भारतीय प्रौद्योगिकी संस्थान तिरुपति
Indian Institute of Technology Tirupati
Renigunta Road, Settipalli Post, Tirupati – 517506
Telephone: 0877- 2503572, Email: purchase@iittp.ac.in

Tender No. IITT/CC/2022-23/18 **Date: 06-June-2022**

NOTICE INVITING TENDER FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF WIRED ACTIVE COMPONENTS

(E-PROCUREMENT MODE ONLY)

CORRIGENDUM-II

The corrigendum is issued to the specifications of the tender as per the below details:

S.No.	TENDER CLAUSE NO.	In place of	To be read as
1	Commissioning Req. (S.No. 3, Pg. No. 7 in Corr: I)	Successful bidder should submit a separate HLD/LLD document WiFi which is validated by OEM.	OEM to prepare and share the HLD & LLD document covering the best practices and provide configuration templates for handholding of remaining devices to be implemented by SI/Bidder . Successful bidder/SI should engage the OEM Professional Services for above scope.
2	N/w functional req. (S.No. 12, Pg. No. 7 in Corr: I)	All devices to have Common Criteria Certification such as EAL/NDPP	All devices/device operating system to have Common Criteria Certification such as EAL/NDPP
3	N/w functional req. (New clause added at S.No. 21, Pg. No. 7 in Corr: I)		As part of the solution, OEM should include and provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); profiling; posture/health check; BYOD, guest management services and TACACS based device administration on a single platform for both wired as well as wireless users from day 1. i)The proposed solution should support all required features to perform above mentioned capabilities for up to 10,000 endpoints with license for 5,000 endpoints from day one. ii) It should allow enterprises to authenticate and authorize

			users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise and it should be able to quarantine any suspicious users on the network using a single console. Solution must help users to securely connect to the organization network from any device, anywhere while restricting access from non-compliant devices. iii) Verification of device posture complies with organization security policy so that risky, unpatched, and outdated devices cannot threaten the network. No network access until endpoint trust is evaluated. iv) Solution should enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services. v) Provides complete guest lifecycle management by empowering sponsors to on-board guests. vi) Proposed solution should include two Virtual appliances to be configured in Active/Standby, necessary hardware for setting up the VM shall be provided by IITT. vii) Solution should deliver customizable self-service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows. viii) Should enforce security policies by blocking, isolating/repairing non-compliant machines in a

			quarantine area without requiring administrator attention. ix) Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers, Certificate Authentication Profiles x) Should utilize standard RADIUS protocol for authentication, authorization, and accounting (AAA) and integrate with existing LDAP seamlessly to have a single source of identity within the complete wired and wireless network. xi) Solution should Include a built-in web console for monitoring, reporting, and troubleshooting to assist helpdesk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network. xii) The solution should have a client-based agent that should support deploying in stealth mode to monitor and enforce posture policies. xiii) For complete integration, the entire solution for access-based policies and control should be from same OEM. xiv) shall have built-in certificate authority (CA) to secure device onboarding without requiring the implementation of an external CA or make changes to an internal public key infrastructure (PKI). xv) Shall support following

			operating systems for endpoint posture checking - Microsoft Windows 7, Apple macOS , Linux - Ubuntu , Linux - RHEL, and Linux - CentOS for security posture checking .
4	OEM criteria. (S.No. 1 Pg. No. 8 in Corr: I)	Similar deployment in India – OEM should have deployed wired networking solutions in at least 3 large CFTIs/publicly listed large enterprise with minimum 250 switches and 5000 LAN nodes and integration with the existing Data centre consisting of 100 compute nodes. All deployments should be successfully working for a minimum of one year as on the date of the bid. Proof to be submitted in the form of Purchase orders/completion certificate from end customer along with contact details of end customer (for verification by IIT).	Similar deployment in India – OEM should have deployed wired networking solutions in at least 3 large CFTIs/publicly listed large enterprises with minimum 250 switches and 5000 LAN nodes. All deployments should be successfully working for a minimum of one year as on the date of the bid. OEM to submit self declaration (on legal letterhead). Proof of the same can be submitted in the form of Purchase orders/completion certificate from the customer end, along with contact details of the customer (for verification by IIT). In addition, OEM shall furnish at least one purchase order copy or proof of contract for AAA/Network Access Control (NAC) solution in India from public sector banks/financial institutions in last three years with minimum 2500 licenses
5	OEM Criteria (S.No. 5, Pg. No. 9, Corr: I)	AMC - AMC to be quoted for a period of 2 years post warranty period and IIT reserves the right to enter into AMC with L1 bidder post warranty period at the prices quoted in the bid. Support during the AMC period will include back lining with OEM, advance replacement of faulty parts, labour and on site support to resolve issues reported by IIT within the SLA defined by IIT. Bidder to undertake preventive maintenance visits once every 6 months and do patch updates and updates to the latest version in the switches during these visits.	AMC - AMC to be quoted for a period of additional 2 years post warranty period, and, in future if needed, IITT reserves the right to enter into AMC with L1 bidder post warranty period at the prices quoted in the bid. However, these 2 years AMC cost shall not be considered for L1 in this RFP. Support during the AMC period will include back lining with OEM, advance replacement of faulty parts, labour and on site support to resolve issues reported by IIT within the SLA defined by IIT. Bidder to undertake preventive maintenance visits once every 6 months and do patch updates

