MILLENNIUM TELECOM LIMITED
(A SUBSIDIARY OF MAHANAGAR TELEPHONE NIGAM LIMITED)

TE No: MTL/COO/WiFi-War Memorial/2019-20
Dated: 10/12/2019

REF: Tender No: MTL/COO/WiFi-War Memorial/2019-20 Dated: 10/12/2019

Dear Sir,

Millennium Telecom Limited invites tender from all empanelled Business Development Associates for Supply, Installation, Testing and Commission of Equipments for providing Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD),Government of India as per specifications given in the Annexure attached to the Tender form.

Please find enclosed the following bid documents in original to be used for selection of Implementing Agency to work with MTL on back-to-back basis arrangement for Supply, Installation, Testing and Commission of Equipments for providing Mesh Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD), Government of India.

S. No.	TITLE	Section No.	Page No.
1.	Notice Inviting Tender	Section -I	2
2.	Terms and Conditions of the Contract	Section -II	3-14
3.	Special conditions of the Contract	Section – III	15-57
4.	Formats Of Documents To Be Submitted	Section – IV	58-100

Your offer complete in all respects as per enclosed documents must reach latest by 12.00 Hrs. of 07/01/2020 at the following address:

The Asst Vice President,
Millennium Telecom Limited,
Cabin No 5110, 5th Floor, Mahanagar Doorsanchar Sadan
9,CGO Complex, Lodhi Road,
New Delhi-110003

The Tender shall be opened at 12.30 Hrs. on 07/01/2020. The representatives of the bidders who wish to be present during bid opening may kindly make it convenient to attend the same.

Thanking you,

Yours faithfully,

Chief Operating Officer,
Millennium Telecom Limited

Encl: Bid documents

Section - I

TE No: MTL/COO/WiFi-War Memorial/2019-20
Dated: 10/12/2019

Notice Inviting Tender

Name of the Work: On behalf of Chairman MTL, Millennium Telecom Limited (MTL) invite sealed tenders (under two bid system), from interested empanelled Business Development Associates through Tender No: MTL/COO/WiFi-War Memorial/2019-20 dated 10/12/2019 for selection of Implementing Agency to work with MTL on back-to-back basis arrangement for Supply, Installation, Testing and Commission of Equipments for providing Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD), Government of India.

Tender document can be downloaded from the websites: www.mtl.in, www.mtnl.net.in, www.etender.mtnl.net.in or www.eprocure.gov.in .

Estimated Cost : Rs.1,71,79,657 (Rupees One Crore Seventy One Lac Seventy Nine Thousand Six Hundred Fifty Seven only)

Security Deposit (SD) : 10% of the Accepted Tendered Amount

Performance Bank Guarantee: PBG amount of 5% of the Accepted Tendered Amount Or amount equal to 5% of the payment of each bill shall be deducted and kept as PBG.

Time Allowed: 12 Weeks for execution and 1 Year Warranty with 4 Years AMC

Tentative date/time schedule for various activities is as mentioned below:

Activity	**Date**	**Time**
Issue of NIT	10/12/2019	
Last date for seeking clarification	17/12/2019 (Five days from date of issue of NIT)	17:00 Hrs
Last Date & Time of Submission of bids documents	07/01/2020 (Four Weeks from date of issue of NIT)	12:00 Hrs
Opening of Techno-Commercial Bids	07/01/2020 (On the same day of last date of submission of bids)	12:30 Hrs

Chief Operating Officer, MTL,
4th FLOOR, MAHANAGAR DOORSANCHAR SADAN,
9,CGO COMPLEX, NEW DELHI-110003
011-24325029

Section - II

TERMS AND CONDITIONS

Tender is called for selection of an Implementing Agency to work with MTL on back-to-back basis arrangement for Supply, Installation, Testing and Commission of Equipments for providing Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD), Government of India., from the Business Development Associates (BDAs) empanelled with Millennium Telecom Ltd. (MTL).

1. SCOPE OF WORK

Sr. No.	Name of the work	Contract Period	Estimated Cost
1.	Supply, Installation, Testing and Commission of Equipments for providing Mesh Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD), Government of India, inclusive of the cost of restoration of all the civil/collateral damages done during the execution to its original specification / shape / design and position.	The bidder shall provide one year warranty and four years AMC beyond warranty period. AMC may be extended further for three years on mutually agreed terms and conditions. During the warranty and AMC period the bidder will provide one service engineer on 7 days a week for attending to Wi-Fi service complaints.	Rs.1,71,79,657

2. The scope of work includes Supply, Installation, configuration, commissioning, testing and maintenance of all equipments including connectivity shall be carried out by the bidder for providing Mesh Wi-Fi services at National War Memorial, India Gate circle, New Delhi. Successful Bidder shall create a free Wi-Fi zone in National War Memorial Complex to cater to approximately 20000 (Twenty Thousand) internet users simultaneously logging-in.

3. The minimum quantity of each item to be supplied by the Successful Bidder is placed at Schedule of Requirements (SoR) in Section – III of this Tender.
4. The delivery schedule/project implementation plan will be as mentioned in Section – III of this Tender.

5. The Successful bidder will enter into a separate contract with MTL on back-to-back basis for a period of at least 5 year (1 Year Warranty + 4 Year AMC). The Successful Bidder agrees to provide comprehensive maintenance for a period of 4 year after expiry of 1 year warranty period of all the systems / items which shall include preventive maintenance and corrective maintenance. The maintenance shall also include replacement of all parts. AMC may be extended further for three years on mutually agreed terms and conditions.
6. Restoration of road cutting, civil work and other related works required for installations of Access points and all other equipments shall be in the scope of successful bidder for which nothing shall be paid. Necessary watch and ward, insurance, ROW permission charges, roads cutting, restoration charges etc if any shall be in the scope of successful bidder for which nothing extra shall be paid.
7. Backhaul Bandwidth will be provided by MTNL and Cost of Internet Bandwidth shall be charged separately by MTNL to National War Memorial. Accordingly, the financial bid to be submitted by the bidder should not include cost of the Internet Bandwidth charges.
8. Successful Bidder shall install all equipments including WiFi NoC, AAA etc at a designated premises / room allocated by National War Memorial. Collocation charges for equipments to be installed by the Successful Bidder including space, electricity and Air Condition will be provided by National War Memorial free-of-cost for complete duration of the project. Accordingly, the financial bid to be submitted by the bidder should not include the above mentioned collocation charges.
9. Provisioning of facilities (Work station/ Server / controller along with required software / Application etc and One colour printer including consumables for printing reports etc) at centralized location to monitor / view the status of Access Points and to see uses of Data shall be in the scope of bidder.
10. Bidder has to ensure OTP based authentication for each user and keep records all logs.
11. Bidder should provide customized logo / Welcome Message and welcome page on Wi-Fi services as per Client's requirement. The page should be disabled friendly and multi-lingual.
12. Bidder to provide Secure Wi-Fi, with capability to block certain type of Web sites like Adult or any other banned websites.
13. Bidder should have the capability to pro-actively monitor and manage the complete Wi-Fi Services.
14. Bidder to provide user based Wi-Fi reports as per below, across all deployed Access points:
    - (i) Live network and usage statistics.
    - (ii) No. of users.
    - (iii) Wireless security statistics like attacks, Rogue AP etc.
    - (iv) Monthly network summary reports.
    - (v) Bandwidth configured and utilization report at each Wi-Fi access points.
    - (vi) Equipment uptime of each Wi-Fi AP .
    - (vii) List of registered and active user base along with their average bandwidth consumption summary reports.
    - (viii) Total aggregate bandwidth consumed per month per AP.
    - (ix) Customizable MIS reports on the above for on demand access by MTNL/National War Memorial officials or any other personnel thus appointed by MTNL.
    - (x) AAA Performance Report

15. Keeping user authentication and verification records as per DoT guidelines for all users accessing the Wi-Fi/ Broadband Services on a non-SIM based device. However, OTP (One

Time Password) authentication on the registered mobile number of the end user should be mandatory for registering non-SIM based devices into the Wi-Fi network.

16. The successful bidder must ensure that records of end users are captured on the Customer Acquisition Forms (CAF) as per Government of India guidelines. In addition, end users may also be registered through OTP authentication through their existing and verified mobile number which is linked to a SIM activated through a valid CAF. This is required to ensure users don't need to register to the network for every session separately.
17. Users authentication for Wi-Fi service, OTP, Email, Admin based authentication for guests/customers. The SMS gateway and SMS charges shall be paid by the successful bidder.
18. Security Requirement shall be as per Section – III of the Tender.
19. Deployed Wi-Fi system should have minimum following user Policies and control:
    (i) Creating time profile (time based services) i.e. SSID broadcasting during specific durations
    (ii) Control user access to the network during a specific time period
    (iii) Blacklisting users
    (iv) Define Usage based policies (in MB)
    (v) Define time based (in hours) policy for Wi-Fi access
    (vi) Decide normal speed and bandwidth throttling limit for each SSID
20. During the warranty and AMC period the bidder will provide one service engineer on 7 days a week for Operation and Maintenance purpose including attending to Wi-Fi service complaints. Service Engineer should be in the General shift for monitoring the Work station/ Server / controller along with required software / Application and printer etc at centralized location to monitor / view the status of APs and to see uses of Data shall be in the scope of bidder.
21. Successful Bidder should provide the following report on monthly basis for all the APs.
    a) Link downtime / Uptime analysis report.
    b) Traffic monitoring, bandwidth utilization report for APs.
    c) In order to monitor the AP up time, latency & packet loss, reports should be provided indicating no. of hours of up time, latency, packet loss when these parameters were below the minimum acceptable parameter defined in SLA.
    d) The Successful bidder shall allocate one User-id & Password for web access for real time monitoring of all Hotspot statistics and reports as mentioned above to the nominated officer of MTNL / National War Memorial. A web console to allow officer of MTNL / National War Memorial to view the details of the SLA metrics including Packet loss, and Latency, performance, availability and interface status in real time.
22. The Web Based Network Monitoring Portal services available from the bidder should comprehensively address all the issues relating to performance, availability and uptime etc. The Web Based Network Monitoring Portal of the bidder should have the following features:
    i) It should be possible to monitor the complete network from a single point.
    ii) It should provide the statistics regarding resource utilization and faults in the network.
    iii) It should be able to detect the number of active and faulty APs on the network at any given time.
    iv) It should offer tabular information giving percentage uptimes of individual APs on a monthly basis.
23. It is the responsibility of the successful bidder to deploy sufficient staff and to store sufficient number of spare parts/Access points to maintain the SLA. If any, Access point theft / break by some incident, it is the responsibility of the successful bidder to replace the same to maintain the SLA.

24. The performance guarantee @5.00% of the accepted tendered amount quoted by the lowest bidder and security deposit @ 10% of the value of the accepted tendered amount shall become security deposit. This security amount of total 15% of tendered amount shall be released after 6 months from the date of successful completion of contract.
25. Bidder shall ensure services round the clock & for all 365 days of the year & in the network.
26. The devices deployed shall not be from any manufacturer who has been black listed/ debarred by any Govt. Department/PSU/autonomous body in India. An undertaking in this regard shall be furnished by the bidder
27. Minimum requirement of Product Description is mentioned in Section - III. The bidder has to submit the Manufacturer Authorization Form (MAF) for this tender and also submit the technical compliance report as per Format B.
28. Also, Bidder shall submit Manufacturer Authorization Form (MAF) Letters from OEM (Original Equipment Manufacturer) stating that they will support the product/solution through the bidder for the next five years from the date of commissioning, as per Format C.
29. In their bid, the bidders are required to provide/submit list of tests, which are proposed to be conducted during the acceptance testing to test the conformance of the equipment to the Technical Specifications. The test schedule and procedures for acceptance testing will be finalized by MTNL in consultation with the successful bidder.
30. Bidder to comply with the Acceptance Testing (AT) & Quality Assurance as per terms mentioned in Section – III of this Tender.
31. Bidder shall provide a full time Service Engineer on-site (Post implementation onsite support –Facility Management Service) 7 days a week for attending to Wi-Fi service complaints.
32. The 'Special Conditions of the Contract' in Section –III has been prepared by MTL's Client of this Project ie. MTNL. Wherever there is a conflict in the Terms And Conditions under Section – I & II, provisions under 'Special Conditions of the Contract' shall prevail.
33. Any other SoW on back-to-back basis mutually agreed.
34. Optical Fiber Location and APs location indicated in the Map of National War Memorial as contained in Section-III are tentative.

35. Eligibility of bidder:

a. Bidder should be empanelled as Business Development Associates with MTL.
b. Bidders should have experience in executing at least one Wi-Fi project of more than 100 APs capacity in metro cities.
c. The bidder has to submit the technical compliance report as per Format B.
d. Bidder shall submit Manufacturer Authorization Form (MAF) Letters from OEM (Original Equipment Manufacturer) stating that they will support the product/solution through the bidder for the next five years from the date of commissioning, as per Format C. Further, the OEM solutions should work on mesh technology and should have deployed in India. In this regard, bidder shall submit Self-Certificate issued by OEM as per Format C1.

Note: Procurement as part of this tender would be in accordance with PMA Policy notified by Government of India and its subsequent amendments, guidelines etc. for preference to domestically manufactured telecom products.

36. All terms and conditions of EOI No: MTL/COO/BDA- Empanelment/2017-18 dated 15/12/2017 **(Annexure – D)** along with its amendments and clarifications shall be applicable.

37. All the terms and conditions including but not limited to payment, penalty etc. will be on back-to-back basis. Any change in terms and conditions by the customer shall be acceptable by the selected agency on back-to-back basis.

38. **General Terms & Conditions:**

(i) The tender is "Two Bid' document. The technical bid should contain all the relevant information and desired enclosures in the prescribed format. The financial bid should contain only commercial document. In case, any bidder encloses the financial bid within technical bid, the same shall be rejected summarily.

(ii) The tender Document can be downloaded from the website i.e. www.mtl.in, www.mtnl.net.in, www.etender.mtnl.net.in or www.eprocure.gov.in.

(iii) The last date & time for submission of bids shall be 07/01/2020 till 12.00Hrs. MTL may in exceptional circumstances and at its sole discretion may extend the last date & time of submission of bids by issuing an appropriate notice. Such extension, if any, shall be notified on respective website including MTL website and shall be applicable to all.

(iv) Tender may be submitted by Registered Post/ Courier service or in person, so as to reach MTL on or before the last date & time set.

(v) Technical bids are to be opened and evaluated first. Financial bids will be opened only of bidders shortlisted on basis of technical bids.

(vi) The COO MTL reserves the right to accept/reject any or all bids without assigning any reason whatsoever.

(vii) Bid will not be accepted /received after expiry of the date and time fixed.

(viii) Offers/Bids for part-work shall be rejected.

(ix) The time limit for bid is given to meet the customer requirement however; the bid submitted by the bidders shall remain valid for acceptance for a period of 150 days after the date of bid opening.

(x) All the bidders are advised to read the Tender carefully and Survey National War Memorial complex for their own assessment. If a bid is submitted, it is understood that all the terms and conditions have been accepted.

(xi) Conditional Tenders/Bids/ Non-compliance of any conditions set in tender document shall render the Bid to be summarily rejected.

(xii) Any information supplied by the Bidder, if discovered to be not correct, at the stage of the opening of the Technical Bid or Financial Bid would result in the immediate rejection of the Bid. In case, the information is not found to be correct at any other later stage, i.e. in case of the contract having been awarded to such Bidder, MTL will be in its right to immediately terminate the contract, besides forfeiture of Performance Security and taking any civil or criminal action, as it may consider appropriate at the risk, cost and consequences of the Bidder.

39. **Submission of bids:**

The Bidders are advised to follow the following instructions. As two bid systems is to be followed, two envelopes duly sealed should be used for submission of tender as detailed below:-

(i) **Envelope No. 1: Technical Bid** (as per Format A,B & C) duly completed and signed should be put in this envelope, also each page of this Tender Document should be

signed by the authorized person of the firm and placed in this envelope. The envelope should be sealed properly and superscribed as **"TECHNICAL BID: Supply, Installation, Integration & Commissioning of W-iFi Network of National War Memorial, India Gate circle, New Delhi".** Firm's name, address, email and Telephone / Mobile No. should be written on the envelope.

(ii) **Envelope No. 2: Financial Bid** (as per Format D) duly completed and signed should be put in this envelope. The envelope should be sealed properly and super scribed as **"FINANCIAL BID: Supply, Installation, Testing and Commission of Equipments for providing Wi-Fi services in National War Memorial, India Gate circle, New Delhi".** Firm's name, address, email and Telephone / Mobile No. should be written on the envelope. Format D should be duly filled with net rates inclusive of all taxes and charges.

(iii) **Envelope No. 3:** All two envelopes No. 1, & 2 as mentioned above, are to be put into this envelope. The envelope should be sealed properly and super-scribed as **"Tender For Supply, Installation, Testing And Commission Of Equipments For Providing Wi-Fi Services With One Year Warranty And Its Subsequent Maintenance For Four Years Of National War Memorial, India Gate Circle, New Delhi".** Firm's name, address, email and Telephone / Mobile No. should be written on the envelope.

Each page of bid should be duly signed and stamped. The tender received after the stipulated time and date will not be entertained. The sealed tender envelope should reach us on or before **07/01/2020 by 12.00hrs** addressed to **AVP (MTL), 5110, 5th Floor, MAHANAGAR DOORSANCHAR SADAN, 9, CGO COMPLEX, NEW DELHI-110003.**

40. Evaluation Of Bids

(i) Technical Bids will be opened in the presence of the representatives of the Bidder, if any. The Technical Bids will be evaluated by the Tender Evaluation Committee (TEC) of MTL, as per requirement of Format A mentioned in tender condition. If bidders fails to submit any of the requirement listed on the 'Eligibility Criteria' of this Tender then the bidder will be considered as techno-commercially non-responsive bidder.

(ii) On a designated day and time, the Financial Bids of only techno-commercially responsive bidders who satisfy all conditions of the eligibility criteria and are technically qualified will be opened in the presence of the representatives of the technically qualified bidder.

(iii) The prices will be evaluated as per the tender rules and the decision of MTL will be final.

(iv) The bidder has to quote for quantity of Items as per Schedule of requirement (SoR). If the bidder quotes prices for lesser quantity of items, then during evaluation the price bid will be increased prorate as per the SOR Quantities and accordingly prorated value will be considered for comparison for arriving at L1 bidder.

(v) The total value including applicable Taxes for all the items will be taken up for Price Bid evaluation. The Bidders who quote L1 Price for the total value of items will be called as L1 Bidder.

(vi) If in the price structure quoted, there is any discrepancy between the unit price and total price, the unit price shall prevail and the total price corrected accordingly, unless in the opinion of the Tender Opening Committee (TOC), there is an obvious misplacement of decimal point in the unit price, in which case the total price as quoted shall govern and the unit price corrected accordingly.

(vii) 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.

(viii) The TEC while evaluating the Technical Bid or the Financial Bid will be at liberty to ask the Bidder(s) to produce the original(s) of the documents submitted by the bidder, if any, in case of doubt.

41. Award Of Work

1. Successful bidder will be decided as per evaluation method mentioned in the above Clause No.41 and its techno-commercial proposal containing Detailed Project Report (DPR) along with financial quote will be forwarded to Mahanagar Telephone Nigam Limited (MTNL) Delhi Unit for acceptance at their end and thereafter onward submission to National War Memorial, Ministry of Defence (MoD), Government of India. The work will be awarded to the successful bidder only after acceptance and confirmed Purchase Order (PO) received by MTL and submission of the following by successful bidder within 15 days of the issue of Letter of Intent:
   a) Your unequivocal and unconditional acceptance.
   b) Irrevocable bank guarantees from any scheduled bank i.e. Performance Bank Guarantee @5.00% of the accepted tendered amount and security deposit @ 10% of the value of the accepted tendered amount. Both Bank Guarantee shall be valid for five year six months from the date of signing of the Agreement or PBG valid up to Three (3) Year or more at the time of signing of agreement with undertaking that PBG will be renewed atleast 3 months in advance for the remaining period without any prior notice / intimation from MTL.
   c) Two copy of the complete filled agreement in the format given by MTL, to be executed on non-judicial stamp worth Rs.100/- & continuation sheets on ledger papers to be submitted neatly type-written sheets on one side of the paper in single line spacing. Please note that in case of consortium, agreement will be signed by all consortium partners.

2. It will be obligatory upon the bidder to make the execution of work with all the items as per terms and conditions of contract. Any item left but necessary for successful completion of project shall deemed to be included in the cost and nothing extra shall be paid. On refusal of the execution of work to the satisfaction of Department, the contract of the bidder will be cancelled, up to date Security Deposited and Performance Guarantee (PG) will be forfeited and other appropriate action as deemed fit will be initiated.

42. Submission of Security Deposit (SD) and Project Specific PBG

a. The successful bidder shall furnish Security Deposit and Project Specific Performance Bank Guarantee (PBG) as per EOI No: MTL/COO/BDA- Empanelment/2017-18 dated 15/12/2017 along with its amendments and clarifications (Annexure D). PBG can be submitted as per choice of bidder either : a) in the form of PBG before issue of work-

order /signing of the contact or b) amount equal to 5% of the payment of each bill shall be deducted and kept as security deposit.

b. The security deposit @ 10% of the value of the tendered amount quoted by the lowest bidder shall become the security deposit amount to be submitted by Successful Bidder.

c. Accordingly, these securities (PBG &SD) shall be released after 6 months from the date of successful completion of contract.

d. Security Deposit and Performance Bank Guarantee shall be payable to MTL as compensation for any loss resulting from the successful bidder failure to complete its obligations under the contract. The performance security shall also be forfeited in case of failure of the successful bidder in performance of the contract.

e. The PBG will be discharged by MTL after completion of the successful bidder's performance obligations including any warranty obligations and AMC under the contract on receipt of the certificate of satisfactory performance from the Customer.

43. Execution Of Agreement

Successful bidder shall also be required to execute an agreement on a non –judicial stamp paper of Rs. 100/- only, at his own cost within 10 days. However COO, MTL may grant the extension if the delay is due to genuine, reasonable and valid grounds. The security deposit and project specific PBG provided by the successful Bidder shall be valid for a period of sixty-six months from the date of signing i.e. for at least six months longer than the anticipated expiry date of the warranty and AMC period. In the event of a breach of contract by the successful bidder, the security deposit and PBG will be forfeited and credited to the MTL.

44. Termination Of Contract

MTL reserves the right to terminate the contract at any time without assigning any reason by giving one month's written notice. In case however, the services are found to be unsatisfactory and no improvement is made after the deficiency in service has been brought to notice orally or in writing, MTL would be at liberty to terminate the contract forthwith without calling for any further explanation, without prejudice to the right of the MTL to impose any penalty in terms of this tender document and to recover the additional cost, including the forfeiture of the Performance Security, which MTL may have to bear on account of engaging any other agency for providing the services.

MTL may also terminate the contract subsequent to awarding the contract if it is discovered that it had been blacklisted/debarred from participating in any tendering process by any Govt. Dept./Institutions/local bodies/Municipal/ PSUs etc.

