झारखण्ड लोक सेवा आयोग,
सर्कुलर रोड, राँची।
प्रेस विज्ञप्ति

झारखण्ड लोक सेवा आयोग, राँची में "Selection of System Integrator for Supply, Installation, Commissioning of WiFi System with 100 MBPS internet at Jharkhand Public Service Commision (JPSC) Ranchi (Jharkhand)" **हेतु निविदा आमंत्रित सूचना**

झारखण्ड लोक सेवा आयोग, राँची में "Selection of System Integrator for Supply, Installation, Commissioning of WiFi System with 100 MBPS internet at Jharkhand Public Service Commision (JPSC) Ranchi (Jharkhand)" हेतु प्रतिष्ठित कम्पनी/एजेंसी/प्रतिष्ठानों से निम्नवत् निविदा आमंत्रित की जाती है :–

1.	Name of Work	Selection of System Integrator for Supply, Installation, Commissioning of WiFi System with 100 MBPS internet at Jharkhand Public Service Commision (JPSC) Ranchi (Jharkhand)
2.	Availability of Tender Document On JPSC Website (www.jpsc.gov.in)	05.05.2026 (Tuesday)
3.	Last Date for sending Pre-Bid Query	09.05.2026 (Saturday)
4.	Pre-bid meeting	11.05.2026 (03:00 P.M.) (Monday)
5.	Start date of bid submission	15.05.2026 (Friday)
6.	Last date and time of Bid Submission at JPSC Office.	25.05.2026 (05:00 P.M.) (Monday)
7.	Date and Time of Technical Bid Opening	26.05.2026 (03:00 P.M.) (Tuesday)
8.	Date and Time of Commercial Bid Opening	To be informed later.
9.	Place of Pre-Bid Meeting/ Communication/Bid Submission/ Bid Opening	Jharkhand Public Service Commission, Circular Road, Deputy Para, Ranchi-834001
10.	Contact/Pre-Bid Query e-mail ID	Tel: -9431301419 Email:- jpsc1@jpsc.gov.in

ह0/–
सचिव (प्रभारी)
झारखण्ड लोक सेवा आयोग, राँची।

Request for Proposal for
Selection of System Integrator for Supply, Installation, Commissioning of WiFi System with 100 MBPS internet at Jharkhand Public Service Commission (JPSC), Ranchi (Jharkhand)

1.	Tender Reference number	1497 Date-05/05/2026
2.	Name of Work	Selection of System Integrator for Supply, Installation, Commissioning of WiFi System with 100 MBPS internet at Jharkhand Public Service Commission (JPSC), Ranchi (Jharkhand)
3.	Earnest Money Deposit (EMD)	INR 100000/- (Rupees One Lakh Only)
4.	Purchase of Tender document	INR 5000/- through Demand Draft In Favor of Jharkhand Public Service Commission, Ranchi
5.	Availability of Tender document	05/05/2026
6.	Last Date for sending Pre-Bid Query	09/05/2026
7.	Pre-bid meeting	11/05/2026, 03:00 PM
8.	Start date of bid submission	15/05/2026
9.	Last date and time of Bid Submission	25/05/2026, 05:00 PM
10.	Technical Bid Opening	26/05/2026, 03:00 PM
11.	Commercial Bid Opening	To be informed later.
12.	Place of Pre-Bid Meeting/ Communication/ Bid Submission/ Bid Opening	Jharkhand Public Service Commission Circular Road, Deputy Para, Ranchi - 834001
13.	Contact/ Pre-Bid query e-mail ID	Tel: 9431301419 Email: jpsc1@jpsc.gov.in

Note:

1. JPSC reserves the right to change the conditions or cancel the tendering process at any stage without assigning any reason thereof. Please visit the portal regularly for the same.
2. The Bidders are advised to submit the bids well in advance as JPSC will not be responsible for non-submission of the bids because of any technical glitches.

JHARKHAND PUBLIC SERVICE COMMISSION (JPSC)

Project Introduction and Objective : Jharkhand Public Service Commission (JPSC), Ranchi, Jharkhand wants to establish with modern art of technology Campus WiFi having all latest IT infrastructure at Ranchi, Jharkhand Campus.

The proposed work is to Supply, Installation and 3 years Maintenance of Wired and Wireless network System, Network equipment's etc. in Ranchi, Jharkhand Campus.

1. Eligible Criteria

Technical Bid should contain.

Sr. No	Description	Document to be submitted
1	The bidder should be a registered company under Indian Companies Act,1956 or 2013 or a partnership firm or a Proprietorship firm for at least 3 years in the field of manufacturing or Supply and installation or Sales & Services of IT-Hardware.	Company's / Organization's Registration Details like- Certification of Registration/ Registered Partnership Deed / Registration Certificate etc.
2	Pan Card	Copy of PAN Card
3	G.S.T. Registration and GST Return	Copy of GST Registration and GST Return copy (GSTR 3B till March 2025 or latest
4	Bidder should have at least 1 Crore average turnover in last Three F.Y. (2022-23, 2023-24 ,2024-25 and 2025-26)	Copy of Audited Balance sheet and Profit Loss A/c document should be attach And CA Certificate to be submitted stating turnover for Last Three Financial Year
5	Income Tax Return (F.Y. 2022-23, 2023-24 , 2024-25 and 2025-26)	Copy of ITR
6	Enclose Product Compliance sheet (Access Point, WiFi Controller, Firewall, Switch, CAT6 Cable, OFC & UPS) on OEM Letter head Annexure - A, along with datasheet.	Compliance with datasheet
7	The OEM has to provide Tender Specific MAF for Access Point, WiFi Controller, Firewall, Switch, CAT6 Cable, OFC & UPS.	Manufacturer Authorization
8	The bidder must have successfully executed/executing project of Supply, Installation and Maintenance or Sales & Services of IT Hardware for any Indian Government Department / Ministry / State / District / PSU during last five FY from 01.04.2019 onwards of following value- a. Single (01) Work order of Value not less than Rs.70 Lakh. or b. Two (02) Work order of Value not less than Rs. 40 Lakh Each or c. Three (03) Work order of Value not less than Rs.30 lakh each	Copy of Work Order, Agreement confirming the Value / Quantity of order along with Satisfactory Performance / Work Completion Certificate from the client or proof of receipt of payment against work done or CRAC raised from GeM.

9	Sight visit by the bidder of the campuses is compulsory before Bid Submission Date. Without visit no tender will be accepted. Attendance for sight visit is compulsory.	Declaration of Site visit by bidder
10	The OEM of Access Point, WiFi Controller, Firewall, Switch, CAT6 Cable, OFC & UPS should not have been blacklisted by any State/Central Government /Government Department/Ministry/State/District /PSU etc. in India for corrupt, fraudulent or any other unethical business practices or for any other reason.	Declaration on the OEM's letter head stating that the OEM has not been blacklisted by any State/Central Government /Government Department/ Ministry/State/District/PSU etc. in India for corrupt, fraudulent or any other unethical business practices or for any other reason must be submitted along with technical bid.
11	Consortium and Subletting is not allowed at any stage.	Declaration on Bidder's Letter Head
12	The bidder should have presence in Jharkhand state. or A commitment from the bidder that they will open their office & Set up Support Service in Jharkhand within 30 days of the work allotment.	Details of the bidder's existing Or A commitment letter on company's letter head regarding opening of their office & Setting up their Service Support in Jharkhand within 30 days of the work allotment.

2. Procedure for bidding

I. <u>Technical Bid</u>

a. Enclosed all documents required to prove the bidder's eligibility as per Eligibility Criteria and Required document mentioned in Tender.
b. Technical bid consisting of all Technical details along with terms and condition. All pages should be properly signed and stamped by bidder.

II. <u>Financial Bid</u>

The bidders shall follow the below guidelines to fill the Financial Bid-

a. The bidders have to fill all the prices including all taxes and duties in figures and also in word and should not leave any cell blank in the BOQ attached as per ANNEXURE I. This filled BOQ must be submit as Financial Bid document..

b. The Bidder must also fill the price breakup of each item in the format of Financial Bid as provided in Annexure I and the same must be submit in Financial Bid. This price breakup will be considered for increasing or decreasing any item(s) in the final supply order or during the project period including maintenance phase.

c. The Bidder shall indicate on the appropriate price schedule attached to this document. The Total Price of complete project as mentioned in the Scope of Work including all duties (Excise) and sales and other taxes (GST).

