
   e. The prices shall be inclusive of all management/monitoring costs of the devices listed in Price Schedule (**Section – V).**
   f. The rates and amounts of applicable taxes should be quoted separately.
   g. In case of change in Government statutory taxes/ duties, the taxes and / or duties applicable as on date of invoice will be paid.
   h. The UNIT prices quoted must remain firm till the entire contract period as per the submitted commercial bid.

3. Security Deposit (SD):

   The successful bidder shall furnish non-interest-bearing Security Deposit for (Ten) 10% value of the initial contract within 15 days from the date of issuance of PO.
   The security deposit should be submitted either in the form of Demand Draft/s or Irrevocable Bank Guarantee (BG) or Electronic Bank Guarantee (eBG) issued by a Scheduled Commercial Bank as per the format attached – Ref Annexure 5, in the name of National E-Governance Services Limited.

The successful bidder may submit one instrument of suitable denominations, towards SD. The BG/s submitted must remain valid for 61 months from the date of submission. The BG should have a claim period of one year beyond the validity of the BG.

If the SD is submitted in the form of BG, the BG must be payable at a bank branch in Bengaluru.

NeSL shall have the right to treat the Security Deposit as forfeited, if the bidder is unable to fulfil obligations as stated in the Contract, or the Service Level Agreement (SLA) (to be signed separately). NeSL will not pay any interest on the Security Deposit amount.

The Security Deposit will be returned to the bidder within 30 days of contract expiry, after deducting the penalties/ due amounts (if any)

4. Warranty and Technical support:

   All the software/hardware components in the proposed solution shall be covered under warranty/AMC/ATS along with back-to-back support from OEM /OSP (original software publisher) throughout the contract period and shall not be declared end of support/service by the OEMs/Original software publishers for a period of minimum 5 years from the date of submission of bids.

5. Insurance:

   The datacentre and IT infrastructure that shall be offered to NeSL shall be covered under comprehensive insurance of adequate value by the successful bidder against all risks of loss or damage, at their cost. However, merely acquiring insurance policy shall not absolve supplier from their responsibility and liability of replacing systems/equipment in the event of loss/damage/misplacement etc., irrespective of whether it is covered by the insurance policy or not.

6. Payments:

   a. No advance payments shall be made.
   b. Payment towards installation and configuration charges (as appearing in column No. 13 of price schedule), of the tool shall be paid within 60 days of installation, completion of user acceptance tests that may include an audit by third party or audit by NeSL, completion of training, successful implementation, and configuration of said solution.
   c. The payments for providing datacentre services will be released on a QUARTERLY basis at the end of every quarter.
   d. The invoices for the services provided in the preceding three months must be submitted within 15 days of the end of the third month. The amount payable will be by NeSL, and payments shall be released within 45 days of submission of invoices subject to approval of same by NeSL.
   e. Applicable TDS / TCS will be deducted. GST payment on invoice only on submission of valid invoice with credit to GSTR 2A of NeSL.

f. In the event of any dispute with respect to the invoice amount, the said period of 45 days to make the payment of the invoice shall commence from the date of settlement of the dispute by the successful bidder.
g. The amount shall be remitted by NEFT/RTGS directly to the bank account of the successful bidder, i.e., the successful bidder.

Note: The payments will be released only against complete and valid Tax Invoice/s (mentioning GST registration number), along with all relevant documentation.

7. SLA & Penalty:

a) Service delivery:

1) One-time installation and configuration services shall be completed within 8 weeks of the date of award of the contract.
2) Request for scaling of services pertaining to number and configuration of VMs, storage space, network bandwidth, shall be honored within 10 days of intimation from NeSL. If any deviation/delay is anticipated, the service provider shall seek formal prior approval from NeSL.
3) Request for provisioning any additional physical device that may require procurement, shall have to be completed within eight weeks from the date of issuance of PO.
4) The infrastructure requirements and all the services under this RFP shall be up and running on 24x7 basis within 8 weeks of date of award of contract.
5) As part of security monitoring, the service provider shall provide intelligence about the potential security threat/vulnerabilities, new global security threats/Zero-day attacks in circulation to the designated NeSL official/s and suggest suitable counter measures to safeguard against such evolving threats/attacks along with analysis and its mitigation. The advisories should be customised to NeSL Infrastructure. Details pertaining to status of such actions shall be reported immediately for severity 1 and 2 cases in addition to the comprehensive monthly service report by service provider.
6) Report on recommendations regarding enhancement of infrastructure including security of NeSL should be part of the monthly report.

b) Penalties:

NeSL reserves the right to levy a penalty in case the performance/ service parameters do not meet the stipulated conditions and/or timelines, as stipulated in table given below.

i.Service Delivery Penalty:

Sr. No	*Particulars*	Penalty
A	**Penalty for Delayed Services**	
1	Delay in commencement of the services beyond 8 weeks of award of contract	Rs. 10000/- Per calendar day of delay
2	Delay in scaling of services pertaining to number and configuration of VMs, storage space, network bandwidth, within 10 days of intimation from NeSL. (In case the requirement results in deploying a new physical device, bidder shall fulfil the same within 8 weeks.)	Rs. 5000/- Per calendar day of delay
3	Delay in provisioning any additional new physical device within eight weeks from the date of issuance of any subsequent PO.	Rs. 10,000/- Per calendar day of delay

ii. Penalty for not meeting up-time requirements:

A	**Infrastructure Availability (all devices under the managed services) (Time measured in hours on monthly basis)**	
1	Less than 99.982 but more than 99.9 %	5 % of Monthly Service Charges
2	Less than 99.89 % but more than 99.8 %	7.5 % of Monthly Service Charges
3	Less than 99.79 % but more than 99.7 %	10 % of Monthly Service Charges
4	Less than 99.69 % but more than 99.6 %	12 % of Monthly Service Charges
5	Less than 99.6 %	50 % of monthly Service Charges. NeSL reserves the right to cancel contract
B	**Internet Availability (Time measured in hours on monthly basis)**	

1	Less than 99.982 but more than 99.9 %	5 % of Monthly Service Charges
2	Less than 99.89 % but more than 99.8 %	7.5 % of Monthly Service Charges
3	Less than 99.79 % but more than 99.7 %	10 % of Monthly Service Charges
4	Less than 99.69 % but more than 99.6 %	12 % of Monthly Service Charges
5	Less than 99.6 %	50 % of monthly Service Charges. NeSL reserves the right to cancel contract

iii.Priority Level Classification:

Priority Level	Classification
Priority 1/ Critical	Any incident that inhibits NeSL's ability to provide service due to underlying Network, Security, Server, Storage issues
Priority 2 / High	Any incident that may potentially lead to service impact such as one of HA device not functioning, one of the disks in RAID configuration is faulty etc) or service requests such as IP whitelisting, blacklisting etc.
Priority 3/ Low	Any other service request not covered above such as Backup Integrity check, Patching/ Maintenance activities etc

iv. Incident / Service Request Management SLA:

Incident Management SLA	Critical (P1)	High(P2)	Low (P3)
Response Time	15 Minutes	30 Minutes	30 Minutes
Resolution Time	Within 45 minutes of call logged	Within 90 minutes of call logged	Within 1 calendar day of call logged
Service Window	24 x 7	24 x 7	24 x 7
Measurement Window	Monthly	Monthly	Monthly

v.Penalty for breach of Resolution Time SLA:

Priority Level	Applicable Penalty
Critical	Fixed Fee: Rs.20000 per hour beyond 45 minutes
High	Fixed Fee: Rs.10000 per hour beyond 90 minutes
Low	Fixed Fee: Rs.5000 per hour beyond 24 hours

Note:

"The total amount of such penalties levied shall not exceed 10% of the "Monthly Support Cost" which is defined as the invoice amount raised for the respective month for which the penalty is being calculated."

If the computed penalty, exceeds more than 10% of the "Monthly Support Cost" in two instances during the contract period, NeSL reserves the right to cancel the contract.

8. Completeness Responsibility

Offer from bidder must be complete in all respects to comply with all the requirements and specifications as detailed out in the entire RFP document, whether some items are specifically mentioned or not, but required to comply with the overall requirements, quality, quantity and other features of the services.
Notwithstanding the scope of work, engineering, supply and services stated in the RFP document, any equipment, item, material, services, licenses, technical data, engineering or technical services etc., which might not have been specifically mentioned under the scope of supply of this RFP and which are not expressly excluded from the RFP, but which are necessary for the performance of the quoted solution to comply with the specifications, will be treated to be included in the bid and will have to be provided (and /or performed) by bidder, at no extra cost to NeSL.

9. Change Request

a) The Service Provider agrees that the requirements given in the RFP are broad requirements and are in no way exhaustive and may be modified at the sole discretion of Client, without any change in time or cost to Client.
b) It shall be the responsibility of the Service Provider to meet all the requirements of technical criteria contained in the RFP or this Agreement and any upward revisions and / or additions of quantities / specifications / sizes given in specifications etc. of the Bid required to be made shall not constitute a Change Order and shall be carried out without any time and cost effect to NeSL.
c) Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the specification etc. of the Bid, which the Service Provider had not brought to NeSL's notice at the time of the Bid, shall not constitute a Change Order and such upward revisions and/or addition shall be carried out by Service Provider without any time and cost

effect to Client.

d) Any upward/downward revision in the quantities of items in Section-V shall not constitute a Change Order and shall be carried out by the Service Provider at respective Unit Prices quoted in the bid document. NeSL will select the appropriate number and configuration depending on their requirements for a particular period and this period will last for a minimum period of one month.

e) The Change Order will be initiated only in case:
   i. NeSL directs the Service Provider in writing to include any addition to the Scope of work covered under this Agreement or delete any part of the Scope of work under this Agreement; or
   ii. The Service Provider requests to delete any part of the work which will not adversely affect the implementation of the Scope of Work under this Agreement and if the deletions proposed are agreed to by NeSL and for which, cost and time benefits shall be passed on to NeSL; or
   iii. NeSL in writing directs the Service Provider to incorporate changes or additions to the technical criteria requirements under this Agreement.

f) Any changes reasonably required by Client over and above the minimum requirements given in the Scope of work included in the RFP, before giving its approval to detailed design for complying with technical criteria and changes required to ensure systems compatibility and reliability for safe (as per codes, standards and recommended practices referred in the RFP, Bid) and trouble free operation shall not be construed to be change in the Scope of Work under this Agreement. In case of a change in codes and standards, post submission of the bid which increases the cost-of-service delivery, Client and Service Provider shall arrive at a mutually agreeable additional contract price to Service Provider. Service Provider shall be required to implement such a change only after the additional contract price is agreed to in writing by both the Parties.

g) Any Change Order comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the subject of an amendment to this Agreement by way of an increase or decrease in the Contract Price prescribed hereunder and adjustment of the implementation schedule, if any.

h) If there is a difference of opinion between the Service Provider and Client Representative whether a particular work or part of the work constitutes a Change Order or not, the matter shall be handled in accordance with the procedures set forth as per clause 10 - 'Procedures for Change Order' subject to the Contact/Agreement to be signed between NeSL and the Successful Bidder.

i) Within 14 working days of receiving the comments from Client on the specification, purchase requisitions and other documents submitted by the Service Provider for approval, the Service

Provider shall respond in writing, which item(s) of the comments is/are potential changes(s) in the Scope of Work covered in this Agreement and shall advise a date by which Change Order (if applicable) will be submitted to Client.

10. Procedures for Change Order

Procedure for Change Order shall be discussed and documented in the Contract/Agreement to be signed between NeSL and the successful bidder.

11. Force Majeure

NeSL may consider relaxing the penalty and delivery requirements, as specified in this document, if and to the extent that, the delay, non- performance, short performance, in services or other failure to perform its obligations under the contract, is the result of a Force Majeure. Force Majeure is defined as an event or effect that cannot reasonably be anticipated such as acts of God (like earthquakes, floods, heavy rains, 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. In view of the business criticality of the services, pandemic, epidemic and subsequent lock-down due the same shall not be treated as force majeure.

12. Arbitration

In case any dispute arises between NeSL and successful bidder with respect to this RFP/ contract, 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 appointed on mutual agreement between NeSL and the successful bidder. 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 and seat of the arbitration shall be Bengaluru. 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 be borne by the party as the arbitrator may decide. Subject to the above, the parties agree to submit to the exclusive jurisdiction of the Courts in Bengaluru in respect of any dispute or claim between the parties under this RFP or the subsequent contract. The applicable Courts in Bengaluru shall have the jurisdiction to execute the award, if need be.

