Information to Bidder for the "Supply of Access Point, WLAN Controller & Radius Server through GeM".

Ref: GeM Bid No. GEM/2020/B/936957,Date 23/12/2020.

1. The item/items in this bid should be quoted as per the technical specifications. *The details of the specifications along with consignee/site details are also available on website www.railtelindia.com*

2. In the specification wherever support for a feature has been asked for, it will mean that the feature should be available without RailTel requiring any other hardware/software/licenses. Thus, all hardware/software/licenses required for enabling the support/feature shall be included in the offer.

3. OEM or Authorized distributor/Partner of OEM should have a registered office in India to provide sales and 24x7 support in India. The certificate to this effect should be submitted. The bidder should be either OEM or his authorized dealer/distributor.

In case of the authorized distributor/partner certificate from the OEM to this effect should be submitted. If OEM is quoting then OEM should submit the certificate.

4. Equipment offered shall have complete data sheets and detailed description on OEM web sites.

5. Bidder shall submit the detailed BOM of the equipment offered duly verified and certified by the respective OEM.

6. GSTIN ID of vendor should be provided from where goods will be supplied.

7. Tender Cost & Earnest Money Deposit (EMD)/ Bid Security:

7.1 Tender Cost: Estimated cost of the Tender is **Rs. 28,58,781/-**

7.2 Earnest Money Deposit (EMD)/ Bid Security as per bid document uploaded on GEM: Rs. 57,176/- in the form of Pay Order / Demand Draft/ BG drawn in favor of RailTel Corporation of India Ltd. payable at New Delhi. The Bid received without EMD will be summarily rejected.

8. Eligibility Criteria for OEM:

a. The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on opening of bid, in India or Abroad. The certificates from the actual users will have to be submitted offline.

b. The OEM should have supplied at least 35% of the tendered quantity of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years)as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with quantities supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.

c. The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of Access Point and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Repair, Service Center Supports for at least past three years in the country from where the proposed equipment are planned to be supplied. In case OEM is located outside India, it should have training repair and service center facilities in India also. The certificates/Undertaking for the same will have to be submitted offline.

(The bidder will have to submit the proof of establishment for the facility).

9. Eligibility Criteria for Bidder:

a. The tenderer should have executed order of supply of **Access Point, WLAN Controller & Radius Server** during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid, as per following:

(A) Single order of atleast 35% of tendered value.
OR

(B) Two orders of atleast 20% each of tendered value.

OR

(C) Three orders of atleast 15% each of tendered value.

Satisfactory Performance certificate issued by customer/s for the Purchase Orders/ Work Orders should be enclosed.

b. Bidder should have authorization specific to this tender from respective OEM as per Annexure-II.

10. SLA:

After having been notified of the defects / service requirement during warrantee period, Seller has to complete the required Service / Rectification within time limit of max. 7 days. If the Seller fails to complete service / rectification with in defined time limit, a penalty of 0.5% of Unit Price of the product shall be charged as penalty for each week of delay from the seller & upto max. of 100% of Unit Price of the product.

Seller can deposit the penalty with the Buyer directly else the Buyer shall have a right to recover all such penalty amount from the Performance Security (PBG) or from the running bills.

11. Long Term Maintenance Support:

DELETED.

12. Payment Conditions: -

i. 100% payment against full supply OR Supply, Installation & Commissioning.

ii. 80% payment against part supply OR Supply , Installation & Commissioning of the completed part as the case may be. The following documents are to be submitted for payment:

a. Original Invoice
b. Delivery Challan
c. Original Consignee receipt with GRN No.
d. Original Inspection Certificate
e. Warranty Certificate of OEM
f. Copy of PBG
g. Certificate of receipt of Goods & installation thereof from RailTel.
h. Original Insurance certificate
i. Bill Passing Authority: Addl.General Manager/Project
Bill Paying Authority: Joint General Manager/Finance

