RFP for IT Equipments Upgrade
of
Odisha State Data Centre (OSDC) Bhubaneswar

RFP Enquiry No. : **OCAC-NEGP-INFRA-0008-2021-22050**

Date : **22 JULY 2022**

DISCLAIMER

The information contained in this Tender document or subsequently provided to **Bidder(s)**, whether verbally or in documentary or any other form by Odisha Computer Application Centre (OCAC) or any of their employees is provided to Bidder(s) on the terms and conditions set out in this Tender Document and such other terms and conditions subject to which such information is provided.

This Tender is not an agreement and is neither an offer nor invitation by the OCAC to the Bidders or any other person. The purpose of this Tender is to provide interested parties with information that may be useful to them in making their technical and financial offers pursuant to this Tender (the "**Bid**"). This Tender includes statements, which reflect various assumptions and assessments arrived at by the OCAC in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This Tender may not be appropriate for all persons, and it is not possible for the OCAC, to consider the technical capabilities, investment objectives, financial situation and particular needs of each party who reads or uses this Tender. The assumptions, assessments, statements and information contained in this Tender, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations, studies and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this Tender and obtain independent advice from appropriate sources.

Information provided in this Tender to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OCAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way in this Bid Stage. OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this Tender.

OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this Tender. The issue of this Tender does not imply that OCAC is bound to select a Bidder or to appoint the Preferred Bidder, as the case may be, for the Project and OCAC reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the Tender, at any time without assigning any reason or providing any notice and without accepting any liability for the same.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OCAC or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and OCAC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

RFP SCHEDULE

Sl. No.	Items	Date & Time
01	Commencement of the bid	22 July 2022
02	Last date for receiving queries through E-mail: osdc@ocac.in, sk.bhol@nic.in and on GEM Portal	28 July 2022 by 05:00 PM
03	Pre Bid Conference (if required)	02 August 2022 by 04:00 PM
04	Issue of Corrigendum (if required)	05 August 2022
05	Last date and time for Submission of Bid through GEM Portal.	17 August 2022 by 02:00 PM
06	Opening of Pre-Qualification (PQ)	17 August 2022 by 04:00 PM
07	Opening of Commercial Bids (CB)	To be Informed.

Table of Contents

1. Fact Sheet

This Fact Sheet comprising important factual data of the tender is for quick reference of the bidder.

Clause Reference	Topic
The Proposal	Odisha Computer Application Centre (OCAC) invites bid for IT Equipments Upgrade of Odisha State Data Centre (OSDC) Bhubaneswar.
Method of Selection	Least Cost Based Selection (L1) method shall be used to select the bidder for Supply, Installation & Warranty Support of IT infrastructure equipments. The bidder has to apply the bid in three envelop system i.e. General (Pre-qualification), Technical & Commercial bids. Technical bid of those bidders who qualify in General Bid/ Pre-qualification, shall be opened. Commercial bid of those bidders who qualify in Technical Bid shall be opened. The least value bid (i.e. the bidder quoting minimum amount) will be given preference in the order of selection.
RFP Document	RFP Document can be downloaded from **http://www.ocac.in,** or **http://www.odisha.gov.in**. The bidders are required to submit the RFP document fee of ₹11,200/- (inclusive of 12% GST) in the form of a demand draft in favour of **"Odisha Computer Application Centre"**, payable at **Bhubaneswar** from any of the Scheduled Commercial Bank along with the Proposal.
Bid Security Declaration Form	Bid Security Declaration Form (Form-3)
Scope of Work	Selected agency is expected to deliver the services listed in Scope of Work as mentioned in this RFP.
Language	Bid must be prepared by the Bidder in English language only
Currency	The bidder should quote in Indian Rupees only. The Total Price inclusive of taxes and duties will be considered for evaluation. So, the bidder must mention the base price and the tax component separately.
Validity Period	Proposals/ bid must remain valid minimum for 180 days from the last date of bid submission.
Bid to be submitted on or before last date of submission at:	The Proposal shall be submitted in online mode only on GEM Portal. The bidder should register himself in GEM Portal to apply for the bid.

2. Information

i. Odisha Computer Application Centre (OCAC) invites responses ("Tenders") to this Request for Proposals ("RFP") from OEMs /authorized Partners ("Bidders") for the provision of items as described in this RFP. OCAC is the Nodal Agency for this Government procurement.

ii. Proposals must be received not later than time, date and venue mentioned in the Fact Sheet. Proposals that are received after the dateline WILL NOT be considered in this procurement process.

3. Background

Odisha Computer Application Centre (OCAC), the Designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, intends to upgrade the existing IT Infrastructure of State Data Centre (OSDC).

To scale-up the existing Compute Infrastructure below is list of devices to be procured through this RFP:-

1.	Router	:	02 Nos.
2.	Core Switch	:	02 Nos.
3.	Network Switch	:	08 Nos.
4.	Access Switch	:	01 Nos.
5.	AAA	:	02 Nos.
6.	NG Firewall	:	02 Nos.
7.	Patch Cords	:	As per the details mentioned in this RFP

4. Instructions to the Bidders

4.1. General

i. While every effort has been made to provide comprehensive and accurate background information, requirements, and specifications, Bidders must form their own conclusions about the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

ii. All information to be supplied by Bidders will be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

iii. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of OCAC with the bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of OCAC.

iv. This RFP supersedes and replaces any previous public documentation & communications in this regard and Bidders should place no reliance on such communications.

4.2. Compliant Tenders / Completeness of Response

i. Bidders are advised to study all instructions, forms, requirements, appendices and other information in the RFP documents carefully. Submission of the bid / proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

ii. Failure to comply with the requirements of this paragraph may render the Proposal non- compliant and the Proposal will be rejected. Bidders must:
   a. Comply with all requirements as set out within this RFP.
   b. Submit the forms as specified in this RFP and respond to each element in the order as set out in this RFP.
   c. Include all supporting documentations specified in this RFP.

4.3. Pre-Bid Meeting & Clarifications

4.3.1. Bidders Queries

a. OCAC shall hold a pre-bid meeting with the prospective bidders on scheduled date at OCAC premises or through Video Web Conference.
b. The Bidders will have to ensure that their queries for Pre-Bid meeting should reach in e-mail id – osdc@ocac.in and sk.bhol@nic.in only on or before the scheduled timeline. Queries submitted after the scheduled date and time, shall not be accepted.
c. The queries should necessarily be submitted in the following format:

Sl. No.	RFP Document Reference(s) (Section & Page Number(s))	Content of RFP requiring Clarification(s)	Points of Clarification
1.			
2.			

d. OCAC shall not be responsible for ensuring that the bidder's queries have been received by them. Any requests for clarifications after the indicated date and time shall not be entertained by OCAC.

4.3.2. Responses to Pre-Bid Queries and Issue of Corrigendum

a. OCAC will endeavor to provide timely response to all valid queries. However, OCAC makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does OCAC undertake to answer all the queries that have been posed by the bidders.
b. At any time prior to the last date for receipt of bids, OCAC may, for any reason, modify the RFP Document by a corrigendum.
c. The Corrigendum (if any) & clarifications to the queries from all bidders will be posted on the websites www.ocac.in, www.odisha.gov.in and on GEM Portal.
d. Any such corrigendum shall be deemed to be incorporated into this RFP.
e. In order to provide prospective Bidders reasonable time for taking the corrigendum

into account, OCAC may, at its discretion, extend the last date for the receipt of Proposals.

4.4. Key Requirements of the Bid

4.4.1. Right to Terminate the Process

i) OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.

ii) This RFP does not constitute an offer by OCAC. The bidder's participation in this process may result OCAC selecting the bidder to engage towards execution of the contract.

4.4.2. Right to alter Quantities

OCAC reserves the right to reduce the quantity or give repeat order to the **L1 bidder as per requirement**, within the tender validity period of **180 days** from the last date of submission of bid under same terms and conditions with same Specifications and Rate. Any decision of OCAC in this regard shall be final, conclusive and binding on the bidder. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.

4.4.3. Confidential Information

OCAC and Selected bidder shall keep confidential and not, without the written consent of the other party hereto, divulge to any third party any documents, data, or other information furnished directly or indirectly by the other party hereto in connection with the Contract, whether such information has been furnished prior to, during or following completion or termination of the Contract.