13. Indemnity

The successful bidder shall indemnify, protect and save NeSL from/against all claims (financial, legal and other), losses, costs, damages, expenses, action suits and other proceeding, resulting from any one or more of the following cases during the Contract period pertaining to this project,

a. any damage / loss to infrastructure for the reasons not attributable to NeSL.
b. infringement of any law by the service provider or their employees / staff (own or outsourced) deployed by them, pertaining to intellectual property, patent, trademarks, copyrights etc, of NeSL.
c. any claims by a third party, other statutory infringements in respect of the DC/DR sites and services provided by successful bidder.
d. breach of confidentiality and/or information security obligations under this RFP, the subsequent contract, and/or the applicable law.
e. failure by the service provider to perform its duties or failure to abide by the terms and conditions of this RFP and/or the subsequent contract.
f. infringement of the Information Technology Act, 2000 or any applicable law by the successful bidder or the staff employed by the successful bidder.

14. Confidentiality

The successful bidder and/or their personnel or staff employed by the successful bidder shall not, either during the term or after expiration of contract under this RFP, disclose any information relating to the services, contract, business, or operations, etc. of NeSL, without the prior written consent of NeSL.

The bidder and/or their personnel shall not, either during the term or after expiration of this contract, undertake any public communication, press/media releases relating to the services, contract, the business or operations, brand name etc. of NeSL, without the prior written consent of NeSL.

NeSL reserves the right to determine the manner any disclosure or communication may be made by the successful bidder regarding the services, contract, the business or operations, etc. of NeSL.

Information already available on public domain is excluded from the confidentiality clause.

The successful bidder is required to sign a Non-Disclosure Agreement (NDA) for this purpose, at the time of award of the contract.

This document shall not be duplicated, disclosed, or distributed to any third party. The file copy should be held confidential and not used for any purpose other than for bid evaluation, response preparation and subsequent discussions with NeSL. The bidder shall safeguard the confidentiality of this document and any copies with the same degree of care with which it will safeguard its own confidential information.

15. IPR

Any Intellectual Property created by NeSL under this RFP shall solely and exclusively be owned by NeSL.

16. Transition Clause

In the event of failure of the successful bidder to render the services or in the event of termination of the contract or expiry of term or otherwise, without prejudice to any other right, NeSL at its sole discretion may make alternate arrangement for getting the services contracted with another Service Provider. In such case, NeSL shall give prior written notice to the existing Service Provider. The successful bidder, as the existing service provider, shall continue to provide services as per the terms of contract until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistance to the new Service Provider within such period prescribed by NeSL, at no extra cost to NeSL, for ensuring smooth switch over and continuity of services. If existing Service Provider is in breach of this obligation, they shall be liable for paying a penalty of up to 10% of the cumulative "Monthly Support Cost" for the entire duration of transition period.

NeSL is liable to pay for the services provided by the existing service provider till termination, subject to deductions of penalties – if any and statutory payments.

17. Termination

The contract will remain valid till all obligations of the successful bidder, as stipulated in the contract are fulfilled.

The successful bidder acknowledges and agrees that timely performance of all obligations is the essence of contract. In case of any delay, under or non- performance, NeSL will issue a 15 days' notice period to the bidder. If the bidder fails to take satisfactory action to make good the said delay or non-performance, within the notice period, NeSL may terminate/ cancel the contract without assigning any reason. The successful bidder agrees and accepts that they shall be liable to pay damages claimed by NeSL, in the event of termination/breach of terms of this RFP/contract etc. However, in case of termination /cancellation of Contract, the Service Provider cannot absolve their responsibility towards the data and IPR stored in their DC and DR facility and must comply with the requirement stipulated at para 1(q)of Section - III of this document.

The successful bidder may terminate the contract by giving 90 days notice to NeSL only if the payment of the due amount to the bidder is delayed beyond 90 days of due date.

18. Non-Waiver

The failure or neglect by either of the Parties to enforce any of the terms shall not be construed as a waiver of its rights preventing subsequent enforcement of such provision or recovery of damages for breach thereof.

19. Assignment

The Service Provider shall not assign, delegate, or otherwise transfer any of its rights or obligation under this Contract to any third party without prior written permission of NeSL.

20. Severability

Should any provision of this Contract for any reason be declared invalid or un-enforceable to any extent by an order of any court of competent jurisdiction or any arbitral body pursuant to the provisions of arbitration hereof, such decision shall not affect the validity of the remaining provisions of this RFP, while remaining provisions shall remain in full force and effect as if this Contract has been executed without the invalid or unenforceable provisions hereof eliminated. In the event any such provision of the Contract is so declared invalid or unenforceable, the Parties shall promptly renegotiate in good faith new provisions to eliminate such invalidity or un-enforceability and to restore this Contract as near as possible to its original intent and effect.

21. Corrupt or Fraudulent Practices

a. It is expected that the bidders who wish to bid for this project have the highest standards of ethics.
b. NeSL will reject bid if it is observed that the bidder recommended for award of contract has engaged in corrupt or fraudulent practices while competing for this contract.
c. NeSL reserves the right to declare a bidder ineligible, either indefinitely or for a specified duration, if, at any point, NeSL determines that the successful bidder has engaged in corrupt or fraudulent practices during the award or execution of the contract.

22. Interpretation of the clauses in the RFP Document / Contract Document

In case even after clarification during pre-bid meeting and any amendment to RFP thereafter bidder finds any ambiguity/ dispute in the interpretation of any of the clauses in this RFP, the interpretation of the clauses by Managing Director & CEO of NeSL shall be final and binding on all parties.

23. Jurisdiction

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

(End of Section – III)

SECTION - IV – Schedule of Requirements

1. Scope

NeSL currently avails hosting services from a facility located in Hyderabad as a managed service. Through this RFP process, it is proposed to identify a second managed services partner, to provide end-to-end infrastructure and managed services.

The bidder shall work in close co-ordination with the existing Managed Service Partner (MSP) for all relevant activities at all stages of the assignment like design, implementation, testing and ongoing operations. Such activities shall be including but not limited to the following: initial setup & testing, ongoing data replication, DR fail over and failback and any other activities that will enable NeSL to provide seamless high available, secure services to its customers. Where required, NeSL will facilitate co-ordination of such activities with the existing MSP and the prospective MSP.

The bidder shall be required to provision all the required infrastructure facilities (Including Compute, Storage, telecom links, Networking, Security, Hypervisors, OS, DB, any system software etc.) in a dedicated fashion and shall offer managed services of the facility on a 24x7 manner as per the technical requirements provided in this RFP document. Data replication is envisaged to be on IPSEC VPN Tunnel over the internet with appropriate security measures for data protection. The successful bidder shall also provide technical training for 10 resources of NeSL on the solutions offered. The successful bidder shall operationalize the services with required manpower within a period of eight (08) weeks from the date of issue of Contract.

The bidder at his own cost shall get the solution architecture and implementation reviewed by the respective OEM, to ascertain adherence to best practices. Any recommendations shall be remediated by the service provider and closure report from OEM/authorized partner be provided to NeSL within the implementation period. This will be part of the acceptance criteria after which billing shall commence. The above report is required for all security solutions, WAN, LAN, Storage, and compute environment (physical as well as Virtual).

2. General Technical requirements

i. The selected bidder shall create a dedicated IT set up for NeSL in racks dedicated for NeSL. Selected bidder shall provide all IT and security equipment/solutions required in OPEX Model. The required IT and security set up shall be provisioned by the bidder for exclusive use of NeSL. The selected bidder shall ensure that the solution shall work as desired and the bidder is also responsible to supply and install any other components that is inadvertently missed out but required for the overall solution to work, without adding any line item in the Bill of Materials.

ii. The proposed "High Availability" solution shall be deployed in two different floors with distribution of underlying infrastructure with adequate redundancy for all components (other than storage and backup infrastructure). The deployment shall be based on design/layout signed-off by NeSL. In the end state (upon provisioning of additional storage device), NeSL should be able to run operations even if one of the floors in the datacentre becomes non-functional. Above distribution of IT setup should be architected and designed and implemented such that the setup on any given floor is independently operable for business operations as well as monitoring and management of IT and security setup.

iii. The cabling infrastructure shall be on OM5 Fiber components across the floors with modular structure architecture. The proposed solution architecture/layout with required fiber components like Cassette Shelves, Fiber Trunk Assembly between floors etc., to be shared with NeSL ahead of implementation. The implementation should ensure near zero latency variation across floors and the same shall have to be measured and demonstrated by service provider.

iv. The bidder shall ensure that NeSL's infrastructure are hosted in dedicated racks with adequate measures for access control, both physical and logical.

v. The commercials for all Hardware equipment/devices shall include all associated costs such as racking, power, cooling etc up to successful installation and commissioning.

vi. Vendor shall be responsible for all implementations such as creation, configuration, management of IT components stipulated under this RFP, including but not limited to virtual machines etc.

vii. The bidder shall provision CCTV surveillance system for the hosted infrastructure and shall provide facility to capture the footage and provide the same to NeSL on demand. The captured footages shall be stored for a period minimum six months by service provider.

viii. Among other things, the selected bidder shall provide following (i) the details of the monitoring and management tools (ii) the detailed BoQ for Network, Security, backup, storage, and compute elements, and (iii) other required details that fulfils requirement of NeSL.

ix. The bidder shall provide a facility to log and track support calls with visibility to NeSL. Bidder shall also provide support escalation matrix.

x. The selected bidder shall provide security solution services as mentioned in this document including all hardware, software, and storage as part of the solution.

xi. Selected bidder shall provide all services to NeSL as per IT/IS policies of NeSL (such as Data Back-up, Patch Management, Password Policy etc..). The gist of such policies will be shared with the selected bidder. All such services shall be performed in alignment with ITIL service management framework.

xii. New Installation/ configuration/Commissioning – Coordination with all third party Selected by bidder or NeSL shall be the responsibility of the selected bidder.

xiii. The selected bidder shall co-ordinate with NeSL to bring up the systems at the selected site.

xiv. The selected bidder shall provide a complete Managed Hosting solution/services as part of their technical bid. Any activities not mentioned here but required for the

implementation, operation, and maintenance and monitoring of datacentre and IT & security set up shall be the responsibility of selected bidder. The solution provided by the Bidder shall meet all the service level requirements. The Selected bidder shall configure all the components and sub-components for end-to-end user access to all applications/services.

xv. Bidder shall provision dedicated independent switching infrastructure for the management/Out-of-Band (OoB) of computing, networking and security devices.

xvi. Internal traffic should be routed through managed L3 switches and not routed through internet facing firewall as per approved design.

xvii. The selected bidder shall provide necessary services for DC/DR activities.

xviii. Successful bidder shall coordinate with existing DC service provider to facilitate DR Drills broadly covering but not limited to the following.

a. The bidder shall coordinate to make sure the data is in sync.
b. Ensure data replication/reverse data replication to confirm to RPO of 5 minutes pertaining to NFS, MySQL master/slave.
c. Bidder to make sure that the RPO is met throughout.
d. Coordinate with other managed service provider to restore service back to the other site.
e. Any network /address level change as may be required.

xix. DR Drill/actual invocation Plans for switching between NeSL's existing MSPs is to be prepared by successful bidder. DR drills are to be conducted once in every quarter or as required by NeSL.

xx. NeSL reserves the right to conduct audit on its own or through a third-party auditor, for the provisioned infrastructure/services at any point of time by providing an advance intimation of 3 days.

xxi. Selected bidder's overall responsibility shall be to host, maintain, monitor, and support the infrastructure as per Section - IV and to operate hardware, network and security requirements for applications of National E-Governance Services Limited. The selected bidder is required to provide the detailed architectural diagram.

xxii. Selected bidder shall carryout hardening of OS (Operating System), patch management activity and other configuration on OS etc. Selected bidder shall undertake BIOS, OS, etc. upgrade based on CVE/CWE notifications or feeds from Cert-IN/NCIIPC etc and approval by NeSL (during the entire contract period).

xxiii. The selected bidder shall submit a detailed project plan within 15 days from the date of signing of Contract. During implementation phase the selected Service Provider shall submit weekly reports on the progress of the project and the status as on the scheduled date and actual date of each activity detailing any deviation from baseline plan. The selected bidder shall take total responsibility for working out macro and micro level details of the project plan and the requirements while responding to this RFP.

xxiv. During the entire duration of the contract,-National E-Governance Services Limited shall have the exclusive right to access, edit or modify the data /information stored. The details of the modality required for this purpose will be covered in the SLA.

xxv. On expiry/ termination/ cancellation of the Contract, the Service Provider shall willingly and un-conditionally transfer/ handover the data/ information stored in the IT set up to National E-Governance Services Limited, in usable form. The details of the modality/mechanism shall be drawn with successful bidder.

xxvi. The selected bidder should provide L1 support for OS layer (both physical hosts and VMs), Web layer (Nginx), App layer and MySQL Database. List of activities assignable to L1 shall be finalised with successful bidder.