45. Payment terms:

(i) No advance payment will be made.

(ii) Payment shall be made in Indian Rupees only. All the payment to bidder will be on back-to-back basis as received from MTNL. However, release of payments to successful bidder shall be restricted as below:

S.No.	**Payment Milestones**	**%age payment of PO value (ceiling)**
1.	Payment against proof of delivery of Equipments /Items	40%
2.	Against Installation and commissioning	30%
3.	Against Final Acceptance	30%

(iii) Entire payment of successful bidder's invoice shall be processed for payment by O/o COO MTL Delhi only after the credit of the GST portion in the invoice is selected in the GSTN portal i.e. the outward return in GSTR 1 is uploaded by the supplier by 10th of the subsequent month and duly reflected in MTL account on GSTN portal. Invoices will be paid, after submission along with all supporting documents by successful bidder in complete shape as follows:

a) Invoice (in duplicate) mentioning the HSN code and clearly indicating break up Price CIF-destination & GST

b) Photo copy of PAN in duplicate.

c) ECS details of Bank.

d) Delivery receipt in original along with other relevant papers duly signed and stamped by consignee i.e. Concern officer of war memorial and attested by the designated unit officer of GM(EB)/GM(BB and P&D) of MTNL Delhi unit as intimated from time to time.

e) The E-waybill as prescribed in the GST law in case of movement of goods (for both intrastate and inter-state movement).

f) Proof of payment of GST, if applicable.

g) Supplier certificate for dispatch

(iv) The following procedure shall be followed for paying the AMC payments under this Agreement:

a. MTL shall not pay any AMC charges in advance.

b. Invoices/Bills for AMC shall be raised by successful bidder on yearly basis and shall be paid by MTL at the end of each year, after successful execution of the works as per contract terms. The certificate for proper execution of work shall be given by the concern officer of War Memorial attested by the designated unit officer of GM (EB)/GM (BB and P&D) of MTNL Delhi unit as intimated from time to time.

c. All Payments shall be made by the Account section of MTL Delhi based on the certificate for proper execution of work, after deducting penalties if any.

d. MTNL reserves the right to adjust any over-payment of AMC charges in any year, any time during the period of AMC.

(v) Payment of GST/Custom duty shall be released on production of necessary supporting documents i.e. GST/customs invoices etc. If the supplier fails to furnish necessary supporting documents i.e. GST invoice/Customs invoices etc., the amount pertaining to such Duties/Taxes will not be paid. Tax amount will be payable to the supplier only after supplier declares the details of the invoices in its GSTR-1 and GSTR-3 and the same is reflected in GSTR-2A of MTL on GSTN portal.

(vi) No payment will be made for goods rejected at the site on testing .For goods rejected at the site on testing the credit note shall be issued by the supplier, failing which the purchaser shall adjust the amount to be recovered by issuing an invoice/debit note for the corresponding amount at the risk and cost to the supplier including applicable GST, if any.

(vii) The successful bidder will have to adhere to the delivery schedule strictly. MTL reserves the right to cancel the purchase order if purchase order is not executed within the stipulated time and to place the order with next successive bidder. Penalty amount(s) if any, will be adjusted in the payment due to the successful Bidder.

(viii) All taxes and other levies imposed by Governments in India will be paid as applicable.

(ix) Tax deduction at source (TDS) shall be deducted as per relevant provision of financial Act from govt. of India in time to time.

46. Facility Management Services (FMS)

46.1 Successful bidder shall be responsible for the operation and maintenance of all the equipments from date of Commissioning. During the warranty and AMC period the bidder will provide one service engineer on 7 days a week for attending to Wi-Fi service complaints.

46.2 During the currency of the project, the Successful bidder shall be responsible for the smooth working of the Equipments / Services.

46.3 The facility management shall comprise the following:

46.3.1 A Helpdesk system with trouble ticketing feature to be setup by the Successful bidder at his own cost.

46.3.2 PCs for Facility management at local level duly manned by the personnel of the successful bidder.

46.3.3 The Successful bidder shall deploy the sufficient trained/skilled manpower in the Customer Premises for facility management to operate, configure, maintain and manage the network infrastructure.

46.3.4 The operating personnel of the Successful bidder shall be equipped with accessories like mobile phones along with other required tools/testers.

46.4 The scope of the facility management is not just limited to the infrastructure pertaining to the network set up in the Customer Premises but also to vendor management. The Successful bidder will develop all the relevant procedures for call management/ fault registration, change management etc. and submit the same to the Customer for approval and shall enforce the adherence of the same. Adherence to the procedures is liable to be

audited by MTL/MTNL/Customer.

47. Warranty:

47.1 The bidder shall warrant that the stores to be supplied shall be new and free from all defects and faults in materials used, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards for materials of the type ordered and shall perform in full conformity with the specifications and drawings. The bidder shall be responsible for any defect that may develop under the conditions provided by the contract and under proper use, arising from faulty material, design or workmanship such as corrosion of the equipment, inadequate quantity of material to meet equipment requirements, inadequate contact protection, deficiencies in circuit design and/or otherwise and shall remedy such defects at his own cost when called upon to do so by MTL who shall state in writing in what respect the stores are faulty.

47.2 Replacement under warranty clause shall be made by the bidder free of all charges at site including freight, insurance and other incidental charges.

47.3 The bidder through OEM should ensure Support for operation, maintenance and upgrade of the quoted product during warranty period (1 year) required from the date of commissioning.

48. Annual Maintenance Clause

The Successful Bidder agrees to provide comprehensive maintenance for a period of 4 years after expiry of 1 years warranty period of all the systems which shall include preventive maintenance and corrective maintenance as per the MoD requirements. The maintenance shall also include replacement of all parts.

49. Spares:

49.1 During the period of Warranty/AMC the bidder shall arrange, at his own cost, all necessary spares which might be required to maintain the equipments/network or the services as per the SLA as part of the requirement.

49.2 The Bidder shall have Technical support centre to meet the criteria for fault restoration/faulty unit repair times as mentioned in the facility Management. The

49.3 Bidder shall furnish the names, locations, complete postal address, Mobile numbers and Email Ids of all the contact persons at the Technical support Centre at the time of signing this Agreement

50. Service Level Agreement (SLA) & Penalty Clause

a. **Supply:** The successful bidders shall commit to supply of the equipments within 4 weeks time from the date of issue of purchase order. In case of late delivery of equipment by the vendor, 1% of the value of undelivered portion of the purchase order after 4 weeks, subject to maximum of 10% of the undelivered portion of the equipment.
b. **During Installation and commissioning:** In case of delay in installation and commissioning of equipments at any location/office even after 8 weeks time date of issue of purchase order or upto the extended period by MoD, Penalty will be charged @ 1% of the contract value for every week's delay subject to maximum of 10%.
c. **During Warranty Period:** the complaints received from the Purchasers should be attended within half working day otherwise bidder shall be liable for a penalty for

non fulfillment of the tender conditions at 1% per week (or part thereof) of breakdown period, on the cost of only those Items, which are non functional. The warranty will cover all the materials and goods supplied by the Successful Bidder under this contract irrespective of the fact whether these have been manufactured by the Successful Bidder or not.

d. **During AMC:** In case of any problem in the equipment, it should be rectified in maximum half working day otherwise replacement should be given to MoD immediately. Failure to do so will attract penalty of 1% of the cost of the equipment subject to maximum of 10% which will be deducted from AMC charges. For first year the penalty will be @ 1% of the cost of the equipment subject to maximum of 10% and PBG may be invoked.

Exclusions

Down time due to following situations will not be considered for the purpose of penalty calculation

a. Schedule maintenance by the service provider with prior intimation
b. Force majeure events

51. **Taxes**

The quoted price should be inclusive of all Taxes.

52. Governing Laws And Disputes

All disputes or differences whatsoever arising between the parties shall be govern by terms and conditions of EOI No: MTL/COO/BDA- Empanelment/2017-18 dated 15/12/2017 (Annexure-D) alongwith its amendments and clarifications shall be applicable.

Section-III

TECHNICAL SPECIFICATIONS AND SOR WITH SPECIAL CONDITION OF THE CONTRACT

SPECIAL CONDITIONS OF THE CONTRACT

1. The special conditions of the contract shall supplement the 'Instructions to the Bidders' & "General (Commercial) Conditions of the Contract" in this tender. Wherever there is a conflict, the provisions under special conditions of contract shall prevail over those mentioned and TEC GRs. (if required).

2. As part of their bid, the bidders will submit supporting documents like test results etc. wherever applicable to prove their eligibility of tender requirements.For each type of item, Bidder will clearly indicate the Model number, Chipset number, complete hardware / software details and the features supported by these items.

3. MTNL at its discretion, during evaluation, may call upon the bidders to give their presentation on their offer, to explain the capability of the offered product in meeting the tender's requirement.

4. Purchaser reserves the right to disqualify such bidders who have a record of not meeting contractual obligations against earlier contracts entered into with the Purchaser.

5. In its business interests, MTNL reserves the right to utilize the equipments commercially, pending Acceptance testing. However, the payment to the bidder will be made as per the payment terms of the Tender.

6. Eligibility Verification: MTNL Reserves the right for verification by visiting some of the installation sites implemented by vendor. The vendor will make necessary arrangements for inspection/verification by MTNL team whereas the cost of travelling and lodging/boarding of MTNL team will be borne by MTNL. The bidder shall have to demonstrate the project as envisaged in the eligibility criteria.

7. MTNL reserves the right to vary the quantities among various types of APs/ other items as per its actual requirements.

8. There should be Ubiquitous RF coverage of -65 dBm or better alongwith 10 Mbps downlink throughput. Quality of browsing experience (website surfing , Email, You-tube , video streaming , audio streaming through APP or thorough browser etc) at proper speed will be ensured by the bidder in the entire coverage area of National War Memorial. QoE may be tested with Smartphone like I-phone or laptop like Macbook Pro etc.

9. For Installation of out-door APs, all the required installation material will be provided by the vendor.

10. Ethernet cables and Ethernet connectors shall be provided by bidder. Any other material such as PVC pipes with accessories, corrugated PVC pipe, PVC baton, Clamps, Raw Plugs, screws/nails/hooks/clips for fixing, fish-wire to pull the cable, crimping tools, drill machines, portable generator sets, field assembly connector tool kit etc required for successful installation/laying of cables, tools, labour and transportation of store/material (including loading & un loading) to the work site shall be provided by the successful bidder. These items should be as per tender specifications.

11. Any damage to the existing infrastructure at site will be restored by the bidder to its original good condition. Restoration charges in this regard will be quoted separately by the bidder.

12. The bidder shall provide one year warranty and four years AMC beyond warranty period. AMC may be extended further for three years on mutually agreed terms and conditions. During the warranty and AMC period the bidder will provide one service engineer on 7 days a week for attending to Wi-Fi service complaints.

13. **DELIVERY SCHEDULE/PROJECT IMPLEMENTATION PLAN:** Under the project, it is expected that the WiFi installations and integration will be carried out at the National War Memorial Site, New Delhi. Accordingly a project implementation plan as per details below is to be adhered to by the successful bidder:

S.N.	**Project Execution Schedule (Time Line in Weeks)**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	**Date of issue of APO (Day-0)**												
2	**Submission of PBG and acceptance by vendor**	2 week											
3	**Date of issue of PO**			1 week									
4	**Delivery of equipment**				4 Weeks								
5	**Site survey**				4 Weeks								
9	**Execution with integration**				8 Weeks(Passive & Active)								
10	**AT & Commissioning of the complete project**				9 weeks								

14. **Acceptance Testing: -** Procedure for Acceptance Testing shall be as per the following

14.1 To establish the compliance to the specifications / requirement as envisaged in the tender for supply of Wi-Fi , MTNL may conduct on-site acceptance testing of the items given in the Schedule of Requirement, for the successful bidder. The acceptance testing / acceptance testing is to be arranged in the city Delhi for which the bid has been submitted.

14.2 ***In their bid, the bidders are required to provide/submit list of tests, which are proposed to be conducted during the acceptance testing to test the conformance of the equipment to the Technical Specifications. The test schedule and procedures for acceptance testing will be finalized by MTNL in consultation with the successful bidder*.**

14.3 The Bidder shall provide, at his own cost all the testing equipments/ instruments as required for all the tests to be conducted for acceptance testing.

14.4 Any deficiency found in performance during acceptance testing of the supplied system as per the tender requirement, the same shall be rectified by the bidder immediately.

14.5 The bidder shall make available the software programs and testers required for carrying out the tests as per the schedule. Details of various items required for the above purpose may be specified in compliance to this clause.

14.6 Any additional test equipment deemed required during acceptance testing shall be arranged by the bidder at no cost to MTNL, so as to complete the testing as per the specified time schedule in this document.

14.7 The bidder has to quote prices for quantity of items as per SOR. If a bidder quotes prices for lesser quantity of items, then during evaluation the price bid will be increased prorate as per the SOR quantities and accordingly prorated value will be considered for comparison for arriving at L1 bidder. But payment shall be made as per his quoted prices.

14.8 The bidder may ensure for quoting BOM, for meeting the specifications as envisaged in the tender. In case it is more than as indicated in SOR then the same shall be taken for evaluation and payment.

14.9 Any additional material required for the commissioning of the project over and above quoted by bidder shall be given free of cost.

14.10 The acceptance testing will be conducted after deploying suitable numbers of Indoor and Outdoor APs, at least one LAN Switch, and all core network equipments like WLC, and NMS as per test setup. For deployment of APs, and other equipment for acceptance purpose, the sites will be provided by MTNL to the successful bidder.

14.11 The successful bidder has to start the acceptance testing of the offered equipments as per delivery schedule specified in clause No 13 of the Section- III : Special Condition of Contract “ .

14.12 Any components or modules failing during the acceptance testing shall be replaced at no extra cost to the Purchaser at site by the bidder. These shall be shipped within four weeks of the initial reports. Should it fail to do so within this time, the purchaser reserves the discretion to reject and replace at the cost of the bidder the whole or any portion of equipment as the case may be, which is defective or fails to fulfill the requirements of the contract, The cost of any such replacement made by the purchaser shall be deducted from the amount payable to the bidder.

14.13 When the acceptance testing called for have been successfully carried out, the Ultimate consignee will issue a Taking over Certificate to the bidder. The ultimate consignee shall not delay the issue of any "Taking Over Certificate" contemplated by this clause on account of minor defects in the equipment which do not materially affect the commercial use thereof provided that the bidder shall undertake to make good the same in a time period not exceeding six months. The Taking Over Certificate shall be issued by the ultimate consignee within four weeks of successful completion of tests.

14.14 After successful carrying out of Acceptance testing as per preceding clauses, MTNL will certify the equipment as fit for commissioning & issue the TOC.

15. Quality Assurance (QA):

15.1 The supply of equipment manufactured in India will be accepted only after Quality Assurance tests are carried out by QA team of MTNL as per prescribed schedule and material passing the test successfully and after Excise gate pass issued by Excise authorities, Government of India for the purpose.

15.2 The supply of imported equipment shall be accepted, only if it is accompanied with factory test reports / certifications of various performance parameters as per special terms and conditions of the tender.

15.3 The details of QA tests, which will be carried out at factory, shall be submitted along with the bid. Any additional test required by MTNL shall also be included in the factory test. The QA will be conducted by MTNL QA, if felt necessary after award of purchase order to the bidder.

15.4 MTNL reserves the right to depute its representatives to the factory premises abroad to inspect/ verify/ witness the QA testing of equipments/software. All the expenses related to travel, boarding and lodging, etc. of MTNL officers shall be borne by MTNL or else MTNL may decide to carry out tests in India at bidder's factory premises.

15.5 A quality manual describing the QA system shall be submitted along with the bid, which should include the details about the component quality assurance and quality system practices, including data on critical components.

15.6 Bidder shall quote for complete bill of material and all other items of cost for complete scope of work. Any deficiency in bill of material or other items of cost will be provided by the bidder free of cost for successful implementation of the project.

16. In case, bidder has not quoted the cost for some of the items, it will be presumed that cost of such items is covered and is part of some other subsystem/ item and no extra amount is payable by purchaser. In the evaluation of bids, cost of such item shall be taken as 'nil' while the same shall be made available to purchaser as per requirement without any additional cost.

17. The successful bidder will be required to supply all material/goods required to make the equipment operative (even if it is not shown in the Bill of Material).

18. **Make and Model of items:**

(a) The bidder should indicate the make and model in respect of each item for which the offer has been given. The technical documentation supplied in support of compliance shall relate only to their offered equipment. MTNL at its discretion, in exceptional cases, after opening of the tender with reasons recorded in writing may allow the changes, provided that the changed equipment is of equal or higher version/capacity than the offered product in the tender.

(b) The purchaser shall have the right to use the itemized cost for add on order in future. The bidders should not quote two different prices for the same item in their offers.

19. Bidder will indicate the optimum infrastructure requirement such as space, power etc for installation of various Wi-Fi network equipment which will be provided by MTNL.

20. **CONFIDENTIALITY:**

20.1 Vendor and the MTNL shall treat all documents/data/software or part of them, which one may provide party to the other, as strictly confidential and maintain secrecy for the same.

20.2 Vendor and MTNL shall not publish, disclose any information about, make available or otherwise dispose of the document/ data/ software or any part or parts thereof to any third party, directly or indirectly without prior written consent of the other party to this agreement.

20.3 Vendor and the MTNL shall restrict access to the documents/ data/ software only to those of their employees to whom it will be felt necessary and relevant for this project and shall draw the provision of this undertaking to the personal attention of those of its employees to whom access to the document/data/software will be granted.

21. **SCALABILITY:**

All components of the architecture must support scalability to meet user demand and business requirements. Scaling is the ability of a system to handle increasing demands at an acceptable performance level. The bidder has to ensure that the proposed solution must be scalable to meet out not only the requirement as envisaged in this Tender but also future requirements depending upon MTNL's requirements. The supplied system should be software scalable to support upto 1,000 numbers of APs.

22. **Delivery and Execution Schedule:**

22.1 The project schedule will be as per Clause-13 of "special condition of contract " with following details :

i) All core equipment including APs, switches etc. against Work/Purchase order shall be supplied within **4 weeks** from the date of **Work/Purchase Order**.

ii) The Installation and commissioning of supplied Core equipment at the NOC and Complete work of providing wireless LAN including commissioning of APs shall be**9 weeks** from the **date of work/purchase Order**.

iii) The supply of APs against repeat order shall be made within **04 weeks** from the date of P.O for repeat order.

iv) The Installation and commissioning of APs against repeat order shall be done within **9 weeks** from the date of P.O. for repeat order.

Note- MTNL reserve the right to pre-pone / postpone the supplies as per its requirement. However same will be done in consultation with the bidder.

23. **Compliance to Applicable Law:**

23.1 **Security Requirements:**

a) The Bidder shall enable the Purchaser to comply with Applicable Laws including but not limited to notifications, circulars etc issued by DoT from time to time.

b) The Bidder recognizes and accepts that in order to make, maintain and ensure Purchaser's networks compliant with security related instructions and guidelines issued by the DoT from time to time, complete cooperation and commitment of the Bidder is necessary. To help and address the business continuity, communication, security requirements and security management of Purchaser's network, the Bidder shall execute an agreement on Rs. 50 Non judicial stamp paper in the form as contained in **Annexure - A** before issuance of any APO by the Purchaser. It is clarified that the execution of such agreement shall be a condition to the effectiveness of the Advance Purchase Order. The Bidder shall indemnify and hold harmless the Purchaser and its employees, agents, shareholders, directors, representatives, against any claims or penalty or consequence arising out of breach of the security related terms of the License as a result of breach or non-compliance by the Bidder with its obligations in this sub-Clause (b) or any separate agreement executed for this purpose.

It is clarified that any expenditure incurred by the Purchaser for complying with security related provisions as prescribed under Applicable Law shall be borne by the Bidder. In the event there is a breach of the security related provisions as prescribed under Applicable Laws, any penalty imposed by the DoT on the Purchaser shall be paid by the Bidder to the Purchaser. Further, any testing of Bidder's equipment including requirement of testing equipment shall be met by Bidder on his own cost.

23.2 **Compliance with Licenses:**

The Bidder shall assist and provide support as and when required to the Purchaser including the providing of information and documents to comply with the provisions of the Licenses, any amendments made thereto as well as any notifications, circulars, letters issued by DoT or any other Governmental Authority from time to time specially in relation to security clearance and lawful interception.

23.3 **Security Clearance of foreign personnel:**

All foreign personnel likely to be deployed by the Successful Bidder for any activity pertaining to this project shall obtain security clearance from the Government of India prior to their deployment. The security clearance will be obtained from Ministry of Home Affairs, Government of India.

23.4 **Non-Compliance:**

The Bidder, including their personnel, employees, associates and sub-bidders shall be solely responsible for complying with the statutes, laws, regulations, subordinate legislation, administrative orders and instructions issued by relevant Government Authorities, regarding, but not limited to, environment, industrial relations, security and taxation, during the performance of their respective obligations under this Contract. Without limiting the generality of the foregoing, the Bidder shall be responsible for compliance with the Applicable Laws and similar regulations applicable to its activities hereunder, at its own cost and expenses.

In the event there is a delay by the Bidder which is solely attributable to Bidder in fulfilling its obligations under this Contract or any non-compliance or breach of obligations under this Contract by the Bidder due to which any Governmental Authority imposes sanctions on Purchaser, which results in financial and other liabilities on the Purchaser, the Bidder shall be liable to make good such loss immediately which has been suffered by the Purchaser.

23.5 In case at any stage, if it is found that the document in support of qualification to tender Conditions is forged or tampered with or manipulated to take undue advantage, then the Concerned bidder shall be liable for forfeiture of Bid Security or Performance Security and/or debarring/ blacklisting from participation in any of the tenders of MTNL for at least one year.

23.6 **Flexibility due to Technological changes:**

Provisions on flexibility to accept advance produce/services/software due to change in technology, software either at the same price or lesser price at the discretion of MTNL/ Committee.