			and updates to the latest version in the switches during these visits.
6	OEM Criteria. (S.No. 7, Pg. No. 9, Corr: I)	OEM participation - OEM should participate via only one authorised partner in this bid. MAF to be provided to the authorised partner and OEM should submit an undertaking that they will support IIT directly if the partner fails to fulfil their contractual obligations with respect to support during warranty or AMC period.	Corrigendum: OEM participation - OEM should participate via authorised partners in this bid. MAF to be provided to the authorised partners and OEM should submit an undertaking that they will support IIT directly/via another authorized partner, if the partner fails to fulfil their contractual obligations with respect to support during warranty or AMC period
7	OEM criteria. (S.No. 13, Pg. No. 10, Table. Row-’Stage3’,’Col3’ in Corr: I)	16 Weeks	24 Weeks
8	Item 1: Core switch (S.No. 1h, Pg. No. 11 in Corr: I)	Switch should support NSF/SSO or Equivalent Technology when connected in virtual stack	Switch should support NSF/SSO or Equivalent/Other stateful switch over Technology when connected in virtual stack
9	Item 1: Core switch (S.No. 3b, Pg. No. 11 in Corr: I)	Switch should support up to 30K multicast routes	Switch should support up to 7K multicast routes
10	Item 1: Core switch (S.No. 3e, Pg. No. 11 in Corr: I)	Switch should support VRF, MPLS, Policy based routing	Switch should support VRF/MPLS, Policy based routing
11	Item 1: Core switch (S.No. 4c, Pg. No. 11 in Corr: I)	Switch should support priority queuing, DSCP, traffic shaping, WRED	Switch should support priority queuing, DSCP, traffic shaping, WRED or equivalent congestion management
12	In Corr: I (S.No. 4b, Pg. No. 12), (S.No. 4b, Pg. No. 17), (S.No. 4b, Pg. No. 19), (S.No. 4b, Pg. No. 21), (S.No. 4b, Pg. No. 23), (S.No. 4b, Pg. No. 25), (S.No. 4b, Pg. No. 26), (S.No. 4b, Pg. No. 30)	Switch shall conform to EN 55022/EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	Switch shall conform to EN 55022/EN 55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.
13	In Corr: I - Item 1: Core switch (S.No. 1i, Pg. No. 11), Item 2: 48-port Dist. switch (S.No. 1h, Pg. No. 14)	Shall support In Service Software Upgrade (ISSU) to provide an upgrade of the entire platform or an individual task/process without impacting	Shall support In Service Software Upgrade (ISSU) or equivalent hitless failover to provide an upgrade of the entire platform or an