13. Online Submissions:

The bidder is required to upload and submit the following documents online before due date & time of bid. The date & time for closing of the bid is **15:00 Hrs of 14.01.2020** and the bid will be opened at **15:30 Hrs of 14.01.2020.**

i. EMD
ii. BOQ of offered equipment
iii. Clause wise compliance along with all mentioned documents/annexures for all clauses of GeM Bid and ATC documents.
iv. Data Sheet of offered equipment.
v. Financial (Certified copies of audited balance sheets/annual reports of last three preceding financial years) and Technical Eligibility Criteria documents.
vi. Technical Compliance of all Specification of items as per GeM Bid and ATC documents.
vii. Certificate from the End user against the Eligibility criteria for OEM para 8.
viii. Proof of document required against Eligibility criteria of OEM and Bidder vide para 8 & 9 respectively.
ix. MAF/ OEM Authorization Letter (as per Annexure-II)

Note: 1) Non-submission of any document online within the prescribed time will make the bid to be summarily rejected.

2) The bidder has to submit the hardcopy of the EMD document submitted on line with in three working days from the date and time of opening of the bid to the RailTel Corporation of India Ltd, 6th floor, III'rd Block, Delhi Technology Park, Shastri Park, Delhi-110053

3) The bidder is required to give acceptance of all the clauses mentioned in the **"Information to the Bidders"** document is mandatory. Any deviation / non-acceptance may lead to rejection of the bid.

4) Information to Bidder viz. corrigendum /addendum/ amendments etc. for this bid shall be posted on www.railtelindia.com only.

5) This bid is governed by the Specific Additional Terms & Conditions and General Terms & Conditions laid down by the GeM against **GeM Bid No. GEM/20202/B/936957, dt.23/12/2020.**

14. Delivery period: **30 days** from the date of PO.

15. **Security Deposit/Performance Bank Guarantee**:

i. The successful bidder shall have to submit a Performance Guarantee (PG) within 30 (thirty) days from the date of issue of Letter of Acceptance (LOA) as per annexure III. Extension of time for submission of PG beyond 30 (thirty) days and upto 60 days from the date of issue of LOA may be given by the Authority who is competent to sign the contract agreement. However, a penal interest of 15% per annum shall be charged for the delay beyond 30 (thirty) days, i.e., from 31st day after the date of issue of LOA. In case the contractor fails to submit the requisite PG even after 60 days from the date of issue of LOA, the contract shall be terminated duly forfeiting EMD and other dues, if any payable against that contract. The failed contractor shall be debarred from participating in re-tender for that work.

ii. "A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel's bank through SFMS (Structured Financial Messaging System) and only after this the BG will become acceptable to RailTel. It is therefore in own interest of bidder to obtain RailTel's bank IFSC code, its branch and address and advise these particulars to the BG issuing bank and request them to send advise of BG through SFMS to the RailTel's bank."

iii. Performance Bank Guarantee of 10% of the total value of the order is required to be submitted and should be valid for a period of 4 months beyond warranty periods. On expiry of the warranty period and issue of the certificate of final acceptance of the entire system the Performance Bank Guarantee will be refunded or Bank Guarantee released to the contractor after adjustment of any dues payable by the contractor.

16. **Inspection:** Pre-shipment/pre-dispatch inspection shall be carried out at manufacturer's / supplier's works by authorized representative of RailTel.

Annexure-I

Technical Specifications

1. All Equipment should be be:

i. Supplied with 3 years warranty, if during the said guarantee / warrantee period, the Goods are found not to conforming to the requisite description and quality and/or not giving satisfactory performance or have deteriorated, and the decision of the Buyer in that behalf shall be final and binding on the Seller and the Buyer shall be entitled to call upon the Seller to rectify and/or replace the Goods or such portion thereof as is found to be defective by the Buyer within 7 days. Otherwise, the Seller shall have to pay Rs 500 per week or part of week for failed equipment subject to a maximum 10% of equipment cost to the Buyer as compensation.

ii. Equipped with necessary hardware/software to comply all above required / support features.

iii. Back-to-Back warranty with respective OEMs for both Hardware and Software. The certificates/Undertaking for the same will have to be submitted along with bid from respective OEM.

iv. OEM should have its Service Centre in India. Service center details to be shared along with address and contact no. and person.

v. UL, CE and FCC Certification is not required for PMA. However they have to produce certificate from standard lab approved/ authorized by Govt. of India that their product are equivalent to UL,CE and FCC and meets all standard and specification of UL,CE and FCC.