III. Submission of Bid

The technical bid and the financial bid should be separately submitted by the bidder.

3. Other terms and condition

a. Jharkhand Public Service Commission reserves the right to accept / reject any or all the tender without assigning any reason thereof.
c. Bid validity should be 90 days.
d. EMD of unsuccessful bidder will be returned without any interest within 30 days after issuance of work order.
e. EMD of successful bidder will be returned after submission of Performance Bank Guarantee.
f. Execution of project should be done within 90 days after issuance of work order.
g. Any conditional bid will be summarily rejected.
h. Bidder should compliance all Parameter of Technical Specification as mentioned in Annexure-A

4. Scope of Work

I. Technical Requirements:

The proposed work should use technologies for platform independence with following features:

a. Easy to handle
b. Clean and professional design
c. Robust and Secure
d. Monitoring and Control management enabled
e. Fast upload/download

II. Functional Specifications

The proposed work should have following components:

a) Support for commonly available IT Hardware in terms of Desktops, Laptops, etc. The support and maintenance plan must include capability to address updates for newer version as they become available to ensure solution continuity.
b) Admin Control mechanism for allowing usages (User Login concept), monitoring and control over working of proposed Internet services. Report generation of uses: As required, the agency would be instructed to create report templates in specified formats and layouts with appropriate header graphics.
c) Secure interface
   i. Web based dashboard
   ii. Efficient, fast loading web interface.
   iii. Area / location wise/ user wise report drill down / view.
   iv. Excel based and statistical summary reports as per requirements.

III. Detailed Requirement

In order to work seamlessly following services need to be supply, install and maintained at Jharkhand Public Service Commission (JPSC) Campus including supply, laying, installation, configuration, and commissioning of campus Wi-Fi equipment's along with 3 years maintenance-

Campus Wide Wired and Wireless Local Area Networking Supply and Installation of Electrical Nodes for Network equipment and LAN node.

A. Technical resource as and when required to maintain Network Infrastructure support and Maintenance Service for 3 Years from the date of installation and functioning.
B. Campus Wireless Networking In order to connect various units of the institution like main building, administration blocks and as required a robust fibre cable has to be laid down.

IV. Scope of work Includes

A. The scope of the work includes supply, installation, configuration, and deployment of the WIFI solution and on-site training to Jharkhand Public Service Commission (JPSC) personnel for one day plus its maintenance during warranty period.
B. The bidder shall be responsible for providing all materials, equipment's and services specified herein or otherwise which are required to fulfil the intent of ensuring operability, maintainability, and reliability of the complete equipment's covered under this tender within bidder's quoted price.
C. All products being quoted should be compatible and seamlessly integrated. The bidders may visit to the campus before submitting the bid.
D. Each product should come with a comprehensive on-site warranty including labour and spares for three years starting from the date of installation and acceptance.

5. Security Deposit

i. Within fifteen (15) days of the award of Work order/Purchase order, the vendor shall furnish a (PBG) Security deposit amounting to 3 % of the purchase order value in the form of Bank Guarantee **(from scheduled Bank only) / NSC/ F.D. etc.** favouring the To, The Jharkhand Public Service Commission, Ranchi, Payable at Ranchi. The security deposit should be valid for the entire warranty period.

ii. All Bank details like Name, address, phone/fax No., e-mail etc. should be mentioned clearly.

iii. The security deposit will be forfeited in the case of non-execution of the order and non-compliance of the terms and conditions provided in the tender document.

6. Payment Terms

A. The offer should include the cost of equipment and all required accessories inclusive of all taxes and statutory levies.
B. Bidders shall indicate their rates in clear/visible figures as well as in words and shall not alter/overwrite/make cutting in the quotation. In case of a mismatch, the rates written in words will prevail.
C. Payment will be made after deduction of I. Tax, TDS and GST, TDS as per applicable rule.
D. 100% payment shall be released on Material delivery, Installation, Testing & Go -Live of the project.

JHARKHAND PUBLIC SERVICE COMMISSION (JPSC)

Required Material

Sl.No.	DESCRIPTION
1	Indoor Access Point
2	WLAN Controller
3	Firewall
4	24 Port PoE Layer 2 Switch
5	24 Port Distribution Switch
6	24 Port Patch Panel with keystone Loaded
7	I/O Box
8	CAT 6 UTP Patch chord
9	CAT 6 Cable with Conduit (305 Mtr Box)
10	SFP 1.25
11	OFC Cable 12 Core Armoured with Conduit
12	LC-LC OFC Patch Chord 3 Mtr.
13	LIU 48 Port with LC Connector
14	LIU 6 Port with LC Connector
15	9U Rack
16	24U Rack
17	Online UPS 5 KVA with 1 hr backup
18	Required Electrification with UPS
19	100 MBPS Internet Connectivity for 3 Years
20	One Time Supply Installation Testing and Commissioning (SITC) including all required material Charges , onsite Service support for 3 Years.

JHARKHAND PUBLIC SERVICE COMMISSION (JPSC)

Annexure 'A' - Technical Specification

1. Indoor Access Point

Make :	**Model No.:**	
Sl.No	**Technical Parameter**	**Compliance (Y/N)**
1	AP must support the 802.11a/b/g/n/ac /ax/be	
2	The clause is amended as "Simultaneous client support on tri band radio i.e 2.4ghz, 5ghz and 6ghz. It should also support MU- MIMO technology. Access Point shall support Dual 5GHz radios to use 6 GHz radio in 5 Frequency.)	
3	The clause is amended as "Must support minimum 4x4 MIMO on all Band". Further, the quantity of Access Points has been revised from 86 to a minimum of 40 numbers (subject to further increase as per actual requirement). Accordingly, bidders shall quote the unit price in the commercial e-bid, keeping in view the minimum quantity of 40 Access Points. Consequently, the quantity of Active/Passive components may increase or decrease as per requirement, on the basis of amendment in the quantity of Access Point (mentioned above) or as per actual implementation. The billing shall be done on actual consumption of equipment's i.e. Active & Passive Components.	
4	All the access points must be centrally configured and managed through the same cloud controller / on prem controller and should support AI Based network operations.	
5	Access Point must support aggregate data rate of maximum 4.5 Gbps.	
6	Security mechanisms must be in place to protect the communication between the Management Platform and the Access Points.	
7	AP must be supplied with all accessories including the appropriate mounting kit.	
8	The antennas must be integrated inside the access point enclosure and should be Omni-directional.	
9	The access point must support WPA2/WPA3 enterprise authentication and AES encryption. AP must support Authentication via 802.1X.	
10	Operating Temperature: 0°C - 40°C	
11	Operating Humidity: 10 % - 90 % non-condensing.	
12	Must be CE/FCC Certified	
13	Must be WPC approved	
14	The AP should have one RJ-45 port 2.5 / 5 Gbps port speed, should support POE	
15	The AP should support Spectrum Analysis and Rogue Detection	
16	The AP should be able to service client as well as rogue detection.	
17	3 Years on-site warranty & support	
18	Switches and AP must be from the same OEM.	