xxvii. The vendor shall review the Capacity utilization for network/security/storage and compute components on a quarterly basis and advise NeSL on the growth trends.

xxviii. Bidder shall provide detailed split-up BoM of all components with make and model, compliance statement with respect to technical requirements for Storage, Server, Firewall, WAF along with reference pages of the supporting technical documents.

xxix. The bidder shall also submit schematic diagram of proposed solution architecture as part of the technical bid.

xxx. **Approximate initial sizing:**

Storage requirement in TB on RAID 6	**200**
Compute requirement	
vCPU	**VRAM**
325	**5TB**
Number of VMs	**38**

Bidder may compute the backup solution storage based on the above initial deployment and factor 20% annual growth.

xxxi. The bidder shall appropriately size and deploy required hardware/software to ensure smooth operation of tools, services, and solutions that are needed for functioning of IT /security setup implemented for NeSL. Such solutions may include but not limited to backup, helpdesk, PAM, HBSS, Active Directory, Antivirus, SIEM, patch management system, VAPT, EMS, AD, DNS, NTP etc. The bidder shall not carve out any such infrastructure from the items listed in the price schedule (Section-V[1-27]), as those are for running NeSL business applications.

xxxii. The proposed rack space will include adjacent 2 (two) rack space available for future expansion on both floors, with the first right of refusal.

xxxiii. Successful bidder shall submit a detailed LLD (Low level design) along with schematic, IP addressing, security policies, capabilities of the proposed solutions etc., within 15 days from the date of issuance of PO.

xxxiv. Successful bidder shall provide draft acceptance test plan and procedure (ATP) document for review and approval by NeSL. NeSL shall carry-out the acceptance tests as per approved ATP document by its own or third-party agency engaged by NeSL.

xxxv. The bidder shall propose complete SOC solution for the hosted infrastructure with appropriate tools, process and resources to monitor, manage, respond, recover from any security incident. The details of the solution shall be submitted in the technical bid. The rules, use cases, thresholds etc shall be finalized by the successful bidder in consultation with NeSL. NeSL requires a complete segregation of data, logs etc from other customers.

xxxvi. The Vendor shall furnish to National E-Governance Services Limited periodical incident reports of security incidents with root cause analysis. Vendor shall provide a view only access to the dashboard of the SOC.

xxxvii. All the software/hardware components in the proposed solution shall be covered under warranty/Annual Maintenance Contract/Annual Technical Support with OEM /OSP (original software publisher) throughout the contract period and shall not be declared end of support/service by the OEMs for a period of minimum 5 years from the date of submission of bids. Vendor shall have formal back-to-back support arrangements with respective OEMs/original software publishers during the entire period of engagement. Vendor to provide the undertaking for the same as part of the bid response. The make, model and OEM part numbers of products and solutions, including subcomponents proposed shall be submitted in the technical bid. Count of Licenses of proposed software products shall be compliant with policies of respective software publishers.

xxxviii. The model of the equipment proposed shall be listed on the respective OEM website. BIS Registration under CRS of MeitY: Servers, Storage, Network and Security Devices provisioned shall have BIS registration under CRS (Compulsory Registration Order) of MeitY. The registration number shall be provided as part of the technical bid.

xxxix. NeSL reserves the right to undertake any activity if required any time during the contract period on its own or through authorized entities beyond those stipulated as bidder's responsibility in this RFP. Such activities may include but not limited to installation of any software, perform additional VAPT, patch management, audits etc. However, such activities will be performed with the knowledge of Service Provider and as per the agreed change management process.

3. Technical Specifications

Following paragraphs, viz A to D provide technical specifications of main constituents/components of the desired solution. Bidders are required to go through each paragraph carefully and submit a constituent/component wise compliance summary in following format: As per Annexure -4 (Table-3). Bidders may please note any unreported deviations, if detected/observed later, bidder will have to comply within 10 days, at no extra cost to NeSL.

Sr No	Name	Completely complied Y/N	Provide details of Deviation if any	Provide Highlights and justification in case of deviation (if any)
A	Compute & Server/Virtual Machines Configurations			
B	Storage Specifications:			
C	Backup Solution: - a) Provisioning of server for data backup is under the scope of the bidder. Please provide make/model/ configuration and			

	specifications of proposed server. b) Provisioning of separate storage for backup. Please provide make, model, configuration. c) Provisioning of adequate number of licenses. d) Implementation as per NeSL			
D	Network Requirements/Specifications			
E	Managed Security Services Specifications			

A. Compute & Server/Virtual Machines Configurations/Specifications:

1. RAM should be of 1:1 Ratio for all VMs.
2. The physical to vCPU ratio will be 1:2.
3. DB server shall be Physical Server
4. Each VM should have 400GB of Storage provisioned from the overall storage.
5. Servers of 3rd Generation or higher with Intel Xeon Gold Scalable processors, of 32 or more physical core for each socket with base frequency of 2.1GHz or higher and 2048GB or higher DDR4 RAM, 960GB NVME/BOSS with RAID 1. The servers shall be provided with Quad port 10G Fiber N/W ports, TPM, IPMI Port etc., fully populated from day to be used.
6. Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber-attacks.
7. Should protect against attack on firmware which executes before the OS boots.
8. Should provide effective protection, reliable detection & rapid recovery using:
   a) Cryptographically signed firmware
   b) Data at Rest Encryption (SEDs with local or external key management)
   c) Secure Boot
   d) Secure Erase
   e) Secured Component Verification (Hardware integrity check)
   f) Silicon Root of Trust
   g) System Lockdown (requires iDRAC9 Enterprise or Datacentre.
   h) TPM 2.0 FIPS
9. VM deployment and management, including VM Patching, cloning, Monitoring of Server and deployed VMs, to be included part of the costing.

10. VMware VCentre and other infrastructure management applications to be factored by the bidder.
11. Other Requirements:
    a) Solution should be scalable to meet the future growth.
    b) Minimum 10G Redundant Card per server with 10G Fiber port.
    c) RHEL Version to be 7.9 or as per the recommendation by the bidder and upon the approval of NeSL.
    d) The solution should be ready with the drivers and latest service packs of these devices.
    e) The solution shall provide the ability to publish updates and patches to any number of virtual desktops/applications without affecting user settings, data or preferences.
    f) Any component of the proposed solution should have proper support from OEM and not end of life and support service should be available for the next 5 years from the date of submission of bid.
    g) The solution should have the ability to provide a separate management interface for a separate set of users (Role Based Access).
    h) The solution should avoid IO surge on the storage during boot phase of the setup.
    i) The solution should be capable of hosting Microsoft Windows and Linux operating systems.
    j) The solution should be linearly scalable. By adding more compute and storage capacity, we should be able to roll out the platform to more users without changes in architecture.
    k) Administrators should be able to centrally control the access to mass storage devices. The Solution should be compatible with the SSL/IPSEC VPN.
    l) The solution should include tools to analyze and troubleshoot the deployment.
    m) End to End stack of the solution should support the proposed Virtualization Layer.

B. Storage Specifications:

1. All flash storage.
2. RAID6 (for Databases and File system) of raid group of 16
3. Should have native NFS support.
4. Initial provisioning of 200TB. Expected 25% growth year on year.
5. NFS mounts to be shared across VM's with daily growth of 60GB.
6. Unified ALL flash storage to be proposed part of the solution.
7. Primary storage to support NFS and support mount points as big as 25TB.
8. Each VM shall have 400Gb of vStorage provisioned from the overall storage.
9. VM's vStorage to be provisioned from the primary storage.
10. MySQL One master and Two slave nodes, each with 30TB of disk size for data and an annual growth rate of 25%
11. Vertical and Horizontal Expansion capability.
12. Should support Inline Data Reduction: Deduplication / Compression.
13. Supported Protocols: File, Block, vVols.
14. Controller based native encryption.

15. Data should be encrypted at rest.
16. Snapshot or point in time rollback option.
17. Async/Sync replication between DC and far DR (WAN replication) over FC and IP
18. MySQL to use Native data replication and NFS to use Storage based replication.
19. FC, iSCSI and VMware Virtual Volumes (vVols) 2.0.
20. Storage Backend Interface to be of 32Gbps redundant FC, with adequate 10G ports.
21. Storage should support Snapshot / Point in time copy / Clone.
22. Minimum 2,00,000 IOPS with 70:30 Read/Write ratio for 8Kb Block size for 100TB, Storage capacity expansion should not reduce minimum 2,00,000 IOPS.
23. Segregation of production and non-production environments workloads within the proposed storage box to ensure production performance is not impacted.
24. No Single Point of Failure of any component
25. Disk Fault Tolerance
    a) Support for Single disk failure
    b) Dual disk failure
    c) Auto rebuild.
26. Ensure zero data loss in case of power failure.
27. Storage should support Integration with Virtualization for offloading storage functions to array intelligently.
28. Storage should be fully provisioned as per the PO and should not be thinly provisioned.
29. Storage should support automatic space reclaim.
30. Storage should support native replication between DC and DR storage boxes and also should support metro replication out of the box.

C. Backup Solution:

1. Separate Storage device for Backup
2. Storage for backup to be in RAID5.
3. Required rack-based server with software for backup to be included.
4. Daily incremental, weekly full, retention 30 days.
5. The bidder shall provide adequate backup storage considering 200TB as the baseline and 25% growth YoY.
6. Should have provision to do data integrity check on the backup every quarter.
7. Should have min 4x10G ports. Bidder to design and compute network ports suitably to support concurrent backup and restore. However, the bidder is expected to provision adequate number of 10g ports to support concurrent backup restore activities considering the overall storage at any point of time during the contract period.
8. The backup solution must support a minimum of 20 TB throughput per hour for both read/write.
9. Backed up data should be encrypted with AES 256 or more.
10. Immutable backup retention should be configurable, with 7 days of initial retention.
11. Backup-Schedule
12. Daily incremental backup for VMs and NFS – retained for 7 days.
13. Weekly full backup for VMs and NFS - retained for 30 days.

D. Network Requirements/Specifications:

1. 10G Switches, WAF, Firewall in redundancy for respective floors.
2. L3 Switches on redundancy should support 10G connectivity on fiber separately for data / backup.
3. Internal traffic should be routed through managed L3 switches and not routed through internet facing firewall as per approved design.
4. 10G Managed L2 Switch.
5. Network/solution must have SSL/IPsec VPN capability inbuilt.
6. Min 1G connectivity for OOB Switch.
7. Management N/W should be planned over a 10G connectivity.
8. Connectivity from P2P/MPLS/Internet common termination point/meet-me room to the infrastructure provisioned through this RFP initially or subsequently upon request from NeSL shall be provided by the bidder without any additional cost to NeSL.
9. HA Network devices to be connected via Fiber.
10. ISP level redundancy shall be provisioned including route diversity for each ISP.
11. Public IPs provisioned shall be from the same dedicated subnet.
12. Network switch to ESXi Server should be on Fiber.
13. Physical F5 WAF (fully loaded with all WAF features) with minimum of 1G effective WAF throughput.
14. WAF / Firewall to support Vertical and Horizontal Scaling
15. Firewall should support VPN bandwidth throughput of min 5Gbps.

E. Managed Security Services Specifications

- Security monitoring services

1. Successful bidder shall monitor security threats/ events from all the security log sources, such as Firewall, WAF, PIM/PAM/AAA, AD, AV, IP Tables in Servers, ACLs in switches etc., using SIEM tool.
2. Bidder should monitor security logs on a 24x7 basis and detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in NeSL environment.
3. The use-cases and correlation rules including cross-correlation rules and other policies shall be documented based on the identified log sources and submitted to NeSL for validation prior to deployment. The use-cases and correlations rules shall be continuously evaluated, additional rules to be configured and review of the effectiveness of all the rules shall be monthly.
4. Bidder should also monitor security events on business applications, databases in consultation with NeSL team and identify network behavior anomalies including zero-day attacks.
5. A dashboard with drill-down facility shall be made available with NeSL to have complete visibility of the security posture at any moment. The dashboard shall be subjected to

change based on NeSL needs to ensure better visibility.