2. SOR wise details are as:

SOR	Item Description	Units	Qty
SOR-1	Wi-Fi Access Point High-Range (Indoor): Supply of Wireless Access Point Model (DUAL-BAND 802.11N): as per Technical specifications of SOR-1 .	Nos.	55
SOR-2	Wi-Fi Access Point High-Range (Outdoor): Supply of Wireless Access Point Model (802.11ac): as per Technical specifications of SOR-2 .	Nos.	15
SOR-3	Supply of WLAN Controller (Support 150 Access Point) with licence Model as per Technical specifications of SOR-3	Nos.	1
SOR-4	Supply of Redundant WLAN Controller Model: as per Technical specifications of SOR-4	Nos.	1
SOR-5	Supply of NMS server and radius server as per Technical specifications of SOR-5	Nos.	1

SOR: 1 Wireless Access Point (Indoor)	
SN	**Description**
1	The APs should support the 802.11a, 802.11b, 802.11g and 11n and ac standards. It should also **support 802.11ac Wave 2 standard** in the 5 GHz band.
2	Simultaneous client support on dual band radio is essential.
3	Shall provide Min 23 dBm Radio output power for both Radio's.
4	Should support minimum 3x3 or higher MIMO on both radio bands for an aggregate capacity of around 1.7Gbps.
5	The Access points should be Centrally Managed by a full-fledged controller.
6	In some small isolated environments, the AP should be able to function as a full-fledged stand-alone access point without the requirement of a controller.
7	Security mechanisms should be in place to protect the communication between the Access Point controller and the Access Points.
8	Since most radio interference come from the WLAN network itself the vendor should specify what mechanisms such as beam steering/ adaptive antenna technology/ beamforming are available in combination to focus the energy on the destination STA and minimize radio interference with the surrounding of the AP. The vendor should specify if the activation of such feature is still compatible with 802.11n spatial multiplexing.
9	Since the WLAN network will be using an unlicensed band the solution should have mechanisms that reduce the impact of interference generated by other radio equipment operating in the same band. Describe techniques supported.
10	The access point should be able to detect clients that have dual band capability and automatically steer those clients to use the 5GHz band instead of the 2.4GHz band.
11	The antennas to be dual polarized and should be integrated inside the access point enclosure to minimize damage and create a low-profile unit that does not stand out visually.
12	The access point should have minimum 1 Gigabit Ethernet port.
13	The access point should support 802.1q VLAN tagging
14	The access point should support WPA2 enterprise authentication and AES/CCMP encryption. AP should support Authentication via 802.1X and Active Directory.
15	Implement Wi-Fi alliance standards WMM, 802.11d, 802.11h and 802.11e
16	The Access Point should provide for concurrent support for high definition IP Video, Voice and Data application without needing any configuration. This feature should be demonstrable.
17	Support RF auto-channel selection by the following three methods: a) measuring energy levels on the channel; b) monitoring for 802.11 signal structures and; (c) detecting radar pulses. Other similar forms of smart selection shall also be accepted.
18	Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method.
19	Should support Transmit power tuning in 1dB increments in order to reduce interference and RF hazards
20	Should support up to 256 clients per AP
21	Should support DHCP Option 82 in standalone mode (without Controller) as well as in Managed mode (with Controller)
22	For troubleshooting purposes, the administrator should have the ability to remotely capture 802.11 and / or 802.3 frames from an access point without disrupting client access.
23	Operating Temperature: 0°C - 40°C
24	Operating Humidity: 10 % - 95% non-condensing.
25	Should be plenum rated and comply to RoHS
26	Should be WiFi certified; WiFi certificate to be enclosed
27	Should be WPC approved; ETA certificate to be enclosed
28	Device should be UL 2043 Plenum Rated.