SCHEDULE OF REQUIREMENTS

The summary of the revised estimated schedule of requirements for the "Supply, Installation, Testing and Commissioning Equipment for providing Wi-Fi Services" tender is given below. **These should be read along-with the Notes given below the tables and also the specifications mentioned in the respective clauses of the tender.**

Sl. No.	ITEM	Quantity	Make & Model/Remark
1	Wi-Fi Indoor Access Points (AP)	12	
2	Wi-Fi Outdoor Access Points (AP)	78	
3	Wireless Controller (WLC)		
	Hardware	2 (1+1)	
	Software	1 package	
	Licenses	100 and expandable up to 250	
4	Network Management System (NMS)		
	Hardware	1	
	Software	1	
	Licenses (wired & wireless devices)	250	
5	Centralized Authentication System		
	Hardware	2 (1+1)	
	Software	1 package	
	Licenses	20,000	
6	Managed Gigabit LAN Switch 8 ports 802.3at	18	
7	Managed Gigabit LAN Switch 24 ports 802.3at	5	
8	IP55 compliant 9U Outdoor Racks	22	

9	Online UPS 1 KVA with Lithium Ion Batteries and 30 minutes	22	
10	Armoured Cat6e Cable	2400 m	
11	Laptop with 3 X 3WiFi	3	
12	PC	3	

List of Passive Components

S. No.	Items	Details	Minimum	Remarks
1	PVC Conduit per mtr for 25mm	Inclusive of required accessories	1000m	
2	PVC Battens per mtr for 25x12 mm	Inclusive of required accessories	300m	
3	Corrugated flexible PVC pipes per meter 25 mm	Inclusive of required accessories	300m	
4	New poles similar to NWM CCTV poles for mounting APs	Inclusive of Installation and accessories	41	

Charges for Passive services

S. No	Item	Details	Quantity
1	Laying of PVC conduit per mtr	Rate to be quoted per mtr	1000
2	Laying of PVC Battens per mtr	Rate to be quoted per mtr	300
3	Laying of Corrugated flexible PVC pipes per mtr	Rate to be quoted per mtr	300
4.	Restoration of site	All the infrastructure at site will be restored to	1
5.	Fixing of Rack on the ground / wherever required	(A strong enough foundation to hold the rack is to be made and rack fixed on iron stand one ft. above ground and construction should match	20

Notes in respect of Bill of Material

1. Schedule of Requirement (SOR) is based on MTNL's estimate, in case the bidder feels that additional equipment is required to implement the solution successfully, he may quote additional equipment in technical and in price-bid, which will be included for the purpose of evaluation.

2. The bidder has to quote prices for quantity of items as per SOR. If a bidder quotes prices for lesser quantity of items, then during evaluation the price bid will be increased prorate as per the SOR quantities and accordingly prorated value will be considered for comparison for arriving at L1 bidder.
3. A package consists of the relevant software modules, number (unless separately specified) and types of licenses, management software (if any) to be quoted by the vendor in order to meet the requirement of the tender.

4. The WLC Software licenses shall be AP based and there will be no restriction on number of subscriber sessions.

5. The quantity of the passive components defined above is tentative and taken for the purpose of evaluation only. Payment of passive components will be made on actual basis. Specifications of the required accessories are defined in Section III under technical specification. Laying charge of Cat 6 Cable/Conduit/Battens and corrugated flexible PVC pipe will be quoted separately from restoration charges. The cost of the required accessories and material required for installation has to be inbuilt along with PVC pipes/ conduit/ batten/ corrugated flexible PVC pipes.

6. Provision should be made for installing ONT, LAN switch, Battery and UPS in 9U wall mounted network rack.

7. Any other item not covered above but essential for successful completion of project should also be added in the price schedule (under Any other HW/ SW/ Misc item of 'SOR') and its details should be given in the separate Annexure.

8. All necessary wiring, cables, connectors, etc. as defined in tender shall be supplied.

9. All necessary electrical wiring both AC and DC (from Power Plant to equipment room) along with AC & DC Distribution Boxes circuit breakers, runways etc. at all the nodes shall be supplied by the bidder along with the above equipment.

10. The cabling shall be Gigabit ready for CAT 6e category for Ethernet Switch. The detailed information of complete wiring implementation shall be provided along with all related accessories.

11. The equipment offered shall meet the technical requirements/ specifications of tender document.

12. The Indoor Access Points shall either be wall /ceiling mountable. The Outdoor AP's should be enabled for fast and easy mounting to street lights, traffic controls and other street furniture. It should include hardened enclosure for outdoor deployment. For Installation of out-door APs, Mounting poles/equipment will be provided by the vendor , if required.

13. There should be Ubiquitous RF coverage of -65 dBm or better along with 10 Mbps downlink throughput. Quality of browsing experience (website surfing , Email, You-tube , video streaming , audio streaming through APP or thorough browser etc) at proper speed will be ensured by the bidder in the entire coverage area of National War Memorial. QoE may be tested with smartphone like I-phone or laptop like Macbook Pro etc.

14. Ethernet cables and Ethernet connectors shall be provided by bidder. Any other material such as PVC pipes with accessories, corrugated PVC pipe, PVC baton, Clamps, Rawl Plugs, screws/nails/hooks/clips for fixing, fish-wire to pull the cable, crimping tools, drill machines, portable generator sets, field assembly connector tool kit etc required for successful installation/laying of cables, tools, labor and transportation of store /material (including loading & un loading) to the work site shall be provided by the successful bidder.

15. Any damage to the existing infrastructure at site will be restored by the bidder to its original good condition. Restoration charges in this regard will be quoted separately by the bidder.

TECHNICAL SPECIFICATIONS

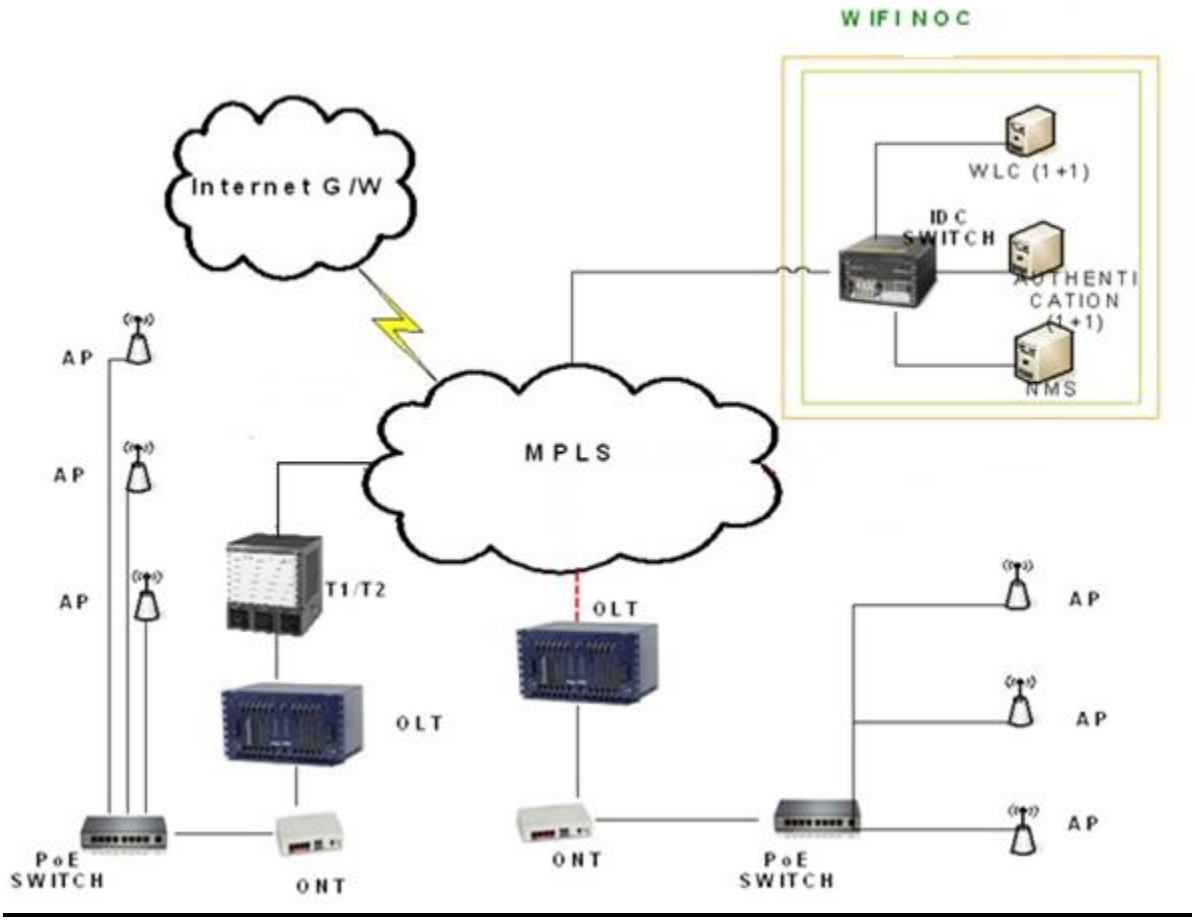
General specifications / Requirements:

Bidder will submit the complete Technical proposal along with the objectives and operational need of the Network, expected data rate, bandwidth requirement, operational requirement in the existing systems etc. The bidder will also submit the network structure diagram, details of all the Wi-Fi network equipment's including make, model, hardware, software, integration, licenses details etc.

Successful bidder upon receipt of purchase order from MTNL will also submit the Acceptance testing procedure (ATP) along for acceptance testing of their offered equipment's. The test schedule / Procedure will be mutually decided between Vendor & MTNL.

Vendor should state the MTBF (Mean Time between Failures) for each of the Wi-Fi Network equipment at specific temperature.

NETWORK DIAGRAM



1. INDOOR Wi-Fi ACCESS POINTS:

<table>
<tr><th>Sl. No.</th><th>Parameter/ Item</th><th>Specification/Requirement</th></tr>
<tr><td>1.1</td><td>Hardware</td><td>● Must have tri-band radios to have concurrent tri band (5 Ghz / 2.4 Ghz operation). One Radio of 5 Ghz for backhaul and one radio each of 2.4 Ghz & 5Ghz for customers.
● The operation shall be in the license free band in 2.4 and 5GHz bands and as per latest National Frequency Allocation Plan (NFAP), revised from time to time.
● Must have a robust design for durability , Wall / Ceiling mountable
● One numbers of 10/100/1000-Tx Mbps Ethernet port RJ-45
● Should support IPv4,IPv6</td></tr>
<tr><td>1.2</td><td>Features</td><td>● Should work in either standalone or centrally managed
● Should support 802.11 a/b/g/n/ac
● Should support 802.1Q
● Upto150 clients per station
● Should support 20/40/80Mhz channels
● Upto 16 SSID with unique QoS and security policies
● Should support mesh networking on 5GHz band
● NAT and DHCP support. Feature may be provided in overall solution.
● Multicast IP video streaming support
● Multiple QoS queues per client station/AP.
● Must support captive portal and guest accounts (when working with WLAN controller)
● Must support load balancing / admission control (when working with WLAN controller)</td></tr>
<tr><td>1.3</td><td>802.11ac</td><td>● Dual radio with 3X3 multiple-input multiple-output (MIMO).
● Compliant with GSR 542(E) of WPC , GOI
<table>
<tr><th>Maximum radiated power output</th><th>Maximum Effective Radiated Power</th><th>Type of Antenna</th><th>Coverage Area</th></tr>
<tr><td>(1)</td><td>(2)</td><td>(3)</td><td>(4)</td></tr>
<tr><td>100 mW (20 dBm) in Spread of 10 MHz</td><td>26 dBm</td><td>Built in or indoor antenna</td><td>Within the single contiguous campus of an individual, duly recognized organization or</td></tr>
</table></td></tr>
</table>

					institution.
		● Maximum transmitted power EIRP should be as per regulatory guidelines. ETA from WPC to be enclosed. ● Similarly Compatibility of Equipments for 5Ghz Radio Band must meet the required criteria as per WPC.(GSR 46(E)) ● This is Subject to any amendment from WPC from time to time. ● AP should be able to radiate at minimum effective radiate power of 24dbm.			
1.4	RF	● Should support spatial multiplexing ● Maximum Ratio Combining for best in class receive sensitivity ● Capable of part-time or dedicated air monitoring, should remotely scan the 2.4-Ghz/5-Ghz radio bands to identify/locate sources of RF interference. ● Must incorporate radio resource management for power, channels. ● Automatic interference avoidance , optimized for high density environments			
1.5	Security	● Should support WPA-PSK(AES),WPA2,802.1x(RADIUS,AD,LDAP),802.11i,AES,TKIP, EAP,EAP-TLS,EAP-TTLS,PEAP ● Should support encryption through Public Key Infrastructure (PKI). ● Integrated wireless intrusion protection to offer threat protection and mitigation and eliminating the need for separate RF sensors and security appliances ● Access Points must support a distributed encryption/decryption model. ● Enables policies to prohibit devices/Rouge AP's that interfere with the Wi-Fi network or jeopardize network security ● Supports rogue access point detection and detection of denial-of-service attacks			
1.6	QoS	● Compliant to 802.11e/WMM ● Software queues based on WLAN priority/traffic type ● Should be able to classify traffic based on TOS, VLAN based ● Dynamic Rate limiting per user /per WLAN			
1.7	Management	● Should support SNMP v1,v2,V2c or higher / TR69 ● Must support SSH/https/console login to APs directly for troubleshooting flexibility ● Should support auto software update			
1.8	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.			
1.9	Flexibility	Shouldalso support mesh capabilities for connectivity in areas with no Ethernet cabling.			

1.10	Power	Compatible with 802.3at or advanced Power over Ethernet plus (PoE+)
1.11	Technical specifications	AP should be compliant with functional and technical requirements of TEC GR No.TEC/GR/CP/WIFI-002/01/SEP-11 or latest.

2. OUTDOOR Wi-Fi ACCESS POINT:

Sl. No.	Parameter/ Item	Specification / Requirement
2.1	Hardware	• Must have dual radios for concurrent dual band (5 Ghz / 2.4 Ghz) operation • The operation shall be in the license free band in 2.4 and 5GHz bands and as per latest National Frequency Allocation Plan (NFAP), revised from time to time. • Enables fast and easy mounting to street lights, traffic controls and other street furniture. Includes hardened enclosures for outdoor deployment • Poles etc. for outdoor mounting to be provided • Must have a robust design for durability , weather proofing • One Ethernet port (1000BASE-X or 10/100/1000BASE-T) • Certified Outdoor AP should be IP65 compliant. • Should support IPv4, IPv6
2.2	Features	• Should work in either standalone or centrally managed • Should support 802.11 a/b/g/n/ac • Should support 802.1Q • Upto150 clients per station • Should support 20/40/80Mhz channelsz • Upto 16 SSID with unique QoS and security policies • Should support mesh networking • NAT and DHCP support. Feature may be provided in overall solution • Multicast IP video streaming support • Multiple QoS queues per client station • Must support captive portal and guest accounts (when working with WLAN controller) • Must support load balancing / admission control (when working with WLAN controller)
2.3	802.11n/ac	• Upto Dual radio with 3X3 multiple-input multiple-output (MIMO) • Compliant with GSR 45(E) of WPC , GOI **Maximum out power of transmitter** | **Maximum Effective Radiated Power** | **Height of Antenna**

		<table><tr><td>(1)</td><td>(2)</td><td>(3)</td></tr><tr><td>1 W (30 dBm) in Spread of 10 MHz or higher</td><td>4 W (36 dBm)</td><td>Within 5 metres above the roof top of existing authorized building</td></tr></table> ● Maximum transmitted power (EIRP) should be as per regulatory guidelines. ETA from WPC to be enclosed. ● Similarly Compatibility of Equipments for 5Ghz Radio Band must meet the required criteria as per WPC, GOI (GSR 38(E)) ● This is Subject to any amendment from WPC from time to time. ● AP should be able to radiate at minimum effective radiate power of 26dbm.
2.4	RF	● External/Internal Dual-Band Omnidirectional/ Sector Antennas ● Should support spatial multiplexing ● Maximum Ratio Combining for best in class receive sensitivity ● Capable of part-time or dedicated air monitoring,the spectrum analyzer remotely scans the 2.4-Ghz/5-Ghz radio band to identify/locate sources of RF interference. ● Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization ● Automatic interference avoidance , optimized for high density environments
2.5	Security	● Should support WPA-PSK(AES), WPA2, 801.1X (RADIUS,AD,LDAP), 802.11i, AES,TKIPEAP, EAP-TLS,EAP-TTLS,PEAP ● Should support encryption through Public Key Infrastructure (PKI). ● Integrated wireless intrusion protection to offer threat protection and mitigation and eliminating the need for separate RF sensors and security appliances ● Enables policies to prohibit devices/Rouge AP's that interfere with the Wi-Fi network or jeopardize network security ● Supports rogue access point detection and detection of denial-of-service attacks
2.6	QoS	● Compliant to 802.11e/WMM ● Software queues based on WLAN priority/traffic type ● Should be able to classify traffic based on TOS, VLAN based ● Dynamic Rate limiting per user /per WLAN
2.7	Management	● Should support SNMP v1,v2,V2c or higher/TR69 ● Must support SSH/https login to APs directly for troubleshooting flexibility ● Should support auto software update

2.8	Monitoring	Must support the ability to serve clients and monitor the RF environment concurrently.
2.9	Flexibility	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling
2.10	Power	Compatible with 802.3at or advanced Power over Ethernet plus (PoE+)

2.11	Environmental	● Wind resistance:
		  ● Up to 100 MPH sustained winds
		  ● Up to 140 MPH wind gusts
		● Operating Temperature -20 to 55 C.
		● Humidity 5-95%

2.12	Technical specifications	AP should be compliant withwith functional and technical requirements of TEC GR No.TEC/GR/CP/WIFI-002/01/SEP-11 or latest.

3. WIRELESS CONTROLLER :

3.1. Requirements

3.1.1. Supplied hardware should be able to manage minimum 100 access points and concurrent 5000 wireless clients.

3.1.2. WLC should have licenses floating on two controllers.

3.1.3. Should support advanced intelligent mesh technology .

3.1.4. Should support multi frequency system 2.4Ghz and 5 GHz.

3.1.5. Smart load balancing feature.

3.1.6. Should support 512 WLAN's

3.1.7. Should support 2048 VLAN's

3.2. Performance

3.2.1. 2 x 10 G ports (SFP+) ports

3.2.2. Two port (1000BASE-X or 10/100/1000BASE-T)

3.2.3. Hardware processing to provide minimum 10 Gbps throughput.

3.3. High Availability

3.3.1. Wireless controller should work in 1+1 mode with auto synchronization (Hot standby). Should also support N+1 redundancy models

3.3.2. Wireless controller should support state-full switchover for all Access Points to the standby wireless controller

3.3.3. Should have redundant power supplies , redundant fans

3.3.4. Multiple link aggregation (LAG)/ VRRP support to protect against link failures while maintaining the optimal network connectivity.

3.4. Management

3.4.1. Web based management.

3.4.2. Intelligent traffic management within mesh network.

3.4.3. Console based management (CLI based)

3.4.4. NMS based management (SNMP v1,v2,V2c or higher)

3.5. **AP discovery & provisioning**

3.5.1. Automatic AP discovery

3.5.2. Automatic provisioning for zero touch deployment

3.5.3. Automatic software upgrade

3.5.4. Must support user load balancing across AP's

3.6. **RF management**

3.6.1. Intelligent RF control plane for self-healing and self-optimization/forming.

3.6.2. Automatically adjust channel and power settings based of RF environment

3.6.3. Should support interference detection and avoidance

3.6.4. Should provide both real-time and historical information about RF interference affecting network performance across controllers using system-wide technology integration

3.6.5. Should support RF management with 40/80 Mhz channels with 802.11n/802.11ac.

3.7. **Software**

3.7.1. Proven and security hardened operating system.

3.7.2. Should provide network services like DHCP, FTP, AAA etc.

3.7.3. Should support 802.1x through local user database or external RADIUS,LDAP,AD

3.7.4. Should have reporting, monitoring, traffic analysis, and troubleshooting tools for wireless network.

3.7.5. Detailed per user , per session RF accounting statistics and management

3.7.6. Improve downlink performance to all mobile devices, including one and two-spatial-stream devices on 802.11n or 802.11ac

3.7.7. Should be able to provide proactive, high-speed spectrum intelligence to combat performance problems due to wireless interference

3.7.8. Should support IPv4,IPv6

3.8. **Comprehensive end-to-end security**

3.8.1. Security standards : Should comply with 802.11i , WPA, WPA2 etc.

3.8.2. Authentication :Should support 802.1X with EAP types like EAP-TLS,EAP-TTLS and PEAP etc.

3.8.3. Should support MAC and VLAN Authentication

3.8.4. Encryption : Should support WEP,TKIP,AES,PSK etc

3.8.5. Access Control Lists : Should support L2,L3,L4 ACL's , should enforce client isolation

3.8.6. Should have Wireless Intrusion Prevention System

3.8.7. Must be compliant with IEEE CAPWAP or LWAPP or equivalent for controller based WLAN's and should provide CAPWAP or LWAPP or equivalent compliant , DTLS/AES/SSL encryption to make sure of encryption between access points and controllers or between controllers.

3.8.8. Should provide protection against

3.8.8.1. Malicious / accidental association

3.8.8.2. Identify theft (MAC spoofing)

3.8.8.3. Man-in-the-middle attacks

3.8.8.4. Session Hijack

3.8.8.5. Password guessing protection

3.9. **Advanced ACL**

3.9.1. Should simplify and centralize security policies through downloadable ACLs.

3.9.2. Implementation of ACL should not impact the throughput of the system.

3.10. **Advanced QoS**

3.10.1. Should be compliant to 802.11e WMM prioritization, 802.1p/DSCP QoS mapping, traffic shaping

3.10.2. Granular QoS policies per access point / SSID

3.10.3. Fair bandwidth allocation across wireless clients on an access point.

3.10.4. Should have technology to provide line-rate performance

3.10.5. Should support over the air, wireless packet capture for export to tools like wireshark etc

3.10.6. Should provide real time charts showing interferers per access point, on a per radio, per channel basis

3.10.7. Optimized video delivery for wireless clients.

3.10.8. Should optimize the delivery of business-critical multicast video applications across the WLAN

3.11. **Mobility**

3.11.1. Should support L2 and L3 roaming

3.11.2. Secure, reliable wireless connectivity and consistent end-user experience.

3.11.3. Increased network availability through proactive blocking of known threats.

3.11.4. Faster radio resource management (RRM) updates for uninterrupted network access when roaming

3.11.5. Efficient roaming improves application performance such as toll quality voice, and consistent streaming of video and data backup

3.12. **Compliance to Standards**

3.12.1. **Wireless**

IEEE 802.11a, 802.11b, 802.11g, WMM / 802.11e, 802.11h, 802.11n

3.12.2. **Wired/switching**

IEEE 802.3u , 1000BASE-T/1000BASE-SX/1000-BASE-L , IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports, IEEE 802.1Q Vtagging

3.12.3. **Data request for comments(RFC)**

RFC 5415 CAPWAP Protocol Specification in case CAPWAP is used.

RFC 5416 CAPWAP Binding for 802.11 in case CAPWAP is used.

3.12.4. **Security standards**

IEEE 802.11i(WPA2,RSN),RFC 1321 MD5 Message-Digest Algorithm, RFC 1851 The ESP triple DES Transform,RFC 2104 HMAC:Keyed Hashing for Message Authentication,RFC 2246 TLS Protocol Version 1.0 ,RFC 2401 Security Architecture for the Internet Protocol , RFC 2451 ESP CBC-Mode Cipher

Algorithms , RFC 3280 Internet X.509 PKI Certificate and CRL Profile , RFC 4347 Datagram Transport Layer Security(in case CAPWAP is used) ,RFC 4346 TLS Protocol Version 1.1 (in case CAPWAP is used). The OEM/Bidder to use any combination of the above security standards in the proposed Wi-Fi network to set up highly secure Wi-Fi network.

