भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान मोहाली

शिक्षा मंत्रालय, भारत सरकार द्वारा स्थापित

सैक्टर 81, नॉलेज सिटी, प० ओ० मनोली, एस० ए० एस० नगर, मोहाली, पंजाब - 140306

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH MOHALI

(Estd. By Ministry of Education, Govt of India)

Sector-81, Knowledge city, PO-Manauli, SAS Nagar Mohali-140306, Punjab

PAN No. - AAAAI1781K GST No. 03AAAAI1781K2ZS

● Phone : +91-172-2240121 ● Fax : +91-172-2240124, 2240266 ● http://www.iisermohali.ac.in ● Email: stores@iisermohali.ac.in

CPPP/Institute Website

IISERM(1726)26/27-Pur. **Dated: 29.10.2026**

शुद्धिपत्र -II / CORRIGENDUM –II

Refer to IISER Mohali e-Tender notice Ref. No. IISERM(1726)26/27-Pur. dated 19.09.2026 for "**Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure",** Knowledge City, PO. Manauli S.A.S. Nagar, Mohali, Punjab-140306.

The on-line submission of bid date is further extended due to amendment with date extension in partial modification in the referred NIT/tender, **as per below schedule**:

In line of tender IISERM (1726)26/27-Pur, a pre-bid meeting was held on 05th October 2026 and 14th October 2026 as per the Page#7, Clause#25 Section-C of NIT and as per the General Condition#6 of General Condition, as well Corrigendum – 1. Following firms participated

Sln	Firm	Meeting	Joined on
01	M/S Arsenal Info Solutions Pvt. Ltd.	Pre-Bid-1	05-10-2026
02	M/S Black Box Limited	Pre-Bid-1	05-10-2026
03	M/S Bright Technologies & Computers Pvt. Ltd.	Pre-Bid-1	05-10-2026
04	M/S D-Link India Limited	Pre-Bid-1	05-10-2026
05	M/S Echelon Edge Pvt. Ltd.	Pre-Bid-1	05-10-2026
06	M/S EZDAT Technologies Pvt. Ltd.	Pre-Bid-1	05-10-2026
07	M/S F5 Network India	Pre-Bid-1	05-10-2026
08	M/S Fortinet Inc.	Pre-Bid-1	05-10-2026
09	M/S Genius Networks	Pre-Bid-1	05-10-2026
10	M/S HTIS Telecom Private Limited	Pre-Bid-1	05-10-2026
11	M/S IDream Networks Pvt. Ltd.	Pre-Bid-1	05-10-2026
12	M/S Ingram Micro India Pvt. Ltd.	Pre-Bid-1	05-10-2026
13	M/S Molex India Pvt. Ltd.	Pre-Bid-1	05-10-2026
14	M/S Momentum Techsys Pvt. Ltd.	Pre-Bid-1	05-10-2026
15	M/S Netgear Inc.	Pre-Bid-1	05-10-2026
16	M/S NETIP Technologies Private Limited	Pre-Bid-1	05-10-2026
17	M/S Nitcon Ltd.	Pre-Bid-1	05-10-2026
18	M/S Palo Alto Networks Limited	Pre-Bid-1	05-10-2026
19	M/S Railtel Limited	Pre-Bid-1	05-10-2026
20	M/S Ruckus Networks	Pre-Bid-1	05-10-2026
21	M/S Techfacto Global Services Pvt. Ltd.	Pre-Bid-1	05-10-2026
22	M/S NETIP Technologies Private Limited	Pre-Bid-2	14-10-2026
23	M/S EZDAT Technologies Pvt. Ltd.	Pre-Bid-2	14-10-2026
24	M/S Molex India Pvt. Ltd.	Pre-Bid-2	14-10-2026

25	M/S Fortinet Inc.	Pre-Bid-2	14-10-2026
26	M/S Kesari Infotech	Pre-Bid-2	14-10-2026
27	M/S Corporate Infotech (P) Ltd.	Pre-Bid-2	14-10-2026
28	M/S Railtel Corporation of India Ltd.	Pre-Bid-2	14-10-2026
29	M/S Takyon Networks Ltd.	Pre-Bid-2	14-10-2026
30	M/S We Excel Software Pvt Ltd.	Pre-Bid-2	14-10-2026
31	M/S Arsenal Info Solutions Pvt. Ltd.	Pre-Bid-2	14-10-2026
32	M/S Genius Networks	Pre-Bid-2	14-10-2026
33	M/S Higher India Pvt Ltd.	Pre-Bid-2	14-10-2026
34	M/S Ruckus Networks	Pre-Bid-2	14-10-2026

As per the requests/queries received on or before pre-bid meeting and on the day of pre-bid meeting, clarification & additional information is provided through this document. Bidders/SI/OEM must comply with all conditions and specs as per this document as well as all other documents along with the original NIT document. Please check carefully all the sections (NIT and Prebid answers) for more detailed explanations wherever it is applicable. No further queries will be entertained.

1. Technical evaluation shall be made strictly based on the original terms and conditions of NIT as well as this document.
2. The replies to the questions from the vendors also form a part of NIT.
3. No verbal communication shall be part of any justifying conditions.

In view of this, all vendors and bidders are required to fully comply with our requirements as per technical specifications as expressed in original NIT, corrigendum and associated annexures.

Amendments:

1. The number of ports specified for each interface type (Ethernet Base-T, SFP, SFP+, QSFP+, QSFP28, etc.) shall be the minimum requirement. Bidders may offer equipment with the same or higher number of ports of the specified type, subject to compliance with all other technical specifications.
2. Any software, firmware, or protocol version specified shall be treated as the minimum requirement. Bidders may offer the same or a higher/latest version, provided all specified functionalities and compatibility requirements are met.
3. Bidders may offer additional certifications, features, functionalities, or test reports in addition to those specified in the tender document. However, such additional offerings shall not be considered for comparative technical evaluation or assigned any additional technical advantage beyond the criteria expressly specified in the tender document. The product/solution offered shall, in all cases, comply with all mandatory requirements, specifications, functionalities, features, certifications, and other terms and conditions stipulated in the tender document.

Sl. No.	Page No. in NIT	Item No. in NIT	Specifications in NIT	Amendment
1	32,33, 60,61, 74,83, 85,87, 89	Section – 4: List of Materials Sl. No 1, 2, 3, 4, 5, 6, 7, 8, 9 Item No. 1.1, 1.2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, Sl. No 10 Item No. 2.8, Annexure – 8: Make and model number of all materials listed in section Sl. No 2 Item No. 1.2, Sl. No 3 Item No. 2.1, Sl. No 3 Item No. 2.1, Sl. No 5 Item No. 2.3, Sl. No 6 Item No. 2.4, Sl. No 7 Item No. 2.5, Sl. No 8 Item No. 2.6, Sl.	7 Year Warranty	Please refer to the corrigendum -1 dated 8/10/2026

		No 9 Item No. 2.7, Sl. No 10 Item No. 2.8, Annexure – 9: Specifications as per the Section – 4 List of Materials Spec No.1.2, Sl. No 2.1, Sl. No 2.2, Sl. No 2.3, Sl. No 2.4		
2	38	General Conditions, Clause 3, Sl. No 3	Transceivers 430 Nos	Please refer to the corrigendum -1 dated 8/10/2026
3	57	Annexure – 7: Service Level Agreement (SLA) Sl. No 1	The entire solution including each software, firmware and hardware component should have at least 7 years on-site NBD warranty. The vendor will be required to attend the complaint if any within two business-days.	The entire solution including each software, firmware and hardware component should have at least 5 years on-site warranty along with 3 years CAMC with NBD. The vendor will be required to attend the complaint if any within two business-days.
4	57	Annexure – 7: Service Level Agreement (SLA) Sl. No 9	All the components should have at least 7 years of End-of-life.	All the components should have at least 8 years of End-of-life.
5	32, 60, 69	In Section -4: In Annexure – 8: Make and model number of all materials listed in section Sl. No 1 Item No. 1.1, and in Annexure - 9:	Next Generation Firewall (NGWF): NGFW Firewall 4 x 100GE/40GE QSFP28 slots, 10 x 25GE/10GE SFP28 slots, 10 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing;HA support; SIEM integration; 7 Year Warranty	Should be read as "*Next Generation Firewall (NGWF): NGFW Firewall at least 2 x 40G/100G QSFP/QSFP28 slots, at least 10 x 10GE SFP/SFP+ slots, at least 12 x 1G/2.5G/5G/10G RJ45 ports, at least 4 x* 25G SFP28, *Dedicated management and HA ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing; HA support; SIEM integration;*" For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
6	69	Annexure – 9: Specifications as per the Section – 4 List of Materials 1.1	Next Generation Firewall (NGWF): NGFW Firewall 4 x 100GE/40GE QSFP28 slots, 10 x 25GE/10GE SFP28 slots, 10 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and	Should be read as "*Next Generation Firewall (NGWF): NGFW Firewall at least 2 x 40G/100G QSFP/QSFP28 slots, at least 10 x 10GE SFP/SFP+ slots, at least 12 x 1G/2.5G/5G/10G RJ45 ports, at least 4 x* 25G SFP28, *Dedicated management and HA ports, and dual AC power supplies with Unified Threat Protection (UTP) (IPS, Advanced Malware*

			Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing; HA support; SIEM integration; 7 Year Warranty (Quantity: 2 Number)	*Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and Premium), Firewall throughput: >40Gbps; NGFW throughput: >20Gbps, threat protection throughput: >10 gbps; concurrent session: 10-20 million; New sessions/sec: >200k; SSL/TLS inspection for all packets; IPv6 support; User identity integration (LDAP); should be integrated to AAA, Radius and other standard network softwares, BGP/OSPF dynamic routing; HA support; SIEM integration;*" For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
7	73	Annexure – 9: Specifications as per the Section – 4 List of Materials Spec No 1.1.3.3	NGFW hardware should have 7 years RMA warranty	Please refer to the corrigendum -1 dated 8/10/2026
8	84, 87, 89, 91, 93, 96, 97,	Annexure – 9: Specifications as per the Section – 4 List of Materials Spec No. 2.1.10, Spec No. 2.2.10, Spec No. 2.3.10, Spec No. 2.4.10, Spec No. 2.5.10, Spec No. 2.6.10, Spec No. 2.7.10	7 year TAC support and comprehensive warranty should be provided by the OEM.	8 year TAC support and comprehensive warranty should be provided by the OEM.
9	91	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 2.5	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 10 Number)	Should be read as : "*AS Switch Type-2: Access Switch/Edge Switch: 48 × 100/1000Base-T RJ45 ports; 4 × 10/25G SFP28 uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps ;field replaceable redundant power supplies and FANs*" For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
10	93	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 75 Number)	Should be read as : "*AS Switch Type-3: Access Switch/Edge Switch: 24 × 100/1000 Base-T RJ45 ports; 4 × 10/25G SFP28 uplink ports; Layer-3 managed switch; Switching capacity at least 248 Gbps ;field replaceable redundant power supplies and FANs*" For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
11	96	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 2.7	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching	Should be read as : "*AS Switch Type-4: Access Switch/Edge Switch: 16 × 100/1000Base-T RJ45 ports; 2 × 1G/10G SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72 Gbps*