SOR: 2 Wi-Fi Access Point High-Range (Outdoor)	
SN	**Description**
1	The APs should support the 802.11a, 802.11b, 802.11g and 11n and ac standards. It should also support 802.11ac WAVE2 standard in the 5 GHz band.
2	Simultaneous client support on dual band radio is essential.
3	Shall provide Min EIRP of 23 dBm transmit power.
4	Should support minimum 2x2 or higher MIMO on both radio bands for an aggregate capacity of 1.1Gbps
5	The access points should be centrally configured and managed through the controller.
7	Security mechanisms should be in place to protect the communication between the Access Point controller and the Access Points.
8	Since most radio interference come from the WLAN network itself the vendor should specify what mechanisms such as beam steering/ adaptive antenna technology/ beam forming are available in combination to focus the energy on the destination STA and minimize radio interference with the surrounding of the AP. The vendor should specify if the activation of such feature is still compatible with 802.11n spatial multiplexing.
9	Since the WLAN network will be using an unlicensed band the solution should have mechanisms that reduce the impact of interference generated by other radio equipment operating in the same band. Describe techniques supported.
10	The access point should be able to detect clients that have dual band capability and automatically steer those client to use the 5GHz band instead of the 2.4GHz band.
11	The antennas to be dual polarized and should be integrated inside the access point enclosure to minimize damage and create a low profile unit that does not stand out visually. The antennas could be omnidirectional or directional as per the requirement or site survey done by the vendor.
12	The access point should have minimum 1 Gigabit Ethernet port.
13	The access point should support 802.1q VLAN tagging.
14	The access point should support WPA2 enterprise authentication and AES/CCMP encryption. AP should support Authentication via 802.1X and Active Directory.
15	Implement Wi-Fi alliance standards WMM, 802.11d, 802.11h and 802.11e
16	The Access Point should provide for concurrent support for high definition IP Video, Voice and Data application without needing any configuration. This feature should be demonstrable.
17	Support RF auto-channel selection by the following three methods: a) measuring energy levels on the channel; b) monitoring for 802.11 signal structures and; (c) detecting radar pulses. Other similar forms of smart selection shall also be accepted.
18	Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method.
19	Should support Transmit power tuning in 1dB increments in order to reduce interference and RF hazards
20	The AP should have inbuilt spectrum analysis tool and preferably a speed testing tool to test speeds from AP to client/wired network.
21	Device antenna gain (integrated) must be at least 3 dBi and should provide automatic interference rejection of about 10dB.
22	Should support up to 256 clients per AP
23	Should support DHCP Option 82 in standalone mode (without Controller) as well as in Managed mode (with Controller)
24	For troubleshooting purposes, the administrator should have the ability to remotely capture 802.11 and / or 802.3 frames from an access point without disrupting client access.
25	Operating Temperature: -20°C - 65°C
26	Should be WiFi certified; WiFi certificate to be enclosed

27	Should be WPC approved; ETA certificate to be enclosed
28	Device should be IP67 certified. Indoor AP with outdoor rated enclosure will not be accepted.
29	Mechanism for physical device locking using padlock /Kensington lock / equivalent

SOR: 3 WLAN Controller with NMS (Supports 150 Access Point)	
SN	**Description**
1	**Product details- Please specify**
1.1	Please mention Make, Model No. and Part Code
1.2	The Proposer shall position two hardware controllers with appropriate specifications, as per the compliance to operate in the capacity of highly Available wireless controllers.
2	**Essential Features**
2.1	The WLC should have 20Gbps of throughput dedicated hardware appliance, purpose built for Wi-Fi Control and management.
2.2	The WLC should have minimum of 4x 10/100/1000 RJ45 Ethernet Ports and 4 x 10G ports
	Controller should have Dual Redundant power supply and Redundant Fans
2.3	WLC should have Easy Setup through UPnP Network Discovery and Installation Wizard.
2.4	Controller should support minimum 150 AP from day one and should be scalable up to 1000 APs or more with support of seamless roaming access over L2/L3 network.
2.5	Support for 100% redundancy for primary controller i.e. N: N for hardware as well all Licenses. In case primary controller goes down all features should be supported by redundant controller.
2.6	Controller should have capacity to handle minimum 20,000 or more Concurrent devices.
2.7	Cntroller should support integrated user authentication capability of minimum 20,000 users without the need for any external database servers (AD/LDAP).
2.8	Redundancy Features: WLC Must provide Active: Active with N+1 redundancy. The WLC's shall be implemented in cluster.
2.9	Controller should support minimum 1000 WLAN's.
2.10	Controller should provide air-time fairness between these different speed clients – slower clients should not be starved by the faster clients and faster clients should not adversely affected by slower clients.
2.11	Ability to map SSID to VLAN and dynamic VLAN support for same SSID.
2.12	support automatic channel selection for interference avoidance.
2.13	External Captive Portal Integration - Web-services based API for external web-portals to integrate with the controller
2.14	should have the capability to limit/prevent clients from using static IP addresses thereby enhancing network efficiency and preventing network conflicts.
2.15	The controller or WLAN solution should support client-troubleshooting feature that allows an administrator to focus on a specific client device and its connectivity status. The tool should track the step-by-step progress of the client's connection, through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type).
2.16	The controller or the WLAN solution should support in built spectrum analysis feature.