6. Bidder shall also deploy and create use-cases using feeds from security advisory agencies like CERT-In, NCIIPC etc., as per the directions from NeSL.
7. Any security incident shall be immediately alerted to NeSL and necessary mitigation steps to be taken. The details of incidents, actions taken, and proactive steps taken to eradicate or minimize such incidents in a later stage to be properly recorded, maintained and shared with NeSL for future references including legal and regulatory purposes.
8. As part of managed services, successful Bidder shall critically analyze and advise NeSL on the security threats and existing vulnerabilities. The bidder shall advise NeSL on measures to be taken on its Network/Security/Computing infrastructure to protect against these vulnerabilities. Bidder shall also provide suggestions on the requirement of any additional component to strengthen the overall security posture.
9. As part of the managed services, the successful bidder shall conduct vulnerability assessment of the IT infrastructural facilities on a quarterly basis and shall provide advisory services for fixing the shortfalls identified during such vulnerability assessment/ penetration testing.
10. NeSL may conduct security assessment with in-house or third-party agencies and successful bidder shall provide all support on the same, including advisory services to mitigate the vulnerabilities identified, if any.
11. Successful bidder shall provide timely support for periodic Cyber drills conducted on the infrastructure by agencies like IDRBT and shall provide report on the mock attacks performed on the infrastructure during the drills.
12. The following activities shall be carried out in a regular manner to face the challenges and protect the assets.
    a) Identification of the vulnerabilities on monitored assets before attackers.
    b) Identification of early warning signs of threat scenarios, especially with a monitoring of suspicious changes in your environment.
    c) Identification of compromised assets or data leaks.
    d) Identification of the risk exposure as seen by third parties.
13. A successful bidder shall provide an SNMP based Enterprise Management System (EMS) to monitor all IP infrastructure including but not limited to the availability, performance, bandwidth utilization etc. The monitoring system shall have capability of auto generation of tickets based on identified/major events from the EMS. A dashboard view pertaining to NeSL infrastructure, with drill down facility shall be provided to NeSL.
14. SIEM features - Enterprise Dashboard for real time visibility, Analyst-centric dashboards, reports, reviews, rules, and alerts, Prepackaged configurations for common security use cases, such as alarms, views, reports, variables, and watchlists, predefined dashboards, audit trails, and reports, compliance reports, rules, and dashboards, event enrichment with contextual information, correlation of suspicious or confirmed threat, collect data from third-party security vendor, threat intelligence

feeds.

4. Detailed Technical Specifications

Following paragraphs, viz (a) to (h) provide detailed technical specification of some constituents/components of the desired solution. Bidders are required to go through each paragraph carefully and a submit a constituent/component wise compliance summary in following format. Bidders may please note any unreported deviations, if detected/observed later on, bidder will have to comply within 10 days, at no extra cost to NeSL. As per Annexure -4 (Table -4)

Sr No	Name	Completely complied Y/N	Provide details of Deviation if any	Remarks
a	Backup Software			
b	Network switches			
c	SNMP based EMS			
d	PAM			
e	Server Security /Antivirus			
f	SIEM			
g	NG Firewall			
h	WAF			

a) Backup Software

Topic	Specification
Analyst Rating	The solution should be "Leader" or "Challenger" in the Gartner Magic Quadrant for last three consecutive years.
Licensing	The proposed Backup software must offer host-based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR site.
Reporting Capabilities	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting, and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied.
	Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.

	Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
	Backup software should support agentless backups of applications residing in VMs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.
Recovery Assurance	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.
	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.
	Backup software should provide Backup and Replication capabilities in one console only and allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only of those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities.
	Proposed backup software should be able to Harden the repository on any Linux platform. This service will prevent backup copies of data from any corruption or ransomware attacks.
	The software should support Group Managed Service Accounts which should have an option for users to allow change passwords after every 30 days and adapt complex password policy.
	The proposed backup software should be able to integrate with anti-virus software and scan before recovery of VMs and ensure that any infected VM is not restored or restore it with disabled network adapters to prevent any infection to spread through the network
	Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten", regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.
	Backup software should support quick file/data mount recovery from storages.
Backup and Replication Performance and SLA	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.
	Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup.
	The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.

b) Network Switches

Component	Description
General Features	High Density Wire-speed Layer3 Switch
	19” rack mountable - 1RU
	Should have high-availability feature for active-active & active-passive operation from day-1
Interfaces	48 x 10G Ports Switch populated with 10G SFP+ appropriate transceivers.
	1 RJ45 console port, 1 RJ45 management port
	HA cables to be included as part of solution
Architecture	Should have redundant hot-swap power supplies & fans
	32MB packet buffer memory
	Modular operating system, support for software defined networking
	CLI commit, Uplink Failure Detection, BFD, Zero Touch Provisioning.
	Should support Leaf/Spine fabric architecture using BGP EVPN, VXLAN.
High Availability	VRRP, active-active, active-passive operation
	Software upgrades with minimal traffic disruption during the upgrade
	LAG load balancing based on L2, IPv4 or IPv6 headers
Layer 2 features	128 LAG groups with 16 ports per LAG
	64K ARP table, 160K MAC addresses
	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs
	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP
Routing Protocols	BGPv4, OSPF v1/v2/v3, VXLAN routing from day one.
	IPv6 routing & VRF-Lite feature from day one.
Security Features	Layer 2-4 Access Control Lists
	ACLs - port based/VLAN based.
	Integrated security features like DHCP relay, Control Plane DoS protection
	Streaming Telemetry, Control Plane Services

	802.1X Network Security and Authentication
	RADIUS, TACACS, sFLow, NTP
Traffic Policing	Ingress/Egress shaping and policies
	Filter, mark and limit traffic flows
	Minimum 8 hardware queues per port
	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN
Multicast	H/W based Ipv4 and Ipv6 Multicasting
	IGMP v1, v2, v3, IGMP Snooping
	Protocol Independent Multicast – Sparse Mode and PIM – SSM
Network Management	SNMP v2 & v3
	IPv6 Management support, telnet, FTP, TACACS, RADIUS, SSH, NTP
Connectivity required	Required number of switches to be proposed in HA to run the overall all solution. SFPs from the same OEM

c) SNMP based EMS (Enterprise Management System)

SNMP based EMS (Enterprise Management System) to monitor the availability and performance of all IP devices in NeSL infrastructure. The solution should provide a detailed visibility of Internet & Intranet traffic to analyze the bandwidth consumption of servers, applications and protocols.

The solution shall have the following features:
a) Resource Discovery b) Network Topology c) Asset Management d) Performance Management e) Traffic Analysis f) SLA Management g) Report Generation

d) PAM

Description
Auto-Onboarding of Users, Assets and Credentials
The solution should have the capability to auto-onboard users, assets, groups, and discover credentials. It should be further able to configure rules to auto-assign the desired relationships/roles based on the least privileges.
Auto Discovery of Privileged Accounts
The solution should be able to perform auto-discovery of privileged accounts on target systems and perform two-way reconciliation.
Ability to identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key-related data, and ascertain the status of each key.

Manage Lifecycle of Human, Non-Human and Cloud Identities
The solution should have the capability to provision/de-provision users to any applications, these may include business applications, shared accounts, and privilege accounts.
The solution should have the capability to provision/de-provision users to infrastructure devices and systems example: Operating Systems, Databases, Network Devices, Security Devices, etc and should also be able to provision/de-provision for shared accounts and privileged accounts.
JIT principles are very critical. The solution should have the capabilities to provision/de-provision users (interactive and non-interactive) based on least privilege with JIT capabilities to ensure that ephemeral accounts are created across technologies i.e., business applications and systems and devices.
Authentication Models
The solution should provide a multi-domain authentication feature whereby the entire operations can operate in a distributed environment. This feature should be provided for authentication of users as well as Identity authentication for target systems.
The solution should allow the use of MFA to specific applications and/or devices, systems based on the criticality of use.
Access Technologies
The solution should provide for both a Native app and an HTML5 based workspace platform (browser-agnostic)
The adapters required for various technologies should be out of the box and for any unsupported technology the solution should provide proven adapter builder technology for quick deployment in a dynamic IT environment.
The solution should include a BOT builder for developing automated functions for transparent target connections, as well as any required dependencies, such as pre/post connection or manual input. For ease of integration, this is a necessity.
For the best path of access, the solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the user level. The solution should be able to intelligently route the user to the intended target system access in the safest possible way, considering simplicity of use and experience.
Access Control
The solution should provide access to end-users based on least privilege principles and then grant the user the ability to elevate his/her access based on certain roles and access approval methodologies with inbuilt dynamic workflows.
The solution should also have the capability to provide restriction, elevation, and delegation rights on the native accounts on the target host (especially Operating System) which should work with or without the access management system.
Privilege Elevation and Delegation
Describe the ability of your solution to elevate privileges in Windows environment for remote execution scenarios
Describe the ability of your solution to elevate privileges in Linux/Unix environment for remote execution scenarios
Vault Integration

The solution should provide a robust and mature vault to manage credentials, passwords, Keys secrets, certificates and such other artifacts as one would like to vault.
The solution should be able to provide rotation capabilities at scale (across technologies)
The solutions should be able to create a sequence or automate events or actions based on technology requirements to ensure that any rotation activity is end-to-end without any manual intervention
The solution should be able to automatically sync any out of sync passwords without using any external utilities (on target systems/applications)
Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online.
Application Password Management (Hard-Coded Password Management)
The solution should have the ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files, etc.
PAM Administration
The solution should have a central administration console for unified administration.
The tool should have a provision to enable maker-checker configuration for critical administrative actions. e.g., new user creation, on-demand password change, etc.
Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle, etc.)
Solution Workflow
The solution should have an inbuilt workflow to manage:- i) Electronic Approval based Password Retrieval ii) Onetime access / Time Based / Permanent Access
Multi-level approval workflow with E-mail and SMS notification and delegation rules
Ability to provide for the delegation at all levels in the workflow
Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g., smartphones
Notification Engine
a) The solution should have the capability to provide alerts and notifications for critical PAM events over SMS & Email b) The solution should have the capability to provide alerts and notifications for all administration/configuration activities over SMS & Email c) Customizable notification for command executed on SSH and Telnet based devices d) Customizable notification for command/Process executed on Windows e) Notification on target being access on criteria like Line of Business or Groups f) The solution should have threat analytics and customized reporting capabilities
Logging, Session Monitoring and Auditing Capabilities

The solution should be able to support a session recording of any session initiated via the access management solution including applications, servers, network devices, databases, and virtualized environments.
The solutions should support selective options for enabling session-based recording on any combination of target account, group or target system and end-user.
The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No etc). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end-user or user group.
The solution should be able to record old and new values for all logs related to the administrative activities within the solution
The session recording should be SMART to help jump to the right session through the text logs
Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings, etc.
The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary
The solution must support an inbuilt CLI proxy for supporting secure session management across distributed environments.
Dashboard, Reporting and Analytics Capabilities
The system shall have the ability to run all reports by frequency, on-demand, and schedule.
The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log
The solution should be able to co-relate multiple reports from different systems and provide exceptions based on use cases for security or operations teams.
The solution should be able to provide automation of use cases from collection of data to analytics to reporting with dashboards.
Access Managment System Security
The solutions should use minimum FIPS 140-2 validated cryptography for all data encryptions.
The Solution should be TLS 1.1 or higher and SHA-2 compliant
The solution should secure master data, records, entitlement, policy data, and other credentials in a tamper-proof storage container.
The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)
System Architecture

The solution should have the following attributes in terms of architecture: a. Support horizontal and vertical scaling b. Offer multi-tier architecture with clear segregation between data and application level. c. Support distributed network architecture with centralized administration. d. Support active-active and active-passive configuration to effectively use provisioned resources and ensure high availability (24x7)
Out of box Integration
The proposed solution should offer following integration out of the box: a. Enterprise authentication methods including LDAP, PKI, RADIUS b. MFA c. ITSM and CMS (Change Management Systems) d. Integration with HSM (for securing encryption keys) e. SIEM solutions f. VAPT and Performance Monitoring tools
Brand and Technology
The solution should be "Leader" or "Challenger" in the Gartner Magic Quadrant for last three consecutive years.
The Solution should have presence and support Centre in India with 24x7 (relevant declaration & proof must be submitted)
The solution should be successfully implemented in at least 3 financial institutions with relevant scope of implementation (100+ Users 300+ devices) (PO/Work order copies to be submitted for the same)
Healthcheck
Health Check to be performed by MSP every quarter and recommend necessary changes
Scope & Licenses
1 Onsite OEM certified Resource to ensure PAM solution is up & running
There solution should be scalable & designed for High Availability.
The solution should be licensed for minimum **100 users and 150 device** licenses.

e) Server Security /Antivirus

General Specification
The solution must provide single platform for complete server protection over physical, virtual & cloud
The solution should be licensed for minimum **50 endpoints** (Linux/Windows)
Should be provided with on premise centralized console, with no requirement of internet access for individual servers/VMs.
Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.
The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server
The proposed solution must be able to provide antimalware and vulnerability protection

The dashboard must be configurable by administrator to display the required information.
Proposed solution must have a management system for administrators to access using web browsers
The solution should be “Leader” or “Challenger” in the Gartner Magic Quadrant for last three consecutive years.
The solution should have a small overhead footprint such that it minimizes impact on system resource
All modules i.e., Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention must be available in single agent
Anti-Virus
Must be able to provide file reputation with variant protection that look for obfuscated, polymorphic by using fragments of previous seen ad detection algorithm
Antivirus should support both Real Time and Schedule scan
Solution should have flexibility to configure different real time and schedule scan times for diff guest VMs
Solution should support excluding certain file, directories, file extensions from scan (real time/schedule)
Solution should support various Actions like, Clean, Delete, Quarantine, Pass
Solution Should have Machine Learning Capabilities
Solution shall be able to scan Object Linking and Embedding (OLE) File
Should support logging reporting and correlation of suspicious events
Solution should support True File Type Detection, File extension checking.
Solution should support heuristic technology blocking files containing real-time compressed executable code.
The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning
The proposed solution should be able to perform “Behaviour Analysis” for advanced threat prevention
Solution should have ransomware protection in “Behaviour Monitoring”.
Intrusion Prevention System
Must be able to provide HIPS/HIDS feature that immediately protects against vulnerabilities.
Virtual Patching should be achieved by using a high-performance deep packet inspection engine to intelligently examine the content of network traffic entering and leaving hosts.
The proposed solution should support Deep Packet Inspection (HIPS/IDS) including the SSL traffic on the host.
Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.

Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.
Solution should provide the ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensors (e.g., Selecting rules, configuring policies, updating policies, etc.)
Solution should support creation of customized DPI rules if required.
Solution should provide recommendations for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.
The solution should allow imposing HTTP Header length restrictions.
The solution should allow or block resources that are allowed to be transmitted over http or https connections.
Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.
Solution should be capable of blocking and detecting IPv6 attacks.
Solutions should offer protection for virtual, physical and cloud environments.
Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).
Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight for servers. For operating systems and applications, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.
Solution should work in Tap/detect only mode and prevent mode.
Solution should support automatic and manual tagging of events.
Solution should provision inclusion of packet data on event trigger for forensic purposes.
Solution should support CVE cross referencing when applicable for vulnerabilities.
The solution shall protect against fragmented attacks
Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.
Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required.
Host Firewall
The firewall shall be bidirectional for controlling both inbound and outbound traffic.
Firewall shall have the capability to define different rules to different network interfaces.

Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans.
The solution should support stateful inspection firewalling functionality.
Solution should provide policy inheritance exception capabilities.
Solution should have the ability to lock computers (prevent all communication) except with management server.
The firewall should be able to detect protocol violations of standard protocols.
Solution should have security profiles that allow firewall rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required.
Solution should provision inclusion of packet data on event trigger for forensic purposes.
Integrity Monitoring
Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behavior, such as modifications, or changes in ownership or permissions.
The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.
Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).
Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.
Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.
Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required.
Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities. Rules/ Detections shall be mapped with relevant MITRE TTP, wherever it is relevant.
In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.
Solution should have Security Profiles which allow Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto provisioned based on server profile.
Solution should have an intuitive rule creation and modification interface that includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.

Solution should support the following: Multiple groups of hosts with identical parameters Regex or similar rules to define what to monitor Ability to apply a host template based on a regex of the hostname Ability to exclude some monitoring parameters if they are not required Ability to generate E Mail and SNMP alerts in case of any changes
Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.
Log Inspection
Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events.
Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.
Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/removal of assignment of rules when not required.
Solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g., all Linux/Windows servers use the same base security profile allowing further fine tuning if required.
Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.
Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered in a match.
Solution must support decoders for parsing the log files being monitored.
Application Control
Solution should allow administrators to control what has changed on the server compared to the initial state.
Solution should have option to allow to install new software or update by setting up maintenance mode
Solution should have the ability to scan for an inventory of installed software & create an initial local ruleset.
Change or new software should be identified based on File name, path, time stamp, permission, file contents etc.
Solution must have ability to enable maintenance mode during updates or upgrades for predefined time-period.
Should have the ability to enforce either Block or Allow unrecognized software.
Solution must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.

f) SIEM

Specification General features
SIEM solution must support heterogeneous systems, applications, and devices with fully developed normalization logic out-of-the-box by the solution.
The solution must support very granular level of role-based access.: i) Allow different teams to get an access to the same physical device and view date related to their role alone ii) It must support log source visualization on the SIEM platform itself
The proposed solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected log data.
The data collector/agent must be able to collect the logs through different methods.
The proposed solution must support the collection of the Net flow logs without additional appliances or components.
The proposed solution must have the capability to drop noisy logs at the collector level.
The proposed solution must provide storage for long term trend visualization and analysis
The solution should be able to import RAW logs from syslog collector and carry out the security analytics.
The proposed solution must have the ability to leverage correlated or anomaly events back into other correlation or advanced analytics rules.
The proposed solution must incorporate data from multiple threat intelligence feeds into its' advanced analytics.
The proposed solution must provide regular updates to analytics rules to detect new and emerging threats.
The proposed solution must provide an ability to interface with a third-party incident response management system (Remedy, etc.)
The proposed solution must provide out-of-the-box alarms designed to enforce continuous compliance and security best practices.
The proposed solution must provide the ability to create customized alarms, distributed to specific groups of individuals and prioritize alarms and alarm delivery.
The proposed solution must email alarm notifications include risk rating priority level with configurable email subject lines.
The proposed solution automated remediation must provide a built-in hierarchy approval workflow, so the actions can be taken automatically or through an approval chain.
The proposed solution built-in case management system. All activity must be tracked as part of the case history, providing real-time status and a tamper-proof audit trail.
The proposed solution must offer the play book functions embedded in the platform.
The proposed solution must secure the communication during the log collection mechanism.
The solution must include incident tracking through a fully integrated Security Incident Response platform capable of designing Workflow and Executive Actions in response to Threat and Incidents triggered by the solution.

	The Playbook must allow the Analyst to build their own incident response procedure/Playbook and track it through the Web UI.
	The platform must provide predictive Threat Intelligence Using Behaviour Modelling
	The proposed solution must include a "PTI: Predictive Threat Intelligence" as well as the "Unique: Static/Dynamic" Threat Intelligence included mentioned in the previous section.
	The proposed PTI platform must be able, through an unsupervised "behavioural model" and supervised methods, to classify and flag unreported cybercriminal activity through regular static threat intelligence. (Through Monitoring IP Registration, DNS, Domain name BGP Announcements etc)
	The proposed solution should provide 1000 sustained EPS and expandable to 2000 EPS without any change in HW/infrastructure.
	Retention of logs for a minimum period of 180 days to be maintained either within the solution or with the support of a separate syslog collector. In either case hot storage for 30 days logs to be available in SIEM for security analytics.

g) NG Firewall

Features	Specification
Type	Next Generation Enterprise Firewall
Equipment Test Certification	FCC Class A, CE Class A, VCCI Class A.
Fans and Power Supply	The offered firewall must be a single appliance and not a cluster and should be provided with redundant Fans and power supplies
Architecture	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).
Storage	The NGFW should have 240GB solid-state drives for System storage
Interface Requirement	Min 8 x 1 Gig Copper interfaces from day one
	8x 1/10Gig SFP/SFP+ with provided with 8*SFP+ appropriate transceivers from day 1
	Dedicated 2x HA ports with active optical cable of required length in addition to requested data ports, OOB, Console Management and USB Port
Performance Capacity	A Minimum NG Firewall application control throughput – minimum 9 Gbps with 64KB HTTP transactions including Application-Identification/AVC/Application control and Logging enabled. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.

	Minimum NG Threat prevention throughput (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking, Sandboxing, advanced DNS Security and logging security threat prevention features enabled – minimum 5 Gbps considering 64KB HTTP transaction size. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.
	IPsec VPN throughput – minimum 6 Gbps or more with 64KB HTTP transaction and logging enabled
	VLAN on single Gateway – 2000
	New Layer 7 HTTP sessions per second – minimum 1,40,000 or New Layer 4 sessions per second - minimum 4,00,000
	Concurrent Layer 7 sessions – minimum 1.4 million or Concurrent Layer 4 Sessions - 6 million
High Availability	Active/Active and Active/Passive and should support session state synchronization among firewalls in a high availability cluster
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in:
	- Tap Mode
	- Transparent mode (IPS Mode)
	- Layer 2
	- Layer 3
	- Should be able operate mix of multiple modes
Next Generation Firewall Features	The proposed firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.
	The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
	The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support. The device should have capability to provide detailed information about dependent applications to securely enable an application
	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment

	The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
	Solution should have machine learning capabilities on the data plane to analyse web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.
	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 inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood(Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc
Threat Protection	Should have protocol decoder-based analysis which can stateful decode the protocol and then intelligently applies signatures to detect network and application exploits
	Intrusion prevention signatures should be built based on the vulnerability itself; A single signature should stop multiple exploit attempts on a known system or application vulnerability.
	Should block known network and application-layer vulnerability exploits
	The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures
	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or Antivirus engines.
	Should be able to perform Anti-virus scans for HTTP, SMTP, IMAP, POP3, FTP, SMB traffic with configurable Antivirus action such as allow, deny, reset, alert etc
	Should support inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile
	The device should support zero-day threat prevention.
	Should have threat prevention capabilities to easily import IPS signatures from cyber security advisory bodies such as Cert-IN, NCIIPC, government entities or regulated entities.
	The solution must be able to define Antivirus scanning on per application basis such that certain applications may be excluded from Antivirus scan while some applications to be always scanned

	The solution must have data loss prevention by defining the categories of sensitive information that is required to filter.
	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
	Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
	The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following:
	· Automatically identify and block phishing sites
URL Filtering features	NGFW should protect against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding based attacks
	NGFW should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use
	NGFW should support policy creation around end user attempts to view the cached results of web searches and internet archives
	NGFW should have a vast categorisation database where websites are classified based on site content, features, and safety.
Advanced Persistent Threat (APT) Protection/Sandboxing	There should be provision to enable the APT solution. This should support unknown malware analysis service.
	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine.
	The solution must be able to use AV and zero-day signatures based on payload and not just by hash values.
	The protection signatures should be payload or content-based signatures that could block multiple unknown malware that use different hash but the same malicious payload.
SSL/SSH Decryption	
	The fire proposed wall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
	The firewall shall have the capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The NGFW shall support SSL inspection policy.
	The device should be capable of SSL automatic exclusions for pinned applications.

	The firewall shall support TLS v1.1 or higher decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.
	SSL decryption must be supported on any port used for SSL i.e., SSL decryption must be supported on non-standard SSL port as well
Network Address Translation	The proposed firewall must be able to operate in routing/NAT mode
	The proposed firewall must be able to support Network Address Translation (NAT)
	The proposed firewall must be able to support Port Address Translation (PAT)
	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6)
	Should support Dynamic IP reservation, tuneable dynamic IP and port oversubscription
IPv6 Support	L2, L3, Tap and Transparent mode
	Should support on firewall policy with User and Applications
	Should support SSL decryption on IPv6
	Should support SLAAC Stateless Address Auto configuration
	Should be IPv6 Logo or USGv6 certified
Routing and Multicast support	The proposed firewall must support the following routing protocols:
	- Static
	- RIP v2
	- OSPFv2/v3 with graceful restart
	- BGP v4 with graceful restart
	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address
	The firewall must support VXLAN Tunnel content inspection
	The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels
	The device should support load balancing of traffic on multiple WAN links based on application, latency, cost and type.
	The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports
	The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application

	-by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
	Bidirectional Forwarding Detection (BFD)
DNS Security features enabled from day 1	The Solution should support DNS security in line mode and not proxy mode
	Solution should support database maintenance containing a BoQ known botnet command and control (C&C) addresses which should be updated dynamically
	DNS Security should support predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control
	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations
	It should support prevention against new malicious domains and enforce consistent protections for millions of emerging domains.
	The solution should support integration and correlation to provide effective prevention against 1. New C2 domains, file download source domains, and domains in malicious email links. Integrate with URL Filtering to continuously crawl newfound or uncategorised sites for threat indicators. 2. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots. 3. Should take inputs from third-party sources of threat intelligence.
	Should support simple policy formation for dynamic action to block domain generation algorithms and sinkhole DNS queries.
	Solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection
	The solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers.
	The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink-holing malicious domains to cut off Command and control and quickly identify infected users.
Authentication	Solution should support the following authentication protocols:
	- LDAP

	- Radius (vendor specific attributes)
	- Token-based solutions (i.e., Secure-ID)
	- Kerberos
	The proposed firewall's SSL VPN shall support the following authentication protocols
	- LDAP
	- Radius
	- Token-based solutions (i.e., Secure-ID)
	- Kerberos
	- SAML
	- Any combination of the above
	should support Multi Factor Authentication for SSL-VPN access by default for all users.
Monitoring, Management and Reporting from day 1	Should support on device and centralized management with complete feature parity on firewall administration. Management and Reporting should be offered.
	There should be provision to permanently block the export of private keys for certificates that have been generated or imported to harden the security posture to prevent rogue administrators from misusing keys.
	The management solution must have the native capability to optimize the security rule base and offer steps to create application-based rules
	The proposed solution must allow single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.
	Should have separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities
	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Should allow the report to be exported into formats such as PDF, HTML, CSV, XML etc.
	Should have capability to create custom report apart from built in report templates based on Applications, Users, Threats, Traffic and URLs
	On device management service should be able to provide all the mentioned features in case of central management server failure.