			capacity at least 72gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 2 Number)	*;field replaceable redundant power supplies and FANs "* For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
12	97	Annexure – 9: Specifications as per the Section – 4 List of Materials	7 years OEM TAC support & 7 years warranty shall be provided by the OEM	8 years OEM TAC support & 5 years warranty along with 3 years CAMC shall be provided by the OEM
13	97	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 2.8	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps; field replaceable redundant power supplies and FANs 7 Year Warranty (Quantity: 4 Number)	Should be read as : *"AS Switch Type-5: Access Switch/Edge Switch: 8 × 100/1000Base-T RJ45 ports; 2 × 1G/10G SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72 Gbps ;field replaceable redundant power supplies and FANs "* For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
14	101, 102	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No. 2.15.8, Sl. No. 2.16.8, Sl. No. 2.17.8	Onsite OEM Warranty (Year) 7	Please refer to the corrigendum -1 dated 8/10/2026
15	104	Annexure – 9: Specifications as per the Section – 4 List of Materials Spec No. 3.1.6	Mandatory Compliance: All switches, NMS, Transceivers, AAA should be from the same OEM for better interoperatability, management and support	All switches should be from the same OEM for better interoperatability, management and support, whereas the software may not be from say OEM but must be compatible in all functionality and features required by the tender.
16	20	General Conditions, Section- 5, Sl. No. 3	L2 Switches	Should be read as *"L2 Switches / L3 Switches with Base-T ports and Fibre uplinks"*
17	116	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No. 3.8.20.15	Server should be provided with 7 Years 24x7x365 Support Directly from OEM. The 7-years support Undertaking should be submitted along with the Bid specific to this tender and the support warranty document at the time of supply of material is required.	Solutions should be provided with 5 Years warranty along with 3 years CAMC of 24x7x365 Support Directly from OEM. The 8-years support Undertaking should be submitted along with the Bid specific to this tender and the support warranty document at the time of supply of material is required.
18	145	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No.6.1 .3	The manpower deployment shall initially be for six (06) months, extendable up to one (01) year based on satisfactory performance and organizational requirement. The quoted total cost for six (06) months shall be considered for determining L1.	Should be read as *"One manpower deployment shall initially be for six (06) months, extendable up to one (01) year based on satisfactory performance and organizational requirement. The quoted total cost of one (1) man-power for six (06) months shall be counted for determining L1. "*
19	60,74	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No1.2	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator,	Should be read as : *"Application Delivery Controllers (ADC) 4x10G/1G RJ45 + 4x1G SFP+/SFP28/SFP ports upgradable to 25G, 1 x 120GB SSD storage, Hardware SSL*

			Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty (Quantity: 2 Number)	*Accelerator, Optional Redundant PSU , Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service;"* For warranty related clause, please refer to the corrigendum -1 dated 8/10/2026
20	60,83	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No2.1	Core Switch (CS): Core Switch Supply of Layer 3, 32 Port x 40/100 Gbps SFP port core switch; Switching capacity: at least 6Tbps; with field replaceable redundant power supplies and FANs; 7 Year Warranty; (Quantity: 2 Number)	Should be read as : *"Core Switch Supply of Layer 3, at least 32 × 40/100G QSFP+/QSFP28 ports core switch; Switching capacity: at least 6.4Tbps; with field replaceable redundant power supplies and FANs;*"
21	60,87	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No2.3	Distribution Switch (DS) Type - 2: DS Switch Type-2: Distribution Switch Supply of Layer 3, 24-port SFP28 10/25 G, with 4x-port 40/100GbE; Switching capacity: at least 2Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty, (Quantity: 10 Number)	Should be read as : "*DS Switch Type-2: Distribution Switch Supply of Layer 3, 24x 1G/10G SFP+ Ports, with 4x-port 40/100GbE; Switching capacity: at least 1 Tbps; field replaceable redundant power supplies and FANs*"
22	108	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 3.7.9	Support for SNMP v1-3, IPv4/IPv6 address range, SNMP Smartscan, hosts file	Should be read As *"Support for SNMP v1-3, IPv4/IPv6 address range, SNMP Smartscan (or equivalent), hosts file*
23	108	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 3.7.11		WMI or equivalent
24	107	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 3.7.2	The NMS shall be able to diagnose its own faults by running diagnostic software	Should be read as *"The NMS shall be able to diagnose its own faults by running diagnostic software or equivalent tools shall be provided"*
25	108	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 3.7.11	MIB Walker, MIB Explorer and MIB Manager	Should be read as *"MIB Walker, MIB Explorer and MIB Manager or equivalent tools"*
26	71	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 1.1.2.8	The proposed solution should support remote user based VPN clients for Windows. Module should be Common Criteria certified for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	Should be read as *"The proposed solution should support remote user based VPN clients for Windows. Module should be Common Criteria certified for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 (equivalent or better) Protection Profile for Application Software Version 1.4 (equivalent or better)"*
27	73	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 1.1.4.1	ISO 27001, ISO 27017, ISO 42001	should be read as *"ISO 27001, ISO 27017, ISO 42001 (or equivalent to ISO 42001 standard)*
28	73, 74	Annexure – 9: Specifications as per the Section – 4 List of	h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection	Should be read as "*h. Common Criteria for NGFW, following criteria must be validated:*

		Materials Sl. No 1.1.4.6	Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625; Functional Package for SSH Version 1. 0 PP-Module for Intrusion Prevention Systems (IPS), Version 1. 0 PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 collaborative Protection Profile for Network Devices Version 3. 0e i. Common Criteria for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	*collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 (equivalent or higher) ; Functional Package for SSH Version 1. 0 (equivalent or higher) PP-Module for Intrusion Prevention Systems (IPS), Version 1. 0 (equivalent or higher) PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 (equivalent or higher) collaborative Protection Profile for Network Devices Version 3. 0e (equivalent or higher) i. Common Criteria for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 (equivalent or higher) Protection Profile for Application Software Version 1.4 (equivalent or higher)* "
29	103, 104	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 3.1.5.1	Perpetual license with 7 Year OEM TAC and OS support for all licenses and Software. All software and Hardware should be included in the solution for 20000 users	Should read as *"Perpetual license with 8 years (5 Years warranty along with 3 years CAMC) of OEM TAC and OS support for all licenses and Software. All software and Hardware should be included in the solution for 20000 users*
30	82	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 1.2.9.2	The WAF solution should be in the Gartner's/Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.	Should be read as *"The bidder shall provide documentary evidence of independent third-party evaluation/recognition of the proposed WAF/WAAP solution by a reputed international cybersecurity analyst/research organization. Such evidence may include Gartner, Forrester or equivalent reports."*
31	52	Annexure - 3, Clause - 5	OEM should be ISO 27001, ISO 27017, ISO 42001, Common Criteria/ISO-IEC 15408 & IPv6/ certification (IPv6 Logo & interoperability certification)	Should be read as *"OEM should be ISO 27001, ISO 27017, ISO 42001 (or equivalent to ISO42001 standard), Common Criteria/ISO-IEC 15408 & IPv6/ certification (IPv6 Logo & interoperability certification)"*
32	117	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 4.1.4	96 core (6/8 Fiber per tube)	Should be read as *"96 core (6/8/12 Fiber per tube)"*
33	117	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 4.1.5	Water Jell	Should be read as "*Water Jelly or cable Jelly or water blocking gel*"
34	101	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 4.1.12	ISO. IEC 11801 - 2nd Edition, type OS2; AS/ACIF S008; AS/NZS 3080, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor	Should be read as "*ISO. IEC 11801 - 2nd Edition, type OS2, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor ducts, direct burial and*

			ducts, direct burial and backbone cabling, RoHS Complaint	*backbone cabling, RoHS Complaint*"
35	103	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 4.2.12	ISO. IEC 11801 - 2nd Edition, type OS2; AS/ACIF S008; AS/NZS 3080, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor ducts, direct burial and backbone cabling, RoHS Complaint	Should be read as "*ISO. IEC 11801 - 2nd Edition, type OS2, ITU-T REC G 657A1 spec for Low Water Peak fiber, IEC 60793/60794-1 Telecordia (BELLCORE) GR 20 STDS, suitable for use in indoor / outdoor ducts, direct burial and backbone cabling, RoHS Complaint*"
36	105	Annexure – 9: Specifications as per the Section – 4 List of Materials Sl. No 4.3.8	End to End Structured Cabling Products from Single Brand and Single OEM. OEMs should have once RCDD / CDCP in India	Should be read as "*End to End Structured Cabling Products from Single Brand and Single OEM. The OEM/Bidder shall demonstrate experience in design and implementation of structured cabling/ICT infrastructure of comparable scale and shall have at least one RCDD-certified or CDCP-certified or equivalently qualified ICT infrastructure design professional based in India*."
37	21	Section-2: Objective, Point No. 02	The design and implementation of the entire Core Network Infrastructure shall be as per Error! Reference source not found.	Should be read as "*The design and implementation of entire Core Network Infrastructure shall be as per 1) Annexure – 10: Building-wise Layout Schematics.*"
38	22	Section – 3: Scope of Work, Point No. 1 (b)(i)	Campus Network Architecture – Prepare a comprehensive architecture illustrating the overall design and hierarchical structure of the campus network based on site survey and as per document Error! Reference source not found.	Should be read as "*Campus Network Architecture – Prepare a comprehensive architecture illustrating the overall design and hierarchical structure of the campus network based on site survey and as per document Annexure – 10: Building-wise Layout Schematics*"
39	54	Annexure – 5: Check List to be submitted by Bidder/OEM, Sl. No. 13	Point by point compliance of all components Annexure – 8: Make and model number of all materials listed in section 4 and Error! Reference source not found.	Should be read as "*Point by point compliance of all components Annexure – 8: Make and model number of all materials listed in section 4 and Annexure – 9: Specifications as per the Section – 4 List of Materials"*

The Specification for BoQ items 7.21 is as follows:

7.21	CAT6A Mounting Box : Mounting Box / Backbox for Face Plate (Quantity: 40 Number)		
Sln	Specifications		Compliance (Y/N)
7.21.1	Surface Mounting Box of the same OEM if manufactured by OEM or equivalent good brand (Anchor & Havells or Equivalent Manufacture) if not manufactured by OEM or sample may be approved by Customer before Delivery.		
7.21.2	Size	3 X 3	

Revised date and Time:

S. No.	Description	Current Date	Extended Due date/Time
01	**Closing Date & Time (Online) submission**	**30th October 2026**	**05th November 2026 upto 02:00 PM**
02	**Opening Date & Time of Technical Bid**	**31st October 2026**	**06th November 2026 upto 02:30 PM**

For any information, other modifications and/or corrigendum may kindly visit IISER Mohali websites http://www.iisermohali.ac.in/ & cppp portal https:/eprocure.gov.in/eprocure/app

Sd/-
सहायक कुलसचिव (क्रय तथा भंडार)
Assistant Registrar (Stores & Purchase)

Answers to pre-bid (IISERM(1726)26/27-Pur) queries:

Query - 1 (M/S Intecinfonet on 29/09/2026)