4.4.4. RFP Document Fees

RFP document can be downloaded from the website www.ocac.in, www.odisha.gov.in & on GEM Portal. The bidders are required to submit the RFP document Fee in form of Demand Draft in favour of "Odisha Computer Application Centre" and payable at Bhubaneswar from any of the Scheduled Commercial Bank along with the Proposal. Proposals received without or with inadequate RFP Document fees shall be rejected.

4.4.5. Bid Security Declaration Form

Bidder needs to be submitted along with this bid as per the prescribed format attached at **Form-3** in tis RFP.

4.4.6. Performance Bank Guarantee (PBG)

i. OCAC will require the selected bidder to provide a Performance Bank Guarantee (PBG) within 15 days from the Notification of award, for a value equivalent to 3% of the total order value.

ii. The Performance Bank Guarantee needs to be valid till Entire Project Period of 5 Years. The Performance Bank Guarantee shall contain a claim period of three months from the last date of validity. The selected bidder shall be responsible for extending

the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period.

iii. In case the selected bidder fails to submit performance Bank guarantee within the time stipulated, OCAC at its discretion may cancel the order placed on the selected bidder without giving any notice and barred the bidder in all the future procurement process as per the Bid Security Declaration.

iv. In that event OCAC may award the Contract, at (L1) rate, to the next best value bidder (L2), whose offer is valid and substantially responsive and determined by OCAC.

v. OCAC shall invoke the performance Bank Guarantee in case the selected bidder fails to discharge their contractual obligations during the period or OCAC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.

vi. Performance Bank Guarantee shall be refunded within three months of the successful completion of the contract period i.e., expiry of "Warranty and Support Services" of individual package.

vii. No interest will be paid by OCAC on the amount of performance Bank Guarantee

4.4.7. Deadline for Submission of proposals

Proposals, in its complete form in all respects as specified in the RFP, must be submitted through online at the GEM potal on or before the due date as per the RFP.

4.4.8. Late Bids

i. Bids received after the due date and the specified time for any reason whatsoever, shall not be entertained.

ii. The bids submitted by telex/ telegram/ fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

iii. OCAC reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities and need.

4.5. Offer Validity

Offers should be valid for minimum One hundred eighty (180) Days from the date of opening the Technical Bid. A bid, valid for a shorter period, is liable to be rejected. OCAC, Bhubaneswar may ask the bidders to extend the period of validity, if required.

4.6. Delivery

The delivery of infrastructure items to be completed within 12 (Tweleve) Weeks from the date of issue of the Purchase Order.

Delivery Location: **Odisha State Data Centre (OSDC), Bhubaneswar**

4.7. Product Specifications & Compliance Statement:

The bidder should quote the products strictly as per the tender specifications and only of technically reputed and globally acclaimed brands / makes. Complete technical details along with brand, specification, technical literature etc. highlighting the specifications

must be supplied along with the technical bid. A Statement of Compliance shall be given against each item in the prescribed format given in Technical specifications. The compliance statements should be supported by authentic documents. Each page of the bid and cuttings / corrections shall be duly signed and stamped by the authorized signatory. Failure to comply with this requirement may result in the bid being rejected.

4.8. Price

The prices are to be quoted in INR in figure only. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.

4.9. Unsatisfactory Performance

The Parties herein agree that OCAC shall have the sole and discretionary right to assess the performance(s) of the Bidder components(s), either primary and or final, and OCAC, without any liability whatsoever, either direct or indirect, may reject the system(s) component(s) provided by the Bidder, in part or in its entirety, without any explanation to the Bidder, either during the pre and or post test period should the same be unsatisfactory and not to the acceptance of OCAC. The Bidder covenants to be bound by the decision of OCAC without any demur in such an eventuality.

4.10. Dispute Resolution

i. Any dispute or difference, whatsoever, arising between the parties to this agreement arising out of or in relation to this agreement shall be amicably resolved by the Parties through mutual consultation, in good faith and using their best endeavours. Parties, on mutual consent, may refer a dispute to a competent individual or body or institution or a committee of experts appointed By OCAC (Nodal Authority) for such purpose and abide by the decisions thereon.

ii. On non settlement of the dispute, same shall be referred to the commissioner-cum-secretary to Government, IT department, and Government of Odisha for his decision and the same shall be binding on all parties, unless either party makes a reference to arbitration proceedings, within sixty days of such decision.

iii. Such arbitration shall be governed in all respects by the provision of the Arbitration and Conciliation Act, 1996 or later and the rules framed there under and any statutory modification or re-enactment thereof. The arbitration proceeding shall be held in Bhubaneswar, Odisha

4.11. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected bidder or OCAC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:

i. Natural phenomenon, including but not limited to floods, droughts, earthquakes and epidemics.

ii. Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos.

iii. Terrorist attack, public unrest in work area provided either party shall within 10 days from occurrence of such a cause, notifies the other in writing of such causes.

In case of a Force Majeure, all Parties will endeavor to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure

4.12. Disclaimer

This Tender / Request for Proposal (RFP) is not an offer by OCAC, but an invitation for bidder's response. No contractual obligation whatsoever shall arise from the RFP process.

4.13. IT Act

Besides the terms and conditions stated in this document, the contract shall also be governed by the overall acts and guidelines as mentioned in IT Act 2000 and subsequent amendments, and any other guideline issued by State from time to time.

4.14. Declaration

The bidder would be required to give a certificate as below in his commercial bid.

A) *"I/WE UNDERSTAND THAT THE QUANTITY PROVIDED ABOVE IS SUBJECT TO CHANGE. I/WE AGREE THAT IN CASE OF ANY CHANGE IN THE QUANTITIES REQUIRED, I/ WE WOULD BE SUPPLYING THE SAME AT THE RATES AS SPECIFIED IN THIS COMMERCIAL BID. I /WE AGREE TO ADHERE TO THE PRICES GIVEN IN THE FINANCIAL BID OF THIS RFP EVEN IF THE QUANTITIES UNDERGO A CHANGE. I/WE FURTHER UNDERTAKE THAT IN CASE OCAC REQUIRES, WE WILL DEMONSTRATE THE QUOTED PRODUCTS WITH 7 DAYS NOTICE FROM OCAC."*

B) *The OEM/ PRODUCT MANUFACTURED IN A COUNTRY SHARING A LAND BORDER WITH INDIA CANNOT PARTICIPATE IN THIS BID.*

5. Scope of Work

Supply, Installation, Configuration & Comprehensive Onsite Warranty Support of supplied IT Hardwares as per the technical specification.

5.1. Router

5.1.1. Total Quantity = 02 Nos

5.1.2. Technical Specification (Make and Model)

Sl. No.	Specifications	Compliance (Yes/No)
OEM Eligibility Criteria		
1	OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI. OEM must have India presence for last 5 years on both Sales and Support operation.	
WAN interfaces		
2	The Router should support 1G,10G WAN ports	
3	The Router should support internal loopback testing for maintenance purposes and an increase in availability, loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility.	
4	The Router should support minimum 4 payload/module slots or more	
Resiliency and high availability		
5	The Router should support Separate data and control planes to provide greater flexibility and enable continual services.	
6	The Router should support Hot-swappable modules	
7	The Router should have redundant hot-swappable power supply	
8	The Router should support Virtual Router Redundancy Protocol (VRRP)	
9	The Router should support Graceful restart including graceful restart for OSPF, IS-IS, BGP, LDP, and RSVP.	
10	The Router should support nonstop forwarding (NSF) and nonstop routing.	
11	The Router should support Hitless/ ISSU software upgrades of software packages.	
12	The Router should support IP Fast Reroute Framework (FRR)/ Multicast over FRR.	
Architecture		
13	The Router should support Distributed/Centralized processing	
14	The Router should support powerful processing, encryption, and comprehensive HQoS functionalities with four levels	
15	19" rack mountable design. Must be offered with rack mounting kit.	
Performance Requirement		