Support & Warranty	OEM should be present in India from at least 5 years. Successful bidder shall have 24x7 OEM support for NGFW, NGIPS, Anti-Virus, Anti Spyware, URL Filtering, Sandboxing and DNS Security capabilities as mentioned above from day 1 and for the duration of the contract period.

h) Web Application Firewall (WAF) Specifications:

Server Load Balancer and Web Application Firewall Specifications
GENERAL
Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF, and it should not white labelled WAF running on third party hardware.
Support of JSON and Rest API for the automated-on boarding of layer2-3 objects such as routes, virtual servers, VLAN's, pools and layer7 configurations
The solution should process each packet by both LB & WAF functions in a single encryption/decryption cycle.
The solution should support template/script driven configurations to abstract the complexity and reduce the misconfigurations for the on boarding of applications
HARDWARE
Virtualization feature that virtualizes the device resources – including CPU, memory, network, operating system and acceleration resources. Each virtual SLB instance contains a complete and separated environment of the following:
i. Resources
ii. Configurations
iii. Management
iv. Operating System
The ADC must use its own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like XEN, KVM etc. The software should provide the ADC operating system with an underlying microservices platform layer.
Minimum 4 x 10G ports populated with 10G SFP+ appropriate transceivers & 4 x 1G RJ45 Ports provisioned from day one. The proposed hardware must support minimum 20 Gbps of SSL throughput (bulk encryption) Appliance must provide minimum SSL TPS of 30K with RSA 2K keys. Minimum compression throughput of 20 Gbps L4/L7 throughput 40 Gbps/30 Gbps Minimum Usable WAF throughput in production environment - 1 Gbps
The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, connection mirroring and heartbeat check and necessary logs to be generated for audit and compliance.
The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys

The proposed appliance should provide multi-tenant design and should have below capabilities: 1) Application traffic isolation: Should be able to define separate address space, VLANs, Routing information and default gateways for each application 2) Administrative Partitions: Should ensure that specific users are granted access to only the partitions for which they are authorized
The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance
The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. It should also support TCL based data plane function to manage network traffic.
Should have administration partitioning and segmentation with different routing separation, whereby the physical device can span across multiple network segments without any inter device routing. The solution should support segmentation to use of the same IP address across the multiple network segments.
The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching, caching & compression, hardware-based SSL offload and server-side compression.
The Proposed solution should be able to monitor the applications using intelligent application monitors which can be either using system defined executable scripts. It should also provide mechanism to bind multiple health checks, support for application specific VIP health check and next gateway health checks
Proposed WAF solution should support cipher suites and SSL/TLS protocol.
The system must support proxy SSL function that allows inspection of SSL encrypted traffic while clients are directly authenticated by the backend servers.
It should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL&TLS connection as per the application need.
The proposed WAF solution should be ICSA certified.
The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and provide suggestions/shortcuts to address the compliances and configure policies for it.
The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system.
The Solution must protect the Application against credential theft from man-in-the-middle (MITM) and MITM browser attacks by encrypting and obfuscating the form parameters. The Solution must be flexible enough to configure the data encryption level, URL list, parameters, etc., to be protected against such attacks.

WAF correlation should identify complex attack chains, and not just aggregate events based on attacks or sources along with advanced BOT detection mechanism based on smart combination of signature-based and heuristic analysis.
WAF should support source based brute force and distributed brute force protection with source IP based and URL based rate limiting.
Solution should provide automatic and manual updates to the signature database to ensure complete protection against the latest web application threats. New signatures should be in detection mode for some days and can be enforced in blocking mode based on our requirement.
Proposed WAF Solution should have capability to automatically learn and provide input validation which should include Directories, URLs, Form Field Values, Content type, Field Consistency, Cookies, http method, Referrer, user authentication forms and fields for application user tracking, XML elements, SOAP Actions, Whether the field values are numeric/alphanumeric/alphabets, length of the field, etc.
The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Webinspect, Acunetix, Qualys, Rapid 7, Appscan, etc (or) Equivalent vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.
The Solution must detect and mitigate L7 DDoS attacks originating from a botnet using application based behavioural analysis that learns application-level parameters like HTTP request methods, reply types, average object size and more.
The solution should be able to "clock" error responses to hide sensitive server related information in the response body and response headers. It should also facilitate hiding/masking sensitive parameters in logs policy wise. Device should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration.
System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.
The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. Necessary logs to be generated for audit and compliance.
Solution should support the following Security Protections:
a) BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats. b) POSITIVE and NEGATIVE SECURITY MODEL should have advanced behaviour-analysis technologies to separate malicious threats from legitimate traffic. The administrators should be able to see all the signatures and not just the signature categories. Admins can apply Specific signatures to specific policies. c) ZERO DAY ATTACK PROTECTION should be provided by behaviour-based protection with automatic signature creation against unknown, zero-day DDoS attacks.

Should be able to uniquely detect and block if required the end user based on internal IP address, Plug-ins Installed in the browser, OS, system files etc. instead of going with traditional IP based blocking only.
Proposed solution should be capable of identifying the Client IP address through Geo-location IP database and provide controls to prevent identity theft, financial fraud and espionage activities. WAF should allow IP addresses or IP range for bypassing applied security policy for specific application but should not bypass for others.
Proposed solution should be capable of detecting unusual or unexpected patterns in the web traffic and rate limit based on specific URI.
Proposed WAF Solution should have capabilities to provide protection against L7 DDoS including but not limited to below mentioned list: 1) HTTPS Rate Limiting 2) HTTPS Malformed filtering 3) HTTPS GET AND POST Flood - HTTPS SLOW GET 4) HTTPS SLOW POST
The solution must be able to block transactions with content matching known attack signatures while allowing everything else. The solution should also have an option to put a signature in staging mode. Meaning that the system applies the attack signatures to the web application traffic but does not apply the blocking policy action to requests that trigger those attack signatures.
The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: 1) Ability to drop requests and responses. 2) Block the TCP session. 3) Block the application user. 4) Block the IP address. 5) Should be able to generate unique identifier to track attack event.
Must support multiple HTTP versions such as HTTP/1.0, HTTP1.1 & HTTP 2.0. Should validate header length, content length, Body length, Parameter length, body line length etc.
WAF must provide inbuilt or via 3rd party integration the capability of API security including support for uploading swagger file and protect leakage of user credentials accessing the web applications using HTML field Obfuscation to protect against malware-based attacks and the solution should have capability to protect Credential Attacks that can steal credentials from the user's browser to avoid cyber exploits. It should be able to authenticate users based on browser type and version, operating system type and version. Necessary logs to be generated for audit and compliance.
Solution should support the performing of comprehensive countermeasure to protect against zero-day attack, Challenge – Response Mechanism like Java script challenge, which should be able to detect and protect attacks in real time through inbuilt Captcha Mechanism. Necessary logs to be generated for audit and compliance
Proposed Solution should have capability to automatically fetch signatures for relevant software, server technology. These signatures need to get updated on regular interval basis as and when released by OEM.
WAF should support normalization methods such as URL decoding NULL byte string, termination, converting backslash to forward slash etc.

Solution must provide the following Features and Protections against various attacks: 1) Open Web Application Security Project (OWASP) Top 10 attacks 2) OWASP Top 10 API security 3) Parameters Tampering 4) Cookie Poisoning 5) SQL Injection 6) Session Hijacking 7) Heavy URL protection 8) Web Page Parameter Security 9) Forceful Browsing 10) L7 DDOS attacks 11) Debug Options 12) Backdoor 13) Buffer Overflow Attacks 14) Data Encoding 15) Cross-Site Scripting (XSS) 16) Brute Force Attacks 17) OS Command Injection 18) Cross Site Request Forgery (CSRF) 19) Information Leakage 20) Path (directory) Traversal 21) Predefined resource location 22) Behavioural based detection and protection 23) Web application layer customized protection 24) White listing based protection 25) API (Application Programming Interfaces) protection 26) Support for JASON and XML format in API security. 27) Dynamic Bot protection and mitigation using script or challenge-response mechanism 28) Sensitive data exposure protection for example, passwords, credit card etc. 29) Anti-site scraping 30) HTTP/OCSP protocol validation 31) Cookie signing validation
The proposed WAF appliance should provide real-time and historical traffic logs with option to filter with multiple parameters i.e., source IP, destination IP, Port, signature, profile, custom words, etc.
The WAF should support specific profiling like parameter length, meta characters etc. to configure granular controls for specific deployed web application.
The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support all the common web application vulnerability assessment tolls (Web application scanners) including Webinspect, Acunetix, Qualys, Rapid 7, Appscan etc. to virtually patch web application vulnerabilities.
Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like-TPS (Transection per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.

The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks.
The solution should be able to perform profiling of JSON with dedicated JSON parser to inspect all JSON messages and apply security policies to embedded object pairs and binary payloads. Solution should enforce JSON security policy parameters, such as restricting URL wildcards and parameters, malformed data, and JSON payloads, methods and objects.
The Solution should support VRF like capabilities to support overlapping address space just like route-domain. This is a must to support multiple applications/clients accessing simultaneously on same IP address space.
DC-DR security policies should be identical and should be capable of export and import seamlessly on each other.
DC and DR WAF should have same set of signatures available and should be applied for application security.
The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • Backend application parser protection against XML DOS • XML Encryption and XML Signatures • Granular WSDL methods selection
The proposed solution must support SSL VPN and Single Sign On functionality on same hardware solution running on same OS version from same OEM in future.
The proposed solution shall employ updated list of threat sources and high-risk IP addresses, IP Intelligence delivers contextual awareness and analysis of IP requests to identify threats from multiple. sources across the Internet. The solution shall draw on the expertise of global threat-sensor network to detect malicious activity and IP addresses.
The proposed solution shall use metadata and multi-vector threat intelligence to help correlate the individual actions of an active attack campaign. With this feature, proposed solution shall be able to identify an attack indicator as part of a threat campaign so that mitigation can be performed.
WAF MANAGEMENT
Should support device management using 1 no. dedicated management port and 1 no. dedicated console port from the day one of supply, CLI (SSH), GUI (HTTPS) and should support authentication, authorization and accounting (AAA) integration with external authentication support providers such as Active Directory, LDAP, RADIUS/TACACS+ and support Role based Access (RBAC) to ensure security.
The proposed WAF and Management solution should be capable for backup and restoration of configuration, traffic logs, system logs, etc.
Proposed WAF Solution and Management solution should be accessible through GUI (including TLS 1.1, TLS 1.2 or TLS 1.3) & SSH (including V3)
Should have diagnostics capability support (e.g., logs, core dumps, syslogs, configurations etc.) which can be used to share with technical support team in case of any malfunctioning by the devices. Should have online vulnerability and configuration diagnosing tool.
The solution must support IPV6 logo ready, or IPv6 ready.org phase 2 certifications

The offered solution should have proven track record. OEM to submit at least 3 PO references with similar value (Purchase Order along with Completion Certificate) from at least 3 Government/PSU/Banking customers in India in last 5 years where OEM's WAF solution has been installed, commissioned and are operational.
Quoted Product should have been in the market for at least 12 months.
Architecture should be DC-DR capable and should failover seamlessly.

Note for WAF Implementation:

1. **Deployment and Configuration:** The MSP will assist in deploying the WAF and configuring it based on your specific needs. This includes setting up rules, policies, and custom security settings to protect your web applications.
2. **24/7 Monitoring:** Continuous monitoring of web traffic and the WAF itself is crucial. The MSP will monitor for suspicious activities, potential threats, and any issues with the WAF's performance.
3. **Traffic Analysis:** Analyzing web traffic patterns to identify anomalies and potential security threats. This can involve the use of machine learning and AI algorithms to detect and respond to evolving threats.
4. **Incident Response:** In the event of a security incident or breach attempt, the MSP will respond promptly, investigate the incident, and take appropriate actions to mitigate the threat. This might include blocking malicious IPs, adjusting security rules, or notifying your team.
5. **Patch Management:** Keeping the WAF software and related components up to date with the latest security patches and updates to protect against known vulnerabilities.
6. **Rule Tuning and Optimization:** Continuously fine-tuning and optimizing WAF rules and policies to minimize false positives (blocking legitimate traffic) and false negatives (missing actual threats).
7. **Policy Management:** Managing access control policies and security rules to align with your application's evolving requirements and security posture.
8. **Log Management:** Collecting, analyzing, and retaining logs from the WAF to ensure compliance, trace potential security incidents, and maintain an audit trail.
9. **Threat Intelligence Integration:** Incorporating threat intelligence feeds and databases to enhance the WAF's ability to detect and respond to emerging threats.
10. **Reporting and Analysis:** Providing regular reports and analysis of WAF performance, security incidents, and compliance with industry standards and regulations.
11. **Backup and Disaster Recovery:** Implementing backup and disaster recovery plans to ensure the availability of the WAF and its configurations in case of hardware failure or other disasters.
12. **Compliance Management:** Ensuring that the WAF is configured and managed in compliance with relevant industry regulations and standards (e.g., PCI DSS, HIPAA, GDPR).
13. **User Training and Education:** Training your team on best practices for using the WAF and understanding security threats and risks.
14. **Performance Optimization:** Monitoring and optimizing the WAF's performance to ensure it doesn't introduce latency or negatively impact the user experience.