3.12.5. **Encryption**

RC4 40, 104 and 128 bits (both static and shared keys) ,AES: CBC, CCM, CCMP ,DES: DES-CBC, 3DES ,SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit ,DTLS: AES-CBC ,IPSec: DES-CBC, 3DES, AES-CBC.The OEM/Bidder to use any combination of the above Encryption standards to set up highly secure Wi-Fi network.

3.12.6. Authentication, authorization and accounting (AAA)IEEE 802.1X ,RFC 2548 , RFC 2716 PPP EAP-TLS,RFC 2865 RADIUS Authentication ,RFC 2866 RADIUS Accounting, RFC 2869 RADIUS Extensions, RFC 3576 Dynamic Authorization Extensions to RADIUS,RFC 3579 RADIUS Support for EAP,RFC 3580 IEEE 802.1X RADIUS Guidelines, RFC 3748 Extensible Authentication Protocol, Web-based authentication, TACACS support for management users

3.12.7. **Management**

3.12.7.1. SNMP v1, v2, V2c or higher , SSH ,SFTP

3.12.7.2. RFC 1350 TFTP, RFC 2030 SNTP, RFC 2616 HTTP, RFC 3164 Syslog

3.12.7.3. Management interfaces

3.12.7.3.1. Web-based: HTTP/HTTPS

3.12.7.3.2. Command-line interface: Secure Shell (SSH) Protocol, serial port

3.13. **Environmental Ranges**

3.13.1. Operating temperature 23 to 113° F (-5 to 45° C)

3.13.2. Relative humidity 5 to 95% (non-condensing)

3.14. **Input power** 100 to 240 VAC; 50/60 Hz or -48V DC. (DC preferred)

4. Wi-Fi NETWORK MANAGEMENT SYSTEM SPECIFICATIONS:

4.1. Management solution should encompass all network elements that are part of Wi-Fi Network including access points, switches etc. Network and Wireless Management can be provided through one umbrella Management suite or as separate management systems. Management platform should include the following functionalities:

4.1.1. Configuration management

4.1.2. Fault management

4.1.3. Performance management

4.1.4. Security management

4.2. Bidder should describe the Network management solution and should describe main characteristics of each element that compose Network management solution.

4.3. Management system (NMS) should provide a solution for comprehensive lifecycle management of the wired/wireless networks. It should have full FCAPS facility in

respect of wireless /wired elements and shouldbe compatible with IPv4 and IPv6.

4.4. The Management system should support configuration, administration, monitoring and troubleshooting of Switches

4.5. Must support following features

4.5.1. Network Monitoring and Troubleshooting

4.5.2. Indoor location monitoring capability

4.5.3. Centralized Software updates

4.6. **Capacity:**

4.6.1. **Modularity and Scalability:** NMS should be dimensioned according to the network size. Bidder should describe the scalability and capacity of the system in all supported configurations. In case separate management system is provided, for Network (Switching) and Wireless Management, than bidder has to provide additional EMS (Element Management System) to provide single window management. Initial Capacity requirement for NMS/EMS is as below-

4.6.1.1. NMS/EMS for Management of Wireless Component like AP's, Wireless Controller etc.

4.6.1.2. NMS/EMS for Management of Wired Component like Switches etc.

4.6.1.3. NMS/EMS includes both hardware and Software.

4.7. NMS/EMSs should provide FCAPS functionality & web based management capabilities for managing the Wired and Wireless Network Elements

4.7.1. Extensive wireless management capabilities

4.7.1.1. radio frequency (RF) management,

4.7.1.2. user access visibility

4.7.1.3. reporting

4.7.1.4. troubleshooting

4.7.2. Network infrastructure lifecycle functions

4.7.2.1. Discovery

4.7.2.2. Inventory

4.7.2.3. Configuration

4.7.2.4. Image management

4.7.2.5. Integrated best practices, and reporting.

4.8. **Deploy**

4.8.1. Schedule the rollout and implementation of network changes.

4.8.2. New configuration or monitoring templates created in the design phase, software image updates, and support for user initiated ad-hoc changes and compliance updates.

4.8.3. Set of guided and advance flows to bulk provision new devices (including the converged access switches on the network) or push an initial configuration to a device to bring it up within a few minutes, thereby drastically reducing IT operational expenses.

4.9. **Operate**

Monitor the overall health of the network using predefined dashboards that provide up-to-date status. Simple one-click workflows and 360-degree views enhance

troubleshooting and reduce the time to resolve network issues. Unified alarm display provides actionable information and links to automatically open service requests with the TAC.

4.10. **Report**

Access a wide variety of predefined reports for up-to-date network information, including detailed inventory, compliance, audit, capacity, end-of-sale, security vulnerabilities, and many more. Operations monitoring and quality of experience workflows reduce instrumentation configuration and data collection complexity to provide real-time insight into network and application performance. Network inventory auditing.

4.11. **Administration**

4.11.1. Role-based access control provides flexibility to segment the network into one or more virtual domains controlled. Virtual domains help network operators deploy both large, multisite networks and managed services

4.11.2. Flexible authentication, authorization, and accounting (AAA) services allow for local, RADIUS, TACACS, and single sign-on options.

4.12. **Converged management**

Single pane-of-glass solution provides complete end-to-end infrastructure management, reducing the need for multiple tools and lowering operating expenses and training costs

4.13. **Complete lifecycle management on Wireless**

Converged solution delivers wireless management capabilities, including RF management, user access visibility, reporting, and troubleshooting - along with network infrastructure lifecycle functions such as discovery, inventory, configuration and image management, and reporting.

4.14. **Interfaces:**

4.14.1. Management system shall support SOAP/CORBA/HTTPS Northbound OSS interface.

4.14.2. North Bound Interface using the CORBA IDL based on the TMF 814 standards.

4.14.3. Management platform should support HW and SW Inventory and provide an interface for Inventory management

4.15. **Fault Management:**

4.15.1. Bidders should describe their fault management solution for the various network elements.

4.15.2. Enhanced alarm management : Fault management solution should support alarm filtering, alarm suppression, change of severity, alarm delay, alarm forward to e-mail and SMS, alarm toggling, on-line help etc.

4.15.3. Management system should support Alarm on threshold that allows alarms to be blocked if a variable number of alarms occur in a variable amount of time

4.15.4. Management system should support alarm correlation. Correlation rules perform alarm grouping and finds dependencies between root causes and symptoms.

4.15.5. Management system should support the alarm history browsing capability. Bidder to state the capability of number of alarm storage / duration for which alarms can be stored.

4.15.6. Alarm display capabilities including support of components in the alarm display, support of probable cause and specific problem and additional text fields in the alarm display, as well as support of viewing the entire raw alarm should be supported

4.16. **Configuration Management:**

4.16.1. Management system shall support the following configuration management functions:

4.16.1.1. Installation of network elements

4.16.1.2. Installation tests which can be performed on the network elements

4.16.1.3. Automatic installation of Wi-Fi AP

4.16.1.4. Modification and removal of network element components

4.16.1.5. Automated download of new network element software

4.16.2. Device inventory management feature should be supported.

4.16.3. Management system should enable policy-based automation of device configuration and management. Bidder to describe available policies.

4.16.4. Management system should support offline configuration of Wi-Fi network.

4.17. **Security Management:**

4.17.1. O&M user authentication should be supported through RADIUS/AAA/ TACACS server and operator should be able to define the roles and profiles of the users.

4.17.2. The management system should have a Logging capability and Centralized Security Log Auditing and Log Browser Utility should also be provided.

4.17.3. Password management: Support of centralized password authentication including complex password acceptance , password dictionary support, Password Storage Encryption should be provided

4.17.4. User authorization and administration: Centralized User Administration, Centralized User Authentication and Authorization, User Session Management should be supported.

4.18. **Software Management:**

4.18.1. The NMS shall provide a Software Management application via a GUI/ web-based interface. The Software Manager shall provide remote software download to all managed network elements. Application shall include reporting of current software status, version number, date of last update, checksum, s/w installation error and status reporting. Application shall include download functionality for Release, Update, Feature and Patch delivery, installation and activation.

4.18.2. **Schedule software download:** It shall be possible to schedule software downloads of any purchased Network Elements configured on the NMS. Software download shall provide capability to allow downloads based on stored start and stop time for each network element, type of element,

percentage of network element type and an editable list of network elements

4.19. **Hardware Requirements:**

4.19.1. The hardware shall be designed for single NMS. Hardware sizing shall be based on the following CPU utilization metric

4.19.1.1. CPU Utilization = (100 – CPU Idle)%

4.19.1.2. Peak CPU Utilization shall not exceed 75% at any time, on 24x7 basis.

4.19.1.3. Average CPU Utilization over any hour, measured at 5 minute intervals, shall not exceed 70%.

4.19.2. In case CPU utilization exceeds the value defined in above Clause, bidder shall supply additional hardware free of cost to MTNL to meet the above conditions.

4.19.3. Bidders must note that the hardware sizing indicated in this document is minimum and indicative.

4.19.4. Bidder shall provide a combined certificate in **Annexure- IV Section IX** from the OEM of HW and application that the hardware/software/licenses etc quoted in the bid is sufficient to meet the application requirements as per the tender, failing which the bid shall be considered non-compliant.

4.19.5. Bidder should provide ample storage (As per guidelines issued by Govt. of India from time to time – minimum 3 TB)has been provided for this purpose. The bidder shall design the system taking in consideration the interface and other requirements of the storage.

4.19.6. If any additional hardware, software and licenses are needed to meet the requirement of this tender document, the same shall be quoted, by the bidder, along with sizing details and bill of material.

4.19.7. If any specific module of the application requires separate hardware for proper functioning, the same shall be quoted, by the bidder, along with sizing details and bill of material.

4.19.8. If at any stage of this project and till the full capacity is reached it is found that the solution requires additional hardware, software, licenses or other resources or any customization effort to meet the requirements envisaged in this tender document, the same shall be supplied and implemented free of any cost to MTNL.

4.19.9. The ambient temperature of the Data center is expected to be approx. 23 degree centigrade. The bidders shall propose their solution taking this into consideration.

4.20. **Servers**

4.20.1. Bidder shall quote Servers based solution.

4.20.2. It must be possible to optimize or improve the performance of the system by distributing the processing resources.

4.20.3. The system must be capable of delivering 99.999% service availability.

4.21. **Server Configuration:**

All the servers shall have following configurations:

4.21.1. The Server shall have latest Operating system with licenses with latest generation.

4.21.2. Minimum 2 GigE Ports (External) on two Ethernet Card to enable LAN Connectivity for redundancy

4.21.3. Minimum of 2 MB of L2/L3 Cache

4.21.4. One DVD-RW Drive (8X or above)

4.21.5. Each server to have 20/40 GB DAT drive or higher.

4.21.6. Minimum 3 PCI (or higher) Expansion slots per server.

4.21.7. Minimum 2 USB ports/server.

4.21.8. Redundant load sharing and hot swappable power supplies. Redundant power supplies shall have multiple feeds.

4.21.9. High availability cluster (wherever applicable)

4.21.10. Journal File System and Volume manager to mirror OS Disks.

4.21.11. The database clustering shall be based on an architecture that shall eliminate the application or its part going down in case of failure of any of the node in cluster.

4.21.12. All necessary patch cords and other installation materials shall be supplied. The servers shall be rack mounted.

5. For Centralized Authentication System for Wifi Users

5.1. INTRODUCTION

5.1.1. MTNL proposes to procure a centralized authentication system for its proposed Wi-Fi network. The system shall authenticate the Wi-Fi users of MTNL (approximate number of users being 5000 scalable to 20000). The system shall also provide facilities like web self care.

5.1.2. The system shall comply to the DoT guidelines regarding provision of Wi-Fi internet service under de-licensed frequency band issued vide letter no. 820-1/2008-DS Pt.IIdt. 23.2.2009 or latest and other guidelines of Government of India.

5.2. GENERIC REQUIREMENTS OF CENTRALIZED AUTHENTICATION SYSTEM:

5.2.1. The Solution Shall Support Captive portal having customizable GUI. This portal should be available to any client coming into the Wi-Fi zone of MTNL.

5.2.2. Captive portal shall allow local branding and content as per the location.

5.2.3. Solution shall be able to restrict the bandwidth as per the policies. Solution shall have configurable GUI for Policy management to differentiate location wise Bandwidth policies.

5.2.4. The solution shall support Usage based as well as Time duration based accounting. It shall support real time disconnection on completion of allotted resources i.e. Time or Data

5.2.5. The solution shall support centralized server for User authentication

5.2.6. **Administration:** The solution shall support the following features:

5.2.6.1. GUI based management console for system administration, policy / package creation, backup and restore accounting data, SMS gateway configuration etc.,

5.2.6.2. Tool for Troubleshooting and Health Diagnostic

5.2.6.3. Creation of batches in advance and activation upon first usage

5.2.6.4. Generation of report of usage and accounting, real time usage of USER etc.

5.2.6.5. Access Control List for different accounting and report related activities

5.2.6.6. Management of different Packages.

5.2.6.7. Centralized system shall available in Failover mode

5.2.6.8. Policy based access control for administrative activities

5.2.6.9. Login and session details, browsing history and audit trails

5.2.7. **Subscriber Management:** The system shall Support following Subscriber management functions

5.2.7.1. Creation of subscribers as per the required packages. Activation of subscribers as per the usage

5.2.7.2. Renewal / Registration of the subscriber.

5.2.7.3. Portal providing Self registration.

5.2.8. **Accounting and Billing features:** The system shall support the following features:

5.2.8.1. Creation of various packages.

5.2.8.2. Integration with billing/payment gateway.

5.2.8.3. Real time accounting of the usage

5.2.8.4. Location/user wise usage and billing detail

5.2.9. All the features and functionalities should be IPv4 and IPv6 compliant.

5.2.10. **Radius / AAA**

The AAA component of centralized authentication system shall have following features:

5.2.10.1. It shall support following Multi-Protocol & Multiple Authentication Method

5.2.10.1.1. File, LDAP and RDBMS support for Authentication

5.2.10.1.2. PAP, CHAP, MS-CHAPv2, and Extensible Authentication Protocol (EAP) and its variants like TLS, TTLS, etc.

5.2.10.1.3. It shall support authorization based on Access Policy, Concurrent Policy and Radius Policy.

5.2.10.1.4. It shall be deployed in 1+1 Mode and support Subscriber DB Failover

5.2.10.2. It shall support secured 802.1x Network Access. Authentication shall be based on the EAP-TTLS which encrypts the user credentials and also ensures mutual authentication of WiFi Access point/Modem and RADIUS.

5.2.10.3. It shall have the option to forward the request to another AAA server based on a RADIUS attribute.

5.2.10.4. Irrespective of the mode of Access (such as dial-up access, outsourced remote access etc), it shall manage the authentication of all users/customers and deliver the appropriate level of service to each customer.

5.2.10.5. The AAA shall have proxy radius functionalities

5.2.10.6. The AAA shall have policy engine for defining and implementing AAA policies. Policies could be based on any attribute value pairs or their conditional operation. It shall be possible to configure policies on per user or user-group basis or service basis for IP address assignment, removal of selected attributes from access accept message, attribute mapping etc.

5.2.10.7. It shall be possible to create Vendor Specific Attribute definitions and update dictionary by the access server vendors.

5.2.10.8. It shall be possible to restrict authentication of one or group of users based on certain policy.

5.2.10.9. It shall enable defining access schemes by time-of-days, days-of-week, special days etc.

5.2.10.10. The RADIUS shall conform to all the latest relevant RFCs. It shall interoperate with all RFC compliant RADIUS for distribution of authentication and accounting information.

5.2.10.11. RADIUS shall be configurable to understand various Vendor Specific Attributes for multi-vendor network elements. It shall be possible to support any other network element which has RADIUS Client support and which are deployed and may be deployed in future.

5.2.10.12. It shall be possible to deploy multiple RADIUS servers for failover in a distributed environment.. It shall also be possible to load balance multiple RADIUS servers.

5.2.10.13. RADIUS Server shall be able to handle at least 300 transactions per second.

5.2.10.14. It shall be capable of authenticating through CLI, DNIS etc.

5.2.10.15. It shall interoperate with external RADIUS servers using RADIUS Proxy functionality of other service providers and enterprise customers.

5.2.10.16. It shall support integration with LDAP-based authentication, billing and provisioning systems.

5.2.10.17. It shall provide the functionality of authentication against credentials stored in text file, LDAP database, SQL Database, RDBMS and any ODBC/JDBC-compliant database. No table or schema redesign should be necessary. Authentication shall be possible against one or more multi-vendor databases. It shall also be possible to run any LDAP filter or SQL query specified, for flexibility in retrieving the information.

5.2.10.18. It shall load balance authentication requests between several databases, to eliminate the risk of a single point of failure, and increase performance on busy networks using optimal network setup design.

5.2.10.19. It shall support concurrent access limits for users set up in database.

5.2.10.20. It shall be able to retrieve stored RADIUS attributes and profiles from the database or LDAP directory to return to the network access equipment.

5.2.10.21. It shall be able to authenticate remote users against the databases using RADIUS interface such as:

5.2.10.21.1. Shall be able to authenticate remote users via proxy RADIUS requests

to RADIUS servers at other sites, which have the necessary database to perform authentication.

5.2.10.21.2. Shall be possible to mix and match these authentication methods, and choose the order in which each is checked.

5.2.10.22. It shall also be able to forward proxy RADIUS requests to multiple target servers.

5.2.10.23. It shall be possible for proxy radius to maintain local copy of the accounting information as well as transferring it to remote radius.

5.2.10.24. It shall also provide proxy packet filtering. It shall use filtering to set up rules for handling packets that are forwarded to or received from target servers.

5.2.10.25. In addition to support for proxy RADIUS, it shall offer:

5.2.10.25.1. Attribute translation capabilities.

5.2.10.25.2. Flexible username format capabilities.

5.2.10.25.3. Full SNMP reporting of proxy activity.

5.2.10.26. The Full support for Extensible Authentication Protocol (EAP) and the EAP authentication types EAP-MD5, EAP-TLS, EAP-PEAP and EAP-TTLS for compatibility with wireless LAN access points and hot spots.

5.2.10.27. It shall provide centralized management and administration associated with VPN/tunnel access. Shall support:

5.2.10.27.1. All standard RADIUS attributes, as well as the vendor-specific attributes including layer 2 tunnel with L2TP, PPTP and Ipsec etc.

5.2.10.27.2. Tunnel authorization based on username format (user@tunnel, tunnel#user), or the number (DNIS)

5.2.10.28. It shall be possible to query the RADIUS server to obtain users connection details, currently assigned IP address, session duration etc.

5.2.10.29. It shall be possible to report activities and system problems via SNMPv2 and V2c or higher, and support RADIUS client authentication and accounting MIBS, enabling proxy RADIUS activities to be reported to EMS.

5.2.10.30. It shall be able to support centralized Session management for Multiple AAA Server instances and should be able to access the session in real-time to another AAA Server in case of the failure of the AAA server instance. Should be able to support administration through Web based GUI for the datacenter customers subscribing to the AAA hosting services.

5.2.10.31. It shall control length of idle sessions and de-activate them after specified duration.

5.2.10.32. It shall simplify the set up and maintenance of multiple RADIUS servers from any Web browser. User profiles and server operation, including status and key statistics, can be configured and monitored remotely.

5.2.10.33. It shall allow view of log files from GUI Interface

5.2.10.34. It shall be able to authenticate access requests based on MAC address of the end device or the Wi-Fi Modem/Access point/Hotspot

5.2.10.35. The simultaneous authentication must be scalable up to 500 TPS.

5.2.10.36. AAA for Wi-Fi authentication should be access agnostic. For authentication,

control etc. of public Wi-Fi users the offered AAA shall be capable of interworking with the Wi-Fi network of any make which is using RADIUS/ open standard based protocols.

5.2.11. **Subscriber Management System & database**

This system shall support following administrative and other feature related to subscriber management and database:

5.2.11.1. It shall offer complete subscriber management features in Subscriber Management options which mainly focuses on creating, editing, updating, renewing, deleting, and managing of accounts for all subscribers.

5.2.11.2. It shall support multiple Login Controls

5.2.11.3. It shall support **Guest Management.**

5.2.11.4. It shall support bulk username and password creation

5.2.11.5. It shall support centralized Profile creation & Subscriber Provisioning

5.2.11.6. It shall support Web self care for subscriber to track usage summary

5.2.11.7. It shall support different customer acquisition process for Home, Office &Public Wi-Fi users

5.2.11.8. It shall support time bound username & password generation for Wi-Fi users

5.2.11.9. It shall be able to bind the MAC of Wi-Fi users

5.2.11.10. It shall have centralized Database which enables administrator easily manage database from a single point in distributed Architecture

5.2.11.11. It shall allow administrator to define whether the subscriber has to be added to the existing customer database or added as a fresh customer. Multiple subscribers shall be added under same customer. Administrator can define the username & password by which the subscriber can login.

5.2.11.12. It shall allow administrator to lists down the complete subscriber list in the system and allows updating or modifying subscriber information as required. Administrator can select the customer name from the list and update details.

5.2.11.13. The system shall access the data related to existing DSL subscribers from the existing database of MTNL.

5.2.11.14. The database for the system is to be provided by the vendor along with the required hardware, software, etc to maintain logs as per TRAI guidelines issued time to time.

5.2.12. **Web Self Care:**

5.2.12.1. This shall work as interface between MTNL and Wi-Fi user. Any prospective user coming into MTNL public hotspot shall be presented a webpage portal giving details of Wi-Fi services, tariffs and procedure to subscribe to the services. The link to payment gateway and to download the dialer shall also be presented to the prospective user. The other features of the web self care shall be as follows:

5.2.12.2. The subscriber shall be able to check his Wi-Fi account details

5.2.12.3. Shall be able to change his password

5.2.12.4. Shall be able to create new Wi-Fi accounts through Captive/Web portal

5.2.12.5. Shall be able to display the complete information includes IP address using which the subscriber logged in as well as the MAC address of the subscriber (if MAC binding option is selected).

5.2.12.6. For security reasons it shall suggest subscribers to regularly change or update their password.

5.2.12.7. It shall allow subscribers to update personal details and contact information

5.2.12.8. Proposed customer Web self care for Wi-Fi users should integrated seamlessly with existing customer Web self care deployed in MTNL for broadband services

5.3. **Lawful Interception Reports**

5.3.1. System shall support all usage tracking which can be formatted into comprehensive reports for security audits to enable service providers to comply with tracking, lawful interception and legal requirements for Public WiFi

5.3.2. It shall be able to provide custom reports so as to be able to generate reports as and when required by security agencies.

5.3.3. The administrator should be able to trace session details based on the IP address and time interval for identification of malicious activities

5.4. **Hardware Requirements:**

5.4.1. The hardware shall be designed for 5000scalable to 20000 AAA licenses. Hardware sizing shall be based on the following CPU utilization metric

5.4.1.1. CPU Utilization = (100 – CPU Idle)%

5.4.1.2. Peak CPU Utilization shall not exceed 75% at any time, on 24x7 basis.

5.4.1.3. Average CPU Utilization over any hour, measured at 5 minute intervals, shall not exceed 70%.

5.4.2. In case CPU utilization exceeds the value defined in Clause-5.4.1, bidder shall supply additional hardware free of cost to MTNL.