		hardware forwarding. ISSU supports upgrades, downgrades, and rollbacks.	individual task/process without impacting hardware forwarding.
14	In Corr: I - Item 1: Core switch (S.No. 5b, Pg. No. 12)	Switch should support VLAN ACL, Port based ACL, Time based ACL	Switch should support VLAN ACL/ Port based ACL/ Time based ACL
15	In Corr: I - Item 1: Core switch (S.No. 5c, Pg. No. 12)	Switch should support IP Source guard, Dynamic ARP inspection, DHCP Snooping	Switch should support IP source guard, DHCP snooping and ARP Inspection or equivalent to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol
16	In Corr: I - Item 1: Core switch (S.No. 5e, Pg. No. 12),	Switch should support real time data collection with line rate hardware based netflow/sFlow/Jflow up to 300 K authentication	Switch should support real time data collection with line rate hardware based netflow/sFlow/Jflow up to 300 K authentication. However, to meet the functional requirement of up to 300K the solution can use 1 or more box.
17	In Corr: I - (S.No. 5f, Pg. No. 12), (S.No. 3i, Pg. No. 15), (S.No. 3h, Pg. No. 17), (S.No. 3h, Pg. No. 19), (S.No. 3h, Pg. No. 21), (S.No.3h, Pg. No. 23), Item 7: 48-port NPoE (S.No. 3h, Pg. No. 25), Item 13: 8-port PoE+ (S.No. 3h, Pg. No. 26)	Switch should have a unique secure identity so that its authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level. (or) During system boots, the system's software signatures should be checked for integrity. System should be capable of understanding that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	During system boots or OS upgrades, the system's software should be checked for integrity.
18	In Corr: 1 - Item 1: Core Switch (S.No. 5n, Pg. No. 12)	Dynamic ARP Inspection	"This clause is removed"
19	In Corr: I - Item 1: Core switch (S.No. 6a, Pg. No. 12)	Switch should support telnet, ssh, https, SNMPv3, IPFIX, configuration rollback feature for ease of management	Switch should support telnet/ssh, https, SNMPv3, sflow/IPFIX, configuration rollback feature for ease of management
20	In Corr: I - Item 1: Core switch (S.No. 6f, Pg. No. 13)	Switch should support beacon/LED technology to identify hardware during troubleshooting	Switch can optionally support beacon/LED technology to identify hardware during troubleshooting
21	Item 1: Core switch (S.No. 6g, Pg.No. 13)	Switch should support AC and DC power supplies	Switch should support AC or DC power supplies

22	In Corr: I Item 1: Core switch (S.No. 6j, Pg. No. 13), Item 2: 48-port dist switch (S.No. 3j, Pg. No. 15)	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+ SSL,SFTP	Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+ , SSL/SSH, SFTP
23	In Corr: I - Item 2: 48-port dist. switch (S.No. 2d, Pg. No. 14)	Switch shall support application visibility and traffic monitoring with minimum 50 K sflow/jflow/netFlow entries.	Switch shall support application visibility and traffic monitoring with minimum 50 K sflow/jflow/netFlow entries. However, to meet the functional requirement of upto 50K entries, the solution can use 1 or more boxes.
24	In Corr: I (S.No. 2f, Pg. No. 14), (S.No. 4d, Pg. No. 17), (S.No. 4d, Pg. No. 20), (S. No. 4d, Pg. No. 21), (S.No. 4d, Pg. No. 23), (S.No. 4d, Pg. No. 25), (S.No. 4d, Pg. No. 27), (S.No. 4d, Pg. No. 30)	The device should be IPv6 ready logo certified from day 1	The device should be IPv6 ready support or logo certified from day one
25	In Corr: I - Item 2: 48-port dist. switch (S.No. 3e, Pg. No. 14)	Switch should support port security, DHCP snooping, first hop security, Spanning tree root guard.	Switch should support port security/DHCP snooping/ first hop security/ Spanning tree root guard or equivalent.
26	In Corr: I (S.No. 5g, Pg. No. 15), (S.No. 5g, Pg. No. 17), Item 5: 48-port PoE+ (S.No. 5g, Pg. No. 20), (S.No. 5g, Pg. No. 23), (S.No. 5g, Pg. No. 25), (S.No. 5g, Pg. No. 30)	Dynamic ARP Inspection	Dynamic ARP Inspection/VXLAN ARP/ND suppression
27	In Corr: I - Item 3: 48-port mGig (S.No. 1b, Pg. No. 15)	Switch shall have 36 number of 2.5G Base-T mGig PoE+ ports and 12 number of 5G Base-T mGig PoE+ ports with minimum 80 Gbps dedicated uplink user bandwidth from Day 1	Switch shall have 36 number of 2.5G Base-T mGig PoE+ ports and 12 number of 5G Base-T mGig PoE+ ports with minimum 2x40 Gbps dedicated uplink user bandwidth from Day 1
28	In Corr: I (S.No. 1e, Pg. No. 16), (S.No. 1e, Pg. No. 18), (S.No. 1e, Pg. No. 20), (S.No 1e, Pg. No. 22)	Should support a minimum 128 Gbps of stacking throughput per switch, with up to 4 switches in a single stack. Required modules and cables to be provided from Day 1	Should support a minimum 320 Gbps of stacking throughput per switch, with up to 4 switches in a single stack. Required modules and cables to be provided from Day 1
29	In Corr: I (S.No. 2e, Pg. No. 16), (S.No. 2e, Pg. No. 18), (S. No. 2e, Pg. No. 21), (S.No. 2e, Pg. No. 22), (S.No. 2e, Pg.	Switch should support at least 15K flow entries	Switch should support at least 15K sflow/Jflow/Nflow entries. However, to meet the functional requirement of upto