2. WLAN Controller

Make :	Model No.:	
Sl. No.	**Specification and Parameter**	**Compliance (Y/N)**
1	The System Architecture enlists the expectation from the "Total Solution", that are common to Wi-Fi services including, but not limited to Wi-Fi Access, WIDS, WIPS, Network assurance & Location tracking	
2	The proposed Wi-Fi controller(s)/ Wireless NMS should be On-premise based software controller or Hardware appliance. Software controllers/NMS should support installation on VM /KVM based platform.	
3	The On-prem Wi-Fi controller / Wireless NMS should be capable of supporting upto 100 APs from Day 1	
4	Solution must support an independent intelligent edge architecture for Wi-Fi access. In case of non-reachability of the controller, all WLAN services should be delivered at the edge.	
5	Solution should support tunnelling throughput of minimum 80Gbps on the controller/ tunnel aggregator device	
6	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management), Wi-Fi client's traffic local switching and client traffic tunnelling services should be functional if the link between Wireless APs and its management controller goes down. It must also be possible to onboard new clients in such a scenario.	
7	The solution must facilitate Control and Provisioning of Wireless Access Point devices and ensure data encryption between access point devices and Management controllers across remote WAN/LAN links	
8	The Architecture should be flexible and future investment proof i.e. Proposed AP Model with same software image should support cloud based migration in future.	
Management Controller		
9	The WLAN Manager must provide centralized Wi-Fi, Network assurance, WIPS and client location tracking management system	
10	The Management controller should have role based admin rights to manage the controller.	
11	The Management users should be able to authenticate to Management controller using Digital certificates, LDAP and RADIUS based authentication	
12	The Management controller should support open API's for integration with 3rd party configuration management, inventory management, performance management, process automation, reporting, WLAN monitoring tools etc.	
13	The Solution should allow blocking traffic based on IP address, port, URL, hostname, application etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).	
14	The WLAN Manager should allow uploading site-wise floor maps to showcase real-time Heat maps and other RF KPIs	

15	The Wi-Fi solution should support sending alerts to on-prem 3rd party SNMP servers via SNMP v1, v2c, v3	
16	The solution should maintain controller user action logs which should include all activities performed by the user like login, any configuration changes made on the system, device deletion, device authorization, log out etc.,	
17	The solution should enable wireless client association logs which should record client MAC address, AP connected to, data transfer, data rate, session duration, content - domain (http, https, IP address), for at least 30 days	
18	The solution must allow VLAN segmentation at the edge.	
19	Time Schedules - the solution must allow configuration of time schedules when WLAN is / isn't available (For example: SSIDs can be active from 9 am to 5 pm and then automatically disabled)	
20	The solution must send event notifications based on location and alarm type	
21	The solution must allow automatic schedules for report generation and distribution of reports to Specific users via email	
22	The Solution shall support RRM features like Auto transmit power control, Client load balancing, Band steering (Bi-direction between 2.4 and 5.0 Ghz), Minimum association RSSI, Sticky client remediation.	
Management and Monitoring		
23	The solution should have all locations consolidated dashboard and location-specific dashboard as well.	
24	The WLAN management plane should have visual hierarchal location tree, where the nodes of location tree inherit settings and configuration from the global level into subsequent levels in the hierarchy.	
25	The solution must provide hierarchical alerts wherein sub-events are correlated under parent incident alert thereby enabling event correlation.	
26	The Management controller must have AP Group based policy management and administration.	
27	The solution should support DHCP fingerprinting to allow or deny a client based on client OS from associating with an access point (AP), restrict clients in a specific VLAN, bandwidth control, apply firewall rules and apply other network policies.	
28	The solution should support floor maps loaded on the Management controller to showcase AP coverage heatmaps and channel distribution	
29	The solution shall support Location tracking of multiple clients on floor Map to highlight associated clients facing connectivity and performance issues.	
30	The controller should enable application visibility and control. It should display list of applications with their data usage for a specific SSID as well as per client.	

31	The system should support remote packet captures on AP radio and Ethernet ports without disrupting the client connectivity of any of the APs.	
32	The solution should support RF spectrum analysis on both 2.4GHz & 5GHz band to visualize spectrum analysis as a real-time spectrogram view RF interference, spectrum density and duty cycle of other RF signals.	
33	The solution should support Bluetooth scanning to detect near by Bluetooth devices	
Network Assurance		
34	The solution should support automated root cause analysis to highlight probable network causes for client impacting wireless issues, WiFi issues such as low RSSI, low data rate, Authentication related issue on per client basis.	
35	The solution should proactively highlight client connection failures during association, authentication and network entry. It should also identify the cause of these failure.	
36	The solution should highlight the reason of client connection failures related to association, authentication and network on boarding of users and specify the exact reason of failure such as association limit, capability mismatch, Radius authentication failure, EAPOL failure, fast roaming failure, Radius server not responding, web authentication failure, DHCP, DNS , WPA2 4 way handshake, incorrect PSK entered by user etc	
37	The Solution must support Synthetic client testing by connecting active sensors/APs to neighbouring APs and simulate real-world client experience by running client connectivity test for PSK and 802.1x SSIDs , application reachability, throughput test and voice calls quality testing. Simulation testing should not disrupt existing user connection. In case separate HW/Sensors are required, they should be accounted as 1:4 ie 1 probe/sensor device for every 4 APs against the indoor AP deployments.	
38	The Solution should highlight User's application experience/performance for well known Voip based application such as Ms Teams, Skype, Zoom,Hangout, Webex etc.	
39	The solution shall support monitoring the performance of custom web-based enterprise applications which are TCP based.	
40	The solution should provide recommendations of possible actions that can be taken for remediation of client's performance impacting issues.	
41	The solution should be able to baseline important metrics related to client connectivity and performance such as Retry rate, data rate, latency and client authentication to define normal for each network/ site and highlight anomalous events that deviate from the regular baseline.	
42	The controller should provide automatic packet capture upon detecting anomaly in client connectivity or on boarding issues for forensic analysis	

Software & System Management		
43	The system should support manual and scheduled automatic system backup.	
44	The controller and AP can be on different software versions.	
45	The system should be able to rollback all APs/group of APs to previous checkpoints/snapshots of configuration and settings.	
46	The Wireless manager and tunnel aggregator/controller Upgrade should not disrupt Wi-Fi and WIPS services.	
47	The AP Upgrade to controller version should be flexible and be scheduled on per AP/AP group or site basis as required.	
48	The Solution must support hitless upgrade/ Rolling Upgrade for APs	
49	For management and monitoring operations, the controller must provide a web interface, command-line interface, and APIs.	
WIPS		
50	The solution must auto-classify APs precisely in different categories as managed / authorized (ie. managed device connected to the networks), external (i.e. un-managed APs not connected to the networks, e.g. neighbours), and rogue APs (un-managed AP connected to the networks)	
51	The solution must have the capability of auto classifying Wi-Fi clients as authorized (managed clients connecting to the network), guest, rogue (un-managed client attempting connection to the network) or external (unmanaged not connecting to the network eg. neighbor), in addition to manual classification	
Technical Parameters		
52	The solution must be able to detect and automatically prevent all types of Rogue (unauthorized APs connected to the network) APs, such as:	
	a) App such as Bridge and NAT	
	b) MAC-adjacent Open/Encrypted Wi-Fi routers	
	c) Non-MAC-adjacent OPEN Wi-Fi routers	
	d) Non-MAC adjacent APs having MAC ACLs	
53	The solution must be able to detect and automatically prevent all Wi-Fi enabled devices such as smartphones bridging / ICS when connected to the network	
54	The solution must detect mis-configured authorized APs that do not comply with the configuration compliance and automatically prevent all client connections to such APs.	
55	The solution should detect and prevent outside client trying to connect to the Authorized WLAN	
56	The solution must detect Honey Pot attacks including its advanced variants such as Multiport attack. It should be able to prevent the authorized client from connecting to a honey pot AP.	
57	The WIPS solution should NOT affect the operation of an external (i.e. neighbours) or a man- aged access point while preventing a rogue AP on the same channel.	
58	The solution must be able to detect wireless Denial of Service (DoS) attacks	

59	The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, Mis-Association.	
60	AP should support detection and prevention of 11ax clients in case of WIPS policy violation.	
61	The solution should support location tracking of Rogue APs, Honeypot APs, DoS attackers etc on floor maps without any external application or server	
62	The solution should be able to do wireless prevention of WIPS on DFS channels as well	
63	The solution should be able to do wired prevention of WIPS, without any proprietary integration with the wired switch, therefore it should work on switches from all OEMs	
64	The solution should support automatic whitelisting of unmanaged APs which co-exist in the enterprise network based on the authorized security policies defined, essentially not running preventions on them.	
65	The solution should be able implement "no WiFi" networks while co-existing with other unmanaged APs, where unmanaged APs running in networks which are defined as a "no WiFi network" will be prevented from functioning even if they adhere to authorized security policies.	
License, Warranty and Support		
66	The Total solution should come with all required feature licenses from first day of installation	
67	The Total solution should have 3 years hardware, Software, Licences warranty for AP's, controllers, Adapters, and every item supplied as a part of the solution	
68	The Total solution should have technical support for Hardware, Software, Software upgrades, all license cost from the OEM for first 3 years.	
69	The Total solution should come with the latest and updated version available at no extra cost	
70	Any new release of firmware and software must be updated regularly within 3 years warranty term.	
71	Should Provide TAC support direct from OEM not from outsourced TAC	
72	Solution should support Next business day RMA for AP	
73	Solution should support Next business day RMA for Gateway / controller/tunnel aggregator	