5.4.3. Bidders must note that the hardware sizing indicated in this document is minimum and indicative.

5.4.4. Bidder shall provide a combined certificate from the OEM that the hardware quoted in the bid is sufficient to meet the application requirements as per the tender, failing which the bid shall be considered non-compliant. Certificate shall be signed by the Authorized Signatory/Country Manager of the Application OEM, Hardware OEM and the Bidder.

5.4.5. Ample storage has been provided for this purpose. The bidder shall design the system taking in consideration the interface and other requirements of the storage.

5.4.6. If any additional hardware, software and licenses are needed to meet the requirement of this tender document, the same shall be quoted, by the bidder, along with sizing details and bill of material.

5.4.7. If any specific module of the application requires separate hardware for proper functioning, the same shall be quoted, by the bidder, along with sizing details and bill of material.

5.4.8. If at any stage of this project and till the full capacity is reached it is found that the

solution requires additional hardware, software, licenses or other resources or any customization effort to meet the requirements envisaged in this tender document, the same shall be supplied and implemented free of any cost to MTNL.

5.4.9. The ambient temperature of the Data center is expected to be aprox. 23 degree centigrade. The bidders shall propose their solution taking this into consideration.

5.5. **Servers**

5.5.1. Bidder shall quote Servers based solution.

5.5.2. All the servers shall be in High availability or Load balancing mode as per the requirement.

5.5.3. It must be possible to optimize or improve the performance of the system by distributing the processing resources.

5.5.4. The system must be capable of delivering 99.999% service availability.

5.6. **Server Configuration:**

5.6.1. All the servers shall have following configurations:

5.6.2. The Server shall have latest Operating system with licenses with latest generation.

5.6.3. Minimum 2 GigE Ports (External) on two Ethernet Card to enable LAN Connectivity for redundancy

5.6.4. Minimum of 2 MB of L2/L3 Cache

5.6.5. One DVD-RW Drive (8X or above).

5.6.6. Each server to have 20/40 GB DAT drive or higher.

5.6.7. Minimum 3 PCI (or higher) Expansion slots per server.

5.6.8. Minimum 2 USB ports/server.

5.6.9. Redundant load sharing and hot swappable power supplies. Redundant power supplies shall have multiple feeds.

5.6.10. High availability cluster (wherever applicable)

5.6.11. Journal File System and Volume manager to mirror OS Disks.

5.6.12. The database clustering shall be based on an architecture that shall eliminate the application or its part going down in case of failure of any of the node in cluster.

5.6.13. High availability cluster (wherever applicable): Bidder shall quote cluster software license along with application HA agents.

5.6.14. All necessary patch cords and other installation materials shall be supplied. The servers shall be rack mounted.

6. **LAN SWITCH 8 Ports**

6.1.	Device Type	Switch - 8 ports – L2 - managed
6.2.	Enclosure Type	Rack-mountable - 1U
6.3.	Ports	8-port 10/100/1000 (PoE+) + 2 x combo Gigabit SFP
6.4.	Power Over Ethernet (PoE) simultaneously)	POE +(All ports should work over PoE+
6.5.	Switching capacity	5.6 Gbps Half-Duplex or more
6.6.	Forwarding performance (64-byte packet size)	4.17 Mpps

	MAC Address Table Size	8k entries
6.7.	Capacity	255 Active VLANs
6.8.	Remote Management Protocol	SNMP, HTTP, HTTPS, SSH, CLI
6.9.	Authentication Method	Secure Shell (SSH)/RADIUS, TACACS

6.10. Features

Layer 2 switching, DHCP support, VLAN support, IGMP snooping, syslog support, DoS attack prevention, port mirroring, broadcast storm control, IPv6 support, multicast storm control, unicast storm control, firmware upgradable, Spanning Tree Protocol (STP) support, Trivial File Transfer Protocol (TFTP) support, access control list (ACL) support, quality of service (QoS), jumbo frames support

6.11.	RAM	64 MB minimum
6.12.	Flash Memory	16 MB flash
6.13.	Status Indicators	Link activity, port transmission speed, system

6.14. Connectivity Interfaces

8 x 10Base-T/100Base TX/1000 Base T - RJ-45 - PoE+ ¦ 1 x console - 9 pin D-Sub (DB-9)/RJ-45/USB management ¦ 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 / SFP (combo)

7. **LAN SWITCH 24 PORT**

7.1.	Device Type	Switch - 24 ports – L2 - managed
7.2.	Enclosure Type	Rack-mountable - 1U
7.3.	Ports	24-port 10/100/1000(PoE+) + 2 x combo Gigabit SFP
7.4.	Power Over Ethernet (PoE) simultaneously)	POE+(All ports should work over PoE+
7.5.	Switching capacity	5.6 Gbps Half-Duplex or more
7.6.	Forwarding performance (64-byte packet size)	4.17 Mpps
7.7.	MAC Address Table Size	8K entries
7.8.	Capacity	255 Active VLANs
7.9.	Remote Management Protocol	SNMP, HTTP, HTTPS, SSH, CLI
7.10.	Authentication Method	Secure Shell (SSH)/ RADIUS, TACACS

7.11. Features

Layer 2 switching, DHCP support, VLAN support, IGMP snooping, syslog support, DoS attack prevention, port mirroring, broadcast storm control, IPv6 support, multicast storm control, unicast storm control, firmware upgradable, Spanning Tree Protocol (STP) support, Trivial File Transfer Protocol (TFTP) support, access control list (ACL) support, quality of service (QoS), jumbo frames support

7.12.	RAM	128 MB minimum
7.13.	Flash Memory	16 MB flash

7.14. Status Indicators Link activity, port transmission speed, system

7.15. Expansion / Connectivity Interfaces
24 x 10Base-T/100Base TX/1000 Base T - RJ-45 - PoE+ ¦ 1 x console - 9 pin D-Sub (DB-9)/RJ-45/USB management ¦ 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 / SFP (combo)

8. Cat 6e Cable

8.1. Conductor –Solid bare copper (23 AWG) and shall be universal RJ-45 type.
8.2. Insulation -HDPE (CMI-75E) , Normal Wall Thickness: 0.178mm , Min. Thickness 0.15mm.
8.3. Degree of protection class – IP21.
8.4. Should support PoE+.
8.5. Data transmission frequencies up to 250 Mhz and supporting 1 Gbps speed.
8.6. Cable core filling- water proof compound to prevent moisture migration and water penetration.
8.7. GI braided wire armoring .
8.8. Double Jacket , Overall Diameter: 9mm ± 0.3mm.
8.9. Electric Requirement (Cable length: 100m) Characteristic Impedance (Zo): 85~115Ω (1~250 MHz) ,Conductor Resistance: 9Ω/100m 20o Max. Capacitance 320-350 pF per 100 meter.
8.10. The UTP Cabling shall meet ISO 11801 cabling standards and local construction and telecommunication regulation.
8.11. Confirming to TIA/EIA 568-C. 2.
8.12. Temperature rating 0 degree to + 60 degree centigrade.

9. 9U IP55 Wall Mount Network Rack

9.1. Front Door with Toughened Glass quality.
9.2. Adjustable Mounting rails - Front and Back
9.3. Fan Mounting provision
9.4. Top and bottom cable entry provides Optimal flexibility for cable management
9.5. Frame structure with max loading capacity up to 60kg
9.6. Compatible with 19” International standards & ETSI standard
9.7. Power strip and cable manager
9.8. Construction- welded galvanized steel 1.2 mm thick , load bearing angles 1.6 mm , 9U with 500 mm depth.
9.9. It should be usable for installing ONT , UPS 1KVA , POE+ switch, network switches , surveillance equipment , fiber management system etc

9.10. IP55 enclosure should provide protection from harmful dust , low pressure water jet and complete protection from rain.
9.11. Cooling option - provision should be there for 2 AC fans for providing cooling and air circulation by eliminating hot air inside the cabinet.
9.12. Front door – Lockable steel door gasket sealing
9.13. Color – White light grey powder coated with fine texture.
9.14. 2 pair heavy duty (1.5 mm) vertical mounting rail for equipment mounting or heavy duty (1.5 mm) base for placing the cabinet one feet above the ground. The vendor has to fix the rack on the ground.
9.15. Power distribution unit – 6 socket , 5 cum 15 Ampere fixed horizontally.
9.16. Load bearing capacity up to 60 Kg.
9.17. PVC cable manager.
9.18. Aluminum wire mesh filter fixed to prevent level of harmful dust entering into cabinet.
9.19. Cable entry cut – Through PG IP Glands , minimum 4 cable entry points.
9.20. Pole mount , tower mount & wall mount through single arrangement , pole dia 2 inch to 10 inch.
9.21. Fully adjustable 19 " mounting channels , mounting rails.
9.22. Provision of Padlock should be there.
9.23. ISO 9001 certified.
9.24. All necessary accessories to be provided.
9.25. Compatible with 19" international standards and ETSI standards.
9.26. Earthing of rack up to 4 Ohm.
9.27. Partitions to accommodate Switch ,UPS , ONT etc.

10. **TRUE ONLINE UPS 1 KVA WITH LI-ION BATTERY**

10.1. True online double conversion UPS of 1 KVA rating with Li-ion Battery .
10.2. IGBT – PWM with inbuilt isolation transformer.
10.3. Should be rack mountable of industries grade quality so that it can function efficiently in extreme outdoor conditions (0 to 60 degree centigrade)
10.4. Should be of sleek design and lightweight.
10.5. Degree of protection – IP21.
10.6. Type of Battery - Li-ion of type LFP/NMC (life span > 7 years , No of charge discharge cycles > 1000 and Recharge time ½ to 1 hour)
10.7. Should have flow through design.
10.8. Input power – single phase 160V – 260 V sine wave 50 Hz.
10.9. Output Power - single phase 230V +, - 1% sine wave 50 Hz.
10.10. Back up time – 30 minutes on load of 300W.
10.11. 20% overload capacity for 10 Minutes.
10.12. 50% overload limit for 1 minute.
10.13. Overall efficiency >=90%.
10.14. Total harmonic distortion <= 3%.
10.15. Protection of overvoltage, short circuit & overload at UPS output terminal.
10.16. Protection for under voltage at battery terminal at 10.5 V per 12 volt battery.
10.17. Indicators for mains presence, charging, discharging, output overload and low battery voltage.
10.18. Digital metering in UPS AC input voltage, output AC voltage, current frequency, battery

voltage and current.

10.19. Availability of the type test report from central Govt. /NABL/ILAC accredit lab covering all technical requirements.

10.20. Dry Heat test : in accordance with IS 9000 (part 3/sec. 5)1977 (reaffirmed 2007) at 55 degree C. for 16 Hrs.

10.21. Damp Heat test : in accordance with IS 9000 (part 5/sec. 2)1981 (reaffirmed 2007) at 40 deg centigrade , two cycles of 12 + 12 Hours each , 2007 .

10.22. Cold test : in accordance with IS 9000 (part 2/sec. 4)1977 (reaffirmed 2007) at -10 degree C. for 4 Hrs.

10.23. ISO 9001 certified .

10.24. Should have bypass option.

10.25. Should have cold start feature.

10.26. All necessary cabling and accessories to be provided.

11. Laying of cable as per requirement. (inclusive of fitting fixture and materials)

Specifications of various types of PVC conduits/pipes and accessories, corrugated flexible pipes, Tuflex pipes, PVC battens and fitting materials which have to be supplied and used by the contractor before and during the execution of work under the items as in SOR.

A. Plain Ended / socket Ended PVC rigid conduits/pipes

Purpose: PVC rigid conduits/pipes of sizes 25mm will be fitted on the wall of the building/blocks and shall be used to protect the Ethernet cable laid in these pipes.

Specifications

2. PVC conduits shall be as per IS: 9537(Part3) 1983 (Reaffirmed 2001) with latest amendment & its related mentioned IS numbers “for specification for PVC conduits for electrical installation”.
3. PVC conduits shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited.

Dimensions

PVC pipe classified as **medium** with following dimensions as specified in the IS shall be supplied.

Nominal size of PVC Conduits	**Outside diameter**	**Inner diameter**	**Wall thickness**	**Classification**
25mm	25	21.4	1.80	**Medium**

Type of PVC conduits

PVC conduits 25 mm shall be socket ended at one side.

Length of Conduits

Standard length of PVC conduits shall be 3 meter as specified in the IS.

General requirement

- The internal and external surface of the PVC pipe shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.
- The colour of the pipes shall be **light Grey/Ivory/white.**
- Each pipe shall be clearly and indelibly marked with manufacture's name or trade mark, size, length, standard mark and information relating to classification etc as per IS standard.

B. PVC Spout type Circular Box three ways with PVC front cover (PVC Tee)

Purpose: PVC Spout type circular box 3 way will be fitted in between the PVC rigid pipes for distribution of fiber to each floor of the building.

Specifications

- Spout type circular box 3 ways with front PVC cover shall be as per Indian Standard IS: 3419- 1988 (reaffirmed 2001) with latest amendment & its related mentioned IS numbers.
- Spout type circular box 3 ways shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited.
- The design of Spout type circular box 3 ways shall be as per the diagram (D) of table 9 on page 10 of the said IS.
- The inner diameter of spouts of Spout type circular boxes of sizes 25mm, shall be such that it should be properly fitted over the outer surface of the supplied PVC rigid conduits of nominal outer diameter 25mm, .

Dimensions

The dimensions of 25 mm spout type box shall be as specified in the said IS. However since the dimensions of spout type box have not specified in said IS, so the size & dimensions etc. spout type boxes shall be such that it should be properly fitted over the outer surface of the supplied PVC rigid conduits of nominal outer diameter similar to that in the case of 25mm box. All other specifications shall be as per IS.

Wall thickness

Wall thickness of the three type of Spout type circular boxes 3 way shall be as mentioned in table given below in order to meet the requirement as set out above.

Size	25mm	40mm	50mm

Minimum Wall thickness of the box	1.6	2.3	2.8

Cover

The cover of the spout type circular box should be made of the same material and specification as the box and shall have minimum thickness equal to wall thickness of the box as specified above and fitted to the box with screws (Refer IS: 4218). The diameter of the cover of the box shall be equal to the external diameter of the box

General Requirement

- The internal and external surface of the box shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.
- Easy to fit over the pipes and no threading is required
- The colour of the spout type boxes shall be **light Grey/Ivory/white** same as per the colour of PVC pipes.

C. Corrugated flexible PVC pipes

Purpose: Corrugated flexible PVC pipes shall be used as long bends at the Turns/corners of the walls depending upon the local constraints and jointed with the rigid PVC pipes through Slip type PVC Couplers. 16mm Corrugated flexible PVC pipes mostly shall be used as to protect the Ethernet cable and to be fitted/ laid inside false ceiling along the tray, runway and wall depending upon the local constraints.

Specifications

- Corrugated flexible PVC pipes shall be as per Indian Standard IS: 9537(Part 4)- 1983 (reaffirmed 1996) & its related mentioned IS numbers 2001 with latest amendment if any.
- The corrugated flexible PVC pipes shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited.

Dimensions

Corrugated flexible PVC pipe classified as **medium** with following dimensions as specified in the IS shall be supplied.

Nominal/ Outside diameter	Tolerance on Outside diameter	Inside diameter	Length of the coils	Reference
25mm	-0.4mm	18.3 mm	50m	IS: 9537 (Part 4) – 1983 (reaffirmed

				1996)

General Requirement

- The internal and external surface of the pipe shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.
- The pipe should be flexible, twistable in vertical and axial direction.
- The colour of the flexible pipes shall be **light Grey/Ivory/white** same as per the colour of rigid pipes.
- Each length shall be clearly and indelibly marked with manufacture's name or trade mark, size, length, standard mark and information relating to classification etc. at regular interval of about 1 metre

D. PVC Slip type coupling Bends

Purpose: PVC slip type coupling bends will be fitted in between the PVC rigid pipes at the corners/turns.

Specifications

- PVC slip type coupling bends shall be as per Indian Standard IS: 3419- 1988 (reaffirmed 2001) with latest amendment if any & its related mentioned IS numbers.
- PVC slip type coupling bends shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited
- The design and dimensions shall be as per the diagram table 5 on page 6 of the said IS.
- The inner diameter of PVC slip type coupling bends of sizes 25mm shall be such that it should be properly fitted over the outer surface of the supplied PVC rigid conduits of nominal outer diameter 25mm.

Inner Diameter

The inner diameter of collar of PVC slip type coupling bends shall be as given below.

Nominal Size	**Inner diameter of collar**	**Reference**
25mm	25.1mm $\pm$0.3	In IS: 3419- 1988 (reaffirmed 2001) with latest amendment

General Requirement

- The internal and external surface of the bends shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.

- Easy to fit over the pipes and without threading.
- The colour of the bends shall be light **Grey/Ivory/white** same as per colour of PVC pipes.

E. PVC Slip Type Coupler

Purpose: PVC slip type coupler will be used for coupling the PVC rigid pipes and also in between PVC corrugated flexible pipe and PVC rigid pipes at bends/turns.

Specifications

- PVC slip type coupler shall be as per Indian Standard IS: 3419- 1988 (reaffirmed 2001) with latest amendment if any & its related mentioned IS numbers.
- PVC slip type coupler shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited.
- The design and dimensions shall be as per the diagram table 1 on page 3 of the said IS.
- The inner diameter of the collar of PVC slip type couplers of sizes 25mmshall be such that it should be properly fitted over the outer surface of the supplied PVC rigid conduits of nominal outer diameter 25mm, 40mm and 50mm respectively (Item A).

Inner Diameter of collar

The inner diameter of collar of PVC slip type coupler shall be as mentioned below.

Nominal Size of coupler	**Inside diameter of collar**	**Reference**
25mm	25.1mm ±0.3	In IS: 3419- 1988 (reaffirmed 2001) with latest amendment

General Requirement

- The internal and external surface of the coupler shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.
- Easy to fit over the pipes and without threading.
- The colour of the coupler shall be **light Grey/Ivory/white** same as per the colour of PVC pipes.

F. PVC Battens

Purpose: The PVC battens 1/2” (12mm) and 1” (25mm) shall be used to protect the ethernet cable at the subscriber premises for providing the FTTH connection / connecting AP to switch.

Specifications

- The PVC battens shall be as per Indian Standard IS: 14927 (Part I) – 2001 with latest amendment if any and its related mentioned IS numbers.
- The PVC battens shall be manufactured in accordance with international standards ISO 9001-2000 for which the manufacture should be duly accredited.

Dimensions

Size	**Internal cross section mm2**	**Outer Width mm**	**Outer Height mm**	**Wall thickness mm**	**Reference**
25x12 mm	239.1	25.0±0.2	12.0 ± 0.2	1.2	27 (Part 1) – 2001

Length of Battens

The length of the battens will be minimum 2 metre as prescribed in the IS specifications.

General Requirement

- The PVC cover of the batten should fit properly in to the PVC batten‘s base and it should be locked properly after laying the cable through the batten.
- The internal and external surface of the batten shall be smooth, clean and free from grooving and other effects for quick laying and easy drawing of cables.
- The colour of the PVC batten shall be light white or ivory.
- Each length shall be clearly and indelibly marked with manufacture’s name or trade mark, size, length, standard mark etc as per IS standard.

G. U Clamps

Purpose: U clamps with rawl plugs & screws shall be used for fitting the PVC pipes on the wall. TEC GR forU Clamps with rawl Plugs & Screws is not available.

Specifications:

PVC U clamp with Base Plate for 25mm PVC pipes

- It is made of high impact PVC. Indian Standard IS: 3419 - 1988 (reaffirmed 2001) ”for fittings for rigid non metallic conduits” shall be followed for general requirement and method of testing of the clamps to ensure the quality of the product supplied.
- The internal diameter of the 25mm U Clamps should be such that the clamps shall be able to hold firmly 25 mm PVC pipes respectively.
- The PVC base plate should be tightly screwed with PVC U clamp with Pan Philip/star head machine screws made of high quality mild steel. The screws should be hot dip galvanized.

The dimensions of the Pan Philip/star head machine screws will be according to the size of the side holes.

- The shape of the hole provided at the centre of the base plate of the clamp should be such that it gives adequate play (adjustment to left or right) to the clamp to align the pipe straight on the wall. The dimensions of center hole should be such that the CSK head screws of size 10x38 mm can easily be inserted and hold the head of the screw on the base plate so that the base plate is firmly fixed on the wall by tightening the screw.
- The depth of side holes &centre holes shall be equal to the depth of the base plate.
- The colour of the Clamp with base plate shall be of **light grey/Ivory/white**colour same as the colour of the PVC conduits supplied. These will have neat finish and free from any sharp edges.

Note: MTNL reserves the right to test on sample basis from the standard testing lab prescribed by the Govt. of India as per Indian Standard (IS) as mentioned under clause 1 item A to H of Section VI of PVC conduits/pipes, and accessories, corrugated flexible pipes, Tuflex pipes, PVC battens and fitting materials which has to be supplied and used by the contractor before and during the execution of work under the item rates as per section V. The cost of the testing shall be borne by the vender.

H. Screws and Rawl Plug

Purpose: The screw with Rawl Plug will be used for fitting the base plate of PVC U clamp with the wall.

Specifications of Screw 10x38 mm

The screw should be made of mild steel, 38 mm long, sharp pointed end, full thread and CSK head of 10mm diameter with a slot minimum 1.4mm x 1.4mm deep. The screw should be hot dip galvanized.

Specifications of 40mm rawl plug

The rawl plug 40mm long with head diameter of 10 mm shall be used for easy & convenient fixing of screw into the wall. The material used shall be Low Density Poly Ethylene (LDPE) plastic. The design of the rawl plug should be such that it should be firmly fitted in the wall for which it should have number of projections on the periphery on whole length and the screw 10x38mm should be tightly screwed in it for which the hole should be of appropriate size and have projections inside.

