RFP No. APSFL-15026(31)/1/2018 , Dated: 25/07/2018
REQUEST FOR PROPOSAL
FOR
SELECTION OF IMPLEMENTATION AGENCY FOR PUBLIC WI-FI
Corrigendum 5, Dated 29th September 2018

Bidders are requested to take note of the following changes in the RFP:

S. No	Section	Old Clause	New Clause
1.	Section 8 Scope of Work	APSFL has identified a monetization partner (Google Station) for providing monetization and management platform. The bidder must ensure that the Access point and controller hardware and software proposed by the bidder must have advance certification from Google for use with the Google Station Wi-Fi solution.	**"APSFL has identified a monetization partner (Google Station) for providing monetization and management platform. The bidder must ensure that the Access point and controller hardware and software proposed by the bidder must have advance certification from Google for use with the Google Station Wi-Fi solution (or) in case of Non Availability of the Certification at the time of bidding, the same can be provided before the signing of MSA failing which the order will be cancelled."**
2.	Section 11.2, Technical bid Evaluation Framework: Important Note	-	**The bidder may note that parameters of the bidder company only will be considered for technical evaluation. The credentials of the parent company shall not be considered for the Technical Evaluation.**
3.	Section 13.8.2.1 WLAN Controller ,clause 2	The controller can be a hardware appliance/multiple appliances or software-based controller. In case software-based controller is being proposed, the controller shall be compatible with a commercial cloud service platform such as Google Cloud Platform or Amazon Web Services.	**The controller can be a hardware appliance/multiple appliances or software-based controller. In case software-based controller is being proposed, the controller shall be compatible with a commercial cloud service platform such as Google Cloud Platform or Amazon Web Services and the vendor has to supply the hardware node to host their controller software.**
4.	Section 13.8.2.1 WLAN Controller ,clause 12	The controller shall be able to raise critical alarms by sending an email and via SNMP V3 traps. The email client on the controller should support SMTP outbound authentication and TLS encryption.	**The Wireless Solution shall be able to raise critical alarms by sending an email and via SNMP V3 traps securely.**

5.	Section 13.8.2.1 WLAN Controller ,clause 16	The controller and APs shall support tunneling modes for dataplane communications: one in which individual APs tunnel data directly to a Wireless Access Gateway (WAG) via SoftGRE/IPv4 or SoftGRE/IPv6, and a second mode in which the APs tunnel data to the controller using an encrypted protocol. In the second mode, data traffic is then aggregated and tunneled in a smaller set of tunnels from the controller(s) to a WAG. In the second mode, the tunneling protocol between the APs and the controller may be vendor-proprietary.	**The controller and APs shall support tunneling modes for dataplane communications: one in which individual APs tunnel data directly to a Wireless Access Gateway (WAG) via SoftGRE/EoGRE (Both IPv4 and IPv6).**
6.	Section 13.8.2.1 WLAN Controller ,clause 18	If in the dataplane, the AP controller shall support northbound dataplane tunneling over SoftGRE/IPv4	**If in the dataplane, the AP controller shall support northbound dataplane tunneling over SoftGRE/EoGRE(IPv4)**
7.	Section 13.8.2.1 WLAN Controller ,clause 19	If in the dataplane, the AP controller shall support northbound dataplane tunneling over SoftGRE/IPv6	**If in the dataplane, the AP controller shall support northbound dataplane tunneling over SoftGRE/EoGRE(IPv6)**
8.	Section 13.8.2.2 Access Point Technical Specifications, Clasue 3	It should be compatible and be able to integrate with the Cloud based Controller. Must support SSH & SNMP protocol for local or remote access to device through CLI or GUI.	**It should be compatible and be able to integrate with the Cloud based Controller hosted on premises. Must support SSH & SNMP protocol for local or remote access to device through CLI or GUI**
9.	Section 13.8.2.2.1, Indoor Access Point, Point 8	Must support up to 21dbm or higher of EIRP transmit power	**Must support up to 20dbm or higher of EIRP transmit power**
10.	Section 13.8.2.2.1, Indoor Access Point, Point 10	Rx sensitivity shall be **-93 dBm** or better at MCS0 and 20MHz channel bandwidth.	**Rx sensitivity shall be -90dBm or better at MCS0 and 20MHz channel bandwidth.**
11.	Section 13.8.2.2.1, Indoor Access	The Access point shall support operating temperature of **0° C to +50° C**	**The Access point shall support Operating Temperature of 0° C to +40°**

	Point, Point 21		
12.	Section 13.8.2.2.2, Outdoor Access Point, Point 11	Rx sensitivity shall be minimum **-92** dBm or better at MCS0 and 20MHz channel bandwidth.	**Rx sensitivity shall be minimum -91 dBm or better at MCS0 and 20MHz channel bandwidth**
13.	Section 13.8.2.2.2, Outdoor Access Point, Point 30	-	**Should support real-time built-in spectrum analysis**
14.	Section 13.8.2.2.2, Outdoor Access Point, Point 31	-	**Access Point should support CleanAir**
15.	Section 13.8.2.2.2, Outdoor Access Point, Point 31	-	**Should have built in console port for management of AP**
16.	Section 13.8.2.3, Access Edge Switch, Point 2	PoE Standard: IEEE 802.3af or **IEEE 802.3at 3**- IPV4,IPV6 Support	**PoE Standard IEE 802af or IEEE 802at IPV4, IPV6 Support**