16	The Router should provide minimum aggregate throughput bandwidth of 5 Gbps scalable up to 20 Gbps and 14 Mpps of forwarding performance or more.	
17	The Router should have 100000 entries (IPv4), 100000 entries (IPv6) in forwarding information base or Routing table size and at least 2000 multicast routes.	
Layer 3 Routing		
18	The Router should support Static IPv4 routing	
19	The Router should support Routing Information Protocol (RIP) V2	
20	The Router should support Open Shortest Path First (OSPF) ,Interior Gateway Protocol (IGP) uses link-state protocol for faster convergence; supports ECMP and MD5 authentication for increased security and graceful restart for faster failure recovery	
21	The Router should support Border Gateway Protocol 4 (BGP-4)	
22	The Router should support Intermediate system to intermediate system (IS-IS) Interior Gateway Protocol (IGP) uses path vector protocol	
23	The Router should support Static IPv6 routing	
24	The Router should maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design The Router should support OSPF for IPv6	
25	The Router should support BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing	
26	The Router should support IS-IS for IPv6	
27	The Router should support IPv6 tunneling	
28	The Router should support Multiprotocol Label Switching (MPLS)	
29	The Router should support Multiprotocol Label Switching (MPLS) Layer 3 VPN	
30	The Router should support Multiprotocol Label Switching (MPLS) Layer 2 VPN	
31	The Router should support Policy routing	
32	The Router should support Multicast VPN	
33	The Router should support Virtual Private LAN Service (VPLS)	
34	The Router should support Bidirectional Forwarding Detection (BFD)	
35	The Router should support IGMPv1, v2, and v3	
36	The Router should support PIM-SSM, PIM-DM/ PIM-SM (for IPv4 and IPv6) and support IP Multicast address management and inhibition of DoS attacks	
37	The Router should support Equal-Cost/Unequal-Cost Multipath (ECMP/UCMP)	
38	The Router should support OSPFv3 Multi-VPN-Instance	

39	The Router should support OSPFv3 Multi-VPN-Instance /6PE feature to create and maintain separate OSPFv3 routing tables for each IPv6 VPN 6PE to isolate VPN services in the device	
Layer 3 Services		
40	The Router should support Address Resolution Protocol (ARP)	
41	The Router should support User Datagram Protocol (UDP) helper	
42	The Router should support Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)	
43	The router should support Data Centre features like DCI, EVPN, VXLAN	
Security		
44	The Router should support Dynamic Virtual Private Network (DVPN), IPSEC VPN or any equivalent mechanism or equivalent	
45	The Router should have Stateful firewall/Zone-based firewall	
46	The Router should support powerful ACLs for both IPv4 and IPv6 to use for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; and support rule based on a Layer 2 header or a Layer 3 protocol header and specific dates or times	
47	The Router should support Secure shell (SSHv2)	
48	Remote Authentication Dial-In User Service (RADIUS)	
49	The Router should support Terminal Access Controller Access-Control System (TACACS+)	
Quality of Service (QoS)		
50	The Router should support powerful processing, HQoS/Nested QoS functionalities with four levels	
51	The Router should support Traffic policing and support Committed Access Rate (CAR) and line rate	
52	The Router should support Congestion management technique like FIFO/PQ/ CQ/ WFQ/ CBQ/ RTPQ	
53	The Router should support Congestion avoidance technique Weighted Random Early Detection (WRED)/Random Early Detection (RED)	
54	The Router should support traffic shaping, MPLS QoS, and MP QoS/LFI	
Management		
55	The Router should support Industry-standard CLI with a hierarchical structure	
56	The Router should support SNMPv1, v2, and v3	
57	provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption; provide alerts (via SNMP, logging, and/or SMTP) for system health and blocking/filtering actions	
58	The Router should support enables or disables console port, Telnet port, or reset button interfaces depending on security preferences:	
59	The Router should support Remote monitoring (RMON)	

Management security		
60	The Router should restricts access to critical configuration commands and offers multiple privilege levels with password protection, ACLs provide Telnet and SNMP access, local and remote syslog capabilities allow logging of all access	
61	The Router should support FTP, TFTP, and SFTP support	
62	The Router should support ping and traceroute for both IPv4 and IPv6	
63	The Router should support Network Time Protocol (NTP)	
64	The Router should support RFC3164 Syslog Support	
Multicast support		
65	The Router should support Internet Group Management Protocol (IGMP)	
66	The Router should support Multicast Source Discovery Protocol (MSDP)	
67	The Router should support Multicast Border Gateway Protocol (MBGP)/BGP.	
Required Interfaces		
68	4 no's 10G SFP+ ports, 4 no's of 1G fibre and 4 no's 1G BaseT ports. All transceiver module to be populated from Day 1. Management port 1G BaseT for monitoring.	
69	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)	

5.2. Core Switch

5.2.1. Total Quantity = 02 Nos

5.2.2. Technical Specification (Make and Model)

Sl. No.	Specifications	Compliance (Yes/No)
OEM Eligibility Criteria		
1	OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI. OEM must have India presence for last 5 years on both Sales and Support operation.	
Solution Requirement		
2	The core layer switches should have hardware level redundancy (1+1) in terms of control plane. Issues with any of the plane should not impact the functioning of the switch. 19" rack mountable design. Must be offered with rack mounting kit.	
3	The switch should have redundant CPUs from day 1. Switch dual supervisor configuration must allow nonstop forwarding (NSF) with a stateful switchover (SSO) when a supervisor-level failure occurs.	
4	The Switch should support non-blocking architecture, all proposed ports must provide wire speed line rate performance	

5	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch	
6	Switch should support the complete STACK of IP V4 and IP V6 services.	
7	All relevant licenses for all the features and scale should be quoted along with switch	
8	Switch and optics should be from the same OEM	
Hardware and Interface Requirement		
9	Switch should have the following interfaces: (i) 1G/ 10G SFP+ 48 Port (Fibre) Line Card = Populated with 24 Nos 10G SFP+ [(20 SR, should work upto 100m) and (4 LR, should work upto 2KM)] Transreciver modules. (ii) 40G/ 100 QSFP+ Port (Fibre) Line Card = Populated with 24 Nos 40G QSFP+ [(20 SR, should work upto 100m) and (4 LR, should work upto 10KM)] Transreciver modules. Populated with 6 Nos with 100G QSFP28 [(2 SR, should work upto 100m) and (4 LR, should work upto 10KM)] Transreciver modules. (iii) Management port 1G BaseT for monitoring. Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)	
10	Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy	
Performance Requirement		
11	Switch should support Graceful Restart for OSPF, BGP etc. Should support uninterrupted forwarding operation to ensure high-availabability during primary controller failure	
12	Switch should support minimum 1000 VRF instances with route leaking functionality	
13	The switch should support minimum 500K IPv4 LPM routes	
14	The line card proposed should have minimum 150MB Packet Buffer per LC	
15	The switch should support 100K multicast routes	
16	Switch should support a minimum of 15 Tbps Bandwidth/ Switching Capacity)	
Network Virtualization Features		
17	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN	
18	Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
19	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
20	Switch should support VLAN Trunking (802.1q)	
21	Switch should support minimum 500K of MAC addresses	

22	Switch should support VLAN tagging (IEEE 802.1q)	
23	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
24	Switch should support layer 2 extension over VXLAN across all DataCenter to enable VM mobility & availability	
25	The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
Layer3 Features		
26	Switch should support static and dynamic routing	
27	Switch should support segment routing and VRF route leaking functionality from day 1	
28	Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Support Multicast Source Discovery Protocol (MSDP)	
29	Switch should support Multicast routing	
Quality of Service		
30	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)	
31	Switch should support for different type of QoS features for ream time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
32	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
Security		
34	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
35	Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
36	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
37	Switch platform should support MAC Sec (802.1AE) in hardware	
38	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
Manageability		
39	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
40	Switch should provide remote login for administration using: a. Telnet b. SSH c. CLI	

	d. Console	
41	• Flow path trace (ingress to egress switch) • Latency and packet drop	
42	• Utilization of Operational like MAC/Route & Hardware resources like port utilization/ BW • Switch environmentals like (CPU/memory/FAN/Power Supply) • Interface statistics like CRC error	
43	Switch should support for management and monitoring status using different type of Industry standard NMS using: SNMP V1, SNMP V2 and SNMP v3 with Encryption Remote monitoring (RMON) support	
44	Switch should provide different privilege for login in to the system for monitoring and management	
QoS and Security Features		
45	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network	
46	Port-based rate limiting and access control list (ACL) based rate limiting	
47	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence	
48	Shall support Strict Priority Queuing (SP)/Weighted Fair Queuing (WFQ)/Weighted Deficit Round Robin (WDRR)configurable buffers and Explicit Congestion Notification (ECN)	
49	Shall support Weighted Random Early Detection (RED) /Random Early Detection (RED) for congestion avoidance	
50	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers	
51	ARP attack protection to protect against attacks that use a large number of ARP requests	
52	Port security to allow access only to specified MAC addresses. Switch should also support 802 1x authentication and accounting, MACSec-128 or equivalent, IPv4 and IPv6 ACLs and Dynamic VLAN assignment	
53	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds	

5.3. Network Switch

5.3.1. Total Quantity = 08 Nos

5.3.2. Technical Specification (Make and Model)

Sl. No.	Specifications	Compliance (Yes/No)
OEM Eligibility Criteria		
1	OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI.	

