All India Institute of Medical Sciences (AIIMS), New Delhi

AMENDMENT NO. – I Dated: 11.04.2017

Name of Project: Development of Network Infrastructure for New OPD Block at AIIMS, New Delhi.
Tender No. : HSCC/AIIMS/New OPD/IT/2017 dated 27/03/2017
Reply to Pre Bid Queries raised by bidders during pre -bid meeting held on 31.03.2017 at HSCC's Corporate Office, Noida

S. No	Volume, Page, Clause	Tender Document Clause	Pre-bid Queries	Reply
1	Volume IV, Page 43, Firewall Specification (Point no. 9)	NGFW must support virtual Firewall option to have on totally different virtualized firewall if required. Bidder must give license for 5 Virtual Firewalls.	Virtual Firewall is required in MSSP environment and not required in Hospitals and Colleges. Request you to please remove this point	**Amended at Annexure-I.**
2	Volume IV, Page 43, Firewall Specification (Point no. 10)	The Firewall solution should support NAT64, DNS64 & DHCPv6.	They are multiple other methods used for IPv4 to IPv6 transition so change this point as "The Firewall solution should support NAT64/Dual Stack/NAT, DNS64/DNS & DHCPv6	**Amended at Annexure-I.**
3	Volume IV, Page 43, Firewall Specification (Point no. 11)	OEM may have NSS labs recommendation for NGFW for 3 years in a row.	Sophos is Checkmark Certified and which is globally accepted certification. Please change this as " OEM may have NSS/Checkmark labs recommendation for NGFW"	**Amended at Annexure-I.**
4	Volume IV, Page 43, Firewall Specification (Point no. 17)	Firewall IPSec VPN throughput should be 14 Gbps	VPN throughput is too High in comparative to Firewall throughput . Request to change it as " Firewall IPSec VPN throughput should be 8 Gbps"	**Amended at Annexure-I.**
5	Volume IV, Page 43, Firewall Specification (Point no. 20)	Firewall should support 250000 New sessions per second	Change this as " Firewall should support 200000 New sessions per second"	**Amended at Annexure-I.**
6	Volume IV, Page 44, Firewall Specification (Point no. 23)	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.	In Sophos,Both mode can be available concurrently so request to change as "The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently"	**Amended at Annexure-I.**
7	Volume IV, Page 45, Firewall Specification (Point no. 54)	Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP	MAPI and NNTP not required for DLP so change this as "Protocol supported: HTTP-POST/HTTP Upload, SMTP"	**Amended at Annexure-I.**
8	Volume IV, Page 46, Firewall Specification (Point no. 58)	Protocols Supported: HTTP-POST, HTTP=GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP	Need to change this as " Protocols Supported: HTTPPOST/HTTP Upload, HTTP=-GET/HTTP Doenload,SMTP/ POP3/ IMAP/MAPI/FTP/ NNTP	**Amended at Annexure-I.**
9	Volume IV, Page 46, Firewall Specification (Point no. 60)	DLP archiving: Records full content in email, FTP, IM, NNTP, and web traffic	Need to change this as " DLP archiving: Records full content in email/FTP/ IM/NNTP	**Amended at Annexure-I.**
10	Volume IV, Page 47, COPPER CABLING SYSTEM, 1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	OEM Specific: CAT6A U/FTP solution is available with limited OEM, suggested CAT6A F/UTP solution for healthy competetion.	Cat6A U/FTP Solution is being manufactured by almost all the approved makes given in RFP.