Sr. No.	Tender Section	Existing Clause	Pre-Bid Query / Clarification Requested/ Suggested Changes	Response
1	Section – 5: General Conditions, Clause 3, Page 37	Past performance: the bidder shall have successfully completed during the last seven years one or more Campus Wide Network (LAN) projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions.	Past performance: the bidder shall have successfully completed during the last seven years one or more Campus Wide Network (LAN) projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions.	Remain unchanged
			Request you to change to	
		Bidder must satisfy both A & B	**Bidder must satisfy both A & B**	
		A. The bidder shall satisfy any one of the following:	**A. The bidder shall satisfy any one of the following:**	
		a) One completed project involving at least 80% of the quantities listed below in table - 1; or	a) One completed similar project of value INR 12 Crore or more ; or	Remain unchanged
		b)Two completed projects, each involving at least 60% of the quantities listed below in table - 1; or	b)Two completed similar projects of value INR 7.5 Crore or more; or	Remain unchanged
		c) Three completed projects, each involving at least 40% of the listed below in table - 1:	c) Three completed similar projects of value INR 6 Crore or more:	Remain unchanged

				Similar Project mean Supply & Installation of Active & Passive Campus Wide Network (LAN) projects which includes L3 Switches, L2 Switches, OFC & UTP.	
		Table - 1			
		Firewall/ADC	2 Nos		
		L3 Fibre Switches	30 Nos		
		L2 Switches	80 Nos		
		OFC Laying	8000m		
		Transceivers	430 Nos		Please check the Amendment corrigendum - 1
		I/O ports as Last-mile connection	1000 Nos		
2	Section – 5: General Conditions, Caluse 3, Page 37	B. The bidder should have supplied and deployed software stack (Item numbers 3.1 to 3.9 in Section – 4: List of Materials.		B. The bidder should have supplied and deployed any 3 software stack from Item numbers 3.1 to 3.9 in Section – 4: List of Materials.	Remain unchanged
3	Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI), Page 50, Clause 1 & 4	As per Clause 1, Bidder should be ISO 9001:2015 certified. As per Clause 4, Bidders should be ISO 9001:2015, 27001:2013 and 20000- 1:2011 certified and shall have a minimum CMMI Level 3 or above for Quality Management Systems. For providing Solutions and Services for Network, Router, Switches, Firewall, Cabling etc.		Please clarify, which all Certificates are required.	All certifications are required

4	Annexure – 1: Eligibility Criteria of Bidder/ System Integrator (SI), Page 50, Clause 3	The bidder shall have successfully completed during the last seven years one or more Campus Wide Network projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions. (Appropriate document should be provided)	This Eligibility Criteria Contradict to clause mentioned in Section – 5: General Conditions, Clause 3, Page 37. As per this clause mentioned here, a customer is asking for one or more Campus Wide Network projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment, whereas in Section- 5 , you are asking for 2 types of qualification mentioned as A & B and both need to be qualified. Please clarify which criteria need to be met.	They are not contradicting, one tells what exactly is required and other tells how such experience would be counted. For clarity: Both A& B in the Section – 5: General Conditions, Clause 3 requires to be met by the bidder.

Query - 2 (M/S Tech-Bridge on 29/09/2026)

Sr.	RFP Page No.	RFP Clause No.	Clause / Clause Title	Queries / Clarification / Suggestion	Justification by Bidder / OEM or Remarks	Response
1	104	Mandatory Compliance	All switches, NMS, Transceivers, AAA should be from the same OEM for better interoperability, management and support	We request the Authority to kindly relax the requirement of sourcing Switches, NMS, Transceivers, and AAA solutions from the same OEM. While switches and transceivers may be sourced from the same OEM to ensure hardware compatibility, NMS and AAA are independent software solutions that can seamlessly integrate with network hardware from different OEMs through industry-standard protocols such as SNMP, RADIUS, TACACS+, and APIs.	Justification: All switches and transceivers shall be from the same OEM. NMS and AAA solutions may be offered from different OEMs, provided they are fully interoperable and compatible with the proposed network infrastructure. The bidder shall ensure end-to-end integration, management, and support for the complete solution." This amendment will encourage wider OEM participation while ensuring interoperability,	All switches should be from the same OEM for better Interoperability, management and support, whereas the software may not be from say OEM but must be compatible in all functionality and features required by the tender. Please check the amendment (refer to Corrigendum - II)

				Mandating a single OEM for hardware, NMS, and AAA may restrict competition, limit technological flexibility, and prevent bidders from offering best-of-breed solutions.	centralized management, and single-point accountability for the complete solution	

Query - 3 (M/S Echelon Edge Pvt. Ltd on 02/10/2026)

S.No	RFP Section	RFP Page No.	Content in the RFP	Clarification sought	Response
1	3.1 : AAA Server.	104	All switches, NMS, Transceivers, AAA should be from the same OEM for better interoperability, management and support.	As envisaged in the RFP, the Department's objective is to deploy a unified NMS that provides end-to-end visibility and management across Fault, Configuration, and Performance Management (FCAPS), Application Performance Monitoring (APM), and Cloud Monitoring from a single platform. In line with this objective, a heterogeneous, multi-vendor COTS NMS is better suited than an OEM-specific management tool. The RFP scope extends beyond network devices to servers, applications, databases, and cloud workloads. Active-device OEM tools are primarily designed to manage their own hardware, whereas a heterogeneous NMS correlates events across all layers from a single console. It also protects the Department's investment: as the infrastructure grows through expansion or technology refresh, devices from other OEMs can be onboarded without replacing the NMS or adding separate monitoring tools. This provides one consistent framework for inventory, topology, alarms, SLAs, and reporting, and avoids long-term lock-in to a single vendor's licensing and support cycles. Since these capabilities are delivered through open, industry-standard protocols and interfaces (SNMP v1/v2c/v3, CDP/LLDP,	All switches should be from the same OEM for better Interoperability, management and support, whereas the software may not be from say OEM but must be compatible in all functionality and features required by the tender. Please check the amendment (refer to Corrigendum - II)

				NetFlow/sFlow/IPFIX, Syslog, WMI, SSH, REST APIs), interoperability with the offered switches, transceivers, and AAA is ensured irrespective of OEM. Mandating the NMS from the same OEM as the active devices would therefore limit the Department's ability to achieve its unified monitoring objective and restrict participation by specialized NMS OEMs. We kindly request the Department to: Exclude the NMS from the "same OEM" requirement applicable to switches, transceivers, and AAA, and allow it to be proposed from a specialized NMS OEM. The NMS must comply with the required standard protocols and demonstrate interoperability with the offered active devices. Amend NMS specifications that reference OEM-specific features or terminology into functional, standards-based requirements for a heterogeneous COTS NMS covering FCAPS, APM, and Cloud Monitoring. Define integration with the offered active devices as interoperability through standard protocols and APIs rather than as a same-OEM mandate.	
2	3.7 : Network Management System (NMS):	107	The NMS shall be able to diagnose its own faults by running diagnostic software	The term "diagnostic software" is open to interpretation and may be construed as a specific or proprietary tool. As per industry practice, the requirement is better met by the NMS platform natively monitoring its own health. This includes its services, processes, database, polling engines, and resource utilization (CPU, memory, disk), with alarms generated on any fault or degradation. We request the Department to confirm this understanding and amend the clause as follows: "The NMS shall support self-monitoring of its own application components and services. The NMS shall also provide built-in troubleshooting utilities such as Ping, Traceroute, and SNMP Walk for ease of diagnosis."	Please check the amendment (refer to Corrigendum - II)

3	3.7 : Network Management System (NMS):	108	WMI application monitoring	WMI is applicable to Windows-based workloads. It is suited to monitoring process, performance counters, and event logs of Windows. It does not extend to applications on Linux, containerized, or cloud-native platforms. Comprehensive application monitoring across heterogeneous environments is achieved through REST API-based and Open Telemetry-based methods. These provide standardized, scalable observability, including transaction monitoring and cloud monitoring. To ensure complete application coverage in line with the RFP's APM requirements, we request the Department to amend the clause as follows: Application monitoring using WMI (for Windows-based applications) and REST API / agent-based / Open Telemetry-based methods for other application environments.	Please check the amendment (refer to Corrigendum - II)
4	3.7.9 Discovery Features	108	3.7.9.1: Support for SNMP v1-3, IPv4/IPv6 address range, SNMP Smartscan, hosts file	The terms "SNMP Smartscan" and "hosts file" refer to discovery features specific to a particular OEM's product. Mandating them restricts participation to a single OEM. For the fair and wider participation please amend the clause as below "The solution should be able to automatically discover network devices and assets using standard industry protocols such as SNMP (v1/v2c/v3), ICMP/ping discovery etc. ."	Please check the amendment (refer to Corrigendum - II)
5	3.7.11 Monitoring Features	108	3.7.11.3: MIB Walker, MIB Explorer and MIB Manager	MIB Walker", "MIB Explorer" and "MIB Manager" are product-specific functions names used by particular OEMs. Making them mandatory requirements effectively limits the tender to a single OEM and restricts other OEMs from bidding. For wider participation, request to remove such OEM specific clauses.	Please check the amendment (refer to Corrigendum - II)

6	3.7.12: Management Console, Alerts Notification and Reporting Features:-	108	3.7.12.1: Web and Windows based management console	A mandatory Windows-based console favours OEM specific function . Web access is more secure and platform-independent. Request to amend the clause as below for wider participation 'The solution should provide a secure web-based management console accessible via standard browsers.	Both required
7	6) Network Software Stack	28	VIII: Inventory Management – Implement an inventory management system for maintaining an up-to-date database of all active network assets and software licenses.	The Institute is establishing a centrally managed campus network to be operated and supported over a 7-year period. For effective operations, the Department may consider IT Incident Management to track the complete lifecycle of every fault as a ticket, from NMS alarm through assignment, escalation and resolution to closure. This provides accountability, a complete audit trail and resolution history. Since Cl. 6(viii) itself calls for an up-to-date database of all active network assets and software licenses, a CMDB auto-populated from NMS discovery is the most direct way to meet its intent. It keeps asset, warranty and EoL records and is linked to incidents. We therefore request the Institute to include an ITIL-aligned ITSM module (Incident Management and CMDB)	Inclusion of this will create more restriction, binders may provide such functionality with no additional cost. Remain unchanged
8	Management Console, Alerts Notification and Reporting Features:-	108	3.7.12.13 Inventory or other device specific information		Remain unchanged
9	3.7.12 : Management Console, Alerts Notification and Reporting Features:	109	3.7.12.5: Mobile Interface with one-click log-in	The Mobile Interface with one-click log-in function is OEM specific. Also one-click log-in feature into NMS is the amplified risk of unauthorized full-system access and does not align with security best practices. Request to amend the clause to make it generic for wider participation The NMS should provide a web-based login functionality with CAPTCHA-based authentication, accessible through standard browsers over	It is a must have requirement. Remain unchanged
10	3.7.12 : Management Console, Alerts Notification and	109	3.7.12.8: Real-time split second and historical graphs	The Real-time split second and historic graph is an OEM specific function. We request you to please amend the clause for wider participation of proven OEMs.	May provide near real-time performance.