	OEM must have India presence for last 5 years on both Sales and Support operation.	
Solution Requirement		
2	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
3	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy. 19" rack mountable design. Must be offered with rack mounting kit.	
4	Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system	
5	IPV6 Compliant: • Solution should be IPV6 ready from day1. No extra cost will be borne for IPV6 implementation • Switch should support the complete STACK of IP V4 and IP V6 services	
6	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied	
7	Switch port should well-matched and linked with firewall, IPS, Blade and Rack servers 10Gb/40Gb ports of OEM like HP, IBM, DELL etc.	
9	Switch should supplied with Indian standard compatible IEC C13/C14 3pin power cord suitable for PDU.	
10	Switch should be supplied with necessary pathcord for HA	
11	Proposed solution should not declared with eol, eos or end of support by OEM. in the day of production.	
Hardware and Interface Requirement		
12	Minimum 48 ports support 1/10/25 Gbps SFP+ ports for host connectivity and 6*40/100G QSFP+ports for uplink connectivity Switch should have the following interfaces: i. 48 x 10/25G SFP+ Fibre ports with 10/25G SFP28 SR modules loaded. ii. 6 x 40/100 QSFP+ GbE fibre ports with 40G QSFP+ SR modules loaded iii. Additional 4 nos. of 1G Base-T copper module. (for downgrade use) Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)	
13	Switch should be rack mountable and support side rails if required	
14	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant hot swappable.	
15	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
16	Switch should support VLAN tagging (IEEE 802.1q)	
17	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
18	Switch should support Configuration roll-back and check point	

19	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc	
20	Switch should have console port	
Performance Requirement		
21	The switch should support 12,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	
22	Switch should support Graceful Restart for OSPF, BGP etc.	
23	Switch should support minimum 500 VRF/VNI instances	
24	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability.	
25	The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG	
26	Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services: a. Switching b. IP Routing (Static/Dynamic) c. IP Forwarding d. Policy Based Routing e. QoS f. ACL and Other IP Services g. IP V.6 host and IP V.6 routing	
Advance Features		
27	Switch should support Data Center Bridging	
28	Switch should support common configuration like mirroring, trunking, port violation, port restriction, inter VLAN routing, STP, BPDU, etc.	
29	Switch should support multi OEM hypervisor environment and should support features for programmable configuration change	
Layer2 Features		
30	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)	
31	Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN	
32	Switch should support basic Multicast IGMP v1, v2, v3	
33	Switch should support minimum 90,000 no. of MAC addresses	
34	Switch should support 8 Nos. of link or more per port channel (using LACP).	
35	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.	
36	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server	
37	Switch should support Jumbo Frames up to 9K Bytes on Ports	
38	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
39	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
Layer3 Features		

40	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface	
41	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing	
42	Switch should support static and dynamic routing using: a. Static routing b. OSPF V.2 using MD5 Authentication c. IS-IS using MD5 authentication or equivalent policy based routing d. BGP V.4 using MD5 Authentication e. Should support route redistribution between these protocols f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)	
43	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols	
44	Switch should be capable to work as DHCP server and relay	
Availability		
45	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
46	Switch should provide gateway level of redundancy in IpV4 and IPV6 using HSRP/VRRP	
47	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
Quality of Service		
48	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point) c. Source physical interfaces d. Source/destination IP subnet e. Protocol types (IP/TCP/UDP) f. Source/destination TCP/UDP ports	
49	Switch should support methods for identifying different types of traffic for better management and resilience	
50	Switch should support for different type of QoS features for ream time traffic differential treatment using a. Weighted Random Early Detection. b. Strict Priority Queuing.	
51	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
52	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
Security		
53	Switch should support for deploying different security for each logicaland physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail	

54	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
55	Time based ACL/Equivalent.	
56	Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
57	Switch should support MAC Address Notification on host join into the network for Audit trails and logging	
58	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
59	Switch should support DHCP Snooping	
60	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
61	Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	
62	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
63	Switch should support Spanning tree BPDU protection	
64	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
65	Switch should support Spanning tree BPDU protection	
66	Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed as per banks ISD rules	
Manageability		
67	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
68	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
69	Switch should provide remote login for administration using: a. Telnet b. SSH V.2	
70	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
71	Switch should support for management and monitoring status using different type of Industry standard NMS using: a. SNMP V1 and V.2 b. SNMP V.3 with encryption c. Filtration of SNMP using Access list d. SNMP MIB support for QoS	

72	Switch should support for basic administrative tools like: a. Ping b. Tracerout	
73	Switch should support central time server synchronization using Network Time Protocol NTPv4/SNTPv4.	
74	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	
75	Switch should support scripting/API for device manage for automatic and scheduled system status update formonitoring and management	
76	Switch should provide different privilege for login in to the system for monitoring and management	
77	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding	
IPv6 features		
78	Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such a. OSPF V.3 b. BGP with IP V.6 c. IP V.6 Policy based routing d. IP V.6 Dual Stack etc e. IP V.6 Static Route f. IP V.6 Default route	
79	Should support route redistribution between these protocols	
80	Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode	
81	Switch should support for QoS in IP V.6 network connectivity	
82	Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: a. SNMPv1, SNMPv2c, SNMPv3 b. SNMP over IP V.6 with encryption support for SNMP Version 3	
83	Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment	
84	Switch should support NTP/SNTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events	
85	Switch should support for IP V.6 different types of tools for administration and management such as: a. Ping b. Traceroute c. VTY d. SSH e. TFTP f. DNS lookup	

5.4. Access Switch

5.4.1. Quantity = 01 No

5.4.2. Technical Specification (Make and Model)

Sl.No.	Tecnical Specification	Compliance (Yes/No)
OEM Eligibility Criteria		
1	OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI. OEM must have India presence for last 5 years on both Sales and Support operation.	
Architecture		
2	19" rack mountable configuration. Rack mounting kit must be provided.	
3	Shall have routing/switching capacity minimum of 560 Gbps of forwarding performance	
4	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.	
5	Shall deliver a maximum of 6 micro second latency with consistent performance across a broad range of applications with typical mixed loads of real-time, multicast and storage traffic.	
6	32K MAC entries or more	
Resiliency		
7	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links	
8	Shall have redundant hot swap power supplies (1+1) from Day 1.	
9	Switch should supplied with compatible IEC C13/C14 3pin power cord suitable for PDU.	
10	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol	
11	IEEE 802.3ad Link Aggregation Control Protocol (LACP)	
Layer 2 Features		
12	Shall support up to 3950 port or IEEE 802.1Q-based VLANs	
13	Shall support Jumbo frames of 9K bytes	
14	Internet Group Management Protocol (IGMP)	
15	Multicast Listener Discovery (MLD) or IGMP snooping	
16	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
17	IEEE 802.3ad Link Aggregation Control Protocol (LACP)	
Layer 3 Features (any additional licenses required shall be included)		
18	Static Routing for IPv4 and IPv6	
19	Dynamic Host Configuration Protocol (DHCP) Client/ Relay or Server.	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
QoS and Security Features		
20	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network	
21	Port-based rate limiting and access control list (ACL) based rate limiting	
22	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence	
23	Shall support Strict Priority Queuing (SP)/Weighted Fair Queuing (WFQ)/Weighted Deficit Round Robin (WDRR)configurable buffers and Explicit Congestion Notification (ECN)	
24	Shall support Weighted Random Early Detection (RED) /Random Early Detection (RED) for congestion avoidance	
25	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers	
26	ARP attack protection to protect against attacks that use a large number of ARP requests	
27	Port security to allow access only to specified MAC addresses	
28	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds	
Management Features		
29	Configuration through the CLI, console, Telnet, and SSH	
30	SNMPv1, v2, and v3 and Remote monitoring (RMON) support	
31	NetFlow/sFlow or equivalent for traffic analysis	
32	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.	
33	RADIUS/TACACS+ for switch security access administration	
34	Network Time Protocol (NTP) or equivalent support	
Required Interfaces		
35	48 ports of 1G BaseT and 4 ports of 10G SFP+ with 10G SFP+ transreciever modules.	
36	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface). All the transceivers should be from the same OEM as the switch.	