	No. 24), (S.No. 2e, Pg. No. 26), (S.No. 2e, Pg. No. 29)		15K entries, the solution can use 1 or more boxes.
30	In Corr: I (S.No. 2f, Pg. No. 16), (S.No. 2f, Pg. No. 18), (S. No. 2f, Pg. No. 21), (S.No. 2f, Pg. No. 22), (S.No. 2f, Pg. No. 24), (S.No. 2f, Pg. No. 26)	Switch should support 128 or more STP Instances.	Switch should support 64 or more STP Instances.
31	In Corr: I (S.No. 3e, Pg. No. 16), (S.No. 3e, Pg. No. 19), (S. No. 3e, Pg. No. 21), (S.No. 3e, Pg. No. 23), (S.No. 3e, Pg. No. 24), (S.No. 3e, Pg. No. 26), Item 13: 8-port PoE+ (S.No. 3e, Pg. No. 29)	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	Switch should support IPv6 Binding Integrity Guard/IPv6 Snooping or equivalent, IPv6 RA Guard, IPv6 DHCP Guard or equivalent, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard or equivalent.
32	In Corr: I - Item 7: 48-port Non-PoE (S. No. 1e, Pg. No. 24), Item-8: 24-port Non-PoE (S.No. 1g, Pg. No. 25)	Switch should support internal field replaceable unit redundant power supply from day 1.	Switch should have an internal field replaceable unit redundant power supply from day 1.
33	In Corr: I - Item 13: 8-port PoE+ (S.No. 1c, Pg. No. 28)	All 24 ports should support PoE (802.3af) and PoE+ (802.3at) with a total PoE power budget of 240W from day-1.	All 8 ports should support PoE (802.3af)/PoE+ (802.3at) with a total PoE power budget of 130W from day-1
33	Item 13: 8-port PoE+ (S.No. 1e, Pg. No. 29)	Should support a minimum 128 Gbps of stacking throughput per switch, with up to 4 switches in a single stack. Required modules and cables to be provided from Day 1	“This clause is removed”
34	Item 13: 8-port PoE+ (S.No. 1g, Pg. No. 29)	Switch should support internal field replaceable unit redundant power supply from day 1.	“This clause is removed”
35	Item 13: 8-port PoE+ (S.No. 2b, Pg. No. 29)	Switch shall have minimum 8K MAC Addresses and 1k VLANs.	Switch shall have minimum 8K MAC Addresses and 512 VLANs.
36	Item 13: 8-port PoE+ (S.No. 2c, Pg. No. 29)	Should support minimum 5K IPv4 routes or more and 1K IPv6 routes or more	Should support minimum 512 IPv4/IPv6 routes or more
37	Item 13: 8-port PoE+ (S.No. 2d, Pg. No. 29)	Switch shall have 1K or more multicast routes.	“This clause is removed”
38	Item 13: 8-port PoE+ (S.No. 2f, Pg. No. 29)	Switch should support 32 or more STP Instances.	Switch should support 16 or more STP Instances.

39	Item 13: 8-port PoE+ (S.No. 3b, Pg. No. 29)	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1	Switch must have functionality like static routing and QoS from Day1
40	Item 13: 8-port PoE+ (S.No. 3e, Pg. No. 29)	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	“This clause is removed”
41	Clause 14, Pg. No. 40 in Corr: I. (New sentence added in the end of the existing Clause)		Within the period of 24 weeks, the liquidated damages shall not be applicable provided the standby stagewise release of temporary items are supplied according to the delivery schedule, and made operational.
42	Clause 15.1, Pg. No. 40 in Corr: I	…..within 16 weeks at IIT Tirupati…	…. within 24 weeks at IIT Tirupati…..

Important Note: All of the aforementioned clauses and their changes are to be applied to their respective clauses in “Technical Compliance” Section of the Corrigendum - I (Corr: I)

Sd/-
Deputy Registrar