3. Firewall

Make :	**Model No.:**	
Sl.No	**Specifications**	**Compliance (Yes/No)**
A	**General Requirements**	

1	The Proposed OEM must be providing network security solution for government segments in India for at least 10 years. The OEM must be provided with the highest security effectiveness of the proposed firewall solution.	
2	Firewall should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet. The proposed solution should have Multicore CPU based architecture for better performance.	
3	The solution must have Firewall, Application visibility and control, IPS, Anti-virus, Anti-malware, Anti-bot ,URL filtering and advanced DNS protection capabilities from day one along with real-time Zero-day threat prevention features.	
4	Licensing should be a per device and not user/IP based (should support unlimited users)	
5	The device should be IPv6 Ready (Both phase 1 and Phase2)	
B	**Hardware and Interface Requirements**	
1	NGFW Ports (Minimum) - 8 X 10/100/1000 Base-T & 2 x 10G SFP+	
2	The firewall shall support dual Redundant Power Supply which is critical for maintaining uptime in case of hardware failure or power issues.	
3	The Appliance should have dedicated Console, 1x Management and 1x USB ports.	
4	The firewall shall support dual storage (SSD) option .	
C	**Performance Requirements**	
1	The proposed NGFW appliance must provide at least 3 Gbps of IPS Throughput.	
2	The proposed solution should provide at least 2.5 Gbps of threat Protection throughput.	
3	The proposed appliance must provide at least 2.5 Gbps of IPSec VPN throughput	
4	The proposed appliance must support at least 1.5 million concurrent connections and at least 25,000 new connections per second.	
5	The proposed NGFW appliance must provide at least TLS throughput 800 Mbps and 75,000 TLS connections.	
D	**Architecture Features**	
1	Proposed appliances must support high-performance inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.	
2	The proposed firewall should support single-pass low-latency architecture simultaneously scans for malware, intrusions and application identification in a single architecture.	
3	The security module scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.	

4	The firewall multi-core architecture provides high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.	
5	The firewall must have single-pass DPI architecture that simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.	
6	It should support User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through DPI.	
7	The firewall scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV.	
8	The firewall Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP. Decodes payloads for malware inspection, even if they do not run on standard, well-known ports.	
9	The NGFW shall support stateful session synchronization in the event of a fail-over to a standby unit.	
10	The NGFW shall support Active-Active/ Active-Passive stateful High Availability.	
11	The HA solutions should support silent firmware upgrade process that ensures minimum downtime.	
12	The NGFW shall support interface link monitoring failover.	
E	**Solution Security Requirements**	
1	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports	
2	The NGFW should have 300 firewall Rules or policies support from day 1.	
3	The IPS should scan all parts of the session in both directions and should be able to scan the complete file during the transit.	
4	The NGFW should support authentication protocols like LDAP, RADIUS or TACACS+ authentication servers, and SAML SSO or X.509 digital certificates.	
5	IPS should have the functionality of Geo Protection to Block the traffic country wise in incoming direction, outgoing direction or both.	
6	NGFW Should support Identity Access for Management Access, User Authentication, and SSLVPN authentication.	
7	IPS should be able to detect and prevent embedded threats within SSL traffic.	
8	The AV engine continues scanning when low on memory and GAV scan TCP stream in the proposed firewall.	
9	DNS Filtering Capabilities: Supports Global and Custom DNS Filtering	
	a) Allows wildcard domain entries and interface-specific DNS proxy actions.	

	b) DNS rules can be applied per interface using custom domain categories.	
10	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.	
11	The firewall shall support following features:	
	c) Malicious files are prevented from entering the network until they have been analysed in the cloud and a verdict returned.	
	d) GAV includes a large cloud DB of AV signatures for greater zero-day protection.	
	e) Unknown/unseen files are sent to multiple engines, rendering	
	verdicts quickly.	
12	Solution should protect from DNS Cache Poisoning, DNS rebinding attacks and prevent users from accessing blocked domain addresses	
13	Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.	
14	The firewall must decrypt and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden inside of encrypted traffic.	
15	The solution must have an easy to use, searchable interface for applications and URLs	
16	Should support Application based routing and Multi Path routing, Quota based Bandwidth Management.	
17	Anti-virus & Content Filtering Service must be able to prevent access to malicious websites	
18	Anti-virus application must be able to inspect SSL encrypted traffic	
19	IPS and Anti-Virus must have real time updates from a cloud-based reputation service.	
20	Anti-Virus & IPS must be able to stop incoming malicious files & scan archive files.	
21	The Appliance should support Deep packet inspection of SSH decrypts and inspect data traversing over SSH tunnels to prevent attacks that leverage SSH.	
22	The solution must provide the ability to Protect against zero-day & unknown malware attacks. sandboxing that detects unknown threats with 100% accuracy and zero false positives, outperforming traditional behaviour-based methods.	
23	Should support min 20K DPI signatures, 70 million Cloud AV signatures and 3500+ Application Signatures from day 1.	
24	The integrated cloud sandbox platform, which includes full system emulation analysis technology, executes suspicious code and analyzes behaviour, providing comprehensive visibility to malicious activity.	

25	The integrated cloud sandbox platform Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK plus multiple operating systems including Windows, Android, Mac OS & multi browser.	
26	The proposed system should be SD WAN Enable without adding any additional hardware components & Necessary licenses, if required, need to be provisioned from day one.	
27	The proposed firewall should zero touch onboarding capabilities using mobile apps.	
28	The proposed firewall shall support stateful synchronization between primary and secondary units. It ensures zero session loss during failover, maintaining uninterrupted user experience and application continuity.	
29	Shall support Stateful HA ensures that VoIP sessions are synchronized between the primary and backup units and allows active voice calls to continue without needing to renegotiate sessions during failover, minimizing call drops and disruptions.	
30	The firewall includes Consistent NAT and SIP Transformation features that enhance VoIP reliability across failovers.	
31	The proposed firewall shall be able to integrate with SIEM, NAC or Microsoft Azure Sentinel for security information event management (SIEM) and security orchestration automated response (SOAR) solution.	
32	Firewall shall support integration and manage DNS security, reputation-based content filtering and at least 1024 DNS proxy rules allowing to optimize the rules when using DNS proxy on VLAN interfaces.	
F	**Management & Reporting**	
1	Firewall must have its own Centralized Management & reporting platform. Extensive Logging, reporting for the NGFW functionalities offered should be available. It should have dedicated hardware or virtual management or cloud platform along with firewall solution from day one.	
2	The proposed solution must support Packet Monitor, Ping, Traceroute Diagnostics tools for troubleshooting.	
3	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
4	The management solution must allow the report to be exported into other formats such as PDF, CSV etc and support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis	
5	Centralized Management of Firewalls shall create templates and perform commits at the "All Tenants" . This streamlines updates across all tenants, ensuring consistency, efficiency, and faster deployments.	
6	Should have reporting functionality base on Applications, Users, Threats, Traffic etc.	