12. **Laptop**
    - 12.1. Processor : 1.4Ghz Quad Core Intel Core i5
    - 12.2. Screen Size : Greater than 13 inches
    - 12.3. Memory (Ram) : 8 GB or higher
    - 12.4. Storage Capacity : 128 GB SSD
    - 12.5. WiFi3X3MIMO
    - 12.6. Built in webcam; integrated sound and graphics controller with stereo speakers & Mic
    - 12.7. Keypad with palm rest & touch pad with scroll/track point

12.8. Screen Resolution : 1680 X 1050

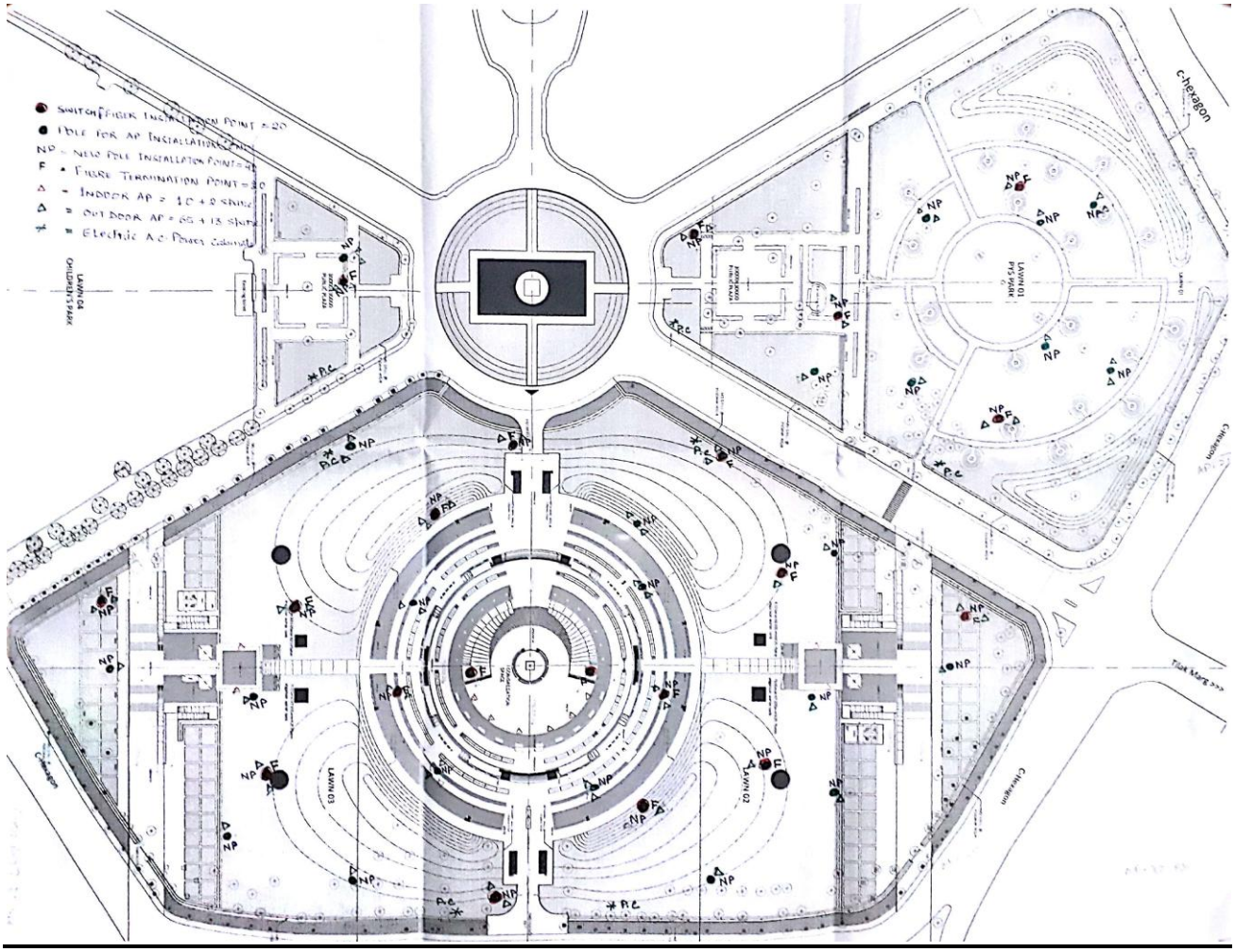
12.9. AC power adapter with good quality carrying case

12.10. Battery Backup : 10 Hours under standard working conditions with rechargeable Li-Ion battery

13. **PC (Desktop)**

13.1. Processor : Intel Core i5/i7 , 2.8 Ghz, Quad Core , 6MB Cache
13.2. Memory (RAM) : 8 GB DDR 4 - 2666 Mhz or higher
13.3. Integrated Sound and Graphics Controller
13.4. TCO 05 Certified 17" or higher TFT LCD Monitor with 5 ms or better response time
13.5. Hard Disk Capacity : 500 GB or higher SATA II at 7200 rpm
13.6. Operating System : Licensed Windows 10
13.7. DVD R/W
13.8. Ipv4/Ipv6 compliant
13.9. 104 keys OEM keyboard , optical scroll mouse

MAP of NATIONAL WAR MEMORIAL



Section-IV

Annexure A

DRAFT AGREEMENT WITH REGARD TO SECURITY REQUIREMENTS

This **AGREEMENT** is made and entered into at **Delhi** on this the [●] day of [●], 20

BY AND BETWEEN

Mahanagar Telephone Nigam Limited, a company incorporated under the Companies Act, 1956 and having its registered office at Mahanagar Doorsanchar Sadan, 9 CGO Complex, Lodhi Road, New Delhi 110003(hereinafter referred to as "**MTNL**" or the "**TSP**", which expression shall, unless repugnant to the context or meaning thereof, include its successors and permitted assigns) of the **FIRST PART**;

AND

[●], a company incorporated under the Companies Act, 1956 and having its registered office at [●](hereinafter referred to as the "**Supplier**" or the "**Bidder**", which expression shall, unless repugnant to the context or meaning thereof, include its successors, and permitted assigns) of the **OTHER PART**.

(MTNL/TSP and the Supplier/Vendor shall be collectively called as the "Parties" and individually a "Party".)

RECITALS

A. The Vendor has been awarded the Tender bearing no [●] for the ("**Contract**").

B. Pursuant to the provisions of Clause [●] of Part [●] of Section [●] of the Contract, the Parties are executing this Agreement, subject to the terms and conditions as provided hereinafter.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL REPRESENTATIONS, COVENANTS AND OTHER VALUABLE CONSIDERATION, THE RECEIPT AND SUFFICIENCY OF WHICH IS HEREBY ACKNOWLEDGED, THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Definition & Interpretation

1.1 Definitions

Unless the context otherwise requires, the different terms and expression used in this Agreement shall have the meaning assigned to them for the purpose of this Agreement :

"Access" shall mean the interconnection with TSP Systems or access to or use of TSP Information stored on TSP Systems through interconnection with TSP Systems or access to or use of TSP Information stored on Vendor Systems or access to or use of TSP Information stored in any mobile device.

"**ApplicableLaws**" shall mean any law, statute, ordinance, rule, regulation, guideline, policy or other pronouncement having the effect of law of any Governmental Authority as interpreted and administered including any modifications or amendments thereto.

"Authorised" shall refer to the approval by TSP of the Access as part of the authorisation process and the Vendor Security Contact has a record of this authorisation. The term "Authorisation" shall be construed accordingly.

"Commencement Date"" shall mean the date when the Agreement is executed

"Contract Personnel" means dedicated resources of the Vendor in terms of employees, subcontractors including employees of sub contractors and agents including agent's sub contractors and their employees engaged for the purpose of this Agreement.

"End Date" shall have the meaning assigned to it in Clause 16.1.

"**Escrow Information"** shall have the meaning assigned to it in Clause 7.11 (a).

"**Governmental Authority**" shall mean any governmental authority, statutory authority, government department, ministry, secretariat, agency, commission, board, tribunal, court or other law, rule or regulation making body/ entity having or purporting to have jurisdiction on behalf of the Republic of India or any other government having or purporting to have jurisdiction over a Party, or any state or other subdivision thereof or any municipality, district or other subdivision thereof including, without limitation, the Chairman, Department of Telecommunications, Ministry of Communications, Government of India and/or any other telecom regulatory authority, including Telecom Engineering Center, having competent jurisdiction; and/or Chairman, Telecom Regulatory Authority of India, and includes any officer empowered by them to perform all or any of the functions of such a governmental authority.

"**Information**" shall mean technical, financial and commercial information and data relating to Party's respective businesses, finances, planning, facilities, products, techniques and processes and shall include, but not limited to, discoveries, ideas, concepts, know-how, techniques, designs, specifications, drawings, blueprints, tracings, diagrams, models, samples, flow charts, data, computer programs, disks, diskettes, tapes, marketing plans, customer names and other technical, financial or commercial information and intellectual properties, whether in written, oral or other tangible or intangible forms.

"**Licensor**" shall mean the Department of Telecommunications, Ministry of Communications & IT, Government of India.

"Personal Data" shall comprise of customer details and Call Detail Record (CDR)..

“Sensitive Information” shall mean any TSP Information marked as classified as per TSP’s data classification policy or deemed business critical. This also includes any other data, or element of information, notified as such by the Government (e.g. IT Act 2000).

“Security Standards” shall mean all the relevant contemporary standards associated with national and international security standard related to IT & Telecom equipment hardware and software and those related to information & communication security, including but without limitation to ISO 27000 series, ISO/ IEC 15408, 3GPP, 3GPP2, WiMAX etc. and as evolved from time to time.

“Subcontractor” shall mean any person, partnership or corporation with whom the Vendor places a contract and/or an order for the supply of any equipment, item, service or for any work in relation to the purpose of this Agreement. The term "Subcontract" shall be construed accordingly.

“Supplies” shall mean all components, materials, plant, tools, test equipment, documentation, hardware firmware, software, spares parts, services and all the things & items to be provided to TSP pursuant to the Agreement together with all Information and Work the Agreement requires to be supplied or performed for TSP.

“Term” shallmean the term of this Agreement starting from the Commencement Date upto the End Date.

“TSP” shall mean Mahanagar Telephone Nigam Limited who has been issued the CMTS license under section 4 of Indian Telegraph Act 1885 by the Licensor, Government of India

“TSP Group Security” shallmean the security organisation based within the TSP.

“TSP Information” shall mean all data including data, text, image, sound, voice, codes, circuit diagrams, core & applications software and database, intellectual property as well as personal, public, operational and services data in TSPs custody which is and /or received which are supplied/ shared with Vendor for the purpose of this Agreement or are obtained by the Vendor on behalf of TSP.

“TSP Items” shall mean all items provided by TSP to the Vendor and all items held by the Vendor which belong to TSP.

“TSP Regulatory Contact” shall mean in-charge of TSP Regulatory Operations or such other person whose details shall be notified by TSP to the Vendor from time to time.

“TSP Security Contact” shall mean in-charge of TSP Security Operations Centre or such other person whose details shall be notified by TSP to the Vendor from time to time.

“TSP Systems” shall mean any TSP computer, application, databases , network infrastructure, network elements and appliances, core and applications software or such other systems as may be agreed in writing from time to time between TSP and the Vendor.

"Vendor" shall mean the vendor who supplies equipment, software and is and/or managed services to TSP for the purpose of installation, testing, commissioning, provision, operations and/or maintenance of TSP's networks.

"Vendor Security Contact" shall mean such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

"Vendor Regulatory Contact" shall mean such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

"Vendor Systems" shall mean any Vendor owned computer hardware or software,

application database or network elements / appliance or such other systems as may be agreed in writing from time to time by TSP and the Vendor.

1.2 Interpretation

Unless otherwise stated or unless the context otherwise requires, in this Agreement:

(a) the headings, whether of Clauses or other parts of the Agreement, are for ease of reference only and shall not be relevant to interpretation;

(b) the references to the Recitals, Clauses, Schedules and Annexures shall be references to the recitals, clauses, schedules and annexures of this Agreement;

(c) words importing the singular shall include plural and vice versa;

(d) words denoting any gender shall include all genders;

(e) where a word or phrase is defined, other parts of speech and grammatical forms of that word or phrase shall have corresponding meanings;

(f) references to statutes or statutory provisions include references to any orders, or regulations made there under and references to any statute, provision, order or regulation include references to that statute, provision order or regulation as amended, modified, re-enacted or replaced from time to time whether before or after the date thereof.

2. Scope

This Agreement sets out the provisions under which the Vendor will be able to supply equipments and services and be granted Access to TSP Systems, network, equipments, data and facilities and TSP Information including Sensitive Information for the purpose of the planning, engineering, supply, installation, testing, commissioning, operations and maintenance, annual maintenance on network/equipment as per the contract.

3. International Security Standard Certification

The Vendor shall have contemporary relevant Security standard certification and shall comply with the provisions of security standards certification with respect to Telecom & IT equipment hardware and software and those related to information & communication security management, such as ISO 15408 standards as applicable to IT and IT related products, ISO 27001 for Information Security Management System, standards used by other relevant standard formulation bodies for Telecom equipment like 3GPP, 3GPP2, ITU standard etc or equivalent acceptable international standards or certification. Based on the requisite testing to be conducted at their labs, vendors will certify their own equipments as required under this clause. IT related elements in the telecom networks of the concerned OEMs, which are already ISO 15408 certified will be accepted as certified. Vendor will submit a relevant self certificate based on test reports in this regards.

4. Security Requirements:

The Vendor shall comply with following security policies:

4.1 General

4.1.1 The Vendor shall be Authorised to access only TSP Systems and Information in accordance with the provisions of this Agreement and only during the Term of this Agreement.

4.1.2 The Vendor shall identify to the TSP, details of Vendor Security Contact at the Commencement Date who will act as a single point of contact for TSP, such as a senior manager or CIO responsible for security, for any security issues. This responsibility shall be detailed within his/her job description. Notwithstanding anything to the contrary, the Vendor shall at all times be responsible to the TSP for any security related issues. It is clarified that the Vendor Security Contact shall be a security cleared Indian national. The security clearance for the Vendor Security Contact will be applied , within one month of date of submission of necessary document by the vendor to TSP.

4.1.3 As part of the Authorization process, details of Vendor's Contract Personnel that need Access will be requested by TSP. The Vendor Security Contact shall at all times ensure that only Contract Personnel who have a need to Access in order to fulfill the purpose of this Agreement are Authorized. This Authorization and any changes in the Contract Personnel would be notified by the Vendor for the information and for the approval (wherever applicable) of the TSP.

4.1.4 Pursuant to Clause 4.1.3 above, the Vendor acknowledges that only the Contract

Personnel having requisite training are authorized to access the TSP System.

4.1.5 The Vendor shall have a well defined Information Security policy compliant with ISO/IEC 27001:2005 or have equivalent standards and in line with the TSP's information security policies and requirements.

4.1.6 The Vendor shall ensure that they have information security organization in place to implement the provisions of TSP's information security policies. The Information Security responsibilities of all Vendor employees working for TSP shall be defined and communicated.

4.1.7 The Vendor shall establish and maintain contacts with special interest groups to ensure that the understanding of the information security environment is current, including updates on security advisories, vulnerabilities and patches and ensure that the same is implemented.

4.1.8 The Vendor shall conduct a Risk Analysis and ensure that all risks due to it own and subcontractors' operations with TSP are identified, measured and mitigated as per the TSPs requirements. The Risk Assessment report is required to be shared with the Chief Security officer/CISO of TSP.

4.2 Physical Security

4.2.1 All Contract Personnel including sub contractors and their employees, agents and their employees of the Vendor working on TSP premises shall be in possession of a TSP Identification or Electronic Access Control ("**TSP ID/EAC**") card. This card is to be used as a means of identity verification on TSP premises at all times and as such the photographic image displayed on the TSP ID/EAC card must be clear and be a true likeness of the Contract Personnel. If the TSP has any advanced identity verification systems the same would also apply. TSP and Vendor will mutually agree to re- define such verification measures from time to time

4.2.2 All Contract Personnel including sub contractors and their employees, agents and their employees of the Vendor accessing premises (sites, buildings or internal areas) , where TSP Information is stored or processed, shall be in possession of an Identification or Electronic Access Control ("**ID/EAC**") card. This card is to be used as a means of identity verification on these premises at all times and as such the photographic image displayed on the ID/EAC card must be clear and be a true likeness of the Contract Personnel or the Subcontractor or the Vendor's employees, subcontractors and agents. If the TSP has any advanced identity verification systems the same would also apply. TSP may re-define such verification measures from time to time

4.2.3 The Vendor shall not (and, where relevant, shall procure that any Contract Personnel shall not) without the prior written Authorisation of the TSP Security Contact connect any equipment, device or software to any TSP System and where it is not intended to be connected at a point in the TSP system.

4.2.4 The Vendor shall be able to demonstrate that it has procedures to deal with security threats directed against TSP or against a Vendor working on behalf of TSP whilst safeguarding TSP Information.

4.2.5 The Vendor and/or its Contract Personnel shall not access TSP's electronic systems without first obtaining the written consent of the TSP Security Contact.

4.2.6 The Vendor's Access to sites, buildings or internal areas where TSP Information is stored or processed, shall be as Authorised and the Vendor and all its Authorised personnel shall adhere to robust processes and procedures to ensure compliance.

4.2.7 The Vendor shall not conduct recording, photography or videography at TSP premises that captures any TSP Information , without prior authorization from the TSP Security Contact.

4.2.8 If already available at the TSP Premises, CCTV security systems and their associated recording medium shall be used by the TSP/Vendor either in response to security incidents, as a security surveillance tool, as a deterrent or as an aid to the possible apprehension of individuals caught in the act of committing a crime. As such, these systems shall be Authorised by appropriate TSP Security Contact when used by Vendor,

4.2.9 The Vendor shall maintain a controlled record of all assigned TSP physical assets and assigned TSP Items to them.

4.2.10 The local area surrounding the Vendor's facilities at TSPs premises over which Vendor has authorized control shall be physically inspected for security risks and threats by the Vendor in case of any abnormal activity / incident found / observed shall report the same to TSP.

4.2.11 The Vendor shall disable the Access immediately if any Contract Personnel is no longer require Access or has changed roles for any reason whatsoever or whose integrity is suspected or considered doubtful or as may be notified by TSP in accordance with clause 4.3.1.

4.3 Logical Security

4.3.1 The Vendor shall notify TSP immediately if any Contract Personnel no longer requires Access or changes role for any reason whatsoever thus enabling TSP to disable or modify the Access rights.

4.3.2 The Parties shall, implement agreed security measures across all supplied components and materials including software & data to ensure safeguard and confidentiality, availability and integrity of TSP Systems and TSP Information , Parties shall prepare documentation in relation to the implementation of logical security and shall ensure that it has such security as:

prevents unauthorized individuals e.g. hackers from gaining Access to TSP Systems; and reduces the risk of misuse of TSP Systems or TSP information, which could potentially cause loss of revenue or service (and its Quality) or reputation, breach of security by those individuals who are Authorised to Access it; and

detects any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained Access and determination of how they obtained it.

4.4 Information Security

4.4.1 The Vendor shall not use TSP Information for any purpose other than for the purposes for which they were provided to the Vendor by TSP and only to the extent necessary to enable the Vendor to perform as per this Agreement.

4.4.2 The Vendor shall ensure that all information security requirements in this Agreement are communicated including in writing to all Contract Personnel in relation to their role.

4.4.3 The Vendor shall ensure procedures and controls are in place to protect the exchange of information through the use of emails, voice, facsimile and video communications facilities.

4.5 Contract Personnel Security

4.5.1 The Vendor shall ensure that the TSP Information provided under this Agreement is used only to the extent necessary to enable the Vendor to perform its obligations as per the terms of this Agreement. All Contract Personnel shall sign a confidentiality agreement either as part of their initial terms and conditions of employment or when they start working in TSP buildings or on TSP Systems and TSP Information. These confidentiality agreements shall be retained by the Vendor and shall be made accessible to TSP, if required.

4.5.2 The Vendor shall deal with breaches of security policies and procedures, including interfering with or otherwise compromising security measures, through a formal disciplinary process.

4.5.3 The Vendor shall provide a 'whistleblower' facility, available to all staff, with all TSP related issues reported back to the TSP Security Contact to the extent permissible by the law in a location in India where the Vendor is providing the services. . For the avoidance of doubt, this facility shall be used by the Contract Personnel if TSP's employee, agent or contractor instructs Contract Personnel to act in an inconsistent manner in violation of the Agreement.

4.5.4 The Vendor shall ensure that in respect to any Contract Personnel assigned to this Agreement, it shall carry out recruitment checks in accordance with its policies.

4.5.5 The Vendor shall ensure that all Contract Personnel maintain a clear-desk and a clear screen policy to protect TSP Information, as per internal policy.

4.5.6 The Vendor shall ensure that an auditable process is developed for the ongoing control and management of Contract Personnel access profiles.

4.5.7 The Vendor shall, and shall procure that if a Contract Personnel's job or role has been changed or terminated, such Contract Personnel shall securely destroy any TSP Information received in a recorded form from TSP (or has recorded received TSP Information) in accordance with its internal policy. Vendor may retain one copy of such information for archival policy provided it does so in a secure manner..

4.5.8 The vendor may perform the above activities as per its internal policy, which shall be shared with MTNL from time to time.

4.6 Additional Security Policies

4.6.1 The Vendor shall have documented operating procedures to discharge the security requirements detailed within this Agreement and provide TSP with access to such documentation in accordance with "Access to Vendor systems" as stipulated in this Agreement.

4.6.2 The Vendor shall implement a controlled exit procedure in respect of the individual Contract Personnel to ensure the return of any TSP assets or TSP Items or TSP Information in the possession of the individual when any of the Contract Personnel who have Access, leave the employment of the Vendor or are no longer engaged for the purpose of this Agreement. Such controlled exit procedure shall include a written communication by the Vendor Security Contact to TSP Security Contact of this removal.

4.6.3 The Vendor shall inform the TSP Security Contact immediately upon its becoming aware of any actual or suspected unauthorised Access or misuse of TSP Systems or TSP Information or breach of any of the Vendor's obligations under this Agreement.

4.6.4 The Vendor shall maintain integrity of the software build including upgrades, operating systems and applications from factory to desk. The Vendor shall demonstrate that the software build (both proprietary and off-the-shelf) delivered to TSP is the same as the software build agreed with TSP. The software as provided by Vendor should not have any known viruses or malware which could hamper security including any unauthorized leakage of TSP Information including Sensitive Information.

4.6.5 Any change of location by the Contract Personnel or Vendors support centers shall be notified to TSP.

4.6.6 Where Vendor uses subcontractors,, TSP may require that the associated security risks are clearly identified and assessed by TSP Group Security or the appropriate TSP line of business security team. This will ensure that any unacceptable security risks are identified and addressed. This in anyway shall not reduce the Vendor from being responsible to TSP for its obligations to be performed under this Agreement relating to security.

4.6.7 Where Vendor uses subcontractors, formal contracts containing all necessary security requirements shall be put in place between the Vendor and its subcontractor before the Subcontractor or its personnel can access TSP Systems and TSP Information or occupy space in TSP's buildings or space in the Vendor's building that is used to access, hold or process TSP Information.

4.6.8 TSP may update from time to time, security related policies, guidelines, standards and requirements. TSP will incorporate such updates by reference which shall be notified in writing by TSP to the Vendor promptly. If the Vendor has an issue with such updates, the Vendor shall promptly detail its concerns to TSP in writing.

4.6.9 The Vendor shall record and maintain detailed information of all Contract Personnel who are authorised to Access TSP Systems or TSP Information.

5. Access to TSP Systems

5.1 Subject to the provisions of this Agreement, the TSP allows (so far as it can and is able to do so) the Vendor, to have Access solely for the purpose as contemplated herein during the Term of this Agreement.