5. Reports

The vendor shall submit the reports on a regular basis in a mutually decided format. The following is only an indicative list of reports. Based on the requirement, the service provider will be required to configure & provide additional reports. Softcopies of these reports shall be delivered automatically via email / Dashboard at specific frequency and to the pre-decided list of recipients. Role based selection of reports, selection of name of the recipients of the reports, frequency of delivery must be parameterized /configurable in the EMS tool.

Following is the indicative list of reports:

1. Daily reports (to be submitted on next working day)

a) Summary of issues / complaints logged at the Help Desk.
b) Summary of resolved, unresolved and escalated issues / complaints.
c) Log of backup and restoration undertaken.
d) Server / Database Utilization Report.

2. Weekly Reports (to be submitted on the first working day of the following week)

a) Issues / Complaints Analysis report for virus calls, call trend, call history etc.
b) Summary of systems rebooted.
c) Summary of changes undertaken including major changes like configuration changes, patch upgrades, database reorganization, storage organization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

3. Monthly reports (to be submitted by 10th of the following month)

a) Component wise physical as well as IT infrastructure availability and resource utilization
b) Summary of component wise uptime.
c) Summary of changes.
d) Log of preventive / scheduled maintenance undertaken
e) Log of break-fix maintenance undertaken
f) Change Management summary report.
g) Capacity Management summary report of servers.
h) Service Level Management – priority/ severity wise response and resolution.
i) Service Failure Analysis, listing out escalations and downtime/ outages, if any.
j) Account Dashboard, listing out:
   - Planned activities carried out during the month.
   - Unplanned activities carried out during the month.
   - Activities planned but missed along with reasons.
   - Challenges faced during the month.
k) Service Operations, listing out:
   - Helpdesk Management, listing out priority/ severity wise calls logged with comparison for the past three months.
   - Incident reporting & Management, giving category wise call details for critical

service areas with comparison for the past three months.

- Operational Activities

l) Service Improvement Plan, listing out:

- Concerns/ Escalations with action plan.
- Planned activities/ initiatives.
- Improvements planned, if any.

4. Any Cyber Security Incident shall be Reported within 4 hours or as per the directives of the government from time to time.

5. Other incidents, but not limited to, with detailed RCCA should be submitted within 48 hours.

- Environmental controls, Physical security violations/ threats
- Hardware/Service breakdown leading to services interruptions.
- Software license violations.

6. Data Centre Features:

Bidders are required to submit compliance to the minimum requirements mentioned below. Deviation if any need to be clearly called out in a tabular form.

SL No	Description	Minimum Requirement
1	Air-Conditioning environment	Precision Air Cooling with N+1 redundancy, with humidity and Temperature control
2	Physical Security	Access control, CCTV with video recording, 24X7 guards,
3	Fire Protection System	Smoke detectors with auto alarm/ indication, Fire suppression system
4	Raw Power	Feed from two different sub-stations
5	Back-up power	DG set with N+1 redundancy
		UPS with min 30 min back-up and N+1 redundancy
6	Building Monitoring System	BMS for 24X7 monitoring HVAC, UPS, DG set, Fire System, Electrical installations, Access control etc.
7	Up-time	99.982 % on yearly basis
8	Other Features	PA system, Rodent repellent system, Water leakage control

(End of Section – IV)

The prices quoted in table below shall be for the items/solution/services that comply with the specifications, features and requirements as stipulated in **Section IV** above.

Sl No.	Component	Description	Unit	Indicative order quantity	Unit monthly Price – for first 3 Years in Rs. (Exclusive of Taxes)	Unit monthly Price – for year 4 & 5 in Rs. (Exclusive of Taxes)	GST % (eg: for 18% enter 18)	Total OPEX for a period of 5 years [(6)*36+(7)*24] *(5) in Rs.	One time Per Unit installation charges – if applicable in Rs. (Exclusive of Taxes)	One time total installation charges in Rs. (Exclusive of Taxes)(10)*(5)	GST % for installation (eg: for 18% enter 18)	Total Cost in Rs. [9+11] (Exclusive of Taxes)	Total Cost Inclusive of GST
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Internet Bandwidth, Network, Security Layer													
1	**Bandwidth**	100 Mbps DDOS Protected	Per 100 Mbps	1.00				0		0		0	0
2	**Bandwidth**	50 Mbps incremental (beyond base requirement) DDOS Protected Internet Bandwidth	Per 50 Mbps	1.00				0		0		0	0
3	**Public IPs**	20 Public IPs	Per set of 20	1.00				0		0		0	0

4	**NG Firewall**	UTM Specification given in Sec-IV,4. Detailed Technical specification(g)	Per No	2.00				0		0		0	0
5	**Physical WAF with LB**	Specification given in Sec-IV,4. Detailed Technical specification(h)	Per No	2.00				0		0		0	0
6	**Switch 10G *48 Port L3**	Switch - 48 X 10 Gbps L3 with active 24 ports	Per No	2.00				0		0		0	0
7	**Switch 10G * 12 Port License**	Pack of License including optics for Incremental 12 Ports	Per pack	1.00				0		0		0	0
8	**Switch 10G *48 Port L2**	Switch - 48 X 10 Gbps L2	Per No	2.00				0		0		0	0
9	**Switch 10G *24 Port L2**	Switch-24 X 10 Gbps L2	Per No	1.00				0		0		0	0
	Storage												
10	**SAN Storage**	All flash usable 200TB configured in RAID 6	Per No	1.00				0		0		0	0
11	**Additional SAN Storage**	Additional all flash usable storage space in incremental size of 10TB configured in RAID6	Per No	1.00				0		0		0	0
12	**SAN switches FC**	32 Gbps -SAN switches -24 Ports activated	Per No	2.00				0		0		0	0

13	**Backup Storage**	Dedicated backup storage (NL-SAS) with usable storage space of 200TB configured in RAID5	Per No	1.00				0		0		0	0
14	**Additional Backup Storage**	Additional NL-SAS usable storage in incremental of 50TB configured in RAID5	Per No	1.00				0		0		0	0
Software Licenses													0
15	**NGINX Plus Support License**	NGINX Plus Support (Business Hours)	Per No	7.00				0		0		0	0
16	**MySQL Enterprise Edition License**	MySQL Enterprise Premier support from Oracle	Per No	3.00				0		0		0	0
17	**OS license**	Windows server 2022 Standard OS license	Per license	1.00				0		0		0	0
18	**RHEL License**	Red Hat Enterprise Linux for Virtual Datacentres - Premium Support	Per Physical Server	3.00				0		0		0	0
19	**RHEL License**	Red Hat Enterprise Linux Server - Premium Support	Per Physical Server	3.00				0		0		0	0
20	**VMware vSphere Enterprise Plus License.**	With support for vMotion, datamotion, 24 x 7 support	Per Processor	6.00				0		0		0	0

Security & Monitoring													0
21	**HBSS (AV+HIPS)**	Host Based Security System, IPS/IDS at Host Layer	Per No	40.00				0		0		0	0
22	**SIEM**	Security Incident and Event Management with sustained 1000 EPS	Per No	1.00				0		0		0	0
23	**SIEM- addon**	Additional sustained 200 EPS	Per No	1.00				0		0		0	0
24	**Log Storage Solution**	180 Days Log retention	Lump-sum	1.00				0		0		0	0
PAM Services													0
25	**PAM**	Privileged Access management Specification given in Sec-III	Per No	1.00				0		0		0	0
Servers													0
26	**Physical Server**	2 X 16 Cores/ 768 GB RAM/ 2 X 960 GB SSD/ Dual-Port FC 32 Fiber Channel HBA	Per No	1.00				0		0		0	0
27	**Physical Server**	2 *32 Cores/ 2TB RAM/ 2 X 960 GB SSD/ Dual-Port FC 32 Fiber Channel HBA Card	Per No	6.00				0		0		0	0
	Miscellaneous Infrastructure												0

28	**Miscellaneous Infrastructure**	Infrastructure cost to cover the requirements specified in Section-IV,2, General Technical requirements(xxxi)	Lump sum	1.00				0		0			0
								Total				**0**	**0**

Note:

1. Please refer to para **2 of Section – III.**
2. The bidder must quote for all the items listed in the price schedule. If "Onetime charges" (Column no. 10 in the price schedule) is left blank, the price for that item shall be deemed to have been included in the unit monthly cost.
3. **For determining L1, sum total of the column "Total Inclusive of GST", i.e., column number 14 will be the basis. Unit rate as per quote for the corresponding year shall be taken for further orders.**
4. The quantities mentioned in this table shall be considered **only for the purpose of computing the total price quoted by a bidder** and the Lowest Bidder will be decided on this Total Price. NeSL reserves the right to award the Contract as per the requirements at the time of award of Contract. However, National E-Governance Services Limited is not bound to award the contract for these quantities or configurations. National E-Governance Services Limited will select the appropriate number and configuration, (either at the time of award of Contract or any time during the tenure of the contract), depending upon the requirement. In such case(s) the unit prices quoted for various components/ services shall apply for addition or deletion. The billing to NeSL for any additional items /services shall be from the date of acceptance by NeSL of such an item/service on a pro-rata basis using the pre agreed unit rate for respective item/service.
5. The bidders are required to quote the prices strictly as per the Price Schedule given enabling National E-Governance Services Limited to arrive at an appropriate price for required configurations and/or requirements.
6. **The bidders are required to mandatorily fill in the columns in red in the spreadsheet Section-V.xlsx. Those mandatory columns are listed below. Incomplete bids will be rejected.**

Column Heading	Column Number
Unit monthly Price – for first 3 Years in Rs. (Exclusive of Taxes)	6
Unit monthly Price – for 4 & 5 Year in Rs. (Exclusive of Taxes)	7
GST % (e.g.: for 18% enter 18)	8
One time installation charges – if applicable in Rs. (Exclusive of Taxes)	10
GST % for installation (e.g.: for 18% enter 18)	12

(End of Section –V)

Annexure – 1: Covering Letter

Date:

To:
Managing Director & CEO,
National E-Governance Services Ltd.
5th Floor, 'The Estate', 121,
Dickenson Road, Bengaluru – 560 042

Subject: Submission of proposal for Data Centre Managed Services

Dear Sir,

We, the undersigned, are interested in providing the Data Centre Services to National E-Governance Services Limited, Bengaluru, in response to your RFP No NESL/AO/RFP-DCMS/2023-24/1001, Dated: 27th October 2023. We are hereby submitting our Techno-Commercial proposal for the same, comprising of two separate folders, with password protection.

We hereby declare that all the information and statements made in this document are true and we accept that any misrepresentation contained in it may lead to our disqualification. We further confirm that we have read and understood all the terms/conditions/clauses stipulated in the RFP and agree to comply /abide by all the terms/conditions/clauses during the course of the RFP and subsequently if we are selected.

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

We also undertake that we have not been blacklisted/banned or debarred from bidding process for any reason, by any Department/Office of the Government of India or of any State Government, or such other authorities of law set-up or established by Government of India or any State Government, as on the date of submission of the bids and that there have been no regulatory actions initiated /pending against us as on the date of release of this RFP.

In we are selected for award of Contract, we undertake to sign with you, the necessary Service Level Agreement and Non-Disclosure Agreement, with appropriate and reasonable terms and conditions.

Yours sincerely,

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

Annexure – 2: Authority Letter

Date:

To:
Managing Director & CEO,
National E-Governance Services Ltd.
5th Floor, 'The Estate', 121,
Dickenson Road, Bengaluru – 560 042

Subject: Authority Letter

Reference: RFP No NESL/AO/RFP-DCMS/2023-24/1001, Dated: 27th October 2023.

Dear Sir,

We, M/s_____(Name of the bidder) having registered office at _____ (address of the bidder) herewith submit our bid against the said RFP 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

Designation
Mobile Number

Annexure – 3 Format of Bank Guarantee for EMD

(On Non-judicial paper of appropriate value)

[Date……..]