5.5. AAA

5.5.1. Quantity = 02 No

5.5.2. Technical Specification (Make and Model)

Sl.No.	Tecnical Specification	Compliance (Yes/No)
	OEM Eligibility Criteria	
1	The AAA solution offered must be rated as leaders or Challenger's in the latest published Magic Quadrant by Gartner for AAA. Offered solution shall be Common Criteria certified for Network Access Control (NAC).	
	Specification	
2	19" rack mountable design. Must be offered with rack mounting kit. The proposed solution shall meet the below specifications. Any hardware/software/ licenses required to enable the functionality shall be provided from Day 1	
3	The solution must support Authentication, authorization, and accounting (AAA) protocols RADIUS and TACACS+	
4	Shall provide authentication, user or administrator access, and policy control for centralized access control. The solution must support an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers.	
5	Offered solution must support scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as authentication protocol, user's role, device attributes, location, and time of day etc.	
6	The solution must support authentication protocols like PAP, MS-CHAP, EAP-MD5, PEAP and EAP-TLS.	
7	Offered solution shall support use of multiple authentication protocols concurrently.	
8	Offered solution shall support multiple identity stores such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy	
9	Offered solution shall provide TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user.	
10	Shall provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type, using contextual data and use this data for optimizing access policies	
11	Shall support identification of device profile changes.	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
12	Shall support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI/Auth or TCP SYN-ACK handshakes	
13	Shall support Support active device profiling methods such as SNMP, Subnet Scan, SSH and NMAP Scan	
14	Shall support user as well as device authentication based on 802.1X, non-802.1X, and Web Portal access methods across multi-vendor wired networks, wireless networks, and VPNs.	
15	Shall support identifying non-802.1x devices as known/unknown type.	
16	Shall provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy	
17	Shall provide for defining sets of ACLs that can be applied per user or per group for layer 3 network devices like routers, firewalls and VPNs	
18	Shall support HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management	
19	Shall support processing of events or data (by using API or Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.	
20	Shall support customizable Reporting with manual or scheduled reports in PDF/CSV/HTML formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email/SMS	
21	Offered solution shall be based on hardware appliance and solution must be deployed with 1:1 redundancy.	
22	The solution must support a web-based GUI centralised management for primary and secondary instances. The centralised management must support management of software upgrades on both primary and secondary instances.	
23	The solution must include monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI	
24	Solution shall be provided with required licenses for minimum 200 concurrent sessions for AAA and TACACS+ access on Day 1. Solution shall be scalable up to 400 concurrent sessions without any hardware change.	
25	Shall have redundant hot swap power supplies (1+1) from Day 1. Switch should supplied with compatible IEC C13/C14 3pin power cord suitable for PDU.	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
26	The device should populated with atleast 5000 node/ device/ equipment licenses for authentication (AAA) management. Minimum ports 2 * 1G Copper (Base-T)	

5.6. Next Generation Firewall

5.6.1. Quantity = 02 Nos.

5.6.2. Technical Specification (Make and Model)

Sl.No.	Tecnical Specification	Compliance (Yes/No)
	OEM Eligibility Criteria	
1	The Firewall solution offered must be rated as “leaders“ in the latest Magic Quadrant for Enterprise Firewall published by Gartner or should be a "Leader" in the latest Forrester Wave for Enterprise Firewall report.	
2	OEM must have India presence for last 5 years for sales and must have support in India	
3	The proposed OEM must have completed NSS Labs’ NGFW Methodology testing with a minimum exploit blocking rate of 95% and should be Leader in the 2021 Gartner Magic quadrant for Enterprise Firewall report or should be a Leader in the latest Forrester Wave for Enterprise Firewall report and must have a track record of continuous improvement in threat detection (IPS)	
4	The OEM should ensure that the solution should be operational for 5 years, with all core feature / functionalities enabled on the platform.	
	Specification	
5	The proposed solution/appliance MUST be for Layer 7 protection. There should be no performance degradation in the overall transaction processing. The solution MUST be deployed in HA mode.	
6	The proposed solution must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS and scheduling.	
7	The proposed solution must allow policy creation for application identification, user identification, threat prevention and content filtering in a single window and not multiple locations	
8	The proposed solution should have the features of stateful firewall, IPS, Application control, Content Inspection, Identity Inspection, Anti-BOT, Antivirus and Zero-day malware protection from day one. Proposed solution should provide a threat prevention throughput of 10 Gbps for traffic conditions enabling application visibility control, user identity, NGIPS, Antivirus and all other security threat prevention	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
	features enabled with HTTP transactions, HTTPS and traffic mix such as HTTPS, SMTP and other protocols.	
9	19" rack mountable configuration. Rack mounting kit must be provided. The proposed solution should have dual redundant power supply and minimum 128 GB memory/RAM and Hardware level redundancy. The device NGFW throughput to be of minimum of 25 Gbps.	
10	The proposed firewall appliance should have at least 12 ports of 1/ 10G SFP+ with 10G SFP+ Transreceiver modules (additional 4 nos of 1G copper to be supplied for downgrade use) and 4 nos of 40G QSFP+ ports with 40G QSFP+ transreciever modules for Uplink. Management Port 1G BaseT for monitoring or SFP port with 1G BaseT suitable module to be supply.	
11	The proposed solution must be able to support Network attack detection, DoS, DDoS,TCP Reassembly , Brute Force, Syn Cookie, IP Spoofing, Malformed Packet etc.	
12	The proposed solution must support Tap mode interface configuration.	
13	The proposed solution should be integrated with the proposed SDN solution for north -south security	
14	The proposed solution be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2 Transparent and Tap modes.	
15	The proposed solution shall support 802.1Q VLAN tagging.	
16	The proposed solution shall support Dual Stack IPv4 / IPv6 application control and threat inspection under various deployment modes.	
17	The proposed solution shall support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth.	
18	The proposed solution shall support logical Ethernet sub-interfaces tagged or untagged.	
19	The proposed solution must support the following routing protocols static, OSPF and BGP4.	
20	The proposed solution must have IPv6 Static Routing Support even for virtual routers.	
21	The proposed solution must support Policies based on Zone, Applications, Source / Destination Address, User or User Group	
22	The proposed solution shall support DHCPv4 and DHCPv6 relay	
23	The proposed solution must be able to support Active/Active , Active/Passive configuration	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
24	The proposed solution must be capable to detect device, link and path failure.	
25	The proposed device should have the following features: a) Proposed appliance must support at least 4 million concurrent/ max sessions and should be scalable to support 25 million concurrent/ max sessions. OR Proposed appliance must support at least 4 million concurrent connections and should be scalable to support 25 million concurrent connections. b) Proposed appliance must support at least 1,50,000 new connections per second from day one and should be scalable to support 3,00,000 new connections. OR Proposed appliance must support at least 1,50,000 new sessions per second from day one and should be scalable to support 3,00,000 new sessions.	
26	The solution must support stateful failover	
27	The proposed solution HA shall support hitless upgrades for both major and minor code releases	
28	The proposed solution shall control parameters by Security Zone, Users, IP, Application, Host Information Profile, URL Category, Schedule, QoS etc.	
29	This solution should support SSL traffic decryption & inspection	
30	The proposed solution shall support the following policy types/capabilities:	
31	The solution must support at least 3200 applications in the application visibility database. Higher number of supported applications are preferable.	
32	Policy-based control by application function (posting, file transfer, desktop sharing, instant messaging, etc.)	
33	Policy-based control by user, group or IP address	
34	-Data filtering: Custom Data Patterns	
35	-QoS Policy-based traffic shaping (priority, guaranteed, maximum)	
36	-Policy support for scheduled time of day enablement	
37	The proposed solution shall have application and application function identification and decoding technology without any additional licensing policy	
38	The proposed solution shall be able to handle applications with multiple action options e.g. alert, block or allow	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
39	The proposed solution shall be able to create custom application signatures and categories	
40	The proposed solution shall allow updating the application database automatically or manually via the control or traffic plane	
41	The proposed solution shall delineate specific instances of peer2peer traffic (e.g. Bit torrent, emule, neonet, etc.)	
42	The proposed solution shall delineate specific instances of instant messaging (e.g. Gtalk, YIM, Facebook Chat, etc.)	
43	The proposed solution shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability	
44	The proposed solution shall delineate specific instances of Proxies (e.g. ultrasurf, ghostsurf, freegate, etc.)	
45	The proposed solution shall support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)	
46	The proposed solution shall support URL-Filtering	
47	The proposed solution shall support custom URL-categorization	
48	The proposed solution shall support customizable block pages	
49	The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution	
50	The proposed solution shall support URL Filtering policies by AD user, group, machines and IP address/range	
51	The proposed solution shall support Vulnerability, Virus and Spyware Protection features across Web and Mail. The solution should support protection against spear phishing attacks	
52	The proposed solution shall block spyware and malware	
53	The proposed solution shall block known network and application-layer vulnerability exploits	
54	The proposed solution shall block buffer overflow, DoS/DDoS , etc type of attacks	
55	The proposed solution shall perform stream-based Anti-Virus and not store-and-forward traffic inspection	
56	The proposed solution shall perform stream-based Anti-Spyware and not store-and-forward traffic inspection	
57	The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4	
58	The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine	
59	The proposed solution shall support the ability to create custom user-defined signatures	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
60	The proposed solution shall support granular tuning with option to configure overrides for individual signatures	
61	The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)	
62	The proposed solution Vulnerability / Virus / Spyware protection updates shall not require reboot of the unit.	
63	The proposed solution shall support several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc.	
64	The proposed solution shall support file identification by signature or file extensions	
65	The proposed solution shall support identification and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via protocols like HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, FTP etc.	
66	The proposed solution shall support compressed information stored in zipped format and be able to unpack and filter per policy	
67	The proposed solution shall support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate without any additional licensing policy	
68	The proposed solution should support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP	
69	The proposed solution shall support user-identification in policy without installing an agent on individual endpoints	
70	The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time	
71	The proposed solution should support the ability to create QoS policy on a per rule basis specifically by Applications e.g. Skype and Static or Dynamic Application Groups , such as P2P , IM groups	
72	The proposed solution should support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype	
73	The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. i.e. Banking, shopping, health and non-personal traffic	
74	The proposed solution shall support IPSec, SSL VPN	
75	IPSec VPN should be integrated with the proposed solution and support full encryption standards suites: - DES, 3DES, AES	