5.2 In relation to Access, the Vendor shall (and, where relevant, shall procure that all

Contract Personnel shall):

a) ensure each individual Contract Personnel has a unique user identification and password known only to such user for his/her sole use.

b) ensure Contract Personnel never share user identification, passwords or security tokens.

c) promptly provide to TSP such agreed reports as TSP shall from time to time require concerning the Vendor's use and security of Access and any related matters to Access.

d) ensure onward bridging or linking to TSP Systems is prevented unless authorized by TSP.

e) use all reasonable endeavors to ensure no viruses or malicious code like malware, spyware, key logger, bots (as the expressions are generally understood in the computing industry) are introduced, and that there is no corruption or modification or compromisation of TSP Systems or TSP Information, while meeting out the obligations under the Contract.

f) Use reasonable endeavours to ensure that personal files which contain information, data or media with no relevance to the purpose, are not stored on TSP building servers or TSP centralized storage facilities or TSP Systems.

5.3 If TSP has provided the Vendor with Access to the Internet/Intranet, the Vendor shall, and shall ensure that the Contract Personnel, access the Internet/Intranet appropriately. It is the Vendor's responsibility to ensure that practical guidance on internet and email abuse (as amended) is communicated to the Contract Personnel from time to time.

5.4 The Vendor shall ensure that all Contract Personnel, subject to the Clauses headed

"Regulatory Matters" and "Confidentiality" comply with classifying and handling of Information.

5.5 Any security software procured by the Vendor shall be used by the Vendor without modification, unless there is an essential need to do so, in which case appropriate controls shall be applied and the agreement of TSP Group Security sought.

6. Access to Vendor Systems

6.1 If Contract Personnel is granted Access to Vendor Systems having bearing on TSP data, information or network, the Vendor shall:

a) ensure each individual has a unique user identification and password known only to such individual for his/her sole use.

b) promptly provide to TSP such reports as TSP shall from time to time require, concerning the Vendor's use and security of access to Vendor Systems.

c) allow Access only to the minimum extent required to enable the Contract Personnel perform their duties.

d) allow Access using a secure login process.

e) establish and implement formal procedures to control the allocation and de-allocation of Access rights.

f) ensure that the allocation and use of enhanced privileges and access to sensitive tools and facilities in Vendor Systems are controlled and limited to only those users who have a business need.

g) ensure that the allocation of user passwords to Vendor Systems that hold or access TSP Information is controlled through a formal auditable management process.

h) provide processes to demonstrate that remote and home working activities are only permitted where Authorised by TSP and subject to appropriate security controls within the Vendor's organisation including but not limited to remote Access by users being subject to strong authentication.

i) demonstrate that users follow security best practice in the management of their passwords.

j) implement a password management system which provides a secure and effective interactive facility that ensures quality passwords.

k) ensure that user sessions are terminated after a defined period of inactivity.

l) ensure that audit logs are generated to record user activity and security-relevant events and securely managed and retained with nil ability on the part of the Vendor to allow any un-authorised access or amendment to the audit logs. Such audit logs must be maintained for future reference for a period of at least one year.

m) ensure that monitoring of audit and event logs and analysis reports for anomalous behaviour and/or attempted unauthorised access are performed by Vendor's staff independent of those users being monitored.

n) make available audit logs where required by TSP for review.

o) ensure all systems holding, processing or accessing TSP Information shall be hardened as per industry standards.

p) ensure that to the extent possible, development, test and live environments are segregated from each other and the other work areas in Vendor buildings.

q) implement controls to detect and protect against malicious software and ensure that appropriate user awareness procedures are implemented.

r) ensure that Vendor has in relation to all Vendor Systems formal security incident management procedures with defined responsibilities.

s) ensure that any unauthorised software is identified and removed from Vendor Systems holding, processing or accessing TSP Information.

t) ensure that Access to diagnostic and management ports as well as diagnostic tools are securely controlled to TSP's reasonable satisfaction.

u) ensure that Access to Vendor's audit tools shall be restricted to Relevant Contract Personnel and their use is monitored.

v) Ensure that data gathered after running audit tool is properly protected.

w) perform enhanced independent code reviews (including penetration testing) onallVendorSystems, as a part of the Vendor's security development lifecycle (SDL).

6.2 The devices which use proprietary encryption technique should not be used for holding TSP information.

6.3 To the extent the servers are used to fulfill the purpose of this Agreement, Vendor's servers shall not be deployed on un-trusted networks without appropriate security controls.

6.4 Changes to individual Vendor Systems shall be controlled and subject to formal change control procedures. All documentation relating to Vendor Systems shall be protected from unauthorized Access or amendment.

6.5 Security procedures and controls shall be used to secure equipment holding, accessing or processing TSP Information in Vendor Systems.

7. Conditions for Equipment Vendors

7.1 Conformance to Security Standards and Policies

The Vendor shall ensure and certify that the supplied equipment has been subjected to penetration testing and all addressable vulnerabilities have been mitigated and the equipment is 'Safe to Connect' in the Telecom Network as per the latest standards and recommendations on the subject from ITU/ISO/IETF/IEC etc. It will also include that the equipment confirms to the security policies of the TSP with respect to network elements. This applies to all telecom network elements and IT equipment used in the network.

The Vendor shall also ensure that the equipment supplied has all the contemporary

security related features, facilities, hardware, software etc for the purpose of Interception, Monitoring, Analysis etc for use by the law enforcement agencies and provide complete information to enable these features and facilities before the supply of the equipment or the procedure of enabling these, if these are to be enabled after the commissioning of the network. The Vendor shall also submit a test report on these features and facilities and also a certificate that all contemporary features and facilities of this category exist in the equipment supplied.

Vendors will be allowed to certify their own equipments based on the testing at the labs which are capable of such testings. IT related elements in the telecom networks which are already ISO 15408 certified will be accepted as certified. Vendor can submit a relevant Self certificate based on test reports in this regard.

7.2 Equipments Configuration Guide

Two sets of equipment configuration guide should be supplied which detail the configuration required to meet the policies and standards at least in respect of following:

Network Element security policies:

- Generic OS

- Technical Standard for Switches and Routers

- Management Standard for Switches and Routers

7.3 Reports

A report on the susceptibility to the attacks on mobile networks shall be provided by the Vendor to the TSP in the following manner:

a) Next Generation Network Equipments are susceptible to several attacks. The Vendor must submit a report categorically stating that the attacks to which the equipment and the network is susceptible, the degree of risk of each type of attack and mitigation technique to deal with these attacks. The Vendor will ensure that whatever mitigation was possible as per the current available technologies, techniques, configuration have already been used and adopted by them before the supply of the equipment.

7.4 Security from Malware

There are no known cases of malware disrupting telecom services, yet. However, malware can cause information leaks and can result in the leak of private user information. However, some viruses, worms and Trojans can infect devices and spread malware via text messages or Bluetooth connectivity. This network-based service will also block Denial of Service attacks and restrict network traffic based on source, destination, IP ports and applications. It will also allow enterprise IT managers to lock and/or delete data on lost or stolen devices. The

connectivity could affect platforms if adequate firewalls, IDPs are not strong. Therefore Vendors would provide adequate firewall and IDPs with the supply of equipment.

7.5 Cryptography Related Security Issues:

Vendors will take suitable measures to deal with cryptography related vulnerabilities and submit a report of the measures along with a relevant certificate(s)that they have taken adequate measures to deal with these vulnerabilities.

i) Attacks on COMP-128 algorithm
ii) Compromised cipher key
iii) Key recovery allowing SIM cloning
iv) Hijacking outgoing calls in networks with encryption disabled
v) Hijacking outgoing calls in networks with encryption enabled
vi) Hijacking incoming calls in networks with encryption disabled
vii) Hijacking incoming calls in networks with encryption enabled
viii) Suppressing encryption between the target user and the intruder
ix) Suppressing encryption between target user and the true network

7.6 Data Flow Attacks

Many sophisticated attacks disguise themselves in data flows across sessions and ports—the more traffic there is, the harder it is to identify the threats. Vendors may ensure that they are aware of this and submit compliance on the same.

7.7 Additional Interfaces

Many of the problems in the data intensive infrastructure may come to increased number of interfaces additionally for data than those were present for voice only PSTN network, hence, the Vendors must give special attention to interfaces and their related vulnerability. Such Vendors may ensure that they provide additional notes that they have taken care of the same and the test mechanism and methodology adopted by them with adequate evidence. Some of these interfaces are listed below:

Gi: Exposed to Internet and corporate networks

Gp: Primary interconnection pt. between operator's n/w and un-trusted external networks

Gc: Allows access (via HLR) to key user info. from remote network during roaming Vulnerable Interfaces

Gi: Exposed to all threats from Internet: viruses, DoS, and malicious network traffic

Gp: Connection hijacking, overbilling from a roaming network during handover

Gn: Not encrypted by default

7.8 Security against Remote Access

The Vendor shall submit a written undertaking to the TSP clearly identifying all possible means of remote control/ remote access/remote command and control in the supplied equipment as well as suitable mitigation means to close such access mechanisms.

7.9 Software and Hardware Design Surety :Vendor may choose one of the following Options for Software and Hardware Design Surety

7.9.1 Option 1:

a) The Vendor shall at TSP's request enter into an escrow deposit arrangement in respect of all Information and documentation in relation to Supplies in respect of Hardware, executable Software/source code/gold build etc, High Level Designs (HLD), Detail Design Documents (DDD), listings and programmer's notes) ("the **Escrow Information**") as would enable TSP to complete any outstanding obligations of the Vendor under this Agreement, including, without limitation, obligations that would have existed (including the requirement to fulfill any orders that TSP would have otherwise placed under this Agreement) had this Agreement not been terminated by TSP before the expiry of its Term.
b) Without affecting any other rights it may have, TSP shall have the right, free of charge, to use the Escrow Information, after its release, in order to use or maintain (including to upgrade) the software, to modify or have modified the software, and to authorize such modified software to or have it maintained by third parties, in case Vendor refuses to do so as per the Agreement.
c) The Vendor shall ensure that the Escrow Information deposited in accordance with Clause 7.11 is and will be maintained as sufficient to allow a reasonably skilled programmer or analyst to maintain, modify and correct the hardware and software without the help of any other person or reference, and the Vendor further undertakes to keep the Escrow Information fully upto-date throughout the Term.
d) On the occurrence of any event permitting the release of the Escrow Information, the Vendor shall immediately provide, at its cost and expense, to TSP for a reasonable period, such advice, support assistance, data, information, access to Vendor's personnel or any key personnel of legal owner of the [Hardware and/or] Software for the purpose of understanding, maintaining (including upgrading), modifying and correcting any of the Hardware and/or Software. The softwares and codes written only in English language shall be acceptable. The code/softwares shall be proven to be operational and correct version and to be certified that it does not have self-destructing programmes. This may be ensured by using the same at least once for loading the system initially before being deposited.

7.9.2Alternative to option 1 is Option 2 as below::

i) Gold software copy or the Executable copy of the software at the discretion of vendor.
ii) Dumb hardware can be loaded with software by the TSP or under the supervision of TSP from Gold software copy or from the executable copy after checking that hardware is free from any software and ensuring that there are no harmful malware into the hardware. Alternatively, vendors will submit a certificate to MTNL that the supplied hardware is free from harmful malware based on the above test.

iii) Upgradation of software for a period of as agreed in the Contract .
iv) Design of network (network diagram of Vendor Implemented equipment under the Contract) in digital form and/ or in hard copy

7.10 Penalty

In the event that the Vendor is unable to comply with its obligations under this Agreement, as a result of which the Licensor imposes any sanction on the TSP, which results in any financial and other liabilities on the TSP, the Vendor shall be liable to make good such loss. In addition to the above, in case of any inadequate measures, act of intentional omissions, deliberate vulnerability left into the equipment or in case of deliberate attempt for a security breach by the Vendor, the Licensor may at its discretion blacklist the Vendor from entering into any supply deals with any Indian telecom operators. The TSP shall give the vendor the opportunity to defend any claim prior to imposing any penalty or blacklisting the vendor on account of security breach being attributable to it.

7.11 Inspection

The Vendor must allow the TSP , Licensor/DoT and/or its designated agencies to inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check at the time of procurement of equipment and upto two more times every year until the supplies under the Contract have been completed, at the sole discretion of the TSP. . All the documents should be in English and handed over to the visiting team of the TSP at least 4 weeks ahead of the visit.

7.12 Language of Supplies

All the software codes, firmware, operating system, hardware details should be in **English** only.

8. Data Protection

8.1 The Parties acknowledge that, in respect of all personal data and processed by the Vendor for the purpose of the provision of supplies under the Contract, TSP alone as data controller shall determine the purposes for which and the manner in which such personal data will be processed by the Vendor.

8.2 Other than at TSP's request, or where required by law to provide the supplies, the Vendor shall not disclose or allow access to any Personal Data other than, subject to Clause 8.4(f) to a person placed by the Vendor under the same obligations as contained in this clause who is employed or engaged by the Vendor or within the control of the Vendor in the performance of the Agreement.

8.3 The Vendor shall not use personal data for any purpose other than the provision of the supplies and shall return any personal data to TSP immediately upon request at any time

providing such return does not prevent the Vendor from fulfilling its obligations under this Agreement. The Vendor shall retain personal data no longer than is necessary for the provision of the supplies, in accordance with the relevant Applicable Law and such instructions as TSP may provide from time to time. Upon expiry or termination of this Agreement for whatever reason, the Vendor shall immediately return to TSP all personal data and certify that no copies have been made or retained by the Vendor or any third party acting on its behalf.

8.4 The Vendor shall:

(a) process personal data only on the instructions of TSP and to the extent necessary for the performance of this Agreement;

(b) not modify, amend or alter the contents of the personal data except as required or permitted by this Agreement or with TSP's prior written consent;

(c) implement the appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, which measures are set out in more detail in Clause 4 and provide to TSP with a written description of the measures taken when requested by TSP;

(d) comply with all relevant provisions of any TSP codes of practice notified to the Vendor from time to time and the Applicable Law ;

(e) keep all personal data secure and confidential, act only on TSP's instructions with respect to it, and comply with such further reasonable requirements from time to time of TSP for the security of it;

(f) ensure that, of the Vendor's staff, only those of the Contract Personnel who need to have access to the personal data are granted access to the personal data only for the purposes of the performance of this Agreement and the Contract Personnel are informed of the confidential nature of the personal data and comply with the obligations set out in this Clause 8;

(g) notify TSP forthwith, and in any event, no later than 12 hours from the time it comes to the Vendor's attention, that personal data transferred by TSP to the Vendor has been the subject of accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any other unlawful forms of processing; and

(h) notify TSP in the event that it receives a request or notice from any person subject to having access to that person's personal data held by it and will provide TSP with full co-operation and assistance in relation to any complaint or request including providing TSP with any relevant personal data it holds within the timescales provided by the request or notice or as otherwise required by TSP.

8.5 In respect of transfer of personal data the following conditions shall apply:

(a) obtain TSP's prior written consent before transferring personal data to any Subcontractors in connection with the provision of the supplies;

(b) prior to any transfer of personal data, enter into or procure that any Subcontractor delivering the supplies will enter into contracts for the transfer of personal data. In respect of personal data transferred by TSP to the Vendor or acquired by the Vendor from TSP's systems to a country outside of India shall be on the basis of Applicable Laws , or such other data protection model contract terms as may be agreed between the Parties from time to time, except where the relevant Applicable Laws provides for a derogation from this requirement.

8.6 Any breach of this Clause 8 by the Vendor shall be deemed to be a material breach of the Agreement and the Vendor shall indemnify TSP from the against any costs, losses, damages, proceedings, claims, expenses or demands incurred or suffered by TSP which arise as a result of such breach.

8.7 The Vendor shall, upon TSP giving reasonable notice, allow TSP or its nominated representatives such access to its premises, Information and records and those of its agents subsidiaries and sub contractors, as may be reasonably required by TSP from time to time to assess the Vendor's and/or Contract Personnel's compliance with this Clause 8.

9. Regulatory Matters

9.1 The Vendor shall

(a) comply with all regulatory matters under Applicable Laws including, without limitation, any actions that TSP may require in connection with any regulatory matter, that are notified to the Vendor Regulatory Contact from time to time by the TSP Regulatory Contact in so far as they relate to the performance by the Vendor under the Agreement.

(b) within 14 days of the Commencement Date, ensure that the Vendor Regulatory Contact contacts the TSP Regulatory Contact to establish the nature and extent of communication between them, to assist them in meeting all regulatory requirement relevant to the Contract, as set by the Licensor or any Governmental Authority or any other person nominated by Licensor

(c) ensure that the Vendor and its Contract Personnel have undergone the proper and adequate training for the purpose of performing its obligations under this Agreement and promptly provide such information to TSP as shall be necessary for TSP to respond fully and to the timescale required to any request or requirement for

information from any Governmental Authority , to the extent that such information relates to the performance of the obligations by the Vendor under the Agreement.

10. Confidentiality

10.1 In this Clause, "**TSPInformation**" which TSP from time to time identifies to the Vendor as being commercially confidential, or is by its nature commercially confidential or defined by TSP as confidential, or confidential as per the Applicable Law. The term "**Information**" shall mean and include all or any communication(s), Information(s) or data disclosed, whether written, visual or oral and other material supplied to or obtained by the Party ("**Recipient**") from the other Party ("**Disclosing Party**") during the course of the Agreement.

10.2 Except with TSP's consent, the Vendor shall not disclose TSP Information to any TSP employee, not authorized to receive such information

10.3 Subject to the Clause 11, either Party receiving Information from the other shall not without the other's prior written consent use such Information except for Contract purposes or disclose such Information to any person other than TSP's employees, agents and contractors or Contract Personnel who have a need to know and who are bound by equivalent obligations of confidentiality. Any breach of such obligations by Contract Personnel or TSP's employees, agents or contractors (as the case may be) shall be deemed to be a breach by the Vendor or TSP respectively.

10.4 Clause 10.2 and Clause 10.3 shall not apply to Information that is:

(a) Published except by a breach of the Contract; or

(b) Lawfully known to the Recipient at the time of disclosure and is not subject to any obligations of confidentiality; or

(c) Lawfully disclosed to the Recipient by a Vendor without any obligations of confidentiality; or

(d) Replicated by development independently carried out by or for the Recipient by an employee or other person without access to or knowledge of the Information.

10.5 The Vendor shall not publicize this Agreement without TSP's prior written consent and shall ensure that any subcontractor is bound by similar confidentiality terms to those in this clause.

10.6 Either Party that has during the course of this Agreement received Information in a recorded form from the other (or has recorded received Information) shall return or destroy in a complete irrecoverable mode (at the option of the disclosing party) such records upon:

(a) expiry or termination of this Agreement; or

(b) upon earlier request unless such records are part of the supplies.

10.7 This clause shall survive termination / expiry of this Agreement.

10.8 The obligations of confidentiality shall also be governed by the Non-Disclosure Agreement dated [●] ("**NDA**"), entered into between the TSP and the Vendor. In the event of any conflict between this Clause 10 and the NDA, the provisions of the NDA shall be applicable.

11. Intellectual Property

11.1 Each Party will retain its right, title and interest in its respective trademarks, service marks and trade names as well as rights in respect of any patent, copyright, trade secrets or other intellectual property used during the performance of this Agreement. Both Parties recognise that except as otherwise expressly provided herein or agreed between the Parties, they shall have no right, title, interest or claim over the others' intellectual property.

11.2 The Vendor agrees that it shall defend, at its own expense, all proceedings, suits and claims against and/or affecting the TSP or any of their officers, directors or employees ("Indemnitees") with respect to infringement, breach or violation of any patent, trademark, copyright, trade secret, mark or other intellectual property rights of any third party in the course of performance of its obligations under this Agreement. The Vendor agrees that it shall indemnify the Indemnitees for all sums, costs, expenses and liabilities including, without limitation, all reasonable attorneys' fees and other costs, incurred by Indemnitees in connection with or otherwise arising out of any such proceeding, suit or claim.

If in any such suit so defended, all or any part of the equipment or any component thereof or the use thereof is held to constitute an infringement or violation of third party intellectual property rights and its use is enjoined, or if in respect of any claim of infringement or violation the Vendor deems it advisable to do so, the Vendor shall at its sole cost and expense take one or more of the following actions: (a) procure the right to continue the use of the same without interruption for the TSP; or (b) replace the same with non-infringing Equipment that meets the technical specifications stipulated under the Contract; or (c) modify the said equipment or any component thereof so as to be non-infringing; provided, that (i) the equipment or any component thereof as modified complies with all of the technical specifications as stipulated under the Contract; and (ii) Vendor shall fully indemnify the TSP for any costs associated with any such action.

12. Security Review-The Vendor shall:

(a) give to (or procure the giving to) TSP (or any person authorised by TSP) such

access at all reasonable times to the Vendor's and any Subcontractor's records and

premises related to this Agreement as TSP may require from time to time to assess

the Vendor's compliance of these policies in this Agreement;

(b) such assessments may include assessments of all elements of physical and logical audits, penetration testing of the Vendor's Systems. The Vendor shall facilitate this assessment by permitting TSP to collect, retain and analyse information to identify potential security risks including trace files, statistics, network addresses and the actual information or screens accessed or transferred; and

(c) provide such reports to TSP and attend such meetings as may be reasonably required by TSP.

13. Network Audit, Test and Certification:

The process of networks audit and certification should be performed by the test and certification agencies to include following activities:

(a) **Network forensics** to identify existing unwanted running processes\ malwares\ backdoors etc. on all networks' elements. The operation includes sniffing of live traffic to identify unwanted redirection and interception of traffic.

(b) **Network Hardening** to map all networks elements and to calibrate them to optimized secured state.

(c) **Network penetration test** to assure system durability against any kind of attack.

(d) **Risk assessment** to understand what actions should be taken to minimize future damage to carrier and what risks are inevitable.

(e) **Actions** to fix found problems by setting systems to default or acquiring relevant IT security technologies to prevent such problems from reoccurring.

An available list of Test and Certification Agencies (Third Parties) in various countries who may take up the regular Technical Audit of Networks and Security Certification is given at Appendix I. The TSP may engage the services of any other Network Audit andSecurity Certification agency also

14 Investigation:

14.1 If TSP believes that there has been a breach by the Vendor of the provisions of this Agreement, TSP will inform the Vendor Security Contact. The Vendor shall cooperate with TSP fully in any ensuing investigation. The Vendor shall provide list of users who have had

access to TSP Systems and TSP Information to TSP and/or any law enforcement agency. TSP shall have access to the Vendor Systems and TSP Information in the Vendor's premises generally with prior notice but include the right to make unannounced visits.

14.2 The Vendor shall report to TSP Security Contact promptly of any potential misuse of TSP Information or improper or unauthorised access to TSP Systems and TSP Information.Upon request, the Vendor shall promptly provide to TSP a written report with details of the potential misuse of TSP Information or improper or unauthorised access to TSP Systems and TSP Information, a remedial plan and a timetable for achievement of the planned improvements and steps to be taken to avoid the repeat of the potential misuse of TSP Information or improper or unauthorised access to TSP Systems and TSP Information.