2.17	The controller should support the ability to create different zones in which AP can be grouped logically or physically based on location e.g. different buildings in a campus can be configured as different zones so that each zone will have different configuration and policies.
2.18	WLC should support Hotspot 2.0 (pass point).
3	**Auto Deployment of AP's at different locations**
3.1	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.
3.2	Access points can discover controllers across Layer-3 network through DHCP or DNS option
4	**Security & Monitoring**
4.1	Controller should support following for security & Authentication:
4.2	WIRELESS SECURITY & Authentication: Open, 802.1x/EAP, PSK, DPSK/MPSK/PPSK/IPSK WISPr, WPA, WPA2-AES, WPA-TKIP, WEP, EAP-SIM, EAP-AKA over WLAN for 802.1x, Authentication through external Radius /Directory services.
4.3	WLC should support WIDS/WIPS for security including Rogue AP detection and prevention, Evil-twin/AP spoofing detection and Ad-Hoc detection.
4.4	WLC Should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.
4.5	Support for Walled garden "Walled Garden" functionality to allow restricted access to select destinations by unauthorized wireless users.
4.6	The proposed architecture should be based on controller based Architecture with thick AP deployment. While Encryption / decryption of 802.11 packets should be able to perform at the AP.
4.7	WLC should support OS/Device finger printing, Bandwidth rate limit, VLAN mapping.
4.8	WLC should support Mesh with both bands.
4.9	WLC should be able to present a customizable dashboard with information on the status of the WLAN network.
4.10	WLC should be able to raise critical alarms by sending an email. The email client on the controller should support SMTP outbound authentication and TLS encryption.
4.11	WLC or integrated solution should provide customized reporting with minimum 14 days of historical WLAN information.
4.12	Filtering of Alarms and event Log based on APs, SSID or Zones
4.13	Syslog support towards external syslog server
4.14	Controller or integrated solution should support URL Filtering
4.15	Controller or integrated solution should support Wireless heat maps to show coverage areas and holes. It should also provide functionality to track wireless clients in heat map.
4.16	Controller or integrated solution should support unique Pre Shared keys to each user separately.
5	**QoS features**
5.1	WLC should support per-SSID or dynamic per-user bandwidth Rate Limiting and Bonjour fencing to limit mDNS/Bonjour traffic.
5.2	Self-healing (on detection of RF interference or loss of RF coverage) and vendor should provide their Interference mitigation techniques.
5.3	System must support Band Steering where 5 Ghz clients are forced to connect over 5Ghz Radio to provide better load balancing among 2.4Ghzand 5Ghz Radios.
5.4	WLC shall support Quality of Service features like 802.11e based QoS enhancements, WMM or equivalent and U-APSD to provide best performance on Video applications.