	Reporting Features:			The solution should provide near real-time and historical performance graphs for monitored parameters (such as bandwidth, utilisation, latency, packet loss, CPU and memory), with a configurable polling interval, and the ability to view trends by hour, day, week, month and year.	
11	3.7 : Network Management System (NMS):	109	Should provide an IP/Mac finder tool to locate an IP or Mac address on a network from the console.	This requirement of a dedicated "IP/MAC finder tool" is an OEM-specific feature, which unnecessarily restricts participation. We request to relax this clause or amend as below to make it generic and for wider participation…. The NMS should have operation tool i.e. Ping, Traceroute, and SNMP Walk for ease of diagnosis.	It is a widely open feature available in several open source tools, thus not restrictive. Remain unchanged
12	3.7 : Network Management System (NMS):	109	Cloud Monitoring	Kindly share the list of cloud platforms to be integrated for cloud monitoring, along with the number of API calls per cluster/account expected for accurate sizing and licensing.	The name of the cloud service is mentioned in spec and it is required to use native API so does not need API counts.
13	3.7 : Network Management System (NMS):	110	Network Traffic Analysis	To have accurate Licensing, sizing and BOM, we kindly request please share the following details: For NetFlow/IPFIX (Network Traffic Analysis): Flow volume/metrics (flows per second) Estimated GB per day data Flow data retention duration Number/list of devices from which flows will be exported For Syslog (Log Management): Syslog volume/metrics (events per second, EPS) Estimated GB per day data Syslog data retention duration Number/list of devices from which syslog will be collected Cloud Monitoring: cloud platforms to be integrated for cloud monitoring, along with the number of API calls per cluster/account expected for accurate sizing and licensing. Number of database instances/Applications/URL,	The number of users, devices, and other relevant infrastructure parameters are already indicated at appropriate places in the tender document. Based on these parameters and the scope of work, the bidder shall assess and estimate the required capacity, data ingestion rate, storage, processing resources, licenses and other sizing parameters necessary to provide the complete solution. The solution shall be offered with perpetual licenses covering the complete scope.

				Virtualization: Type of virtualization i.e. To have accurate sizing and BOM, we kindly request please share the following details: Cloud Monitoring: Details of Cloud platforms to be integrated for cloud monitoring, along with the number of API calls per cluster/account expected for accurate sizing and licensing. Number of database instances/Applications/URL Virtualization, Microsoft Hyper-V, VMWare etc.	
14	3.7 : Network Management System (NMS):	110	Log Management		
15	3.7.8 NMS Licensing should be Device based	108	3.7.8.1 Network mapping and discovery software using Layer 2/ Layer 3 protocols for devices.		
				Echelon Sumit Sharma: SNMP Smartscan, hosts file" with "discovery via SNMP/ICMP/ARP/LLDP/CDP, seed device, IP range/subnet and CSV import" - oem specific product wording MIB Walker, MIB Explorer and MIB Manager with "MIB browser with ability to import/compile third-party MIBs". -- OEM/Product-specific naming. update query for this as well - 3.7.12.1 Web and Windows based management console -- A mandatory Windows console favours one product. Web-based access is more secure and platform-independent. 3.7.12.5 Mobile Interface with one-click log-in , 3.7.12.8 Real-time split second and historical graphs - Product-specific wording. One-click login also conflicts with the security requirements.	Not Applicable

				NMS Licensing should be Device based. 3.7.8.1 Network mapping and discovery software using Layer 2/ Layer 3 protocols for devices --- let's ask them detailed insights about licensing - flow, log, cloud, app, db, and all devices - -count and type of virtualization 3.9 Software Stack Deployment: The successful bidder must deploy above network services along with DHCP, DNS (internal & external), Directory Server (DC/ ADC and LDAP), NTP, Syslog and User Access Log. All these servers must be configured preferably using Open Source. (Quantity: Job Complete) - open source ?? lets ask not for NMS: Separate line item lets push for ITSM - viii. Inventory Management – Implement an inventory management system for maintaining an up-to date database of all active network assets and software licenses. ,,, 3.7.12.13 Inventory or other device specific information The Institute is establishing a centrally managed campus network to be operated and supported over a 7-year period. For effective operations, the Department may consider IT Incident Management to track the complete lifecycle of every fault as a ticket, from NMS alarm through assignment, escalation and resolution to closure. This provides accountability, a complete audit trail and resolution history. Since Cl. 6(viii) itself calls for an up-to-date database of all active network assets and software licenses, a CMDB auto-populated from NMS discovery is the most direct way to meet its intent. It keeps asset, warranty and EoL records and is linked to incidents.We therefore request the Institute to include an ITIL-aligned ITSM module (Incident Management and CMDB) . --something on these lines	Not Applicable

Query - 4 (M/S NETIP Technologies Pvt. Ltd. on 02/10/2026)

Sr. No.	Product / Clause	Tender Reference	Existing Tender Provision	Query / Requested Amendment	Response
1	EMD Exemption	Page 5, Clause 12	The tender permits EMD exemption for eligible MSE manufacturers of goods and service providers for services, subject to valid supporting documents; traders are excluded.	The present tender is a comprehensive Supply, Installation, Testing and Commissioning (SITC) Work Contract, comprising not only the supply of networking equipment and related materials but also a substantial component of services, including installation, configuration, integration, testing, commissioning and overall project implementation. Since a significant portion of the project scope falls under the responsibilities of the executing service provider/ Bidder , we kindly request the authority to reconsider the existing EMD Exemption clause and extend the applicable exemption to eligible MSME/NSIC-registered Service Providers and System Integrators participating in this tender, subject to the prevailing Government of India guidelines. We would also like to highlight that, in several similar SITC and comprehensive networking infrastructure projects floated by IITs, IISERs, Central Universities and other Government educational institutions, eligible MSME/NSIC-registered service providers have been permitted to avail EMD exemption, in accordance with the respective tender conditions and applicable procurement policies. In view of the substantial service component involved in the present project, restricting the exemption may limit the	The EMD applicable as per procurement rules has been mentioned in the tender document. As per the bid estimation the majority of the bid value comprises the equipment. Hence, bidders are requested to comply. Remains Unchanged

				participation of capable MSME bidders with relevant technical expertise and proven project execution experience. We, therefore, sincerely request your good office to kindly consider amending the EMD Exemption clause to facilitate wider participation of eligible MSME/NSIC-registered service providers, promote fair competition and support the Government's initiatives for the promotion of MSMEs, without compromising the technical and financial eligibility requirements of the tender.	
2	Past Project Experience / Eligibility Criteria	Page 38, General Conditions, Clause 3	At least one completed project involving 80% of the stated quantities: Firewall/ADC 2 Nos.; L3 Fibre Switches 30 Nos.; L2 Switches 80 Nos.; OFC Laying 8,000 m; Transceivers 430 Nos.; I/O Ports as Last-Mile Connection 1,000 Nos.	Kindly revise the transceiver quantity from 430 Nos. to 250 Nos. and include NMS as 1 No. Proposed criteria: Firewall/ADC 2 Nos.; L3 Fibre Switches 30 Nos.; L2 Switches 80 Nos.; OFC Laying 8,000 m; Transceivers 250 Nos.; I/O Ports as Last-Mile Connection 1,000 Nos.; NMS 1 No. The bidder should demonstrate at least 80% of these revised quantities in one completed project.	Please check the amendments and corrigendum - 1
3	Payment Terms	Tender Payment Terms; Manual for Procurement of Goods, Second Edition, 2024, Chapter 6, Clause 6.3, pp. 141–142	Milestone payments: passive components 2.5%; active components 45%; OFC laying and commissioning 2.5%; active installation/configuration/commissioning 15%; software stack 15%; integrated testing and acceptance 10%; PBG and warranty documents 10%. Total 100%.	Kindly review the payment terms in line with the suggested terms in the Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142 Proposed structure for the supply component: 90% upon delivery, inspection and acceptance of goods at site with required documents, and 10% upon successful installation, configuration, commissioning, testing and acceptance. Separately identifiable installation/work components may be paid	Remain Unchanged

				against suitable milestones determined by the procuring authority.	
4	Next Generation Firewall (NGFW)	Annexure 9, Section 4, Page 69, Clause 1.1	Heading states: 4 × 100GE/40GE QSFP28 slots; 10 × 25GE/10GE SFP28 slots; 10 × 10GE RJ45 ports; 2 × 10G SFP+ HA slots; 2 × 1G management ports. Detailed specification instead requires minimum Day-1 I/O: 12 × 1G/2.5G/5G/10G; 10 × 1G/10G SFP/SFP+; 4 × 25G SFP28; 2 × 40G/100G QSFP/QSFP28; at least 2 × 10G SFP+ SR optics, 300 m over OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR.	Kindly amend the NGFW heading as per specification Day-1 I/O ports: 12 × 1G/2.5G/5G/10G; 10 × 1G/10G SFP/SFP+; 4 × 25G SFP28; and 2 × 40G/100G QSFP/QSFP28. Each firewall shall include at least 2 × 10G SFP+ SR optical transceivers supporting 300 m over OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant.	Please check the amendment (refer to Corrigendum - II)
5	Access Switch Type 2	Page 91, Clause 2.5	Heading states: 48 × 10/100/1000Base-T RJ45; 4 × 10/25GbE SFP/SFP+ uplinks; Layer 3 managed; minimum 296 Gbps switching capacity; field-replaceable redundant power supplies and fans. Detailed specification does not explicitly mention redundant PSUs/fans.	Kindly align the heading as per specification Proposed: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25G SFP28 uplinks operational from Day 1;.	Please check the amendment (refer to Corrigendum - II)
6	Access Switch Type 3	Page 93, Clause 2.6	Heading states: 24 × 10/100/1000Base-T RJ45; 4 × 10GbE SFP/SFP+ uplinks; Layer 3 managed; minimum 128 Gbps switching capacity; field-replaceable redundant power supplies and fans. Detailed specification does not explicitly mention redundant PSUs/fans.	Kindly align the heading as per specification Proposed: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10/25G SFP28 uplinks operational from Day 1;	Please check the amendment (refer to Corrigendum - II)
7	Access Switch Type 4	Page 96, Clause 2.7	Heading states: 16 × 10/100/1000Base-T RJ45; 2 × 10GbE SFP/SFP+ uplinks; Layer 3 managed; minimum 72 Gbps switching capacity; field-replaceable redundant power supplies and fans. Detailed specification does not explicitly mention redundant PSUs/fans.	Kindly align the heading as per specification Proposed: 16 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)