Sl.No.	Tecnical Specification	Compliance (Yes/No)
	- MD5 and SHA-1 authentication - Diffie-Hellman Group 1 , Group 2 and Group 5 - Internet Key Exchange (IKE) algorithm - AES 128, 192 & 256 (Advanced Encryption Standard)	
76	The proposed solution administrative module shall support the following authentication protocols: - LDAP - Radius (bidder specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos	
77	The proposed solution shall support packet captures based on Source Address, Destination Address, Applications, Unknown Applications, Port, Threats, Data Filters and / or any combination as specified	
78	The IPS should be constantly updated with new defences against emerging threats	
79	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related	
80	A minimum storage capability of 2TB /minimum 180 days log retention whichever is higher (should be inbuilt or on a separate management appliance) need to be provided as part of the solution for logging and reporting.	
81	The proposed system should have option for creating customized reports. The reports should be accessible through Http/Https based.	
82	The administration software must provide a means of viewing, filtering and managing the log data	
83	The proposed system must have support for sending log information to an external log server via an encrypted connection	
84	Additional components (hardware, software, accessories etc) if required, for providing the total solution as mentioned in the RFP document should be specified and quoted.	
85	Five years comprehensive warranty from OEM (Proof of the warranty must be attached) with onsite service support from the date of installation without any extra cost.	
86	Five years comprehensive technical support for software upgrades for all the major and minor releases	

5.7. Patch Cord Details (Make - AMP/ Rosenberg/ CommScope/ Molex)

5.7.1. Fibre Patch Cord (Fibre - OM4/ OM5 or latest with ULL as per TIA/ IEEE)

(i) Quantity (02 Mtrs. LC-LC) = 40
(ii) Quantity (15 Mtrs. LC-LC) = 40
(iii) Quantity (25 Mtrs. LC-LC) = 40

Note: - 1. *The products quoted are not "end of life or end of sale products" as on Bid Submission date and during the bid process completion. If in case the support for the product quoted has been stopped/ withdrawn till the time of delivery of equipment, the same will be changed with the superior product at no extra cost.*

2. *Bidder has to submit a undertaking mentioning that, the support including spares, patches, upgrades for the quoted products shall be available for the period of 5 years from the date of acceptance.*

3. Bidder has to submit a undertaking mentioning that, all the supplied network devices must be IPV6 complaint and IPV6 ready from day 1. All the functionality and licences as required to fulfill the RFP conditions needs to be supplied with devices from day 1. OCAC will not pay any additional cost for the same.

5.8. Eligibility Criteria

Following table mentions the pre-qualification criteria. A bidder participating in the procurement process shall possess the following minimum pre-qualification/ eligibility criteria. Any bid failing to meet the stated criteria shall be summarily rejected and will not be considered for Commercial Evaluation.

5.8.1. Pre-qualification Criteria

Sl. No.	Clause	Documents Required
1.	The bids should be submitted by only Prime Bidder, no consortium is allowed in this bid.	Declaration in this regard needs to be submitted.
2.	The Bidder should have positive net worth during last three financial years, ending 31.03.2021.	A certified document by the Chartered accountant stating the net worth and average annual turnover of the bidder
3.	The Bidder's average annual turnover should be more than (INR) 5 cores in last three financial years and profitable during each of the previous three financial years ending on 31.03.2021. Note: The turnover refers to the Bidder's firm and not the composite turnover of its subsidiaries/sister concerns etc.	Copy of audited profit and loss account/ balance sheet/ annual report of the last three financial years.
4.	(a) The bidder must be registered under the Companies Act 1956 or a Partnership firm registered under LLP Act, 2008 and must have in operation for a period of at least 5 (Five) years as of March 31, 2022. (b) The company must be registered with appropriate authorities for all applicable statutory duties/taxes	(a) Valid documentary proof for :- ✓ Certificate of incorporation (b) Valid documentary proof for: ✓ GST Identification number (GSTIN) ✓ Income Tax registration/ PAN number ✓ Up to date GST Return ✓ Income Tax returns for last three financial years.
5.	Bidder should have experience of Supply, Installation and Warranty/ Annual maintenance services for IT Infrastructure projects and should have been in the business for a period five years as on 31.03.2022.	1. Work Orders confirming year and area of activity 2. Memorandum and Articles of Associations 3. Relevant legal documentation confirming the acquisition/ merger, if any
6.	The bidder must have successfully undertaken at least the following numbers of systems implementation engagement(s) of value specified herein during the last Five Financial Years : ➢ One project of similar nature not less than the amount Rs. 1 Crore. OR ➢ Two projects of similar nature each of which not less than the amount Rs. 80 Lakh.	Work order, Completion Certificate or phase completion certificate for ongoing project from the client

Sl. No.	Clause	Documents Required
	OR ➢ Three projects of similar nature each of which is not less than the amount Rs. 60 Lakh. **'Similar Nature' is defined as:-** Supply & Installation of Router, Switches, Security Devices, Servers, Storage and their associated maintenance support services for any Government/ Public Sector Enterprises/BFSI in India.	
7.	The Bidder shall not be under a Declaration of Ineligibility for corrupt or fraudulent practices or blacklisted with any of the Government.	Declaration in this regard by the authorized signatory of the Bidder
8.	I. The Bidder must have a registered Branch office in Odisha or if not having office in Odisha should submit an undertaking to open office within one month after getting the Purchase Order. II. The Bidder must have 5 IT Service Engineer/ Professionals available in Bhubaneswar (Odisha).	Office Address or Undertaking A self certified letter by an authorized signatory mentioning the list of IT service engineer/professionals.
9.	The bidder should submit the valid letter from the OEMs confirming the followings: • Authorization from OEM for the quoted product. • Confirm that the products quoted are neither declared End of Sale and End of Support or End of Life at the time of Bid Submission and during the completion of procurement phase. • Confirm that the products would be covered under comprehensive warranty for the contract period. • Undertake that the support including spares, patches for the quoted products shall be available for entire contract period.	a) MAF (Form 4) b) Undertaking from OEM (Form 5)
10.	Quality Certification	Valid ISO 9001 of the bidder Valid ISO 14000 of the OEM
11.	EMD/ Bid Security Declaration	Bid Security Declarattion to be submitted
12.	RFP document fee of Rs. 11,200/- (inclusive of 12% GST)	Demand Draft Detail

6. Bid Evaluation

6.1. Pre-Qualification

i. Bidder shall comply the Pre-Qualification Criteria metioned in respective packages.
ii. Bidders only Qualified in the Pre-Qualification Criteria are eligible for Techinical bid Evaluation.