From:

Bank _____

_____

To,

National E-Governance Services Limited (NeSL)

5th Floor, The Estate, 121, Dickenson Road,

Bengaluru – 560 042

Dear Sir,

Whereas <<name of the bidder>> (hereinafter called 'the Bidder') has submitted the proposal against RFP NESL/AO/RFP-DCMS/2023-24/1001, Dated: 27th October 2023 for Providing _____ (nature of work) Services for Maintenance and Support of the _____ to National e-Governance Services Limited (NeSL).

The conditions of said RFP mention that the bidder shall submit Earnest Money Deposit of Rs. _____/- (Rs. _____) . M/s (Name of bidder) has agreed to submit the Earnest Money Deposit in the form of Bank Guarantee on their part. M/s. _____ (name of bidder) holds an account with us and has approached us and at their request and in consideration of the promises, we hereby furnish such guarantee as mentioned hereinafter.

1. We _____ (Name of the Bank), (hereinafter referred to as the "Bank"), do hereby undertake to pay to the NeSL forthwith on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding Rs _____/- (Rupees _____ only) and the guarantee will remain valid up to a period of 180 days from _____(the last day for submission of application) with claim period of one year. It will, however, be open to the NeSL to return the Guarantee earlier than this period to the Applicant, in case the applicant has been notified by the NeSL as being unsuccessful.
2. In the event of the successful application, if the applicant fails to acknowledge and accept the Letter of Award of Empanelment from NeSL in accordance with the terms and conditions of the

Empanelment Application, the EMD deposited by the applicant stands forfeited by the NeSL. We also undertake not to revoke this guarantee during this period except with the previous consent of the NeSL in writing and we further agree that our liability under the EMD shall not be discharged by any variation in the term of the said tender and we shall be deemed to have agreed to any such variation.

3. No interest shall be payable by the NeSL to the Applicant on the guarantee for the period of its currency.

4. Notwithstanding anything contained hereinabove:

a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs…….. (Rupees ……only)

b) This Guarantee shall remain in force up to……..(validity date) with claim a period till ……(claim date)(*one year beyond the validity of the BG)

c) Unless the demand/claim from the date of validity under this guarantee is served upon us in writing before _____(*) (one year beyond the validity of the BG)) all the rights of NeSL under this guarantee shall stand automatically forfeited and we shall be relieved and discharged from all liabilities mentioned hereinabove.

Dated this_____day of _____ 2023

For the Bank of _____

(For……..(Manager)

_____

Notes:

- The amount of bank guarantee is 2% of the total bidding value.
- *Claim period will be 1 year additional, beyond the validity date of bank guarantee under b) above
- Bank account details for NeSL

National E-Governance Services Limited

Canara Bank

Cantonment Branch

A/c no: 0404214000030

IFSC no: CNRB0000404

To:

Managing Director & CEO
National E-Governance Services Ltd.
5th Floor, 'The Estate', 121,
Dickenson Road, Bengaluru – 560 042

Dear Sir,

We, the undersigned, offer to provide Data Centre Services, in response to your RFP No NESL/AO/RFP-DCMS/2023-24/1001, Dated: 27th October 2023

We have read and understood the requirements of NeSL including those described in section IV titled SCHEDULE OF REQUIREMENTS. We hereby confirm that our bid/ offer meets all requirements of RFP. We hereby submit our complete compliance with each sub-section of section IV titled SCHEDULE OF REQUIREMENTS. We further confirm that we comply with each granular line item mentioned in respective sub sections 1 to 6 of the section IV SCHEDULE OF REQUIREMENTS. Deviations if any have been specifically mentioned in the section wise tables below. We further undertake that that any unreported deviations, if detected/observed later, we shall achieve complete compliance with respect to each such deviation within 10 calendar days from date of detection/observation any time during the contract period, at no extra cost to NeSL.

Table - 1: Scope

Sr No	Name	Completely complied with the stipulated specifications - Y/N	Provide Highlights and justification in case of deviation (if any)
1	Para-a		
2	Para-b		
3	Para-c		
4	Para-d		

Table - 2: General Technical requirements

Sr No	Name	Completely complied with the stipulated specifications - Y/N	Provide Highlights and justification in case of deviation (if any)
1.	Point-I.		
2.	Point-II.		
3.	Point-III.		
4.	Point- IV.		
5.	Point-V.		
6.	Point-VI.		
7.	Point-VII.		

8.	Point- VIII.		
9.	Point-IX.		
10.	Point-X.		
11.	Point-XI.		
12.	Point- XII.		
13.	Point-XIII.		
14.	Point-XIV.		
15.	Point-XV.		
16.	Point-XVI.		
17.	Point-XVII.		
18.	Point- XVIII.		
19.	Point-XIX.		
20.	Point-XX.		
21.	Point-XXI.		
22.	Point- XXII.		
23.	Point-XXIII.		
24.	Point-XXIV.		
25.	Point-XXV.		
26.	Point-XXVI.		
27.	Point-XXVII.		
28.	Point- XXVIII.		
29.	Point-XXIX.		
30.	Point-XXX.		
31.	Point-XXXI.		
32.	Point- XXXII.		
33.	Point-XXXIII.		
34.	Point- XXXIV.		
35.	Point-XXXV.		
36.	Point- XXXVI.		
37.	Point-XXXVII.		
38.	Point- XXXVIII.		
39.	Point- XXXIX.		

Table – 3: Technical Specifications

Sr Ref	Name	Completely complied with the stipulated specifications - Y/N	Provide Highlights and justification in case of deviation (if any)
A	Compute & Server/Virtual Machines Configurations		
B	Storage Specifications:		
C	Backup Solution: -		

	e) Provisioning of rack-based server for data backup. Please provide configuration and specifications. f) Provisioning of separate storage for backup. Please provide make, model, configuration. g) Provisioning of adequate number of licenses. h) Implementation as per NeSL		
D	Network Requirements/Specifications		
E	Managed Security Services Specifications		

Table - 4: Detailed Technical Specifications

Sr Ref	**Name**	**Completely complied Y/N**	**Provide details of Deviation if any**
a	Backup Software		
b	Network switches		
c	SNMP based EMS		
d	PAM		
e	Server Security /Antivirus		
f	SIEM		
g	NG Firewall		
h	WAF		

Table - 5: Reports

Sr No	**Name**	**Completely complied Y/N**	**Provide details of Deviation if any**
1	Daily reports (to be submitted on the next working day)		
2	Weekly Reports (to be submitted on the first working day of the following week)		
3	Monthly reports (to be submitted by 10th of the following month)		
4	Any Cyber Security Incident shall be Reported within 4 hours or as per the directives of the government from time to time.		
5	Other incidents, but not limited to, with detailed RCCA should be submitted within 48 hours.		

Table - 6: Data Centre Features

Sr No	**Name**	**Completely complied Y/N**	**Provide details of Deviation if any**
1	Air-Conditioning environment		
2	Physical Security		
3	Fire Protection System		
4	Raw Power		
5	Back-up power		
6	Building Monitoring System		
7	Up-time		
8	Other Features		

Yours sincerely,

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

Annexure – 5: Format of Bank Guarantee for Performance Security

(On Non-judicial paper of appropriate value)

Bank Guarantee No._____

[Date]

From:

Bank _____

To,

National E-Governance Services Limited (NeSL)

5th Floor, The Estate, 121, Dickenson Road,

Bengaluru – 560 042

Dear Sir,

This has reference to the contract / Order No. _____ Dated _____ been placed by National E-Governance Services Limited (NeSL) on M/s_____ (Name & Address of vendor) for Providing _____(nature of work) to National e-Governance Services Limited (NESL) The conditions of this order provide that the vendor guarantees successful and satisfactory performance of the _____ and/ or deployed, as per the requirements stipulated in this document and provide the _____ support as stipulated in the order/contract.

M/s_____ (Name of Vendor) has accepted the said purchase order / Contract with the terms and conditions stipulated therein and have agreed to issue the Performance Security in the form of Bank Guarantee on their part, towards promises and assurance of their contractual obligations vide the said Contract/Order. 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.

1. We ..... (hereinafter referred to as the "Bank") hereby undertake to pay to NeSL on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding Rs-------/- (Rupees ---- only) and the guarantee will remain valid for a period …….

2. We ..... do hereby undertake to pay the amounts due and payable under this Bank Guarantee without any demur, merely on a demand from NeSL stating that the amount claimed is required to meet the recoveries due or likely to be due from the said Applicant.
Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this Guarantee. However, our liability under this Guarantee shall be restricted to an amount not exceeding Rs. ----------/- (Rupees --------).

3. We, the said Bank, further undertake to pay to NeSL any money so demanded notwithstanding any dispute or disputes raised by the Applicant in any suit or proceeding pending before any Court or Tribunal or Board relating thereto, our liability under this Guarantee being absolute and unequivocal. The payment so made by us under this Guarantee shall be a valid discharge of our liability for payment thereunder, and the Applicant shall have no claim against us for making such payment.

4. We ..... further agree that the Guarantee herein contained shall remain in full force and effect during the period of contract with NeSL, or till NeSL certifies that the obligations of the Applicant have been fully and properly carried out by the said Applicant, and accordingly discharges this Bank Guarantee.

5. We ..... further agree with NeSL that it shall have the fullest liberty without our consent, and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said Empanelment or to extend time of performance by the said Applicant from time to time or to postpone for any time or from time to time any of the powers exercisable by NeSL against the said Applicant, and to forbear or enforce any of the terms and conditions relating to the said Empanelment, and we shall not be relieved from our liability by reason of any such variation or extension being granted to the said Applicant or for any forbearance, act of omission on the part of NeSL or any indulgence by NeSL to the said Applicant or by any such matter or thing whatsoever which under the law relating to sureties shall, but for this provision, have effect of so relieving us.

6. This Guarantee shall not be discharged due to the change in the constitution of the Bank or the Applicant.

7. We .....lastly undertake not to revoke this Guarantee except with the previous consent of the NeSL in writing.

8. This Guarantee shall be valid up to .....unless extended on demand by the NeSL. Notwithstanding anything mentioned above, our liability against this Guarantee is restricted to Rs. ----/- (Rupees --- only), and unless a claim in writing is lodged with us by NeSL within .....*(one year beyond the validity of the BG) all our liabilities under this Guarantee shall stand discharged.

Dated the ..... day of.....

For .....

(Indicate the name of the Bank)

_____ Notes:

1. The amount of bank guarantee is 10% of the total amount contract value including GST.
2. * Claim period shall be minimum one year from the end of the validity of bank guarantee
3. Bank account details for NeSL

   National E-Governance Services Limited

   Canara Bank

   Cantonment Branch

   A/c no: 0404214000030

   IFSC no: CNRB0000404

Annexure – 6: List of Abbreviations

SLNO	Abbreviations	Expansion
1	AD	Active Directory
2	AMC	Annual Maintenance Contract
3	AT	Acceptance Testing
4	ATP	Acceptance Test Plan and Procedure
5	ATS	Annual Technical Support
6	BG	Bank Guarantee
7	BMS	Business Management System
8	BOM	Bill Of Material
9	BOQ	Bill of Quantities
10	DC	Data Centre
11	DCO	Data Centre Operators
12	DR	Disaster Recovery
13	eBG	Electronic Bank Guarantee
14	EMD	Earnest Money Deposit
15	GST	Goods and Service Tax
16	GSTR	Goods and Services Tax Return
17	IBBI	Insolvency and Bankruptcy Board of India
18	IBC	Insolvency and Bankruptcy Code
19	IOPS	Input Output Per Second
20	IP	Internet Protocol
21	IPSec	Internet Protocol Security
22	ISO	International Organization for Standardization
23	LLD	Low Level Design
24	MSP	Managed Service Provider
25	MySQL	My Structured Query Language
26	NEFT	National Electronic Funds Transfer
27	NeSL	National E-Governance Services Limited
28	NFS	Network File System
29	OEM	Original Equipment Manufacturer
30	OoB	Out of Band
31	OS	Operating System
32	OSP	Original Software Publisher
33	PAM	Privilege Access Module
34	PO	Purchase Order

35	RFP	Request for Proposal
36	RHEL	Red Hat Enterprise Linux
37	RPO	Recovery Point Objective
38	RTGS	Real Time Gross Settlement
39	SD	Security Deposit
40	SIEM	Security Information and Event Management
41	SLA	Service Level Agreement
42	SOC	Security Operations Centre
43	SSL	Secure Sockets Layer
44	TCS	Tax Collected at Source
45	TDS	Tax Deducted at Source
46	TEC	Technical Evaluation Committee
47	TIA	Telecommunications Industry Association
48	VM	Virtual System
49	VPN	Virtual Private Network
50	WAF	Web Application Firewall
51	WAN	Wide Area Network

(End of Document)