8	Access Switch Type 5	Page 97, Clause 2.8	Heading states: 8 × 10/100/1000Base-T RJ45; 2 × 10GbE SFP/SFP+ uplinks; Layer 3 managed; minimum 56 Gbps switching capacity; field-replaceable redundant power supplies and fans. Detailed specification does not explicitly mention redundant PSUs/fans.	Kindly align the heading as per specification 8 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)
9	AAA Server / OEM Interoperability	Page 102, Clause 3.1.6	All switches, NMS, transceivers and AAA are required to be from the same OEM for interoperability, management and support.	Kindly amend the clause to all the switches, transceivers, AAA from same OEMs, provided they meet technical specifications and interoperate through standard	Please check the amendment (refer to Corrigendum - II)
10	Performance Bank Guarantee	Page No 7 , Clause no 22	Security deposit/Performance Bank Guarantee @ 5% of the value of supply order as per norms may be sought from the firms, in terms of Ministry of Education, GOI, OM No. F. No. 29- 1/2019-IFD dated 06th April, 2023 for compliance of Ministry of Finance, DoE, GOI, OM No.F.1/2/2023-PPD dated 03.04.2023	Kindly Amend it 3% as the Tender Estimated value is 14 Crore . which is as per the Rule of Ministry of Finance, Department of Expenditure	Remain Unchanged
11	LIQUIDATED DAMAGES	Page no 7 , Clause no 23.	The Liquidated damages @ 0.5% per week subject to a maximum of 10% of the value of the order can be imposed	kindly request the Institute to amend the Liquidated Damages (LD) clause and prescribe LD at 0.5% of the value of the delayed supply/work per week or part thereof, subject to a maximum of 5% of the total value of the order/contract, in line with the applicable Government of India procurement provisions.	Remain unchanged

Query - 5 (M/S TechFacto Global Services Pvt. Ltd. on 03/10/2026)

S. No.	Tender Reference	Existing Requirement	Clarification / Amendment Requested	Justification	Response

1	Page 5, Clause 12 EMD Exemption	EMD exemption is available to eligible MSE manufacturers of goods and service providers for services, subject to valid documents; traders are excluded.	Please allow eligible MSME/NSIC-registered Service Providers and System Integrators to claim EMD exemption.	The scope of the tender is a complete SITC project involving supply, installation, configuration, integration, testing and commissioning. The amendment would increase participation by technically competent MSMEs.	The EMD applicable as per procurement rules has been mentioned in the tender document. As per the bid estimation the majority of the bid value comprises the equipment. Hence, bidders are requested to comply with the rules.
2	Page 38, General Conditions, Clause 3 Past Project Experience	One completed project meeting at least 80% of the specified quantities, including Firewall/ADC: 2; L3 Fibre Switches: 30; L2 Switches: 80; OFC: 8,000 m; Transceivers: 430; and I/O Ports: 1,000.	Revise the experience criteria to: Firewall/ADC: 2; L3 Fibre Switches: 30; L2 Switches: 80; OFC: 8,000 m; Transceivers: 250; I/O Ports: 1,000; and NMS: 1. The bidder should demonstrate at least 80% of the revised quantities in one completed project.	The revised quantities would continue to demonstrate substantial large-scale networking experience, while adding NMS experience to reflect the requirement for centralized monitoring and management.	Please check the Amendment (as per Corrigendum - I)
3	Tender Payment Terms; Manual for Procurement of Goods, 2nd Edition, 2024, Chapter 6, Clause 6.3, pp. 141-142	Milestone-based payment terms as specified in the tender.	For the supply component, allow 90% payment upon delivery and 10% after successful installation, configuration, commissioning, testing and acceptance.	High-value active and passive equipment requires significant advance financial commitments to OEMs/manufacturers. The proposed structure would support SI's to timely procure the material.	Remain unchanged

4	Page 43, Clause 8 Project Completion Period	Complete the project within 180 days from the date of award of the tender.	Extend the project completion period from 180 days to 270 days from the date of award of the tender.	Procurement and phased delivery may require approximately 3-4 months. The extension would support timely execution with coordinating with all stakeholders.	Remain unchanged

Query - 6 (M/S Ezdat Technology Pvt. Ltd. on 03/10/2026)

Sr. No.	**Product / Section**	**Tender reference**	**Existing provision**	**Query / requested amendment**	**Response**
1	NGFW	Annexure 9, Section 4, p. 69, Section 1.1	Heading and detailed Day-1 I/O specifications differ.	Kindly align the heading with the detailed specification: 12 × 1G/2.5G/5G/10G RJ45, 10 × 1G/10G SFP/SFP+, 4 × 25G SFP28 and 2 × 40G/100G QSFP/QSFP28. Include at least 2 × 10G SFP+ SR optics per firewall, supporting 300 m over OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR.	Please check the amendment (refer to Corrigendum - II)
2	Access Switch Type 2	p. 91, Section 2.5	Heading specifies 48 RJ45 ports and 4 × 10/25GbE uplinks, while redundant PSU/fan requirements are not explicit in the detailed specification.	Kindly align the heading and detailed specifications, confirming 48 × 10/100/1000Base-T RJ45 ports and 4 × 10/25G SFP28 uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)
3	Access Switch Type 3	p. 93, Section 2.6	Heading specifies 24 RJ45 ports and 4 × 10GbE uplinks; redundancy requirements are unclear.	Kindly align the specifications to 24 × 10/100/1000Base-T RJ45 ports and 4 × 10/25G SFP28 uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)
4	Access Switch Type 4	p. 96, Section 2.7	Heading specifies 16 RJ45 ports and 2 × 10GbE uplinks; detailed redundancy requirements are unclear.	Kindly align the specifications to 16 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)

5	Access Switch Type 5	p. 97, Section 2.8	Heading specifies 8 RJ45 ports and 2 × 10GbE uplinks; detailed redundancy requirements are unclear.	Kindly align the specifications to 8 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplinks operational from Day 1.	Please check the amendment (refer to Corrigendum - II)
6	AAA / OEM Interoperability	p. 102, Section 3.1.6	Switches, NMS, transceivers and AAA must be from the same OEM.	Kindly permit equipment from different OEMs, provided all components meet the technical specifications and support interoperability through standard protocols.	Please check the amendment (refer to Corrigendum - II)
7	Past Project Experience	p. 38, General Conditions, Section 3	One completed project demonstrating at least 80% of specified quantities is required: Firewall/ADC 2; L3 switches 30; L2 switches 80; OFC 8,000 m; transceivers 430; last-mile I/O ports 1,000.	Kindly revise the transceiver quantity to 250 and include NMS (1 No.). The proposed experience criteria should be based on at least 80% of the revised quantities: Firewall/ADC 2; L3 switches 30; L2 switches 80; OFC 8,000 m; transceivers 250; I/O ports 1,000; NMS 1.	Please check the amendment and Corrigendum - 1
8	Payment Terms	Tender payment terms; Manual for Procurement of Goods, 2nd ed., 2024, Chapter 6, Section 6.3, pp. 141–142	Payments are divided across passive components, active equipment, OFC, installation, software, testing and warranty documentation.	Kindly consider 90% payment for the supply component upon delivery, inspection and acceptance at site, and 10% after installation, configuration, testing, commissioning and acceptance. Pay separately identifiable work components against suitable milestones.	Remain Unchanged
9	EMD Exemption	p. 5, Section 12	EMD exemption is available to eligible MSE manufacturers and service providers, subject to supporting documents; traders are excluded.	As this is a comprehensive SITC contract involving supply, installation, configuration, integration and commissioning, kindly consider extending EMD exemption to eligible MSME/NSIC-registered service providers and system integrators, subject to applicable Government of India guidelines and tender eligibility conditions.	The EMD applicable as per procurement rules has been mentioned in the tender document. As per the bid estimation the majority of the bid

					value comprises of the equipment. Hence, bidders are requested to comply with the rules.
10	Product Warranty		Asking for 7 years Warranty for the Items describe in tender		Please refer to Contrigendem - I
			During the site survey and our review of the tender documents, we identified certain points that require further clarification to ensure accurate technical compliance, proper planning, and transparent pricing.		-
			UPS Installation Location and Environmental Requirements		Not in the scope of the tender
			Kindly confirm the exact location proposed for UPS installation, along with the necessary arrangements for adequate ventilation and airflow to dissipate heat. We request clarification regarding the availability of suitable space and the environmental conditions, including humidity, temperature, and other factors that may affect UPS performance, reliability, and service life.		Not in the scope of the tender
			Clarification of Colour Coding (Location-wise)		No color coding for bandwidth

			The colour-coding scheme mentioned in the tender documents is difficult to interpret clearly. We request you to kindly provide a detailed explanation of the colour codes, including their respective meanings and applications, preferably in a location-wise format or through a clearly marked layout/drawing. This will help us ensure proper identification, installation, and compliance with the required standards.		No color coding for bandwidth
			Final BOQ and Detailed Technical Specifications for OFC and High-Speed Connectivity		BoQ is already in the NIT Document
			We request you to kindly provide the final Bill of Quantities (BOQ) and detailed technical specifications for OFC core connectivity and all high-speed network connections. In particular, the following details are required for each connection:		BoQ is already in the NIT Document
			Required speed and bandwidth.		Available in NIT
			Quantity and number of connections.		Available in NIT
			Interface and port type.		Available in NIT
			Cable type and technical specifications.		Available in NIT
			Approximate cable length/distance.		Available in NIT
			Exact installation location and termination points.		Available in NIT

Query - 7 (Fortinet on 03/10/2026)

S No	Page No	Clause Heading	Spec. Number	Parameters	Sub Items No	Technical Specifications	Change Request	Justification	Responses

1	54	Annexure – 5: Check List to be submitted by Bidder/OEM	NA	NA	8	A letter of commitment for seven years from the date of installation, with respect to hardware and firmware support from OEM should be enclosed in the cover for a technical bid.	Please amend the clause to A letter of commitment for seven years from the date of bid submission, with respect to hardware and firmware support from OEM should be enclosed in the cover for technical bid.		Please check the amendment as per corrigendum - I The warranty starts as per the clause - 4, Annexure - 7: SLA.
2	69	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1	Hardware features and throughputs	1.1.1.1	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall appliance should have minimum 20 core processing and management purposes along with minimum 48 GB RAM	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall appliance should have minimum 16 core processing and management purposes along with minimum 48 GB RAM	Every OEM has its own architecture and methodology to process the traffic and restricting their participation specifically on cores does not align with their performance capabilities and restricts their participation.	remain unchanged
3	69	Annexure – 9: Specifications -	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.2	Next Gen Firewall throughput measured with Application Control/Identification and logging enabled, utilizing L7 transactions	Please amend the clause to "Next Gen Firewall throughput measured with Application	We request the authority to kindly consider defining a common and equivalent	remain unchanged .