11	Volume IV, Page 47, COPPER CABLING SYSTEM, 1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	Mechanical Characteristics: NVP:75-77%	OEM Specific: NVP should be 67-76%%, please change.	**Amended at Annexure-I.**
12	Volume IV, Page 48, COPPER CABLING SYSTEM, 1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	Mechanical Characteristics: Resistance Unbalance: 2% max.	OEM Specific: that should be between 2-5%, please change.	**Amended at Annexure-I.**
13	Volume IV, Page 50, COPPER CABLING SYSTEM, COPPER CABLING SYSTEM, 1.4 CAT6A 24 PORT SHIELDED JACK PANEL UN-LOADED:-	Features: Be made of cold rolled steel, in 24 port configurations. Each jack for the jack panel should have spring loaded shutter inside the jack for 100% dust free environment.	Please change spring loaded shutter or hinged dust cover (Both for same use)	Both are acceptable
14	Volume IV, Page 51, COPPER CABLING SYSTEM, COPPER CABLING SYSTEM, 1.5 CAT6ASHIELDED MOUNTING CORDS (1 Mtr and 2 Mtr)	Electrical Characteristics:-Plug: Operating Temperature range: -40 ˚C to +85 ˚C	OEM Specific: In India weather that is not required, that should be -10 ˚C to + 75 ˚C, please change.	No Change. Tender Conditon prevails.
15	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Max. Tensile Strength-Short Term @ 3500N	OEM Specific: That should be between 2000 to 2600N, please change.	**Amended at Annexure-I.**
16	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Max. Crush Resistance-Short Term @ 6000N/10 cm	OEM Specific: That should be between 3500 to 4000N, please change.	**Amended at Annexure-I.**
17	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Operating Temperature range @ -40°C to +70°C	OEM Specific: In India weather that is not required, that should be -10 ˚C to + 70 ˚C, please change.	**Amended at Annexure-I.**
18	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Optical Characteristics:- (Attenuation) At 850 nm @ <= 2.7dB/km	OEM Specific: That shouls be <= 2.7dB/km ± .5db, Attenuation is nominal 5 - 10%.	No Change. Tender Conditon prevails.

19	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Optical Characteristics:- (Attenuation) At 1300 nm @ <= 0.8 dB/km	OEM Specific: That shouls be <= 0.8dB/km ± .2db, please change	No Change. Tender Conditon prevails.
20	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Optical Characteristics:- (Bandwidth) At 850 nm @ >= 2000 MHz · km	OEM Spcific: That should be ≥ 1500 (50 OM3, please change.	No Change. Tender Conditon prevails.
21	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Mechanical and Environmental Performance:- Max. Tensile Strength-Short Term @ 3500N	OEM Specific: That should be between 2000 to 2600N, please change.	**Amended at Annexure-I.**
22	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Mechanical and Environmental Performance:- Max. Crush Resistance-Short Term @ 6000N/10 cm	OEM Specific: That should be between 3500 to 4000N, please change.	**Amended at Annexure-I.**
23	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Mechanical and Environmental Performance:- Operating Temperature range @ -40°C to +70°C	OEM Specific: In India weather that is not required, that should be -10 ˚C to + 70 ˚C, please change.	**Amended at Annexure-I.**
24	Volume-IV, Page 56,OPTICAL FIBER CABLING, 2.1.5 Fiber Optic Pigtail 9/125 Singlemode OS1 SC Type:-	Operating Temp. @ -20ºC to 75ºC	OEM Specific: In India weather that is not required, that should be -20 ˚C to + 60 ˚C, please change.	No Change. Tender Conditon prevails.
25	Volume-IV, Page 57,OPTICAL FIBER CABLING, 2.1.6 Fiber Optic Patch Cord SC-LC 9/125 OS1Singlemode:-	Operating Temp. @ -40ºC to 75ºC	OEM Specific: In India weather that is not required, that should be -20 ˚C to + 60 ˚C, please change.	No Change. Tender Conditon prevails.
26	Volume-IV, Page 57,OPTICAL FIBER CABLING, 2.1.8 Fiber Optic Pigtail 50/125 Multimode OM3 SC Type:-	Connector Insertion Loss @ 0.30dB(Max)	OEM Specific: As per EIA/TIA that should be ≤ 0.40 dB/km	No Change. Tender Conditon prevails.
27	Volume-IV, Page 58,OPTICAL FIBER CABLING, 2.1.9 Fiber Optic Patch Cord SC-LC 50/125 OM3 Multimode:-	Connector Loss @ 0.30dB(max)	OEM Specific: As per EIA/TIA that should be ≤ 0.40 dB/km	No Change. Tender Conditon prevails.