14.3 If any audit or investigation reveals that there is a potential risk to the confidentiality, integrity or availability of TSP Information in the Vendor's processes or Vendor Systems, Vendor shall promptly correct any security risk in the Vendor's processes or Vendor Systems promptly.

14.4 During investigation, the Vendor shall co-operate with TSP, providing reasonable access, accommodation, facilities and assistance to all Vendor Systems as reasonably necessary to investigate the breach of the provisions of this Agreement including permitting interview of any sales, engineering or other operational personnel of Vendor. TSP shall, or at TSP's request shall instruct the Vendor to, confiscate for evaluation any tangible or intangible asset suspected to have been used for information/ security breach or provide lead to investigation belonging to the Vendor or its subcontractor to aid the investigation.

15. Limitation of Liability

The aggregate liability of the Vendor to the TSP in respect of any breach of obligations under this Agreement shall not exceed the sum of Rs. 50,00,00,000 (Rupees Fifty Crores only) per breach, provided that such limitation shall not apply to claims arising pursuant to Clauses 10 and Clause 11.2 or pursuant to any other Clause where such limitation is expressly excluded.

16. Term and Termination

16.1 This Agreement shall be effective from the Commencement Date .Notwithstanding anything contained herein or in the Contract, this Agreement shall survive till any equipment is working, which is supplied and served by the Vendor under this Contract or for a period of ten years after signing of this Agreement whichever is later ("**EndDate**").

16.2 This Agreement may also be terminated in the event it is so determined by the Licensor or under Applicable Laws.

16.3 The termination of this Agreement shall be without prejudice to the rights and obligations of the parties which have accrued up to the date of termination.

17. Indemnity

17.1 The Vendor shall indemnify and hold harmless the TSP and its employees, agents, shareholders, directors, representatives, against any claims or penalty or consequence arising out of breach of the security related terms of the license granted by the Licensor as a result of breach or non-compliance by the Vendor with its obligations in this Agreement.

17.2 It is clarified that any expenditure incurred by the TSP for complying with security related provisions as prescribed under Applicable Law shall be borne by the Vendor. In the event there is a breach of the security related provisions as prescribed under Applicable Laws, any penalty imposed by the DoT on the TSP shall be paid by the Vendor to the TSP. Further, any testing of Vendor's equipment including requirement of testing equipment shall be met by Vendor at his own cost.

18. Governing Law

This Agreement shall be governed by laws of India and the Parties agree to the exclusive jurisdiction of the Indian courts where the registered office of the TSP is situated.

19. Arbitration

19.1 In the event of any question, dispute or difference arising under this Agreement or in connection there-with, the same shall be referred to the sole arbitration of the ED,MTNL or in case his designation is changed or his office is abolished, then in such cases to the sole arbitration of the officer for the time being entrusted (whether in addition to his own duties or otherwise) with the functions of the ED, MTNL or by whatever designation such an officer may be called (hereinafter referred to as the said officer), and if the ED, MTNL or the said officer is unable or unwilling to act as such, then to the sole arbitration of some other person appointed by the ED, MTNL or the said officer. The agreement to appoint an arbitrator will be in accordance with the Arbitration and Conciliation Act 1996. There will be no objection to any such appointment on the ground that the arbitrator is a government servant or that he has to deal with the matter to which the agreement relates or that in the course of his duties as a government servant he has expressed his views on all or any of the matters in dispute. The award of the arbitrator shall be final and binding on both the parties to the agreement. In the event of such an arbitrator to whom the matter is originally referred, being transferred or vacating his office or being unable to act for any reason whatsoever, the ED, MTNL or the said officer shall appoint another person to act as an arbitrator in accordance with terms of the agreement and the person so appointed shall be entitled to proceed from the stage at which it was left out by his predecessors.

19.2 The arbitrator may from time to time with the consent of both the Parties enlarge the time frame for making and publishing the award. Subject to the aforesaid, Arbitration and Conciliation Act, 1996 and the rules made there under, any modification thereof for the time being in force shall be deemed to apply to the arbitration proceeding under this clause.

19.3 The venue of the arbitration proceeding shall be the office of the ED MTNL, Delhi or such other places as the arbitrator may decide.

20 Notices

20.1 Any notice, documents, information, direction and any other communications required or permitted to be (or such other addresses as specified in writing by the respective Party from time to time) hereunder shall be sent in writing and sent by registered post, courier and or by facsimile transmission or delivered personally by hand or sent by email addressed to the other Party to the relevant addresses set out below at the following addresses:

If to the TSP:

1. G.M.(EB), Room No.423,
2. 4th Floor, Khursheed Lal Bhawan,
3. Janpath, New Delhi- 110001

Attention: [●]

Fax: [●]

Email: [●]

If to the Vendor:

[Name]

[Address}

Attention: [●]

Fax: [●]

Email: [●]

20.2 Any such notices and other documents shall:

(a) if delivered by hand, be deemed to have been given and received at the place of receipt on the date of delivery;

(b) if mailed by post or couriered, be deemed to have been given and received at the place of delivery on the date of delivery.

(c) if given by facsimile transmission be deemed to have been given and received, at the place of receipt on the date as shown in the facsimile transmission report; and

(d) if given by e-mail be deemed to have been given and received at the place mentioned in Clause 19 above on the same day.

20.3 Either Party shall inform the other of any change in its address above through a notice in writing to the other Party in the manner set forth above.

IN WITNESS WHEREOF THE PARTIES HAVE CAUSED THESE PRESENTS TO BE EXECUTED ON THE DAY, MONTH AND YEAR HEREINBELOW WRITTEN TO BE EFFECTIVE FROM THE DATE FIRST MENTIONED ABOVE

SIGNED for and on behalf of	SIGNED for and on behalf of [●]
Mahanagar Telephone Nigam Limited	
……..	……..
Signature	Signature
……	……..
Name	Name
……	……..
Position	Position
…….....	…….....
Witness Signature	Witness Signature
…….	…….

…… ……

…… ……

Name & Address Name & Address

Format-A

Technical Bid Proposal

Application to be submitted by bidders

(A) PART- A: BIDDER DETAILS

S. No.	**PART A**	GENERAL INFORMATION
1.	Name the company / Agency/Consortium	
2.	Registered Office Address	
3	Year Incorporated	
4	Address for communication	
5	Contact Person	
6	Name	
7	Designation	
8	Phone No.	
9	Mobile No.	
10	Email address	
11	Company Website	
12	Number of years of experience in implementation of the similar projects in India.	

PART- B: APPLICATION DETAILS

Sl. No	**Required Information**	**Documents to be attached in Annexure wise**
1	Name and address of the Person Signing the document.	Power of Attorney attested by Notary or Copy of the board Resolution

		certified by the Company secretary for appointing the Power of Attorney or **Attach as Annexure 1.**
2	The Bidder should have empanelled as Business Development Associates in MTL	Copy of empanelment letter issued by MTL **Attach as Annexure 2**
3	The Bidder should have a valid GST registration certificate.	Copy of relevant GST registration certificates. **Attach as Annexure 3**
4	Experience in executing at least one Wi-Fi project of more than 100 APs capacity on mesh technology.	PO copies or Satisfactory Completion Certificate from the end Customer **Attach as Annexure 4**
5	Acceptance of all terms and conditions in the Tender	A copy of the tender document signed, in the bottom of all pages as a token of acceptance of all terms and conditions. **Attach as Annexure 5**
6.	Technical Compliance Report as per Format A	**Attach as Annexure 6**
7.	Detailed Project Report (DPR) including Diagram and write –up on the quoted product/Brand. Technical Brochures of the product quoted and also current certifications, if any, should also be enclosed. Bidder will also submit the complete Technical proposal along with the network structure diagram, details of all the Wi-Fi network equipment's including make, model, hardware, software, integration, licenses details etc.	**Attach as Annexure 7**
8.	Bidder shall submit MAF Letters from OEM (Original Equipment Manufacturer) stating that they will support the product/solution through the bidder for the next five years or as per the requirement of customer **As per format B**	**Attach as Annexure 8**
9.	Bidder shall submit an undertaking stating that the equipments / APs quoted in their bid are not from any manufacturer who has been black listed/ debarred by any Govt.	**Attach as Annexure 9**

	Department/PSU/autonomous body in India.	
10.	Bidder shall submit list of tests, which are proposed to be conducted during the acceptance testing to test the conformance of the equipment to the Technical Specifications as per Section- III.	**Attach as Annexure 10**
11.	Bidders shall submit necessary document showing compliance with PMA Policy notified by Government of India and its subsequent amendments, guidelines etc. for preference to domestically manufactured telecom products.	**Attach as Annexure 11**

Format-B

Technical Compliance Report

Active Components

Sl. No.	ITEM	Quantity	Make and Model of the product offered by Bidder	*Technical Specifications'* under Section – III	Complied (Yes/NO)	Remarks (In case of deviation, technical specifications of the item in non-compliance statement)	Documentary Evidence Product Brochure issued by OEM for same Make & Model attached
1	Wi-Fi Indoor Access Points (AP)	12					
2	Wi-Fi Outdoor Access Points (AP)	78					
3	Wireless Controller (WLC)						
	Hardware	2 (1+1)					
	Software	1 package					
	Licenses	100 expandable upto 250					
4	Network Manageme						

	nt System (NMS)						
	Hardware	1					
	Software	1					
	Licenses (wired & wireless devices)	250					
5	Centralized Authentication System						
	Hardware	2 (1+1)					
	Software	1 package					
	Licenses	20,000					
6	Managed Gigabit LAN Switch 8 ports 802.3at	18					
7	Managed Gigabit LAN Switch 24 ports 802.3at	5					
8	IP55 compliant 9U Outdoor Racks	22					
9	Online UPS 1	22					

	KVA with Lithium Ion Batteries and 30 minutes						
10	Armoured Cat6e Cable	2400m					
11	Laptop with 3 X 3WiFi	3					
12	PC	3					

Passive Components

S. No	Items	Details	Minimum	Make and Model of the product offered by Bidder	*Technical Specifications'* under Section – III	Complied (Yes/NO)	Remarks (In case of deviation, technical specifications of the item in non-compliance statement)	Documentary Evidence Product Brochure issued by OEM for same Make & Model attached
1	PVC Conduit per mtr for 25mm	Inclusive of required accessories	1000m					
2	PVC Battens per mtr for 25x12 mm	Inclusive of required accessories	300m					

3	Corrugated flexible PVC pipes per meter 25 mm	Inclusive of required accessories	300m					
4.	New poles similar to NWM CCTV poles for	Inclusive of Installation and accessories	41					

Passive services

S. No	Item	Details	Quantity	Agree to comply as per 'Technical Specifications' under Section – III (Yes/No)
1	Laying of PVC conduit per mtr	Rate to be quoted per mtr	1000m	
2	Laying of PVC Battens per mtr	Rate to be quoted per mtr	300m	
3	Laying of Corrugated flexible PVC pipes per mtr	Rate to be quoted per mtr	300m	
4.	Restoration of site	All the infrastructure at site will be restored to original good condition	1	

5.	Fixing of Rack on the ground / wherever required	(A strong enough foundation to hold the rack is to be made and rack fixed on iron stand one ft. above ground and construction should match the CCTV switch plate form	20	

Notes in respect of Bill of Material

1. Schedule of Requirement (SOR) is based on MTNL's estimate, in case the bidder feels that additional equipment is required to implement the solution successfully, he may quote additional equipment in technical and in price-bid, which will be included for the purpose of evaluation.

2. The bidder has to quote prices for quantity of items as per SOR. If a bidder quotes prices for lesser quantity of items, then during evaluation the price bid will be increased prorate as per the SOR quantities and accordingly prorated value will be considered for comparison for arriving at L1 bidder.
3. A package consists of the relevant software modules, number (unless separately specified) and types of licenses, management software (if any) to be quoted by the vendor in order to meet the requirement of the tender.

4. The WLC Software licenses shall be AP based and there will be no restriction on number of subscriber sessions.

5. The quantity of the passive components defined above is tentative and taken for the purpose of evaluation only. Payment of passive components will be made on actual basis. Specifications of the required accessories are defined in Section III under technical specification. Laying charge of Cat 6 Cable/Conduit/Battens and corrugated flexible PVC pipe will be quoted separately from restoration charges. The cost of the required accessories and material required for installation has to be inbuilt along with PVC pipes/ conduit/ batten/ corrugated flexible PVC pipes.

6. Provision should be made for installing ONT, LAN switch, Battery and UPS in 9U wall mounted network rack.

7. Any other item not covered above but essential for successful completion of project should also be added in the price schedule (under Any other HW/ SW/ Misc item of 'SOR') and its details should be given in the separate Annexure.

8. All necessary wiring, cables, connectors, etc. as defined in tender shall be supplied.

9. All necessary electrical wiring both AC and DC (from Power Plant to equipment room) along with AC & DC Distribution Boxes circuit breakers, runways etc. at all the nodes shall be supplied by the bidder along with the above equipment.

10. The cabling shall be Gigabit ready for CAT 6e category for Ethernet Switch. The detailed information of complete wiring implementation shall be provided along with all related accessories.

11. The equipment offered shall meet the technical requirements/ specifications of tender document.

12. The Indoor Access Points shall either be wall /ceiling mountable. The Outdoor AP's should be enabled for fast and easy mounting to street lights, traffic controls and other street furniture. It should include hardened enclosure for outdoor deployment. For Installation of out-door APs, Mounting poles/equipment will be provided by the vendor , if required.

13. There should be Ubiquitous RF coverage of -65 dBm or better along with 10 Mbps downlink throughput. Quality of browsing experience (website surfing , Email, You-tube , video streaming , audio streaming through APP or thorough browser etc) at proper speed will be ensured by the bidder in the entire coverage area of National War Memorial. QoE may be tested with smartphone like I-phone or laptop like Macbook Pro etc.

14. Ethernet cables and Ethernet connectors shall be provided by bidder. Any other material such as PVC pipes with accessories, corrugated PVC pipe, PVC baton, Clamps, Rawl Plugs, screws/nails/hooks/clips for fixing, fish-wire to pull the cable, crimping tools, drill machines, portable generator sets, field assembly connector tool kit etc required for successful installation/laying of cables, tools, labor and transportation of store /material (including loading & un loading) to the work site shall be provided by the successful bidder.

15. Any damage to the existing infrastructure at site will be restored by the bidder to its original good condition. Restoration charges in this regard will be quoted separately by the bidder.

Format C

MANUFACTURER'S AUTHORISATION FORM
(To be submitted by authorized dealers/representatives/importers)

No. Dated:

To

COO (MTL),
Millennium Telecom Limited

Sub: Product Compliance with the tender specifications for "Supply, Installation, Testing and Commission of Equipments for providing Wi-Fi services with one year warranty and its subsequent maintenance for four years of National War Memorial, India Gate circle, New Delhi under Ministry of Defence (MoD), Government of India".

Dear Sir,

Tender No Equipment Name

1. We …… (name of the OEM) are the original manufacturers of the above equipment having registered office at …….. (full address with telephone number/fax number & email ID and website), having factories at _____ and _____ , do hereby authorize M/s._____ (Name and address of tenderer) to submit tenders, and subsequently negotiate and sign the contract with you against the above tender no..

2. No company or firm or individual other than M/s._____ are authorized to bid, negotiate and conclude the contract in regard to this business against this specific tender.

3. We also hereby undertake to provide full guarantee/warrantee /AMC as agreed by the tenderer in the event the tenderer is changed as the dealers or the tenderer fails to provide satisfactory after sales and service during such period of Comprehensive warranty/CMC/AMC and to supply all the spares/reagents during the said period.

4. We also hereby declare that we have the capacity to manufacture and supply, install and commission the quantity of the equipments tendered within the stipulated time.

(Name)
for and on behalf of
M/s._____
(Name of manufacturers)

Date:
Place:

Note: This letter of authority should be on the letterhead of the manufacturing concern and should be signed by a person competent and having the power of attorney to bind the manufacturer.

Format C1

MANUFACTURER'S LETTER HEAD
(To be submitted by concerned OEM)

No. Dated:

To

COO (MTL),
Millennium Telecom Limited

Sub: Self-Certificate regarding technical solutions works on mesh technology and deployed in India.

Dear Sir,

Tender No Equipment Name

1. We …… (name of the OEM) are the original manufacturers of the above equipment having registered office at …….. (full address with telephone number/fax number & email ID and website), having factories at _____ and _____ , do hereby certify that our technical solutions submitted by our authorize M/s._____ (Name and address of tenderer), works on mesh technology and have been deployed in India.

2.We also hereby submit the copy of Work Order / Purchase Order / Acceptance Letter regarding deployment of mesh technology in India.

(Name)
for and on behalf of
M/s._____
(Name of manufacturers)

Date:
Place:

FORMAT - D

Financial Bid

PRICE BID SCHEDULE

A. Supply

S.No	Item Particulars	Qty (a)	Make and Model	Unit Price in Rs. (b)	%age of GST (C)	GST Amount (Rs.) (d)=(b) *(c)/100	Total Unit Price inclusive of GST (Rs.) (e)=(b)+ (d)	Total Price including GST (Rs.) (F)= (a).(e)
1	Wi-Fi Indoor Access Points (AP)	12						
2	Wi-Fi Outdoor Access Points (AP)	78						
3	**Wireless Controller (WLC)**							
	Hardware	2 (1+1)						
	Software	1 package						
	Licenses	100 and expandable up to 250						
4	**Network Management System (NMS)**							
	Hardware	1						
	Software	1 package						
	Licenses	250						

5	**Centralized Authentication System**							
	Hardware	2 (1+1)						
	Software	1 packag e						
	Licenses	20,000						
6.	Managed Gigabit LAN Switch 8 ports 802.3at	18						
7.	Managed Gigabit LAN Switch 24 ports 802.3at	5						
8.	IP55 compliant 9U Outdoor Racks	22						
9.	Online UPS 1 KVA with Lithium Ion Batteries and 30 minutes	22						
10.	Armoured Cat 6e Cable	2400 m						
11.	Laptop with 3 X 3WiFi	3						
12.	PC	3						
List of Passive Components								
13	PVC Conduit per mtr for 25mm (inclusive of required Accessories)	1000m						
14	PVC Battens per mtr for 25x12 mm (inclusive of required Accessories)	300m						
15	Corrugated flexible	300m						

	PVC pipes per meter 25 mm (inclusive of required Accessories)							
16	New poles similar to NWM CCTV poles for mounting APs (inclusive of Installation and Accessories)	41						
Grand Total (A)								

B. Laying and Restoration Charges

S.No.	**Item Particulars**	**Qty** **(a)**	**Unit Price in Rs.** **(b)**	**%age of GST** **(C)**	**GST Amount (Rs.)** **(d)=(b) *(c)/100**	**Total Unit Price inclusive of GST (Rs.) (e)=(b)+ (d)**	**Total Price including GST (Rs.) (F)= (a).(e)**
1.	Laying of PVC conduit per mtr	1000 m					
2.	Laying of PVC Battens per mtr	300 m					
3.	Laying of Corrugated flexible PVC pipes per mtr	300 m					
4.	Fixing of Rack on the ground / wherever required (A strong enough foundation to hold the rack is to be made and rack fixed on iron stand one ft. above ground and construction should match the CCTV switch plate form foundation of NWM with	20					

	granite stone flooring)						
5.	Restoration charges of all the civil/collateral damages done during the execution of work in five years periods to its original specification in accordance to customer requirements i.e. Ministry of Defence (MoD).	1					
Grand Total (B)							

C. Installation & Commissioning including warranty of one year

S. No.	**Particulars (Installation & Commissioning charges)**	**Amount (Rs.)**	**% age of GST**	**GST Amount (Rs)**	**Total Amount inclusive of GST (Rs)**
Grand Total (C)					

D. Annual Maintenance Charges (AMC) after 1 Year Warranty

S. No.	**Details**	**Amount (Rs.)**	**%age of GST**	**GST amount (In Rs)**	**Total Amount inclusive of GST (Rs)**
1.	Annual Maintenance Charges for whole setup (for the 2nd Year)				
2.	Annual Maintenance Charges for whole setup (for the 3rd Year)				
3.	Annual Maintenance Charges for whole setup (for the 4th Year)				
4.	Annual Maintenance Charges for whole setup (for the 5th Year)				
Grand Total (D) = (1+2+3+4)					

E. Facility Management Services (FMS

S.No	Facility Management Services (FMS) charges – During the warranty and AMC period the bidder will provide one service engineer on 7 days a week for attending to maintenance and operation of Wi-Fi service including	**%age of GST**	**GST amount (In Rs)**	**Total Amount inclusive of GST (Rs)**

	complaints.			
1.	For First Year……Rs			
2.	For Second Year……Rs			
3.	For Third Year……Rs			
4.	For Fourth Year……Rs			
5.	For Fifth Year……Rs			
Total Five Year Grand Total (E)				

F. Any Other Items

S.No	It shall be the Bidder's responsibility to ensure that any additional equipment required for satisfactory performance of the services as per customer requirement mentioned in this tender document, is also quoted in the Bid Document under "Any other items", not included in the Schedule of Requirements, but required for successful implementation and commissioning of the network as well as its management in next five years includes the following: 1. Equipment / Software/ Licence any other items not included in the SoR (Schedule of Requirments). 2. Charges of digging for laying of OFC/Cables if required and installation of poles etc. 3. Any other charges.	**%age of GST**	**GST amount (In Rs)**	**Total Amount inclusive of GST (Rs)**
1.	……Rs			
Grand Total (F)				

G. Grand Total

Particulars	**Amount (Rs.)**
Grand Total (A)	
Grand Total (B)	
Grand Total (c)	
Grand Total (D)	
Grand Total (E)	
Grand Total (F)	
Grand Total (G) = (A + B+C+D+E+F)	

Note:-

1. We have read and understood the Terms & Conditions and the Scope of Work with all technical requirements mentioned in the tender while quoting the rates.
2. L1 bidder will be decided based on lowest Prices of Grand Total (G) = (A + B+C+D+E+F).

3. All accessories to be included in above quoted rates. Rates for all the items must be quoted else the price bid will be rejected.
4. Warranty for the equipments (whole set-up) should be at least 1 year from the day of commissioning and 4 years AMC.
5. The Specifications listed are minimum requirement and any item of higher specification will be accepted.
6. All equipments/components of the solution should be compatible with one another and there should not be any proprietary items. Items quoted by us meet all the technical specifications mentioned in this tender. All other items to be supplied shall also meet the technical specifications mentioned in tender.
7. Manufacturer Authorization Form (MAF) from the OEM specific to this work duly filled are attached herewith.
8. The rates quoted by us are competitive.
9. I/We verify the genuineness and correctness of the information furnished in this document. I/We am/are also aware that I/we shall be held responsible in case any information/document is found false/forged/fabricated/ tempered/manipulated at any stage and the MTL is fully competent to take any action against me/our firm as deemed fit in accordance with the terms and conditions of the empanelment and law of the land.

Name…….
Signature……
Seal of the Bidder