7	Should be capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses	
8	Solution must allow administrator to choose to login in read only or read-write mode	
G	**Services and Support**	
1	The complete solution should be provided with a comprehensive warranty, subscription and support for 3 years.	
	License for NGFW high availability with next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, DNS protection, advanced threat protection, Anti-Spam, Cloud Management with 7 days reporting and Basic 24x7 Support.	
2	Offered model should have also FCC, CE, UL, TEC certifications. Certified by ICSA, IPv6, and compliant with Country of Origin (CoO) & TAA, ensuring high trust and regulatory alignment.	
3	Offered product should have in 2019 SVM NGFW report of NSS and above 97% of Block Rate & 94% security effectiveness. Also, should feature in the recommended quadrant of the Security Value Map (SVM) of NSS Labs report 2019 for Next Generation Firewall (NGFW). Report to be submitted by the bidder.	
4	The Proposed NGFW firewall should have under cyber warranty or cyber insurance that offers limited compensation for covered losses that lead to business interruption from Non-volumetric DDOS attack and Unauthorized remote access types of events. OEM must provision the services from day one.	
5	OEM should have TAC and R&D centre in INDIA. The proposed solution should support 24x7 remote technical support by OEM through chat/email / remote access.	
6	Supply, Integration, testing commissioning and training as per site requirements shall be done by the product certified Engineer of bidder/ OEM.	
7	Firewall Installation shall be done by the product certified Engineer of Bidder/OEM.	
8	During Technical evaluations or Prior to Price bid open, Bidder need to do 7-15 Days POC if asked; POC will be at our premises and during POC if found product is not complying with mentioned requirement than authorities have the right to reject the bid during technical evaluations.	

4. 24 Port PoE Layer 2 Switch

Make :	**Model No.:**	
Sl. No.	**Specification and Parameter**	**Compliance (Y/N)**
	Form Factor	
1	19" Rack Mountable 1U Height with Redundant Power Supply (RPS) from day 1	
	Architecture	

2	Switch Should support enough memory to support multiple software images for backup purposes, log report and future scalability	
3	The switch throughput of minimum 128 Gbps from day 1	
4	Should support jumbo frames	
5	Switch should have minimum POE budget of 400 Watt	
6	Minimum MAC Addresses 16K	
7	All type of switches , Access Point and Fiber Modules should be of same OEM	
Interfaces		
8	Minimum 24 x 1G POE+ copper ports from day 1	
9	Should have at least 4 x 10G Uplink Interfaces	
Protocols		
10	Should support Static routing	
11	IEEE Standards IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae / End to End Encryption, 802.3x, 802.1p, 802.1Q, 1588v2/NTP	
12	Should Support Access List/ Firewall Filters, IPv6, NTP, SNMP, TACACS/RADIUS AAA, IEEE 802.1 Q VLAN	
13	IPv6 Ready from day 1	
Security		
14	802.1x authentication and accounting, IPv4 and IPv6 ACLs,	
15	Should provide IPv4 and IPv6 Security mechanism to safeguard against IP and DHCP spoofing attacks for both IPv4 and IPv6.	
16	Should Support Access List/ Firewall Filters, QoS, Policy based routing, IPv6, NTP, SNMP, TACACS/RADIUS AM	
17	TeLemetry & VisibiLity using NetfLow/jfLow/sfLow, SPAN, ERSPAN	
18	The switch must be MTCTE Certified	
19	All required Licences should be provided and All Fiber Modules should support hot swappable from Day-1	
Warranty & Support		
20	3 Years on-site warranty & support	
21	Secure boot or equivalent functionality is required in order to provide assurance that the firmware is authentic to avoid loading of untrusted software.	

5. 24 Port Distribution Switch

Make :	**Model No.:**	
Sl. No	**Technical Parameters**	**Compliance (Y/N)**
Form Factor		
1	19" Rack Mountable 1U Height with Redundant Power Supply (RPS) from day 1	
Architecture		

2	Switch Should support memory of minimum 8 GB DRAM and 16 GB Flash memory or more to support multiple software images for backup purposes, log report and future scalability	
3	The single switch throughput of minimum 1.28 Tbps or more from day 1	
4	Minimum MAC Addresses 128K	
5	Should support jumbo frames	
6	The switch should have Redundant Power supply from day one	
7	Should have at least 80k IPv4, 40k IPv6 routes and minimum 20k Multicast Routes	
8	All type of switches , Access Point and Fiber Modules should be of same OEM	
Interfaces		
9	Minimum 24 x 1/10 Gbps SFP+ Ports from day 1	
10	Should support at least 6 x 40/100 Gbps Uplink Interfaces.	
Protocols		
11	Should have static routing, RIP, OSPF, OSPFv3, uRPF/RPF, VRRP, PBR, IP SLA/RPM or equivalent, PIM, PIM SSM	
12	IEEE Standards IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae / End to End Encryption / VXLAN Encapsulation , 802.3x, 802.1 p, 802.1 Q, 1588v2/NTP	
13	Segmentation Protocol Network segmentation protocols VXLAN and VRF/virtual router, EVPN.	
14	At least 128K MAC Addresses and at least 4000 active VLAN.	
15	Should Support management protocols SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.	
16	IPV6 Ready from day 1 duly certified by NABL Labs	
Security		
17	802.1x authentication and accounting, IPv4 and IPv6 ACLs, Dynamic VLAN assignment and MACSec- 256 (or higher) or equivalent to ensure 256 bit End to End encryption or VxLAN encapsulation and security on hardware for applicable ports and should support SSH, TLS based access to the switch for Management	
18	Should provide IPv4 and IPv6 Security mechanism to safeguard against IP and DHCP spoofing attacks for both IPv4 and IPv6.	
19	Telemetry & Visibility using Netflow/jflow/sflow, SPAN, RSPAN /Remote Port Mirroring/ERSPAN	
20	Should support SDN functionality using open / REST APIs/NETCONF/RESTCONF using YANG/XML data models for external tools to automatically provision network resources/configuration from day one.	
21	Should support QOS 802.1p class of service, marking, classification, policing and shaping and at least eight egress queues.	
22	The switch Must be MTCTE Certified	
23	All required Licences should be provided and All Fiber Modules should support hot swappable from Day-1, 2 nos. x Stacking Cable @100G should be provided from Day-1 to stack both switch	
Warranty & Support		
24	3 Years on-site warranty & support	

25	Secure boot or equivalent functionality is required in order to provide assurance that the firmware is authentic to avoid loading of untrusted software.	

6. 24 Port Patch Panel with keystone Loaded

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compiance (Yes / No)**
1	The Cat-6 transmission performance is in compliance and Exceeds ANSI/TIA/EIA-568-C.2 Standard. Supports 1000-Base-T.	
2	90 Degree (Top Entry) Punch Down Design for Convenient Network Terminations.	
3	Ease of Installation with built in Rear Cable Management.	
4	Removable Module Design	
5	6x4 Module Specially Designed Jack Configuration	
6	Contacts pins and IDC mountings assembled in PCBs by Solderless Press-fit process. PCB: FR4, 1.6mm Thickness 2 Layers	
7	Jack Wire: 30µgold plating over 40µ ~ 80µ nickel plating (Square Wire, 360°plated)	
8	IDC Conductor : 0.5 mm Phosphor Bronze (Base Material), 100µ Tin Plating	
10	Contact Compatibility : 22~26 AWG Stranded and Solid Wires	
11	1U Patch Panel to Mount In any Standard Rack. Panel Frame : SPCC Powder Coating In Matt Finish Black Colour.	
12	Housing : High Impact Flame Retardant Plastic, UL 94V-0 Rated	
13	Easy Port Labelling Identification Provision	
14	**Electrical Characteristics:**	
a	Current Rating : 1.5amps	
b	Insulation Resistance : >= 500mΩ	
c	Contact Resistance : <=10mΩ	
d	DC Resistance : <=0.1Ω	
e	DC/AC Volt Endurance : DC 1000V/AC 750V 1 Min	
15	**Mechanical Characteristics:**	
a	Plug Insertion Life : >= 750 Cycles with FCC Compliant RJ-45 Plug	
b	Plug & Jack Contact : >= 100 Grams with FCC Compliant RJ-45 Plug Force	
c	Plug Retention Force : >= 11 LBF	
d	Durability : 200 Termination Cycles	
e	Operating Temperature : -10 Degree ~ 60 Degree	
f	Operating Humidity : 10% ~ 90% RH	
g	Storage Temperature : -40 Degree ~ 68 Degree	
16	**Standard Verification:**	
a	ANSI/TIA-568-C.2	
b	ISO/IEC 11801:2002/AMMD.2:2010	
d	ISO/IEC 60603-7 Compliant	
e	RoHS Directive 2002/95/EC/Compliant	
f	UL LISTED	