6	**Client/Guest Management**
6.1	WLC should provide a Guest Login portal in order to authenticate users that are not part of the organization.
6.2	WLC should be able to provide a web-based application that allows non- technical staff to create Guest accounts with validity for fixed duration like hours or days.
7	**Management Features**
7.1	WLC should be have administration access through HTTPS GUI, SSH CLI.
7.2	Administrative users should have account security features such as session idle timer, account lockout, password expiration, password reuse, two factor authentication. Should have option to enable captcha to make sure a human is logging into the system.
7.3	WLC should have library of well-documented REST-APIs and full set of MQTT/GPB to allow integration with 3rd party apps.
8	**Mandatory Compliance :**
8.1	All categories of Controller and Access Point should be from same OEM
8.2	If any of the features above require separate license, it should be quoted along with controller.
9	**Product brochure**
9.1	Vendor should provide printed technical catalogs/brochures for the quoted model containing technical specifications, features. Should also provide Manufacturer's Authorization.

SOR: 4 Redundant WLAN Controller	
SN	**Description**
1	**Product details- Please specify**
1.1	Please mention Make, Model No. and Part Code
1.2	The Proposer shall position two hardware controllers with appropriate specifications, as per the compliance to operate in the capacity of highly available wireless controllers.
2	**Essential Features**
2.1	The WLC should have 20Gbps of throughput dedicated hardware appliance, purpose built for Wi-Fi Control and management.
2.2	The WLC should have minimum of 4x 10/100/1000 RJ45 Ethernet Ports and 4 x 10G ports
	Controller should have Dual Redundant power supply and Redundant Fans
2.3	WLC should have Easy Setup through UPnP Network Discovery and Installation Wizard.
2.6	Controller should have capacity to handle minimum 20,000 or more Concurrent devices.
2.7	Cntroller should support integrated user authentication capability of minimum 20,000 users without the need for any external database servers (AD/LDAP).
2.8	Redundancy Features: WLC Must provide Active: Active with N+1 redundancy. The WLC's shall be implemented in cluster.
2.9	Controller should support minimum 1000 WLAN's.
2.10	Controller should provide air-time fairness between these different speed clients – slower clients should not be starved by the faster clients and faster clients should not adversely affected by slower clients.
2.11	Ability to map SSID to VLAN and dynamic VLAN support for same SSID.

2.12	support automatic channel selection for interference avoidance.
2.13	External Captive Portal Integration - Web-services based API for external web-portals to integrate with the controller
2.14	should have the capability to limit/prevent clients from using static IP addresses thereby enhancing network efficiency and preventing network conflicts.
2.15	The controller or WLAN solution should support client troubleshooting feature that allows an administrator to focus on a specific client device and its connectivity status. The tool should track the step-by-step progress of the client's connection, through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type).
2.16	The controller or the WLAN solution should support in built spectrum analysis feature.
2.17	The controller should support the ability to create different zones in which AP can be grouped logically or physically based on location e.g. different buildings in a campus can be configured as different zones so that each zone will have different configuration and policies.
2.18	WLC should support Hotspot 2.0 (passpoint).
3	**Auto Deployment of AP's at different locations**
3.1	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.
3.2	Access points can discover controllers across Layer-3 network through DHCP or DNS option
4	**Security & Monitoring**
4.1	Controller should support following for security & Authentication:
4.2	WIRELESS SECURITY & Authentication: Open, 802.1x/EAP, PSK, DPSK/MPSK/PPSK/IPSK WISPr, WPA, WPA2-AES, WPA-TKIP, WEP,EAP-SIM, EAP-AKA over WLAN for 802.1x, Authentication through external Radius /Directory services.
4.3	WLC should support WIDS/WIPS for security including Rogue AP detection and prevention, Evil-twin/AP spoofing detection and Ad-Hoc detection.
4.4	WLC Should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.
4.5	Support for Walled garden "Walled Garden" functionality to allow restricted access to select destinations by unauthorized wireless users.
4.6	The proposed architecture should be based on controller based Architecture with thick AP deployment. While Encryption / decryption of 802.11 packets should be able to perform at the AP.
4.7	WLC should support OS/Device finger printing, Bandwidth rate limit, VLAN mapping.
4.8	WLC should support Mesh with both bands.
4.9	WLC should be able to present a customizable dashboard with information on the status of the WLAN network.
4.10	WLC should be able to raise critical alarms by sending an email. The email client on the controller should support SMTP outbound authentication and TLS encryption.
4.11	WLC or integrated solution should provide customized reporting with minimum 14 days of historical WLAN information.
4.12	Filtering of Alarms and event Log based on APs, SSID or Zones
4.13	Syslog support towards external syslog server
4.14	Controller or integrated solution should support URL Filtering