28	Volume-IV, Page 58,OPTICAL FIBER CABLING, 2.1.9 Fiber Optic Patch Cord SC-LC 50/125 OM3 Multimode:-	Operating Temperature @ -40°C to +85°C	OEM Specific: In India weather that is not required, that should be -20 ˚C to + 60 ˚C, please change.	No Change. Tender Conditon prevails.
29	Volume-I, Page 5, Clasue 1.3, Eligibility Criteria for bidders	Addition requested	We request hereby to add ISO/IEC 20000-1 : 2011 which certify Information Technology Service Management System. ISO/IEC 20000-1:2011 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an Service Management system. Considering AIIMS being premier institute of Country, we request hereby to add above clause so that well established SI participate for this Tender.	No Change. Tender Conditon prevails.
30	Volume-I, Page 5, Page No. 2 and 7, Last date of Submission of Tender	Last date of Submission of Tender	Date of upload of Tender is indicated 20/04/2017 on Page no.2 of Vol 1 while it is referrred 31/04/2017 on page no. 7 (Point no. 1.6) . Please Confirm exact date. However we request hereby to keep it 31/04/2017 only as Project includes detaiuled survey at scheduled site.	**Amended at Annexure-I.**
31	Volume-II, Page 25 Clause 36. Payment Term	(a) Hardware (Active and Passive items) & Software for LAN & Wi-Fi works (i) 50% on delivery of the equipments at site subject to submission of inspection report. (ii) 25% on installation and commissioning of the equipments. (iii) 20% on handing over to client. (iv) 5% on successful completion of 3 years OEM warranty/operation & maintenance support.	We request hereby to change Payment term as following to make this Tender do-able.: (i) 70% on delivery of the equipments at site subject to submission of inspection report. (ii) 20% on installation and commissioning of the equipments. (iii) 5% on handing over to client. (iv) 5% on successful completion of 3 years OEM warranty/operation & maintenance support.	No Change. Tender Conditon prevails.
32	Volume-II, Page 25 Clause 37. Factory Inspection		Tender includes SITC of Multiple components. It will not be feasible to arrange Travel of representative(s) of HSCC/Clients to factory location of OEM as maximum of them are out of India. We request HSCC/Clients to manage this cost on their own if visit is required.	No Change. Tender Conditon prevails.
33	Volume-II, Page 26 Clause 38. Site Preparation	Clause 38. Site Preparation - The agency should provide the power, UPS & internet during the implementation period of the project.	Request to provision power by HSCC/Clients themselve as it will not be possible for us to measure such requirement and relevant cost. Also request to mention minimum requirement of Internet and also confirm if it is subject to IT firm's own requirement only.	No Change. Tender Conditon prevails.
34	Volume-IV, Page 10	18. The IT firm shall install, wire the UPS power at required locations and provide proper electrical ground for the same before installation of the equipment. Civil works if any required for installation of the system will be the responsibility of the SI.	Scope of install, wire the UPS power at required locations must be clearly defined in terms of no.s of such power points or qty of wire to be laid.	No Change. Tender Conditon prevails.
35	Volume-IV, Page 13	3. Establishment of Server Room	We request hereby to remove defined scope under this clause from IT scope of work. However if it is mandatory, we request hereby to specify requirment clearly so that all Bidders remain on same parameter for costing of required Jobwork.	No Change. Tender Conditon prevails.