		Next Generation Firewall (NGWF)				should be 25 Gbps or higher |OR| 32 Gbps or higher standard NGFW performance as measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.	Control/Identification and logging enabled, utilizing HTTP transactions should be 35 Gbps or higher"	performance benchmark for all OEM's. A standardized benchmark will ensure fair comparison and wider OEM participation.As per our understanding all leading OEM measure Application Control throughput in HTTP transactions only.	
4	69	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.3	Threat Prevention throughput measured with Application Control/Identification, IPS, antivirus, antispyware, sandboxing, file blocking, and logging enabled, utilizing L7 transactions should be 15 Gbps or higher |OR| 30 Gbps or higher standard Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic	Please amend the clause to threat protection throughput measured with Firewall, IPS, Application Control, and Malware Protection enabled (enterprise mix traffic) should be 25 Gbps or higher	We request the authority to kindly consider defining a common and equivalent performance benchmark for all OEM's. A standardized benchmark will ensure fair comparison and wider OEM participation. As per our understanding all leading OEM measure threat protection throughput in enterprise mix traffic only.	remain unchanged

5	69	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.5	Max concurrent sessions are measured utilizing L7 transactions should be 2 million or higher |OR| Concurrent Sessions (TCP) should be minimum 40 million	Please amend the clause to Max concurrent sessions are measured utilizing HTTP transactions should be 10 million or higher |OR| Concurrent Sessions (TCP) should be minimum 20 million	We request the authority to kindly consider a common and equivalent methodology for evaluating concurrent sessions, as OEMs may publish session capacity using different traffic profiles and measurement methodologies. This will ensure a fair comparison and allow wider OEM participation. As per our understanding all leading OEM measure concurrent sessions in either HTTP or TCP sessions only	remain unchanged
6	70	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.6	New sessions per second utilizing L7 transactions should be 200K or higher |OR| New Sessions/Second (TCP) should be minimum 600K	Please amend the clause to New sessions per second utilizing HTTP transactions should be 400K or higher |OR| New Sessions/Second (TCP) should be minimum 600K	We request the authority to kindly consider a common and equivalent methodology for evaluating concurrent sessions, as OEMs may publish session capacity using different traffic profiles and measurement	remain unchanged

								methodologies. This will ensure a fair comparison and allow wider OEM participation. As per our understanding all leading OEM measure new sessions per second in either HTTP or TCP sessions only	
7	70	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.7	Minimum I/O Ports required from Day 1: Min.1G/2.5G/5G/10G (12 Nos.), 1G/10G SFP/SFP+ (10 Nos.), 25G SFP28 (4 Nos.), 40G/100G QSFP/QSFP28 (2 Nos.) For each NGFW: SFP+ I/O ports to be loaded with at least 2 Nos. SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant. QSFP28 I/O ports to be loaded with at least 2 Nos. QSFP+ form factor, 40Gb SR4 optical transceiver, short reach 100m OM3, 8/12 strand MPO connector, IEEE 802.3ba 40GBASE-SR4 compliant	Please amend the clause to Minimum I/O Ports required from Day 1: Min.1G/10G RJ 45 Ports (12Nos.), 1G/10G SFP/SFP+ slots (10 Nos.), 25G SFP28 slots (4 Nos.), 40G/100G QSFP/QSFP28 slots (4 Nos.) For each NGFW: 1. SFP+ I/O slots to be loaded with at least 2 Nos. SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant. 2. QSFP28 I/O slots to be loaded with at least 2 Nos.		Please check the amendment (refer to Corrigendum - II)

							QSFP+ form factor, SR 25Gb optical transceiver, short reach 100m, MMF, duplex LC, IEEE 802.3ae 25GBASE-SR compliant. 3. QSFP+ I/O slots to be loaded with atleast 2 Nos. QSFP+ form factor, 40Gb SR4 optical transceiver, short reach 100m OM3, 12 strand MPO connector, IEEE 802.3ba 40GBASE-SR4 compliant		
8	70	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1	Hardware features and throughputs	1.1.1.10	Power Supply: Redundant 100–240 VAC (50–60Hz) Operating temperature: 0°C to 50°C Humidity tolerance: 10% to 90%	Power Supply: Redundant 100–240 VAC (50–60Hz) Operating temperature: 0°C to 40°C Humidity tolerance: 10% to 90%	We request the authority to kindly consider this revision to avoid restricting participation based on a specific operating-temperature specification and to allow wider OEM participation. The appliance will be placed in the datacentre with enough cooling, please approve the change.	Remain Unchanged

9	71	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.7	IPsec and SSL VPN: Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3des, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Secure access over IPsec or SSL VPN tunnels using VPN Gateway and portals	Please amend the clause to IPsec or SSL VPN: Key exchange: manual key, IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3des, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Secure access over IPsec or SSL VPN tunnels using VPN Gateway and portals	Most global cybersecurity OEMs are dropping support for IKEv1 as it is legacy protocol. We request the authority to kindly consider this revision considering IKEv2 as the current-generation IPsec key-exchange protocol supporting the required authentication mechanisms. This will allow wider OEM participation while retaining the required IPsec VPN functionality.	Remain Unchanged

10	71	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.8	The proposed solution should support remote user based VPN clients for Windows. Module should be Common Criteria certified for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	Please amend the clause to "The proposed solution should support remote user based VPN clients for Windows"	Please allow the change to allow wider OEM participation, as most OEMs do not restrict their agent for VPN functionalities and offer a unified agent with more capabilities like EPP, ZTNA, VA on the same agent so this clause restricts the participation.	Please check the amendment (refer to Corrigendum - II)
11	71	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.13	Should provide visibility into TLS traffic, such as the amount of encrypted traffic, SSL/TLS versions, cipher suites, and more, without decrypting.	Please amend the clause to "Should provide visibility into TLS traffic, including SSL/TLS versions, cipher suites, without decrypting"	We request the authority to kindly consider this revision to focus on the required visibility into TLS traffic and associated security parameters without prescribing a specific reporting methodology. This will allow wider OEM participation while	Remain unchanged

								retaining the intended security objective.	
12	72	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.17	Should prevent corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.	Please amend the clause to "Should help prevent corporate credentials from being submitted to malicious/unauthorized third-party websites and should support network-layer MFA for protected applications/access scenarios without requiring changes to the protected application"	We request the authority to kindly consider this revision to retain the intended security objective of credential protection and network-layer MFA while allowing equivalent technologies and architectures to participate. This will enable wider OEM participation.	Please check the amendment (refer to Corrigendum - II)
13	73	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.4	Certifications	1.1.4.1	ISO 27001, ISO 27017, ISO 42001	Please amend the clause to "ISO 27001, ISO 27017"	Please allow this change, as this certificate is quite latest and most of the global NGFWs OEMs are still in the application process of this certificate, but they have built their AI capabilities by keeping the standards of this	Please check the amendment (refer to Corrigendum - II)

								certification in consideration.	
14	73	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.4	Certifications	1.1.4.6	Following OEM certificates to be uploaded: a. Land Border Declaration b. Manufacturer Authorization Form for bidder c. Escalation Matrix and Toll Free Support Number d. SELF-CERTIFICATION for MII e. Non-Malicious Code Certificate f. Non-Blacklisting Declaration g. End of Life/Support of the Hardware h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 Functional Package for SSH Version 1. 0 PP-Module for Intrusion Prevention Systems (IPS), Version 1. 0	Please amend the clause to Following OEM certificates to be uploaded: a. Land Border Declaration b. Manufacturer Authorization Form for bidder c. Escalation Matrix and Toll Free Support Number d. SELF-CERTIFICATION for MII e. Non-Malicious Code Certificate f. Non-Blacklisting Declaration g. End of Life/Support of the Hardware h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection Profile Module for Stateful Traffic Filter	Please allow the change to allow wider OEM participation, as most OEMs do not restrict their agent for VPN functionalities and offer a unified agent with more capabilities like EPP, ZTNA, VA on the same agent so this clause restricts the participation.	Please check the amendment (refer to Corrigendum - II)

						PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 Collaborative Protection Profile for Network Devices Version 3. 0e i. Common Criteria for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	Firewalls v1.4 + Errata 20200625 Functional Package for SSH Version 1. 0 PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 Collaborative Protection Profile for Network Devices Version 3. 0e		
15	NA	Annexure – 9: Specifications - Next Generation Firewall (NGWF)	NA	NA	NA	New Suggestion	The proposed firewall shall support SSL inspection (including TLS 1.3) and shall provide a minimum SSL Inspection throughput of 20 Gbps and support at least 2 million SSL Inspection concurrent sessions.	SSL/TLS inspection is essential with the increasing use of HTTPS encrypted traffic and threats such as malware, malicious downloads and unauthorized application activity can be concealed within encrypted sessions. Without SSL/TLS decryption and inspection, critical NGFW security controls such as IPS, Anti-Malware, Application Control and	Not Applicable

								URL Filtering may have limited visibility into the actual content of the traffic. Therefore, defining minimum SSL Inspection throughput and concurrent SSL/TLS session capacity is necessary to ensure that encrypted traffic can be inspected at the required scale without creating a security or performance gap.	
16	102	Annexure – 9: Specifications - AAA Server:	3.1.1.	Make	3.1.1.2	The offered solution shall be ON Premises Virtual appliance to be provided in High Availability with all the necessary Operating system, required RAM, CPUs to cater the required number of devices mentioned in the subsequent clause. Licenses/subscriptions should be provided to 5000 users with 3 devices each from day 1.	The offered solution shall be ON Premises dedicated hardware appliance to be provided in High Availability with all the necessary Operating system, required RAM, CPUs to cater the required number of devices mentioned in the subsequent clause. Perpetual licenses shall be provided for 5000 users with 3 devices each from day 1.		Remain unchanged

17	102	Annexure – 9: Specifications - AAA Server:	3.1.2	Functionality	3.1.2.3	Solution should support up to 5000 users with 3 devices each from day 1. Licenses/Subscription to be considered accordingly. The solution should be scalable to support 20000 users or more in future.	Solution should support minimum 5000 users with 3 devices each from day 1. Perpetual licenses to be considered accordingly. The solution should be scalable to support 16000 users or more in future.		Remain unchanged
18	103	Annexure – 9: Specifications - AAA Server:	3.1.2	Functionality	3.1.2.6	Solution should have device profiling functionality	It's a NAC feature. Please put this clause under NAC		Remains unchanged
19	103	Annexure – 9: Specifications - AAA Server:	3.1.5	Licenses/Subscription & support	3.1.5.1	Perperual license with 7 Year OEM TAC and OS support for all licenses and Software. All software and Hardware should be included in the solution for 20000 users.	Perpetual license for 5000 users with 3 devices with 7 Year OEM TAC and OS support for all licenses and Software. Hardware shall be provisioned for 16000 users from day 1		Please check the amendment (refer to Corrigendum - II)
20	104	Annexure – 9: Specifications - AAA Server:	3.1.6	Mandatory compliance	3.1.6.1	All switches, NMS, Transceivers, AAA should be from the same OEM for better interoperatability, management and support.	Please remove AAA from this clause for wider OEM participation.		Please check the amendment (refer to Corrigendum - II)

21	104	Annexure – 9: Specifications - Network Access Control (NAC)	3.2	Network Access Control (NAC)	3.2	Network Access Control (NAC): Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network Infrastructure.	Please clarify the total number of endpoints/devices, maximum concurrent endpoints, number of switches, number of access points, other network infrastructure devices requiring NAC integration to be supported by the NAC solution		The number of users, devices, and other relevant infrastructure parameters are already indicated at appropriate places in the tender document.
22	75	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.1	GENERAL	1.2.1.5	The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects and shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	Please amend the clause to The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects.	For wider OEM participation please allow this change	The requirement for per-namespace operations is intended to provide granular WAF policy and service management in containerized environments. Remain unchanged

23	75	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.1	GENERAL	1.2.1.6	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should register to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource Queue maintained by the controller.	Please amend the clause to Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should register to the Kubernetes using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to and maintained by the controller.	For wider OEM participation please allow this change	Remain unchanged
24	76	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.3	Load Balancing Features	1.2.3.3	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2	Please amend the clause to Server Load Balancer should support for the following databases for health checks: • Oracle • MSSQL • MySQL •	For wider OEM participation please allow this change	Remain unchanged
25	76	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.3	Load Balancing Features	1.2.3.4	The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum	Please amend the clause to The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify	For wider OEM participation please allow this change	Remain unchanged

						RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance	TCP parameters like keep alive interval, maximum RTO, window size, delay window control, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance		

26	77	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.3	A given user must be enforced to follow a sequence of pages while accessing without any script and should have provision to apply the restriction to the application or part of the application based on Geo Location	Please amend the clause to A given user must be enforced to follow a and should have provision to apply the restriction to the application	For wider OEM participation please allow this change	Remain unchanged
27	77	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.4	The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.	Please amend the clause to The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including and. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.	For wider OEM participation please allow this change	Remain unchanged

28	77	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.6	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	Please amend the clause to The solution should have pre-built templates for well-known applications attack signatures.	For wider OEM participation please allow this change	Remain unchanged
29	78	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.8	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)	Please amend the clause to The WAF Solution should have mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)	For wider OEM participation please allow this change	Remain unchanged
30	78	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.9	System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

						credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance			
31	78	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.10	The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance (without accessing the internet/cloud service) to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCI DSS compliance requirements for web application servers. Necessary logs to be generated for audit and compliance.	Please amend the clause to The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCI DSS compliance requirements for web application servers.	For wider OEM participation please allow this change	Remain unchanged

							Necessary logs to be generated for audit and compliance.		
32	79	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.15	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
33	79	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.16	The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.	Please amend the clause to The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including	For wider OEM participation please allow this change	Remain unchanged
34	79	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.17	The WAF must provide BOT mitigation functionality (including CAPTCHA) without having to go on internet for some cloud based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT,	The WAF must provide BOT mitigation functionality (including CAPTCHA) and must have inbuilt dedicated BOT signatures with	For wider OEM participation please allow this change	Remain unchanged

						Malicious Bot, Suspicious Browser, Unknown etc.	different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc.		
35	80	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.20	The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • Backend application parser protection against XML DOS • XML Encryption and XML Signatures • Granular WSDL methods selection	Please amend the clause to The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • XML Encryption and XML Signatures	For wider OEM participation please allow this change	Remain unchanged
36	80	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.21	The proposed solution must support SSL VPN and Single Sign On Functionality on the same hardware solution running on the same OS version from the same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

						application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and the same should be configurable. * Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken			
37	81	Annexure – 9: Specifications -	1.2.7	MONITORING, LOGGING AND REPORTING	1.2.7.1	The proposed solution should have the capability to create a granular	Please amend the clause to The proposed solution should have the capability to create a granular	For wider OEM participation please allow this change	Remain unchanged

		Application Delivery Controllers (ADC)				logging policy per application. The system shall have the ability to customize logging. The proposed solution should have the capability to define a customized log format for each application.	logging policy per application. The system shall have the ability to customize logging.		
38	81	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.7	MONITORING, LOGGING AND REPORTING	1.2.7.2	The proposed solution should have the capability to define multiple log destinations for each application	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
39	82	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.8.2	ADMINISTRATION	1.2.8.2	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password	Please amend the clause to The solution must support the following password management capabilities without relying on any external system: b. Password length (minimum required number of characters in the password.) d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password	For wider OEM participation please allow this change	Remain unchanged

						Complexity)	Complexity)		
40	82	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.9	Product / OEM Evaluation Criteria	1.2.9.1	WAF / WAF's Operating System should be tested and certified for NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
41	82	Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.9	Product / OEM Evaluation Criteria	1.2.9.2	The WAF solution should be in the Gartner's/Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

Query - 8 (Accretive Technologies Private Limited. on 04/10/2026)

Sr. No.	Tender Clause	Page No.	Point No. C	Section/Annexure	Tender Clause	Request for Amendment	Response
1	Past Performance	38	3	Section -5 - General Conditions	Past performance: the bidder shall have successfully completed during the last seven years one or more Campus Wide Network (LAN) projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions	It is requested that the past performance criteria may kindly be amended to consider relevant experience of either the Bidder/OEM. This will enable participation of technically competent and experienced system integrators/channel partners while ensuring that the proposed OEM possesses the requisite expertise and credentials in enterprise networking solutions.	Remain unchanged
2	Eligibility Criteria	50	3	Annexure -1	The bidder shall have successfully completed during the last seven years one or more Campus Wide Network projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, any other Institute of National Importance, Central or State funded Govt Universities & academic Institutions. (Appropriate document should be provided)	The bidder/OEM shall have successfully completed during the last seven years one or more Campus Wide Network projects involving supply, installation, configuration, testing and commissioning of enterprise networking equipment in IISERs, IITs, NITs, Central/State funded Government Universities, Private Universities, reputed Educational Institutions, Research Institutions or other academic institutions.”	Remain unchanged

3	Additonal Request					We kindly request the authority to allow Consortium participation in the tender. Permitting consortiums will enable participation of technically competent organizations with complementary expertise and resources, thereby encouraging wider participation and healthy competition while ensuring successful execution of the project.	Not Applicable

Query - 9 (Array Networks on 05/10/2026)

Spec. No	**Parameters**	**Technical Specifications**	**Clarification Required**	**Response**
1.2.2	HARDWARE	The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 1.2 million 2) Network interfaces: 4x10G/1G RJ45 and 4x1G SFP+/SFP28/SFP from day 1. The 1G SFP interface should be upgradable to 10G and 25G by changing the transceivers. 3) SSL Throughput: at least 20 Gbps with 30K SSL TPS with 2K keys and 14K with ECC 4) Storage: at least 480 GB SSD 5) Memory: at least 64GB	All the parameters are specific to single OEM.	All specs are as minimum requirements. Thus remain unchanged

		The proposed solution must support SSL VPN and Single Sign On functionality on the same hardware solution running on the same OS version from the same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and the same should be configurable. * Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken	The mentioned feautres are typically part of SSL VPN, not a Web Application Firewall.For wider participation of OEM, it is request to delete this clause.	Remain unchanged
1.2.9	Product / OEM Evaluation Criteria	WAF / WAF's Operating System should be tested and certified for NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	For wider participation of OEM, it is suggested to amend this clause as "The WAF solution should be EAL2 certified or EAL 2 Apply for or TEC certified .	Remain unchanged
		The WAF solution should be in the Gartner's/Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and API Protection/WAF.	This is bid MII and because of foreign certificate not able to participate. It is suggested to delete for wider participation.	Please check the amendment (refer to Corrigendum - II)
5	Eligibility Criteria of OEM	OEM should be ISO 27001, ISO 27017, ISO 42001, Common Criteria/ISO-IEC 15408 & IPv6/ certification (IPv6 Logo & interoperability certification)	All the ISO are the same purpose for wider participation, it is amend as "OEM should be ISO 27001 or ISO 27017 or ISO 42001 or Common Criteria/ISO-IEC 15408 & IPv6/ certification (IPv6 Logo & interoperability certification)	Please check the amendment (refer to Corrigendum - II)

Query - 10 (Ruckus Networks on 03/10/2026)

S.NO	Page No	RFP Clause No	RFP Clause	Request for Change	Justification	Response
1	32	Point 7 : 2.5 :	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 ×10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
2	32	Point 7 : 2.6 :	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 ×10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
3	32	Point 7 : 2.6 :	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 ×10GbE SFP/SFP+ uplink ports; Layer-3	Kindly Change the Uplink ports to 4 ×10/25GbE SFP/SFP+ uplink ports. All other technical specifications shall remain unchanged.	The Requirement for 4 ×10GbE SFP/SFP+ uplink ports is mentioned as 4 ×10/25GbE SFP/SFP+ uplink ports in the Detailed technical specification of the Access Switch type 3	Please check the amendment (refer to Corrigendum - II)

			managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty			
4	32	Point 7 : 2.7 :	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 ×10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
5	33	Point 7 : 2.8 :	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
6	51	Point 8	Proposed OEM products should not be declared end of support life in the next 7 years.	Kindly revise the end of support life to next 5 years for the Proposed OEM Products	The requested amendment will align the product support lifecycle requirement with the proposed 5-year warranty and TAC support period and also facilitate wider OEM participation	Please check the amendment (refer to Corrigendum - II)

7	61	Point 7 : 2.5 :	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 ×10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
8	61	Point 7 : 2.6 :	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 ×10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
9	61	Point 7 : 2.6 :	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 ×10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly Change the Uplink ports to 4 ×10/25GbE SFP/SFP+ uplink ports. All other technical specifications shall remain unchanged.	The Requirement for 4 ×10GbE SFP/SFP+ uplink ports is mentioned as 4 ×10/25GbE SFP/SFP+ uplink ports in the Detailed technical specification of the Access Switch type 3	Please check the amendment (refer to Corrigendum - II)

10	61	Point 7 : 2.7 :	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 ×10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
11	61	Point 7 : 2.8 :	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps ;field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
12	83	2.1	2.1 Core Switch (CS): Core Switch Supply of Layer 3, 32 Port x 40/100 Gbps SFP port core switch; Switching capacity: at least 6Tbps; with field replaceable redundant power supplies and FANs; 7 Year Warranty; (Quantity: 2 Number)	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)

13	84	2.1.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	Kindly revise to Switch/ Switch OS(operating system) common criteria / NDPP / NDcPP certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain Unchanged
14	84	2.1.10.1	Warranty7 year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the Amendment (refer to Corrigendum - II)
15	86	2.2	Distribution Switch (DS) Type - 1: DS Switch Type-1: Distribution Switch Supply of Layer 3, 48-port SFP28 10/25GbE, with 8xport 40/100GbE; Switching capacity at least 4Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty; (Quantity: 10 Number)	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the Amendment (refer to Corrigendum - II)
16	86	2.2.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	Kindly revise to Switch/ Switch OS(operating system) common criteria / NDPP / NDcPP certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain Unchanged

17	87	2.2.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
18	87	2.3	Distribution Switch (DS) Type - 2: DS Switch Type-2: Distribution Switch Supply of Layer 3, 24-port SFP28 10/25 G, with 4x-port 40/100GbE; Switching capacity: at least 2Tbps; field replaceable redundant power supplies and FANs 7 Year Warranty, (Quantity: 10 Number)	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
19	89	2.3.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	Kindly revise to Switch/ Switch OS(operating system) common criteria / NDPP / NDcPP certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain Unchanged
20	89	2.3.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)