7. I/O Box

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compiance (Yes / No)**
	Dual Face Plate	
1	Single, Dual Face Plate Square (86 x 86mm) x 12 mm	
2	One Piece design : Mounting Frame with screw caps, Screw Size : M4 x 25mm	
3	Shutter on Face Plate for closing ports to prevent from dust entry	
4	Port labeling with paper label and transparent plastic window to hold paper label	
5	Ease in snap in and out of RJ45 keystone connector,	
6	Cover Material : ABS-UL94-V2, Base Material : ABS-UL94-V2, Dust Cover Material : ABS-UL94-V2	
7	Plug Retention Force : 14Kgf (140N)	
8	Supports UTP and STP Jacks Cat5e, Cat6 and Cat6A	
9	Suitable for 86 x 86 mm Square type Back box	
10	Installation Temperature: -20°C to +70°C, Operating Temperature: -20°C to +70°C	
11	Standards : ANSI/TIA-568-C.2, ISO/IEC 11801:2002 AMMD.2:2010, ISO/IEC 60603-7 Compliant, RoHS Directive 2002/95/EC/Compliant	
	Surface Mount Boxes	
1	Should have Robust and installer friendly design Surface Mount Boxes for Face Plates for a variety of media including voice and data, Audio, video and CATV distribution to the work area.	
2	Should secure and protect wire with durable wall box	
3	Material : ABS	
4	Shape : Square Size : 86 x 86	
5	Colour : White	
	Category 6 Keystone	
1	Category 6 Keystone is Tool less Design 30 Micron Gold Plating Suitable for 23~24 AWG Solid Copper Wire, Easy For Termination and Compliant to T568A and T568B Wiring Schemes, UL Listed.	
2	Efficient rotation design tool free, press with click to terminate wires	
3	Cable holder with strain relief function for better termination and transmission	
4	Fast, Easy, Reliable Termination	
5	Reliable IDC contacts with colour coding for better contact resistance and transmission	
6	Removable Shutter Option	
7	Keystone Jack Can Be Easily Terminated by Hand, Optional Termination by Hand Tool	
8	Backward compatible with both RJ11/RJ12 Plug	
9	**Physical Specification:**	
9.1	Housing : High impact flame retardant plastic, Polycarbonate UL 94V-0 rated	
9.2	PCB : FR4, 1.6mm Thickness	

9.3	Jack Wire Terminals: Phosphor bronze base, gold over nickel plating Gold Plating : 30µ, Nickel Plating Base(Ni) : 40µ~80µ	
9.4	IDC Terminals: Insulation displacement connector: Phosphor bronze base, Tin Plated 100µ	
9.5	(IDC) Accept #23~24 AWG solid copper wire	
10	**Electrical Specification:**	
10.1	Current Rating : 1.5 Amps	
10.2	Insulation Resistance : 500 MΩ minimum	
10.3	Contact Resistance : 10 mΩ maximum	
10.4	DC Resistance : 0.1 Ω maximum	
11	**Mechanical Specification:**	
11.1	Plug Insertion Life : 750 Cycles minimum using FCC-approved plug	
11.2	Plug & Jack Contact Force :100 Grams minimum using FCC-approved plug	
11.3	Plug Retention Force : 11.0 lbf minimum	
11.4	Durability : 200 Termination cycles	
11.5	Storage Temperature : -40°F to 150°F (-40°C to 68°C) Operating Temperature : -10°C to 60°C	
12	ETL Verified 4 connector channel performance Certificate	
13	Keystone UL listed certified.	
14	**Standard Verification:**	
14.1	Qualified unscreened Class E/Cat.6.	
14.2	Permanent Link & Channel ANSI/TIA-568-C.2	
14.3	IEC 60603-7-4 2nd Edition	
14.4	ISO/IEC 11801 2.2 Edition	
14.5	CENELEC EN 50173-1:2011	
14.6	RoHS Directive 2002/95/EC/Compliant	

8. CAT 6 UTP Patch chord

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	Category 6 patch cords with four pair twisted stranded copper wire cable terminated with RJ45 modular plugs at both the ends.	
2	Patch Cords 100% factory tested for better quality and suitable for the high speed data transmission.	
3	Complies with the ANSI/TIA/EIA-568-C.2, ISO/IEC 11801, RoHS compliant Standard. Supports Data Networks Speeds Up to 10/100-Base-T and 1000-Base-T.	
4	Patch cord with LSZH jacket to reduced toxic/corrosive gasses emitted during combustion	
5	Transparent modular plugs with transparent slip on boot and cable assemblies	
6	T568B wiring scheme crimped at both connector ends.	
7	Available in different colours and different length on request	
8	Patch cord conductor: 24 AWG, Stranded copper wires, Insulation : HDPE	

9	Connector Plug: 30µ'' Gold plated contact, Phosphor Bronze base material	
10	Jacket Diameter : 5.8 ± 0.1mm	
11	Plug Insertion/Extraction Life: 750 Cycles min. using FCC approved plug &	
12	Plug & Jack Contact Force : 100 Grams min. using FCC approved plug	
13	Plug Retention Force : 11 lbf min.	
14	Current Rating: 1.5 amps, Voltage Rating: 72 Vdc max.	
15	Insulation Resistance : 500MΩ min, Contact Resistance : 20mΩ max, DC Resistance: 0.1Ω max.	
15	Need to submit ETL Verified 4- Channel Performance Certificate along with the bid	
16	Need to submit Zero Bit Error Channel Performance Certificate along with the bid	
17	Operating Temperature : -20 °C to +70° C and Installation Temperature : -20 °C to +70° C	

9. CAT 6 Cable with Conduit (305 Mtr Box)

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	The 4 pair Unshielded Twisted Pair cable shall be ULÒ Listed and ETL verified	
2	This cable well exceeds the requirements of ANSI/TIA-568-C.2 and ISO/IEC 11801 Class E	
3	Nominal Outer Diameter of Cable should be 5.8 ± 0.2 mm and Conductor Diameter 23 AWG	
4	Construction: 4 twisted pairs separated by internal PE Cross Separator. Full separator. Half shall not be accepted. Rip Cord is must.	
5	Conductor: Solid bare Copper, Outer jacket sheath: FRPVC with UL approved CM/CMR rated cable. Jacket colour: Grey	
6	Insulation Material: High Density Polyethylene (HDPE) with Insulation Diameter : 0.89 ± 0.01 mm	
7	Dielectric Strength of cable should be 2.5 KVDC for 2 seconds	
8	Bending Radius : < 4X Cable Diameter at -20°C ± 1°C	
	Pulling Force: 25.35 lbs	
9	Electrical Parameters: Insertion loss (Attenuation), NEXT, PSNEXT, ELFEXT (ACRF), PSELFEXT (PSACRF), Return Loss, ACR and PS ACR.	
10	Insertion Loss of 32.8 db/100m at 250 MHz	
11	Cable should support operating temperature from -20° to +70°C	
12	Cable support Conductor Resistance ≤ 9.38 Ω/100m Max.	
13	Mutual Capacitance of cable should be < 5.6 nF/100m Max.	
14	Resistance Unbalance of cable should be 5% Max.	
15	Capacitance Unbalance of cable should Max. 330 pF/100m	
16	Cable support Delay Skew: < 45 ns/100m, Operating Voltage: 72V	
17	Nominal Voltage of Propagation (NVP): 69% and Current Rating: 1.5 A Max.	