6.2. Technical Bid Evaluation

The Technical Evaluation will be based on the following broad parameters:

i. Compliance to Technical Specifications as specified in the RFP.

ii. Review of written reply, if any, submitted in response to the clarification sought by OCAC/ OSDC, if any.

iii. The Compliance Statement by the bidder to the technical specifications of respective package along with relevant product brochure, technical documents etc. Bids without proper Compliance Statement will be rejected.

iv. To assist in the examination, evaluation and comparison of bids, OCAC may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

v. OCAC may interact with the Customer references submitted by bidder, if required.

vi. OCAC reserves the right to shortlist bidders based on technical evaluation criteria.

vii. The onsite warranty services must be provided at OSDC, Bhubaneswar. The bidder must provide the plan / arrangement in escalation matrix, for warranty services to be provided at OSDC, Bhubaneswar

viii. Acceptance to the terms and conditions laid down in the tender document. A scanned copy of the bid document duly signed by the bidder's authorized representative is to be submitted in token of acceptance of the same. Any deviation in the general terms and condition may lead to the rejection of the bid.

6.3. Commercial Bid

i. Commercial Bid should be submitted online as per the given format.

ii. The PRICE PART shall contain only schedule of rates duly filled in. NO stipulation, deviation, terms & conditions, presumptions etc. is permissible in price part of the bid. OCAC shall not take any cognizance of any such conditions and may at its discretion reject such commercial bid.

iii. Prices should be given in INR in figures Only.

iv. Bidders are advised strictly not to alter or change the BOQ format /contents. Bidders are also advised not to paste any image file with BOQ

v. Price offered by the bidder shall not appear anywhere in any manner in the technical bid.

6.4. Commercial Bid Evaluation

i. The financial bids of bidders who qualify in Pre-Qualification and Technical evaluation shall be opened at the notified time, date and place by OCAC in the presence of the bidders or their representatives who choose to be present.

ii. The process of opening of financial bids/ covers shall be similar to that of Pre-Qualification – cum – Technical bids

iii. The names of the firms, the rates given by them shall be read out and recorded in tender opening register.

To evaluate a financial bid, the tendering authority shall consider the following: -

- The bid price as quoted in accordance with bidding document.
- Price adjustment for correction of arithmetic errors in accordance with bidding document.

iv. The evaluation shall include all costs and all taxes and duties applicable to the bidder as per law of the Central/ State Government/ Local Authorities. Treatment of GST etc.

v. The evaluation shall be made adding all schedules to arrive lowest quoted bid.

vi. All rates quoted must be FOR destination/on site and should include all taxes, levies and duties. In case of local supplies the rates should include all taxes, etc., and no cartage or transportation charges will be paid by the Government. And the delivery of the goods/services shall be given at the premises/onsite.

6.5. Correction of Arithmetic Errors

Provided that the bid is substantially responsive, the competent Purchase Committee shall correct arithmetical errors on the following basis: -

i. if there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.

ii. if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected; and if there is a discrepancy between words and figures, the amount in words shall prevail.

7. Other Terms & Conditions of RFP

7.1. Bid Submission

i. Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

ii. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by Department.

iii. Bidder has to select the payment option as per the tender document to pay the tender fee / Tender Processing fee & EMD declaration as applicable and enter details of the instrument.

iv. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same is

to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.

v. The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

vi. The uploaded bid documents become readable only after the tender opening by the authorized bid openers.

vii. Upon the successful and timely submission of bid click "Complete" (i.e. after Clicking "Submit" in the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

viii. The tender summary has to be printed and kept as an acknowledgement of the submission of the tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

7.2. Authentication of Bids

A Proposal should be accompanied by a power-of-attorney/ authorization in the name of the signatory of the Proposal.

7.3. Special Conditions of Contract

7.3.1. Price Basis

Price basis should be for OCAC, Bhubaneswar in INR only. Price quoted should be in the prescribed format as per BOQ. The quoted price will be considered firm and no price escalation will be permitted

7.3.2. Billing

Billing is to be done in the name of Odisha Computer Application Centre, Plot No.-N1/ 7D, Acharya Vihar Square, RRL Post Office, Bhubaneswar -751013. The payment would be on the basis of the actual bill of material supplied, duly certified by our authorized representative at OSDC, Bhubaneswar.

7.4. Payment

One Time 100% of the invoice value will be paid to the successful bidder, after delivery of OEM Warranty Support Certificate, Installation & Final Acceptance Test (FAT), with submission of Performance Bank Guarantee issued from a nationalized / scheduled bank, equivalent to 3% of the amount of Respective Package Contract Value. This Bank Guarantee should remain valid for a period of 60 days beyond the warranty period, commencing from the date of satisfactory completion of entire job.

7.5. Penalty

Penalty for Delayed Services: Penalty will be charged @ 0.5% of the contract value per week subject to maximum of 10% of total order value, in case of delayed in supply of stipulated time period.

7.6. Warranty

All the items covered in the schedule of the requirements /Bill of Material (BOM), shall carry 24 x 7 Comprehensive Onsite Warranty support from OEM . All the items quoted should include 5 years of OEM onsite warranty.

8. Appendix I: Pre-Qualification & Technical Bid Templates

8.1. General

The bidders are expected to respond to the RFP using the forms given in this section and all documents supporting Pre-Qualification Criteria.

Pre-Qualification Bid Proposal shall comprise of following forms :

Forms to be used in Pre-Qualification Proposal

Form 1: Compliance Sheet for Pre-qualification Proposal

Form 2: Particulars of the Bidders

Form 3: Bid Security Declaration

Form 4: Manufacturers /Producers Authorization Form

Form 5: Declaration and Undertaking from OEM

Form 6: Self Declaration against the rule 144 (xi) in GFRs 2017

Forms to be used in Technical Proposal

- Letter of Proposal
- Compliance Sheet for Technical Proposal
- Escalation matrix should also be provided along with the technical bid.

8.1.1. Form 1: Compliance Sheet for Pre-qualification Proposal

(The pre-qualification proposal should comprise of the following basic requirements. The documents mentioned in this compliance sheet along with this form, needs to be a part of the Pre-Qualification proposal)

Sl. No.	Basic Requirement	Documents Required	Provided	Reference & Page Number
1.	Document Fee	Demand Draft	Yes / No	
2	Power of Attorney	Copy of Power of Attorney in the name of the Authorized signatory	Yes / No	
3	Particulars of the Bidders	As per **Form 2**	Yes / No	
4	Bid Security Declaration Form	Letter of authorization as per template provided: **Form 3**	Yes / No	
5	Average Sales Turnover in Hardware & Maintenance services	Extracts from the audited Balance sheet and Profit & Loss; OR Certificate from the statutory auditor	Yes / No	
6	Letter of authorization from OEM	Letter of authorization as per template provided: **Form 4**	Yes / No	
8	Letter of Undertaking from OEM	Letter of authorization as per template provided: **Form 5**		
9	Technical Capability	Copy of work order	Yes / No	
10	Local Service Centres	A Self Certified letter by an authorized signatory	Yes / No	
11	Quality Certifications	Valid ISO 9001of the bidder. ISO 14000 certification of the OEM	Yes / No	
12	Legal Entity	Copy of Certificate of Incorporation, GST, PAN, IT return, Up to Date GST Return	Yes / No	
13	Blacklisting & Performance	A self certified letter	Yes / No	
14	Declaration	Self Declaration against the rule 144 (xi) in GFRs 2017: **Form 6**	Yes/ No	

8.1.2. Form 2: Particulars of the Bidders

Sl. No.	Information Sought	Details to be Furnished
A	Name, address and URL of the bidding Company	
B	Incorporation status of the firm (public limited / private limited, etc.)	
C	Year of Establishment	
D	Date of registration	
E	RoC Reference No.	
F	Details of company registration	
G	Name, Address, e-mail ID, Phone nos. and Mobile Number of Contact Person	

8.1.3. Form 3: Bid Security Declaration Form (BDF)

To
General Manager (Admin.)
Odisha Computer Application Centre
OCAC Building, Plot No. N-1/7-D
Acharya Vihar Square, RRL Post Office
Bhubaneswar - 751013

Reference: (1) Enquiry No. _____.
(2) Our Bid No. _____ date _____.