36	Volume IV, Page 38, Wireless Access Point Specification (Point no. 3)	AP should have 1x10/100/1000 Ge LAN port.	AP should have 2x10/100/1000 Ge LAN port.	Bidder is open to propose anything additional to the minimum specification mentioned in RFP
37	Volume IV, Page 38, Wireless Access Point Specification (Point no. 9)	Access point should support 802.11ac beamforming for 802.11ac.	Access point should support 802.11ac beamforming/Adaptive antenna for 802.11ac.	No Change. Tender Conditon prevails.
38	Volume IV, Page 38, Wireless Access Point Specification (Point no. 12)	Access point should have console port.	Kindly remove this, AP is managed by cotroller and doesn't allow local management	**Amended at Annexure-I.**
39	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 2)	Should have atleast 2 x 10 Gigabit Ethernet interface.	Kindly change it to 4X1G, in distributed architecture data routes locally	No Change. Tender Conditon prevails.
40	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 5)	Controller should have internal hotswapable redundant power supply. In HA mode	Kindly remove this, in case of HA when complete hardware is in redundancy then no need to go with redundant power	**Amended at Annexure-I.**
41	Volume IV, Page 40, Wireless Access Controller Specification (Point no. 11)	The Controller must support interference detection and avoidance for both Wi-Fi and non-Wi-Fi interferes. Quoted Access point must support necessary spectrum analysis functionality to achieve this.	Kindly remove non-wifi interference, AP is working on 2.4 and 5.8 Ghz channel.	**Amended at Annexure-I.**
42	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 29)	WIPS solution should Automatically blacklist clients when it attempt any attack.	WIPS solution should Automatically drop clients traffic when it attempt any attack.	No Change. Tender Conditon prevails.
43	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 30)	WIPS solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an organization's wireless client connecting to rogue AP and also prevent an outside client trying to connect to organizational WLAN.	Please make it "WIPS solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an outside client trying to connect to organizational WLAN.	**Amended at Annexure-I.**
44	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 31)	WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP) as well as windows bridge (client that is associated to AP is also connected to wired network and enabled bridging between two interfaces)	Please make it "WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP)	**Amended at Annexure-I.**
45	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 32)	The system should detect an invalid AP broadcasting valid SSID and should prevent valid clients getting connected from these AP's.	The WIDS system should detect an invalid AP broadcasting with valid SSID	No Change. Tender Conditon prevails.
46	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 34)	For advance forensic WIPS solution should perform spectrum analysis to detect and classify sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.	For advance forensic WIPS solution should perform spectrum analysis to detect sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.	**Amended at Annexure-I.**
47	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 36)	The WIPS solution should able to detect and prevent if a client use FATA-Jack 802.11 DoS tool (Available free on internet) and tries to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.	Please remove this, limited to few vendor	**Amended at Annexure-I.**

48	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 37)	The WIPS solution should detect and protect if a client probe-request frame will be answered by a probe response containing a null SSID to crash or lock up the firmware of any 802.11 NIC.	Please remove this, it is limited to 802.11b/g/n devices, with 802.11ac wave 2 this attack is not possible	**Amended at Annexure-I.**
49	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 39)	The WIPS solution should detect and protect if a client/tool keep on sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF) disconnect all stations on a network for a widespread DoS.	Please remove this. DoS solution prevent all kind of broadcast and multicast attack	**Amended at Annexure-I.**
50	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 40)	The WIPS solution should detect and protect if somebody try to spoof mac address of client or AP for unauthorized authentication.	Please change it to " The WIPS solution should detect and protect if somebody try to spoof mac address of AP for unauthorized authentication.	No Change. Tender Conditon prevails.
51	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 41)	The WIPS solution should detect and protect if a client/tool try deauthentication broadcast attempts to disconnect all clients in range rather than sending a spoofed deauth to a specific MAC address.	Please remove this because with DOS attack to block aal broadcast and multicast request it is not possible to broadcast attack.	**Amended at Annexure-I.**
52	Volume IV, Page 42, Wireless Access Controller Specification (Point no. 42)	The WIPS solution should detect and protect if an attacker attempts to lure a client to a malicious AP using SSID on fake AP in close proximity of the premises. It should detect When the Valid Client probes for Valid SSID and these malicious APs respond and invite the client to connect to them.	Please change it to : WIPS solution able to detect Rogue SSID with same and able to locate the same on map.	No Change. Tender Conditon prevails.
53	Volume IV, Page 42, Wireless Access Controller Specification (Point no. 43)	When client radio is in sleep mode to save battery and AP then begins buffering traffic bound for that client until it indicates that it is awake .The WIPS solution should detect and protect if intruder try sending spoofed frames to the AP on behalf of the original client to trick the AP into believing the client is asleep to buffer the AP beyond limit.	Please remove this, it is supporting specific vendor	**Amended at Annexure-I.**
54	Volume-IV, Page no.-61, List of approved makes for IT Work,/ S. No 3 / Network Management Solution	Network Management Solution: HP/Cisco/Juniper/Brocade	Request for clearification for NMS requirement that only few OEMs provide NMS for both wired and wireless. Is NMS require only for switches or wirless & switches both. Also request to add open NMS venders DMX Everest and Solarwinds.	No Change. Tender Conditon prevails.
55	Volume-IV, Page no.-34, Core Switch specification, Point 11.	Switch should support min 100K IPv4 routes and 6K IPv6 routes. It should suppor t minimum of 6k Multicast Routes.	The asked Multicast Routes is very high considering the campus core switch requirement. Request to kindly modify the multicast routing table to 4K to bidder to propose the right products and solutions addressing the requirements. **Requested Change :** "Switch should support min 100K IPv4 routes and 6K IPv6 routes. It should suppor t minimum of 4k Multicast Routes."	**Amended at Annexure-I.**
56	Volume-IV, Page no.-36, 24 Port Access Switch specification, Point no. 13	The Access Switch should support internal/ external redundant power supply.	External Power Supply unit requires additional Rack Space as a 1U device, optimizing the Rack Space request to consider Internal Power Supply module supported by all OEM. **Requested Change :** "The Access Switch should support internal redundant power supply."	No Change. Tender Conditon prevails.

57	Volume-IV, Page no.-37, 48 Port Access Switch specification, Point no. 13	The Access Switch should support internal/ external redundant power supply.	External Power Supply unit requires additional Rack Space as a 1U device, optimizing the Rack Space request to consider Internal Power Supply module supported by all OEM. **Requested Change :** "The Access Switch should support internal redundant power supply."	No Change. Tender Conditon prevails.
58	Volume-IV, Page no.-37, 24 Port POE+ Access Switch specification, Point no. 1	Access Switch should have 24 ports of 10/ 100/ 1000 PoE/ PoE+ RJ45 and 4 port of 10G fibre based.	Considering in 30watt PoE+ power in all 24 Port, the switch must support 30.4x24 = 730Watt Approx of PoE+ Power to power all Access Point. Requested to mentioned the Poe Power requirements in Switch to all bidder to consider equivalent Switch Models. **Requested Change :** "Access Switch should have 24 ports of 10/ 100/ 1000 PoE/ PoE+ (740 Watt) RJ45 and 4 port of 10G fibre based."	**Amended at Annexure-I.**
59	Volume-IV, Page no.-38, 24 Port POE+ Access Switch specification, Point no. 13	The Access Switch should support internal/ external redundant power supply.	External Power Supply unit requires additional Rack Space as a 1U device, optimizing the Rack Space request to consider Internal Power Supply module supported by all OEM. **Requested Change :**"The Access Switch should support internal redundant power supply."	No Change. Tender Conditon prevails.
60	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 1)	WLAN Cont roller should support minimum of 1500 Access points in a single chassis. If any OEM/ Bidder can't provide WLAN cont roller to suppor t 1500 AP in single RU form factor, mult iple cont rollers must be proposed to meet the requirement from day one. Proposed cont roller should support N+N redundancy from day one.	Considering the Day-1 35 Qty Access Point requirements and future expansion support in single wireless lan access point suggested to consider 512 access point support in single chassis to optimizing the project cost. **Suggested Changes :** "WLAN Cont roller should support minimum of 512 Access points in a single chassis. If any OEM/ Bidder can't provide WLAN cont roller to support 512 in single RU form factor, mult iple cont rollers must be proposed to meet the requirement from day one. Proposed cont roller should support N+N redundancy from day one.	**Amended at Annexure-I.**
61	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 6)	Cont roller should have capacity to handle minimum 20000 or more concurrent devices.	Considering the Day-1 750 User requirements and future expansion support in single wireless lan access point suggested to consider 16k or more concurrent devices support in single chassis to optimizing the project cost. **Suggested Changes :** "Cont roller should have capacity to handle minimum 16000 or more concurrent devices.	**Amended at Annexure-I.**
62	General, Security of Network	Not mentioned	Today it is becooming difficult to protect networks. We would request to add AAA soltion in the network requirements to make the network secured. We are attaching the suggested specifications as well.	No Change. Tender Conditon prevails.

Please note that this Amendment no. – I, shall form part of the tender and all others terms & conditions of the tender shall remain unchanged.

Prospective bidders are advised to regularly scan through HSCC e-tender portal http://www.tenderwizard.com/HSCC as corrigendum/amendments etc., if any, will be notified on this portal only and separate advertisement will not be made for this.

General Manager (IT), HSCC (I) Ltd.
For & on Behalf of Director, AIIMS, New Delhi

Annexure-I

All India Institute of Medical Sciences (AIIMS), New Delhi

AMENDMENT NO. – I

Name of Project: Development of Network Infrastructure for New OPD Block at AIIMS, New Delhi.

S. No	Volume, Page	Tender Document Clause	Amended As
1	Volume-I Page -7, Clause No. 1.6	Last date to fill/upload the tender through e-Tendering is 31/04/2017 upto 14:30 hrs. Opening at 15.00 hrs.	Last date to fill/upload the tender through e-Tendering is 20/04/2017 upto 14:30 hrs. Opening at 15.00 hrs.
2	Volume-IV, Page no.-34, Core Switch specification, Point 11.	Switch should support min 100K IPv4 routes and 6K IPv6 routes. It should support minimum of 6k Multicast Routes.	Switch should support min 100K IPv4 routes and 6K IPv6 routes. It should support minimum of 4k Multicast Routes.
3	Volume-IV, Page no.-37, 24 Port POE+ Access Switch specification, Point no. 1	Access Switch should have 24 ports of 10/ 100/ 1000 PoE/ PoE+ RJ45 and 4 port of 10G fibre based.	Access Switch should have 24 ports of 10/ 100/ 1000 PoE/PoE+ (minimum 360 Watt) RJ45 and 4 port of 10G fibre based.
4	Volume IV, Page 38, Wireless Access Point Specification (Point no. 12)	Access point should have console port.	Access point should have console port or should be able to manage through controller.
5	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 1)	WLAN Cont roller should support minimum of 1500 Access points in a single chassis. If any OEM/ Bidder can't provide WLAN cont roller to support 1500 AP in single RU form factor, multiple cont rollers must be proposed to meet the requirement from day one. Proposed controller should support N+N redundancy from day one.	WLAN Cont roller should support minimum of 500 Access points in a single chassis and in future should be able to support 1500 APs in single/virtual chassis mode. If any OEM/ Bidder can't provide WLAN cont roller to support 500 in single RU form factor, multiple cont rollers must be proposed to meet the requirement from day one. Proposed cont roller should support N+N redundancy from day one.
6	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 6)	Cont roller should have capacity to handle minimum 20000 or more concurrent devices.	Cont roller should have capacity to handle minimum 16000 or more concurrent devices.
7	Volume IV, Page 39, Wireless Access Controller Specification (Point no. 5)	Controller should have internal hotswapable redundant power supply. In HA mode	Deleted

8	Volume IV, Page 40, Wireless Access Controller Specification (Point no. 11)	The Controller must support interference detection and avoidance for both Wi-Fi and non-Wi-Fi interferes. Quoted Access point must support necessary spectrum analysis functionality to achieve this.	The Controller must support interference detection and avoidance for Wi-Fi interferes. Quoted Access point must support necessary spectrum analysis functionality to achieve this.
9	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 30)	WIPS solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an organization's wireless client connecting to rogue AP and also prevent an outside client trying to connect to organizational WLAN.	WIPS solution should be capable of wireless intrusion detection & prevention .The WLAN should be able to detect Rogue AP and take corrective action to prevent the rogue AP. The system should detect and prevent an outside client trying to connect to organizational WLAN.
10	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 31)	WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP) as well as windows bridge (client that is associated to AP is also connected to wired network and enabled bridging between two interfaces)	WIPS solution should detect & prevent an Ad-hoc connection (i.e. clients forming a network amongst themselves without an AP)
11	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 34)	For advance forensic WIPS solution should perform spectrum analysis to detect and classify sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.	For advance forensic WIPS solution should perform spectrum analysis to detect sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.
12	Volume-IV, Page No. 41, Wireless Access Controller, point no. 36	The WIPS solution should able to detect and prevent if a client use FATA-Jack 802.11 DoS tool (Available free on internet) and tries to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.	Deleted
13	Volume IV, Page 41, Wireless Access Controller Specification (Point no. 37)	The WIPS solution should detect and protect if a client probe-request frame will be answered by a probe response containing a null SSID to crash or lock up the firmware of any 802.11 NIC.	Deleted
14	Volume-IV, Page No. 41, Wireless Access Controller, point no. 39	The WIPS solution should detect and protect if a client/tool keep on sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF) disconnect all stations on a network for a widespread DoS.	Deleted
15	Volume-IV, Page No. 41, Wireless Access Controller, point no. 41	The WIPS solution should detect and protect if a client/tool try deauthentication broadcast attempts to disconnect all clients in range rather than sending a spoofed deauth to a specific MAC address.	Deleted