18	Impedance: 100 ± 15 Ω @100 MHz. and Propagation Delay @250 MHz : 536 ns/100m	
19	ETL Verified 4-Connector Channel performance certificate	
20	Need to submit complete and satisfactory type test Report from Central Government NABL accredited laboratory to conformity of the specification along with bid.	
21	Need to submit Zero Bit Error Channel Performance Certificate along with the bid	
22	RoHS Compliant	
23	Printed sequential Length Counter of each meter on Outer Jacket	
24	Category 6 UTP cables shall Supports Gigabit Ethernet (1000 base-T) verified upto 600 MHz	

10. SFP

Make :	**Model :**		
Sl no	**Specification**		**Compliance (Yes/No)**
1	**Architecture**	1000 Base LX Single-mode Fiber Transceiver	
2	**Connector**	It should have duplex LC Connector	
3	**Flow control.**	Support 802.3x	
4	**Mode**	9/125 um Single mode Fiber Type up to 20 KM.	
5	**Support wavelength**	1310nm	
6	**Case Operating Temperature:**	support up to 0º~70º	
7	**Storage Relative Humidity:**	support upto 5% to 95%	
8	**Warranty**	3 Year	

11. OFC Cable 12 Core Armoured with Conduit

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	06/08/12/24-Core, Single mode 9/125 micron primary coated buffers, 10G Ethernet OS2, Armoured Loose Tube, ECCS (Electrolytic Chrome Coated Steel) Tape, Jelly Filled Loose Tube.	
2	Two Steel Wires/Rods embedded in outer periphery of the jacket as strength members. UV Stabilised jacket and protected from Rodent attacks	
3	Complying to ANSI/TIA-568-C.3, ISO/IEC 11801, Telecordia GR-20 Core, ITU-T REC G.652D, IEC 60793-1/60794-1, EN 50173, RoHS Compliant	
4	Suitable for use in indoor/outdoor ducts, direct burial and backbone cabling	
5	Loose tube material : Polybutylene Terephthalate (PBT) with Natural/White Colour having Inner Diameter/Outer Diameter 1.7/2.5 ± 0.1 mm	

6	Peripheral strength member as two steel wires/rods having dimensions as 0.6 ± 0.05 mm	
7	Moisture Barrier as Water Swellable Tape, Armouring ≥ 0.150 mm (ECCS Tape), Number of Ripcords as 01 no polyester based yarns.	
8	Outer sheath material as HDPE/LSZH with diameter as 7.5/8.5 ± 0.5 mm having thickness of 1.5mm nominal	
9	Weight of the cable for 04/06/08/12 core (HDPE/LSZH): 65.0/75.0 ± 10 kg/km, for 24 core (HDPE/LSZH): 75.0/95.0 ± 5 kg/km	
10	Fiber colour and Loose tube colour as per ANSI/TIA standards.	
11	Tensile Strength : 1000 N, Crush Resistance : 4000 N/100mm	
12	Minimum bend radius : 20 x Diameter (during installation), Minimum bend radius : 10 x Diameter (during full load)	
13	Fiber Type : G. 652D (OS2)	
14	Attenuation : ≤ 0.38 dB/km (@1310 nm), ≤ 0.25 dB/km (@1550 nm)	
15	Chromatic Dispersion : ≤ 3.5 ps/nm.km (@1285 - 1330 nm), ≤ 18 ps/nm.km (@1550 nm)	
16	Zero Dispersion Wavelength : 1300 - 1324 nm	
17	Zero Dispersion Slope : ≤ 0.092 ps/nm².km	
18	Polarisation Mode Dispersion : ≤ 0.2 ps/√km	
19	Cut-off Wavelength : ≤ 1260 nm	
20	Mode Field Diameter : 9.2 ± 0.4 µm (@1310 nm) , 10.4 ± 0.4 µm (@1550 nm)	
21	Core Cladding Concentricity Error : ≤ 0.8 µm	
22	Cladding Diameter : 125 ± 1 µm , Coating Diameter : 245 ± 10 µm	
23	Cladding Non-circularity : ≤ 1 %	
24	Installation Temperature : -20 °C to +70° C, Operating Temperature : -20 °C to +60° C	
25	Cable Size and Standard Length: 4F to 12F : 4.0 kms ± 10% 24F : 2.0 kms ± 10%	

12. LC-LC OFC Patch Chord 3 Mtr.

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	Fiber optic patch cord with two core (Duplex) fiber cable terminated with LC connector at one end and LC connector at other end	
2	The terminated connectors in assemblies are designed and are compatible with industry standards (ANSI/TIA-568-C.3, ISO/IEC 11801).	
3	Have good geometrical characteristics of apex offset & radius of curvature & fiber height	
4	100% factory terminated and tested for optical characteristics & fiber end face finish.	
5	Fiber type G. 652D standard. OS2 (9/125 µm),	
6	Buffer Diameter : 0.9 ± 0.05 mm, Jacket Thickness : 0.35 ± 0.05 mm, Strength Member as Aramid yarn	
7	Cable Diameter : 2.0 x 3.8 ± 0.2 (Duplex)	
8	Jacket colour : Yellow, Jacket Material : LSZH, Length : 3 Mtr	

9	Connector Ferrule : Ceramic, Apex Offset should be <50um, Fiber height should be ±100nm	
10	Connector Repeatability ≤ 0.2dB with 1,000 times mating cycles.	
11	Connector cable retention : 50 N (11.24 lbs), Crush resistance : 100N/100mm, Bend Radius: 20xDiameter of cable	
12	Attenuation : ≤ 0.36 dB/km (@1310 nm), ≤ 0.25 dB/km (@1550 nm)	
13	Chromatic Dispersion : ≤ 3.5 ps/nm.km (@1285 - 1330 nm), ≤ 18 ps/nm.km (@1550 nm)	
14	Zero Dispersion Wavelength : 1300 - 1324 nm	
15	Cut-off Wavelength : ≤ 1260 nm	
16	Mode Field Diameter : 9.2 ± 0.4 µm (@1310 nm) , 10.4 ± 0.5 µm (@1550 nm)	
17	Insertion Loss (@1310 &1550nm) : SM (UPC/PC) Type : SC/LC/ST/FC : ≤ 0.3 dB Return Loss (@1310 &1550nm) : SM (UPC/PC) Type : SC/LC/ST/FC : ≥ 50 dB	
18	Insertion Loss (@1310 &1550nm) : SM (APC) Type : SC/LC/ST/FC : ≤ 0.3 dB Return Loss (@1310 &1550nm) : SM (APC) Type : SC/LC/ST/FC : ≥ 60 dB	
19	Traceability sticker available for product tracking and Interferometry report need to submit	
20	Standards: IEC 60332-1, ANSI/TIA-568-C.3, ISO/IEC 11801 RoHS Compliant	
21	Installation Temperature : -20 °C to +70° C, Operating Temperature : -20 °C to +70° C	

13. LIU 48 Port with LC Connector

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	The Fiber Rackmount LIU loaded having Adapter panel fixed on drawer base frame, with Adapters and with Pigtails and assembled with splice tray as per the Loaded fiber port requirement and their applicable accessories.	
2	Suitable to mount at different positions (depth wise) on standard 1U 19 inch racks. Drawer type to pull out for easy maintenance when assembled in racks.	
3	Cold Rolled Steel material with black powder coating	
4	Three types of cable entry holes for different size cables through cable glands, covered with rubber cable grommets/covers.	
5	Splicing of 24 fibers in each plastic fiber splicing trays with integrated cable spool design.	
6	Non removable top cover and no rear cover. Drawer type to pull out for better access of interior.	
7	As per the BOM requirement,06/12/24/48 LIU Loaded with 03/06/12/24 (LC Duplex) adapters and 06/12/24 (LC Simplex) Pigtails on rackmount ports.	
8	As per the Loaded fiber port requirement Accessories kit consists of Cable management rings/Cable saddles, Cable glands (PG13.5, 2 nos), Splice rods, Blanking clips, Velcro ties, Cable ties, Cable inlet/outlet hole covers(2 types, 2 nos each)	

9	Cable management rings/Cable saddles can be mounted inside the rackmount, no provision to mount outside in front of the adapter panel.	
10	Suitable for storing up to 3 meter of 900 µm tight buffered fiber pigtail per adapter.	
11	Panel Dimensions : 482 x 220 x 44.3 mm (Length x Width x Height)	
12	Splice Tray Dimensions : 220 x 90 x 15 mm (Length x Width x Height)	
13	Port identification numbers printed on the Adapter panel	
14	Standards: Comply as per ANSI/TIA-568-C.3, ISO/IEC 11801, RoHS Compliant.	
15	Operating Temperature : -20 °C to +70° C Installation Temperature : -20 °C to +70° C	