I/ We, _____ irrevocably declare as under:

I/ We understand that, as per Clause _____of Tender/ bid conditions, bids must be supported by a Bid Security Declaration in lieu of Earnest Money Deposit.

I/ We hereby accept that I/ We may be disqualified from bidding for any contract with you for a period of **Three Years** from the date of disqualification as may be notified by you (without prejudice to OCAC's rights to claim damages or any other legal recourse) if,

1) I am /We are in a breach of any of the obligations under the bid conditions,
2) I /We have withdrawn or unilaterally modified/ amended/ revised, my/our Bid during the bid validity period specified in the form of Bid or extended period, if any.
3) On acceptance of our bid by OCAC, I /we failed to deposit the prescribed Performance Bank Guarantee (PBG) or fails to execute the agreement or fails to commence the execution of the work in accordance with the terms and conditions and within the specified time.

Signature:

Name & designation of the authorized person signing the Bid-Securing Declaration Form:

Duly authorized to sign the bid for and on behalf of: _____ (complete name of Bidder)

Dated on _____ day of _____ month, _____ year.

(Note: In case of a Joint Venture, the Bid Security Declaration must be in the name of all partners to the Joint Venture that submits the bid).

8.1.4. Form 4: Manufacturers /Producers Authorization Form (MAF)

Letter No._____ Date:_____

To

The General Manager(Admin)
Odisha Computer Application Centre
Bhubaneswar

Sub : OEM Authorization Letter

Dear Sir:

Ref: Your RFP Reference No: OCAC-NEGP-INFRA-0008-2021-22050

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at (*address of factory / facility)* do hereby authorize M/s _____ *(Name and address of Agent)* to submit a Bid, and sign the contract with you against the above Bid Invitation.

We hereby extend our full guarantee and warranty for the Solution, Products and services offered by the above firm against this Bid Invitation.

We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products manufactured or distributed by the Supplier :

a. Such Products as OCAC may opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract; and

b. in the event of termination of production of such Products:

   i. Advance notification to OCAC of the pending termination, in sufficient time to permit to procure needed requirements; and

   ii. Following such termination, furnishing at no cost to OCAC, the blueprints, design documents, operations manuals, standards, source codes and specifications of the Products, if requested.

We duly authorize the said firm to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

Yours faithfully,

(Name)
(Name of Producers)

Note - 1: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it.

8.1.5. Form 5: Declaration and Undertaking from Original Equipment Manufracturer (OEM)

(To be submitted Original on the OEM Letter Head)

Date: _____

To
The General Manager (Admin)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O. - RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Sub: Undertaking by Original Equipment Manufacturer against tender No. _____ dated _____ for RFP for IT Equipments Upgrade of Odisha State Data Centre (OSDC) Bhubaneswar.

Dear Sir/ Madam,

I/We, M/s _____(Name of the OEM) having registered office at _____(address of the manufacturer) by virtue of being original equipment manufacturer for the _____ (Name of the product/s).

We hereby confirm the following points.

1. Parts supplied by us are certified and compatible with the offered solution.
2. Parts supplied and available are not declared as End-Of-Life/ EOS for next Seven Years fron the date of acceptance. After installation, if such parts are found End-Of-Life, then it will be our responsibility to replace with newer and higher compatible parts along with implementation at no cost to the OCAC.

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

For M/s _____(Name of the manufacturer)
Signature & company seal

Name
Designation
Email
Mobile No.

Note: Separate undertakings from each individual OEM.

8.1.6. Form 6: Self Declaration against the rule 144 (xi) in GFRs 2017

<To be in Company Letter Head>

< Location, Date>

To
The General Manager (Admin)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O. - RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Subject: RFP for IT Equipments Upgrade of Odisha State Data Centre (OSDC) Bhubaneswar

RFP Reference No: OCAC-NEGP-INFRA-0008-2021-22050

Dear Sir/Madam,

I/ We, represent that company is not a subsidiary/ affiliate/ attached office of any Border Companies as may be banned by Government of India for doing business in India as per revision of GFR rule 2020 or if from such a country, has been statutorily registered with the competent authority as per the procedure laid down in reference to Government Orders in this regards.

I/ We, hereby agree to provide copy of and/ or produced original of all such documents as may be necessarily required to be submitted evidence in this regard.

I/ We, hereby certified that this bidder fulfills all requirements in this regard and is eligible to be considered.

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

8.2. Appendix II : Commercial Proposal Templates

The bidders are expected to respond to the RFP using the forms given in this section for Commercial Proposal.

Form 7: Covering Letter

Form 8: Commercial Proposal

8.2.1. Form 7: Covering Letter

< Location, Date>

To

The General Manager (Admin)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Subject: RFP for for IT Equipments Upgrade of Odisha State Data Centre (OSDC) Bhubaneswar.

RFP Reference No: OCAC-NEGP-INFRA-0008-2021-22050

Dear Sir/Madam,

We, the undersigned, offer to provide the Implementation services for IT infrastructure supply & related services in accordance with your Request for Proposal cited above. Our attached Financial Proposal is for the sum of [*Amount in words and figures*]. This amount is exclusive of the local taxes.

Our Financial Proposal shall be binding upon us, up to expiration of the validity period of the Proposal, i.e., [*Date*].

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

We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

8.2.2. Form 8: Financial Proposal

RFP Reference No: OCAC-NEGP-INFRA-0008-2021-22050

COMMERCIAL BID FORMAT

Sl. No.	Item	Bill of Quantity (A)	Unit Price (B)	GST Per Unit (C)	Total Unit Cost (D) (D=B+C)	Total (A x D)
1.	Router	2				
2.	Core Switch	2				
3.	Network Switch	8				
4.	Access Switch	1				
5.	One Time Deployment Cost (Serial No – 1, 2, 3 and 4) (One Time Implementation, Configuration and Integration)	1				
6.	AAA	2				
7.	AAA Deployment Cost (One Time Implementation, configuration and integration)	1				
8.	NG Firewall	2				
9.	Firewall Deployment Cost (One Time Implementation, configuration, integration and migration from existing to new)	1				
10.	Fibre Patch Cord (02 Mtrs. LC-LC)	40				
11.	Fibre Patch Cord (15 Mtrs. LC-LC)	40				
12.	Fibre Patch Cord (25 Mtrs. LC-LC)	40				
					Grand Total Incuding	
Total Cost In Words						

Seal of the Company Authorised Signatory

"I/WE UNDERSTAND THAT THE QUANTITY PROVIDED ABOVE IS SUBJECT TO CHANGE. I/WE AGREE THAT IN CASE OF ANY CHANGE IN THE QUANTITIES REQUIRED, I/ WE WOULD BE SUPPLYING THE SAME AT THE RATES AS SPECIFIED IN THIS COMMERCIAL BID. I /WE AGREE TO ADHERE TO THE PRICES GIVEN ABOVE EVEN IF THE QUANTITIES UNDERGO A CHANGE".

9. Performance Bank Guarantee (PBG)

To

The General Manager (Admin)
Odisha Computer Application Centre
Plot No. - N-1/7-D, Acharya Vihar
P.O.- RRL, Bhubaneswar - 751013
EPBX: 0674-2567280/2567064/2567295
Fax: +91-0674-2567842

Whereas, < < name of the supplier and address > > (hereinafter called "the Bidder") has undertaken, in pursuance of contract no. < < insert contract no. > > dated. < < insert date > > to provide Implementation services for < < name of the assignment > > to OCAC (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the Bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, < < name of the bank > > a banking company incorporated and having its head /registered office at < < address of the registered office > > and having one of its office at < < address of the local office > > have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, upto a total of Rs.< < insert value > > (Rupees < < insert value in words > > only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs .< < insert value > > (Rupees < < insert value in words > > only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until *< < Insert Date > >*)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs < < insert value > > (rupees < < insert value in words > > only).

II. This bank guarantee shall be valid up to < < *insert expiry date* > >)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before < < *insert expiry date* > >) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)
Seal:
Date: