No.PC-49/001/WiFi-Solu/NIA/2017-18/492
National Investigation Agency
Government of India
MINISTRY OF HOME AFFAIRS
OPPOSITE CGO COMPLEX,
LODHI ROAD, NEW DELHI -110001

Dated: 12 Feb 2018

CORRIGENDUM

In continuation to this office tender notice No.02/2018 dated 22 Jan 2018 for supply, installation, testing and commissioning of Centralized WiFi solutions at NIA HQ New Delhi, the technical bids will now be opened on 20 Feb 2018 at 1600 hrs instead of 13 Feb 2018 due to administrative reasons.

2. Further, based on the pre-bid meeting held on 05 Feb 2018, the following amendments are hereby issued which will be in continuation to the tender notice No.02/2018:-

I. **Scope of Work:**

a. Scope of work was clearly explained to all the representatives. It was decided that the WiFi connectivity in the basement and stair case area can be excluded. It has been decided that Indoor type APs will suffice the wifi network coverage of NIA outdoor premise. The APs must be installed according to the heat map generated at the time of survey by the bidder.

b. Bidder must conduct the wifi coverage heat mapping (Site survey) based on following parameters. Details are attached as Annexure B.
   i. Type of devices (Concurrent) - laptop, mobiles, tabs, Printers/scanners.
   ii. Minimum Signal strength of -65db.
   iii. Area Density
   iv. Application types – browser based applications both internet and intranet, email, Video Streaming and VoIP based applications.
   v. Environment like type of obstacles.

c. Bidders must provide the structured cabling with all required items (standard certified) like Cat 6 Shielded cables, conduit pipe for laying cables, required Patch cord, Patch Panels, IOs etc.

d. The APs should be connected to PoE+ switches (No use of AC/DC power adapters for the wifi access points).

e. 10 % of the total unit of WAPs must be supplied with AC/DC power adaptor.

12/2

II. Changes/modifications to the WiFi controller and WiFi Access Point technical specifications as per tender document.

Tech. Spec. Point No.	Specification Description	Modifications/Amendment
1.10	The proposed Wi-Fi controllers should be of software based. Should be compatible to run as a VM on various Hypervisors like VMWARE, KVM and Virtual-box etc. Should support remote replication w.r.to DR.	The proposed Wi-Fi controllers should be of software/hardware based or an equivalent solution with features of a Wi-Fi controller. Software controller should be compatible to run as a VM on various Hypervisors like VMWARE/KVM/Virtual-box etc. Should support remote replication w.r.to DR
1.11	Solution must support controller-less, intelligent edge architecture for Wi-Fi access. All WLAN services should be delivered at the edge and hence eliminating the dependency on the controller	Solution must support an independent (No dependency on controller) intelligent edge architecture for Wi-Fi access. In case of non-reachability of the controller, all WLAN services should be delivered at the edge
1.12	Solution must support controller-less, intelligent edge architecture for wireless intrusion prevention (WIPS)	Solution must support an independent (No dependency on controller) intelligent edge architecture for WIPS. In case of non-reachability of the controller, all WIPS services should be delivered at the edge.
2.13	The quoted Wi-Fi controller should be capable of supporting 500 Access Point devices without need of any additional Hardware and Software other than licenses.	The quoted Wi-Fi controller should be capable of supporting 300 Access Point devices without need of any additional Hardware and Software other than licenses.
2.23	The system must provide historical location tracking (eg. location of switched off Rogue AP)	The system must provide historical location tracking (eg. location of switched off Rogue AP) at least for 1 year.
2.42	Solution should support External Splash Page	Solution should support External Splash Page. Support for custom pages (externally hosted) during client authentication process.
2.61	The system must detect Honey Pot attacks including its advanced variants such as MultiPot attack. It should be able to prevent the authorized client from connecting to a honeypot AP.	The system must detect Honey Pot attacks including its advanced variants such as MultiPot attack. It should be able to prevent the authorized client from connecting to a honeypot AP and tarpitting.
2.69	WiFi controller should support both active / active and active / passive modes of operation.	WiFi controller should support both active / active and active / passive modes of operation (Full fledge failover).