14. LIU 6 Port with LC Connector

Make :	Model No.:	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	The Fiber Rackmount LIU loaded having Adapter panel fixed on drawer base frame, with Adapters and with Pigtails and assembled with splice tray as per the Loaded fiber port requirement and their applicable accessories.	
2	Suitable to mount at different positions (depth wise) on standard 1U 19 inch racks. Drawer type to pull out for easy maintenance when assembled in racks.	
3	Cold Rolled Steel material with black powder coating	
4	Three types of cable entry holes for different size cables through cable glands, covered with rubber cable grommets/covers.	
5	Splicing of 24 fibers in each plastic fiber splicing trays with integrated cable spool design.	
6	Non removable top cover and no rear cover. Drawer type to pull out for better access of interior.	
7	As per the BOM requirement,06/12/24/48 LIU Loaded with 03/06/12/24 (LC Duplex) adapters and 06/12/24 (LC Simplex) Pigtails on rackmount ports.	
8	As per the Loaded fiber port requirement Accessories kit consists of Cable management rings/Cable saddles, Cable glands (PG13.5, 2 nos), Splice rods, Blanking clips, Velcro ties, Cable ties, Cable inlet/outlet hole covers(2 types, 2 nos each)	
9	Cable management rings/Cable saddles can be mounted inside the rackmount, no provision to mount outside in front of the adapter panel.	
10	Suitable for storing up to 3 meter of 900 µm tight buffered fiber pigtail per adapter.	
11	Panel Dimensions : 482 x 220 x 44.3 mm (Length x Width x Height)	
12	Splice Tray Dimensions : 220 x 90 x 15 mm (Length x Width x Height)	
13	Port identification numbers printed on the Adapter panel	
14	Standards: Comply as per ANSI/TIA-568-C.3, ISO/IEC 11801, RoHS Compliant.	

15	Operating Temperature : -20 °C to +70° C Installation Temperature : -20 °C to +70° C	

15. 6U Rack

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	600(W) X 500(D) X 347(H)	
2	Minimum 6U	
3	IP 65 compliant providing a secure and weather resistant environment for installed equipment	
4	For flexible installation and maintenance, air ventilation should be provided and should support minimum operating temperature inside cabinet	
5	Precision engineering capabilities and best efficient software configuration product technology provide the best product quality and fastest delivery in the industry.	
6	Standard 19" installation.	
7	Front with metal door and secure lock.	
8	Cable entry/exit provision at bottom with glands.	
9	Cooling fan fitted at front door or button or side wall with air filters.	
10	Power Coated	
11	Powder coated finish with Seven Tank pre- treatment process meeting all industrial standards	
12	Colour RAL7035	
13	Wall/Pole/Floor mounting as per site requirement	
14	Conforms to DIN 41494 OR equivalent ISO Standards.	

16. 24U Rack

Make :	**Model No.:**	
Sl.No.	**Minimum Specification**	**Compliance (Yes / No)**
1	Rack should have 100% assured compatibility with all equipment's conforming to DIN41494 (General Industrial Standard for equipment's) or Equivalent EIA /ISO / EN Standard	
2	The Rack should be 24U in height, 600mm in width and 800mm in depth, basic frame in Steel, all door with powder coated metal	
3	Rack should have 2 side panels and grounding and bonding accessories preinstalled by the manufacturer.	
4	The Rack should have 2 No's adjustable, 19" verticals with punched 10mm square hole and Universal 12.7mm-15.875mm- 15.875mm alternating hole pattern offers greater mounting flexibility, with numbered U positions	
5	The front glass and rear metal doors should be easily detachable. And easily Openable. The doors of the rack should be reversible such that it can be mounted on either side	

6	Construction: Welded OR CKD (Knock Down)	
7	Manufacturer must certify that the products are RoHS Compliance	
8	The unit should have ventilated front and rear doors to provide adequate airflow required by the major server and Network manufacturers.	
9	Supply Exhaust Fans with 180CFM or more Fan Module on the top end	
10	Rack Power Distribution Units – 1 Nos with following specifications Phase : 1Phase, Rating :3.5 KVA, Current : 16A, Type of Outlet : 5/15A Indian Round Pin, No Of Outlet : 6, PDU Mounting : Vertical	
11	Rack should be with swing handle locking with Common Key	
12	OEM Should is ISO 9001 and ISO 14001 Certified or Equivalent Indian Certificates.	
13	Product should be certified with UL certification	

17. Online UPS 6 KVA with 1 hr backup

Make :	**Model No.:**	
Minimum Specification		Compliance (Yes / No)
Parameters	**6KVA (1ph-1ph) IGBT Based Online UPS.**	
Topology	True Online Double Conversion Online UPS.	
INPUT		
Phase	Single Phase	
Voltage	230V AC	
Voltage Range	176V - 300V AC 110V - 300V AC @ 50% Load	
Input Power Factor	0.99	
Current THD	<7%	
DC Volt	240DC	
Battery VAH	9600 VAH	
OUTPUT		
Nominal Output voltage	220VAC / 230VAC / 240VAC /± 1%	
Frequency	50Hz ± 0.1Hz	
Frequency synchronisation	46 to 54 Hz	
Voltage THD	<3% Linear Load	
	<5% Non Linear Load	
Efficiency		
AC/AC (Overall efficiency)	Up to 92%	
ECO mode		
Overload capacity		
105 - 110%	30 Min	
111 - 130%	5 Min	
Communication		
RS 232	Required RS 232	
Operating Temperature	0 ~ 50°C Continuous	
Electrical		

Input Terminal	Input Breaker +Terminal	
Output Terminal	Terminal	
Features		
Convert Mode	UPS Should have Convert Mode	
Bypass parameters Configurable	Should be available	
Display	LCD display + LCD Display	
Mechanical		
Ingress Protection	IP 20	
Safety	EN 62040 - 1	
EMI / EMC	EN 62040 - 2	
Performance	IEC 62040 - 3	
Certification	UPS Should have Certified with ISO 9001,14001 & 45001	
Compliance	ROHS, CE,PEP & BIS	
Warranty	3 Years Warranty on UPS & 2 Years on SMF battery, (Warranty Certificate from OEM Mandatory)	
Service Centre	OEM Should have own service centre 6/7 in Jharkhand.	
Other Terms		
1. OEM must be registered in India past 12 years or more and in continuously manufacturing and selling the same product line.		
2. Land Border Sharing Declaration: Any OEM from a country which shares a land border with India will be eligible to bid in this tender only if the OEM is registered with the Competent Authority. A declaration from OEM in this regard to be submitted.		
3. The OEM should have Factories in India details required		
4. Central/State Gov - Pollution Control Board certificate for Air & Water from OEM		
5. Central/State Gov - Pollution Control Board certificate for E-Waste from OEM		
6. Mandatory Certificate to be shared (No undertaking shall be accepted)		

Annexure- I

(On Bidder's Letter Head)

Financial Bid

Tender Reference No. –

To,
The Chairman
Jharkhand Public Service Commission,
Ranchi, Jharkhand

Sl.No.	Item Description	UoM	Quantity	Unit Price including GST	Total Amount including GST
1	Indoor Access Point	Nos.			
2	WLAN Controller	Nos.			
3	Firewall	Nos.			
4	24 Port PoE Layer 2 Switch	Nos.			
5	24 Port Distribution Switch	Nos.			
6	24 Port Patch Panel with keystone Loaded	Nos.			
7	I/O Box	Nos.			
8	CAT 6 UTP Patch chord	Nos.			
9	CAT 6 Cable with Conduit (305 Mtr Box)	Box			
10	SFP 1.25	Nos.			
11	OFC Cable 12 Core Armoured with Conduit	Mtr.			
12	LC-LC OFC Patch Chord 3 Mtr.	Nos.			
13	LIU 48 Port with LC Connector	Nos.			
14	LIU 6 Port with LC Connector	Nos.			
15	9U Rack	Nos.			
16	24U Rack	Nos.			
17	Online UPS 5 KVA with 1 hr backup	Nos.			
18	Required Electrification with UPS	Lot			
19	100 MBPS Internet Connectivity for 3 Years	Nos.			
20	One Time Supply Installation Testing and Commissioning (SITC) including all required material Charges , onsite Service support for 3 Years.	Lot			
				Grand Total	
In Words :					

Bidder Seal & Signature Date :

Name :
Address :