4.15	Controller or integrated solution should support Wireless heat maps to show coverage areas and holes. It should also provide functionality to track wireless clients in heat map.
4.16	Controller or integrated solution should support unique PreShared keys to each user separately.
5	**QoS features**
5.1	WLC should support per-SSID or dynamic per-user bandwidth Rate Limiting and Bonjour fencing to limit mDNS/Bonjour traffic.
5.2	Self-healing (on detection of RF interference or loss of RF coverage) and vendor should provide their Interference mitigation techniques.
5.3	System must support Band Steering where 5 Ghz clients are forced to connect over 5Ghz Radio to provide better load balancing among 2.4 Ghz and 5Ghz Radios.
5.4	WLC shall support Quality of Service features like 802.11e based QoS enhancements, WMM or equivalent and U-APSD to provide best performance on Video applications.
6	**Client/Guest Management**
6.1	WLC should provide a Guest Login portal in order to authenticate users that are not part of the organization.
6.2	WLC should be able to provide a web-based application that allows non-technical staff to create Guest accounts with validity for fixed duration like hours or days.
7	**Management Features**
7.1	WLC should be have administration access through HTTPS GUI, SSH CLI.
7.2	Administrative users should have account security features such as session idle timer, account lockout, password expiration, password reuse, two factor authentication. Should have option to enable captcha to make sure a human is logging into the system.
7.3	WLC should have library of well-documented REST-APIs and full set of MQTT/GPB to allow integration with 3rd party apps.
8	**Mandatory Compliance:**
8.1	All categories of Controller and Access Point should be from same OEM
8.2	If any of the features above require separate license, it should be quoted along with controller.
9	**Product brochure**
9.1	Vendor should provide printed technical catalogs/brochures for the quoted model containing technical specifications, features. Should also provide Manufacturer's Authorization.

SOR: 5 Radius Server	
SN	**Description**
1	The AAA solution should be available as a hardware based appliance
2	The AAA Server should provide authentication services to all the users connecting to the network, should enforce security policies on the end Stations.
3	The AAA Server should offer centralized command and control for all user authentication, authorization and accounting from a Web-based, graphical interface and distribute those controls to hundreds or thousands of access gateways in the network
4	The AAA Server should provide the manageability and administration of user access for routers VPNs, firewalls, dialup and DSL connections, cable access, storage, content, voice over IP (VoIP), wireless solutions and switches using IEEE 802.1x access control
5	The same AAA Server should leverage access framework to control Administrator

	access and configuration for all RADIUS enabled network devices in the network
6	The same AAA Server should leverage access framework to control administrator access and configuration for all TACACS+ enabled network devices in the network
7	Solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices
8	TACACS+ device administration should support: i. Role-based access control Per Command level authorization with detailed logs for auditing
9	The solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, (any character), * (matches any), etc and support stacking as well
10	The AAA solution should support using custom TACACS+ port
11	Solution should support MAB address based authentication for unmanaged endpoints
12	It should support Authentication by validating any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access
13	The proposed solution should be able to integrate with industry leading Directory server like but not limited to LDAP server, Microsoft Active Directory, RSA Secure ID server
14	The AAA server should support the following authentication methods Native User Authentication Pass Throught Authentication Proxy RADIUS Authentication External Authentication Directed Authentication HTTP Digest Access Authentication
15	The AAA server should support the following authentication protocols EAP Generic Token Card (EAP-GTC) EAP State of Health (EAP-SOH) EAP-PEAP EAP-TLS EAP-MD5 PAP CHAP MS-CHAP and MS-CHAPv2
16	Device command set authorization Network access restrictions and administrative access reporting. Restrictions such as time of day, day of week and session time limits. User and device group profiles. Should have a Web-based user interface to simplify and distribute configuration for user group profiles
17	The AAA Server should be able to support large networked environments and support for redundant servers, remote databases, and user database backup services. Lightweight Directory Access Protocol (LDAP) authentication forwarding support for authentication of user profiles stroed in directories from leading vendors
18	Different access levels for each AAA Server administrator- and the ability to group network devices- enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a networks
19	The AAA server should be compatible with all the components of SIEM, FLOW and Networking solutions quoted for this RFP
20	The AAA server should support Time Based Access
21	The solution should be vendor agnostic and based on open standard
22	The AAA server should support Location-based profiles for groups
23	The AAA server should support Account lockout and account blacklisting
24	The AAA server should support Proxy filtering
25	The AAA server should support IP address assignment via locally managed IP or Dynamic Host Configuration Protocol (DHCP) pool
26	The AAA server should support directed realms to provide virtualized instances of the server, allowing requests to be managed according to their nature.
27	The AAA server should support IPv6
28	The AAA server should support Attribute translation and mapping to translate from one type of network access equipment to another