16	Volume-IV, Page No. 42, Wireless Access Controller, point no. 43	When client radio is in sleep mode to save battery and AP then begins buffering traffic bound for that client until it indicates that it is awake .The WIPS solution should detect and protect if intruder try sending spoofed frames to the AP on behalf of the original client to trick the AP into believing the client is asleep to buffer the AP beyond limit.	Deleted
17	Volume IV, Page 43, Firewall Specification (Point no. 9)	NGFW must support virtual Firewall option to have on totally different virtualized firewall if required. Bidder must give license for 5 Virtual Firewalls	Deleted
18	Volume IV, Page 43, Firewall Specification (Point no. 10)	The Firewall solution should support NAT64, DNS64 & DHCPv6	The Firewall solution should support NAT64/Dual Stack/NAT, DNS64/DNS & DHCPv6
19	Volume IV, Page 43, Firewall Specification (Point no. 11)	OEM may have NSS labs recommendation for NGFW for 3 years in a row	OEM may have NSS/Checkmark labs recommendation for NGFW
20	Volume IV, Page 43, Firewall Specification (Point no. 17)	Firewall IPSec VPN throughput should be 14 Gbps.	Firewall IPSec VPN throughput should be 8 Gbps
21	Volume IV, Page 43, Firewall Specification (Point no. 20)	Firewall should support 250000 New sessions per second.	Firewall should support 200000 New sessions per second"
22	Volume IV, Page 44, Firewall Specification (Point no. 23)	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently
23	Volume IV, Page 45, Firewall Specification (Point no. 54)	Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP	Protocol supported: HTTP-POST/HTTP Upload, SMTP
24	Volume IV, Page 46, Firewall Specification (Point no. 58)	Protocols Supported: HTTP-POST, HTTP=GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP	Protocols Supported: HTTPPOST/HTTP Upload, HTTP=-GET/HTTP Doenload, SMTP/ POP3/ IMAP/MAPI/FTP/ NNTP

25	Volume IV, Page 46, Firewall Specification (Point no. 60)	DLP archiving: Records full content in email, FTP, IM, NNTP, and web traffic	DLP archiving: Records full content in email/FTP/ IM/NNTP
26	Volume IV, Page 47, COPPER CABLING SYSTEM, 1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	Mechanical Characteristics: NVP:75-77%	Mechanical Characteristics: NVP:72-76%
27	Volume IV, Page 48, COPPER CABLING SYSTEM, 1.1 CAT6A U/FTP SHIELDEDTWISTED PAIR CABLE	Mechanical Characteristics: Resistance Unbalance: 2% max.	Mechanical Characteristics: Resistance Unbalance: 2-5% max.
28	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Max. Tensile Strength-Short Term @ 3500N	Performance:- Max. Tensile Strength-Short Term @ 2600N
29	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Max. Crush Resistance-Short Term @ 6000N/10 cm	Performance:- Max. Crush Resistance-Short Term @ 4000N/10 cm
30	Volume-IV, Page 53,OPTICAL FIBER CABLING, 2.1.1 6 CORE Single-Mode 9/125 µm OS1 Armoured Multi-Tube Optical Fiber Cable:-	Performance:- Operating Temperature range @ -40°C to +70°C	Performance:- Operating Temperature range @ -20°C to +70°C
31	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Mechanical and Environmental Performance:- Max. Tensile Strength-Short Term @ 3500N	Mechanical and Environmental Performance:- Max. Tensile Strength-Short Term @ 2600N
32	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3	Mechanical and Environmental Performance:- Max. Crush Resistance-Short Term @ 6000N/10 cm	Mechanical and Environmental Performance:- Max. Crush Resistance-Short Term @ 4000N/10 cm

	Armoured Multi-Tube Optical Fiber Cable:-		
33	Volume-IV, Page 55,OPTICAL FIBER CABLING, 2.1.2 6 CORE Multi-Mode 50/125 µm OM3 Armoured Multi-Tube Optical Fiber Cable:-	Mechanical and Environmental Performance:- Operating Temperature range @ -40°C to +70°C	Mechanical and Environmental Performance:- Operating Temperature range @ -20°C to +70°C