29	The proposed AAA solution should have a built-in Profiler for network device visibility. Solution should be able to detect both new and existing endpoints and categorizes them based upon the type of endpoint (Ex:Windows, Printer, Network Device, IP Camera, Android, iPad,etc)
30	The proposed AAA solution must support network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network
31	The proposed AAA solution should provide support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network all within the same appliance
32	The proposed AAA solution must support Profiling via Active and Passive collectors like DHCP, SNMP, HCP fingerprinting, HTTP-agent, NMAP, WMI, TCPIP, SMB, etc.
33	The proposed AAA solution must provide active scanning via WMI, SSH,LDAP, SNMP and MDM Collector.
34	The proposed AAA solution must provide flexible filtering capabilities to sort out device information based on differen attributes (e.g MAC address, Manufacturer name, hostname, IP address, etc.)
35	The proposed AAA solution should produce a real-time endpoint discovery with detailed information including which switch port the device is connected.
36	The proposed AAA solution must provide device inventory in CSV, Tab Delimiter and PDF exportable format.
37	The proposed AAA solution must provide capability to import device inventory via CSV and binary file.
38	The proposed AAA solution must provide information on how many devices are not profiled, how many devices are newly seen in day/week/month, etc.

Annexure-II

Executive Director, **Dated: …….**
RailTel Corporation of India Ltd.
……
……....
……....

Subject: Manufacturer Authorisation form (MAF) to M/s …… for ……

Ref: GeM Bid No. ……

Dear Sir,

We, M/s……, are established and reputed manufacturer and service provider of ……. (Product details), having our registered office at ……..

We hereby authorize M/s …….. (bidder name), Office ……. to participate in bid and subsequently upon award of the bid to execute the supply and Installation & Commissioning of our range of products against your above said bid.

We further extend our warranty for …… years for our range of products offered by M/s ……. against the above-said bid.

Thanking you,

Best regards,

Authorized Signatory

Annexure-III

GURANTEE BOND FOR SECURITY DEPOSIT

(On Stamp Paper of requisite value)

(To be used by approved Scheduled Banks)

In consideration of the RailTel Corporation of India Limited: 6th Floor, Block-III, Delhi IT Park, Delhi-110053.

1. (Herein after called RailTel) having agreed to exempt …….. (Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Agreement No. …… …… dated …… made between …… and …….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, or production of a Bank Guarantee for Rs. …….. (Rs. …….. only). We, ……(indicate the name of the Bank) hereinafter referred to as " the Bank") at the request of ……. ……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……. Against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……Bank and our **local branch at New Delhi (indicate detail address of local New Delhi Branch with code no.)** do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. ……

3. We, ……..….bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor (s) / Supplier (s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal.

The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Supplier(s) shall have no claim against us for making such payment.

We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its

claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly

discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. (1) ……. We shall be discharged from all liability under this Guarantee thereafter.

We,……..…We……...…… (indicate the name of Bank) Further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) Supplier(s).

We, the …… Bank further agree that this guarantee shall be invokable at our place of business at ……/New Delhi (indicate detailed address of local New Delhi Branch with code no.). The branch at New Delhi is being advised accordingly.

(indicate the name of Bank) lastly undertaken not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

Dated the day of 2020

for ……..
(Indicate the name of the Bank)

Witness

1. **Signature**

   Name

2. **Signature**

   Name