21	89	2.4	Access Switch (AS) Type - 1: AS Switch Type-1: Access Switch/Edge Switch: 24x1/10GbE Base-T RJ45 ports; 4 × 25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 680gbps; field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
22	91	2.4.9.1	All categories of Switches, Transceivers & Switch OS should be from same OEM & Switch should be Ipv6 logo, ROHS and common criteria / NDPP / NDcPP certified at the time of bidding	Kindly revise to Switch/Switch OS(operating system) common criteria / NDPP / NDcPP certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain Unchanged.
23	91	2.4.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
24	91	2.5	Access Switch (AS) Type - 2: AS Switch Type-2: Access Switch/Edge Switch: 48 × 10/100/1000Base-T RJ45 ports; 4 × 10/25GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 296Gbps; field replaceable	Kindly remove the requirement for "field-replaceable redundant power supplies and fans" and revise the warranty requirement from 7 years to 5 years. All other technical	The requirement for "field-replaceable redundant power supplies and fans" appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to	Specs remain unchanged For warranty terms, please check the amendment (refer to the

			redundant power supplies and FANs 7 Year Warranty	specifications shall remain unchanged.	maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Corrigendum -1) for warranty period
25	93	2.5.8.2	Switch should be certified by NDcPP and TEC Certified	Kindly revise to Switch / Switch OS(operating system) common criteria / NDPP / NDcPP certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain unchanged
26	93	2.5.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
27	93	2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps; field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period

28	93	2.6	Access Switch (AS) Type - 3: AS Switch Type-3: Access Switch/Edge Switch: 24 × 10/100/1000Base-T RJ45 ports; 4 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 128gbps; field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly Change the Uplink ports to 4 ×10/25GbE SFP/SFP+ uplink ports. All other technical specifications shall remain unchanged.	The Requirement for 4 ×10GbE SFP/SFP+ uplink ports is mentioned as 4 ×10/25GbE SFP/SFP+ uplink ports in the Detailed technical specification of the Access Switch type 3	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
29	95	2.6.8.2	Switch should be certified by NDcPP and TEC Certified	Kindly revise to Switch/ Switch OS(operating system) should be NDcPP and TEC Certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remains unchanged
30	96	2.6.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
31	96	2.7	Access Switch (AS) Type - 4: AS Switch Type-4: Access Switch/Edge Switch: 16 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 72gbps; field replaceable redundant power supplies and FANs 7 Year Warranty	Kindly remove the requirement for “field-replaceable redundant power supplies and fans” and revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period

32	97	2.7.8.2	Switch should be certified by NDcPP and TEC Certified	Kindly revise to Switch / Switch OS(operating system) should be NDcPP and TEC Certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain unchanged
33	97	2.7.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	Kindly revise the warranty requirement from 7 years to 5 years. All other technical specifications shall remain unchanged.	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure wider OEM participation and competitive commercial offerings.	Please check the amendment (refer to Corrigendum - II)
34	97	2.8	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps; field replaceable redundant power supplies and FANs 7 Year Warranty	Access Switch (AS) Type - 5: AS Switch Type-5: Access Switch/Edge Switch: 8 × 10/100/1000Base-T RJ45 ports; 2 × 10GbE SFP/SFP+ uplink ports; Layer-3 managed switch; Switching capacity at least 56gbps; 5Year Warranty	The requirement for “field-replaceable redundant power supplies and fans” appears in the summary/heading but is not specified in the corresponding detailed technical specifications. We therefore request that this requirement be removed to maintain consistency between the summary and detailed specifications. Additionally, we request that the warranty period be revised from 7 years to 5 years.	Specs remain unchanged For warranty terms, please check the amendment (refer to the Corrigendum -1) for warranty period
35	99	2.8.8.2	Switch should be certified by NDcPP and TEC Certified	Kindly revise to Switch / Switch OS(operating system) should be NDcPP and TEC Certified	The Common Criteria certification tests the switch Operating system for certification so we request the change	Remain unchanged
36	99	2.8.10.1	7-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from the OEM of the item. OEM should have an India toll-free number	5-year TAC support and comprehensive warranty should be provided by the OEM. The warranty certificate/declaration shall be from	We request that the TAC support and comprehensive warranty period be revised from 7 years to 5 years to align with the proposed warranty period for the active networking equipment. This will ensure	Please check the amendment (refer to Corrigendum - II)

			reflected on the official web site.	the OEM of the item. OEM should have an India toll-free number reflected on the official web site.	wider OEM participation and competitive commercial offerings.	

Query - 11 (M/S NETIP Technologies Pvt. Ltd. (2nd Representation) on 11/10/2026)

Sr. No.	Product / Clause	Tender Reference	Existing Tender Provision	Query / Requested Amendment	Response
1	EMD Exemption	Page 5, Clause 12	The tender permits EMD exemption for eligible MSE manufacturers of goods and service providers for services, subject to valid supporting documents; traders are excluded. As per MSMEs in India registered with appropriate authority as per latest notification shall be exempted from EMD payment provided they are registered for the item being quoted. Micro & MSME/NSIC and Firms registered and the firms registered with concerned Ministries/ Departments, the bidders are exempted from payment of Tender Fee/EMD as per GOI notifications/GFR (2017) and Ministry of Finance OM No. F.9/4/2020-PPD dated 12 November 2020	The Tender published under the Services Category for "Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure." The scope involves the provision of technical and professional services along with the supply, installation, integration and commissioning of network infrastructure. In this regard, we request the Tender Inviting Authority to consider the provisions of Rule 170(i) of the General Financial Rules (GFR), 2017, read with the Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012, as amended, regarding exemption from payment of Earnest Money Deposit (EMD) for eligible MSEs. Accordingly, we request that the EMD clause be suitably amended to extend the applicable exemption to eligible Micro and Small Enterprise service providers holding valid Udyam/MSME and/or NSIC registration under the relevant service category/NIC Code, subject to the applicable Government of	The EMD applicable as per procurement rules has been mentioned in the tender document. As per the bid estimation the majority of the bid value comprises

				India procurement rules and eligibility conditions. The inclusion of supply and installation activities within the scope of a services-category tender should not, by itself, be the sole basis for denying an otherwise admissible exemption. The eligibility for exemption may kindly be determined based on the actual nature and classification of the procurement and the applicable Government provisions. We therefore request Competent Authority to issue a suitable clarification/corrigendum permitting eligible MSE service providers to claim EMD exemption wherever admissible under the prevailing rules, thereby ensuring fair competition and wider participation of eligible MSEs in Government procurement. Since the tender has been published under the Services Category, eligible Micro and Small Enterprise service providers holding valid Udyam Registration and registered for the relevant services/NIC Code may kindly be considered for EMD exemption, subject to the applicable eligibility conditions and procurement classification. We request issuance of a suitable corrigendum to ensure that eligible MSE service providers receive the benefits admissible under the applicable Government of India procurement policy. DOCUMENT ATTACHED References: 1. Department of Expenditure, Ministry of Finance – Manual for Procurement of Non-Consultancy Services, 2025: *https://doe.gov.in/files/circulars_document/Mf PoNCS_2025.pdf* 2. General Financial Rules (GFR), 2017 – Rule 170(i), including the applicable amendment: *https://doe.gov.in/en/orders-circulars/31* 3. Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012, as amended, subject to applicable conditions. 4.	of the equipment. Hence, bidders are requested to comply with the rules.

				Document Attached : 1) Letter No : F.9/4/2020-PPD Dated 12th Nov 2020. 2) Letter No : F.20/2/2014-PPD(Pt) dated July 2017	
3	Payment Terms	Tender Payment Terms; Manual for Procurement of Goods, Second Edition, 2024, Chapter 6, Clause 6.3, pp. 141142	Milestone payments: passive components 2.5%; active components 45%; OFC laying and commissioning 2.5%; active installation/configuration/commissioning 15%; software stack 15%; integrated testing and acceptance 10%; PBG and warranty documents 10%. Total 100%.	Kindly review the payment terms in line with the suggested terms in the Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142 Proposed structure for the supply component: 90% upon delivery, inspection and acceptance of goods at site with required documents, and 10% upon successful installation, configuration, commissioning, testing and acceptance. Separately identifiable installation/work components may be paid against suitable milestones determined by the procuring authority. (DOCUMENT ATTACHED) Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142	Remain Unchanged

10	Performance Bank Guarantee	Page No 7 , Clause no 22	Security deposit/Performance Bank Guarantee @ 5% of the value of supply order as per norms may be sought from the firms, in terms of Ministry of Education, GOI, OM No. F. No. 29- 1/2019-IFD dated 06th April, 2023 for compliance of Ministry of Finance, DoE, GOI, OM No.F.1/2/2023-PPD dated 03.04.2023	Kindly Amend it 3% as the Tender Estimated value is 14 Crore . which is as per the Rule of Ministry of Finance, Department of Expenditure	The Security Deposit/ PBG is in line with the notification of GOI. Please comply.

11	LIQUIDATED DAMAGES	Page no 7 , Clause no 23.	The Liquidated damages @ 0.5% per week subject to a maximum of 10% of the value of the order can be imposed	kindly request the Institute to amend the Liquidated Damages (LD) clause and prescribe LD at 0.5% of the value of the delayed supply/work per week or part thereof, subject to a maximum of 5% of the total value of the order/contract, in line with the applicable Government of India procurement provisions.	Remain Unchanged

Query - 12 (F5 on 05/10/2026)

S.No.	Component	RFP Clause	Suggested Change	Justification	Response

1	Section – 4: List of Materials, Page no 32 Annexure 8, Page no 60	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defense, Guard Data Loss Prevention Service; 7 Years Warranty Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x GE RJ45 ports, 4 x SFP GE ports, 4 x SFP+ 10GbE ports, 1 x 120GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security - Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning, iADC Cloud Sandbox, Credential Stuffing Defence Guard, Data Loss Prevention Service; 7 Years Warranty	Application Delivery Controllers (ADC): Application Delivery Controllers (ADC) 4 x G/10G RJ45 ports, 4 x 10G SFP+ ports, 1 x 480GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU, Application Security / Network Security Bundle Plus WAF Signatures, WAF Adaptive Learning/ Credential Stuffing Defense Guard/ L7 Application Security ; 7 Years Warranty	There is a mismatch in the interface and features asked in the specification and BoQ. We request to change this to remove the ambiguity. This transition will also ensures zero performance bottlenecks by shifting resource-heavy SSL/TLS offloading and behavioural bot/DLP inspection onto to dedicated hardware-accelerated platform, resulting in a more reliable, scalable, and secure application delivery architecture.	Please check the amendment (refer to Corrigendum - II)

Query - 13 (M/S Molex on 05/10/2026)

Sl.No		**Specifications**	**Remarks**	**Response**
4.1	96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket.			-
4.1.4	No of fibers:	96 core (6/8 Fiber per tube)	Request you to change no of fiber core in oper tube from 6/8 to 6/08/12 core oer tube	Please check the amendment (refer to Corrigendum - II)
4.1.5	Water Blocking	Water Jell	it should be jelly	Please check the amendment (refer to Corrigendum - II)
4.2	48 Core OFC: Single Mode fiber 48 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 2500 Meter)			-

Query - 14 (Genius Network on 05/10/2026)

Category	**Clause #**	**Clause Name**	**Parameter**	**Query**	**Response**
Eligibility criteria of OEM (Passive Components)	1	The passive components' OEM must be ISO 9001 and ISO 14000 certified. The material must have been manufactured in the OEM's own manufacturing facilities and not outsourced.		Kindly confirm if OEM should get these products manufactured/ sub contracted within India, to comply to requirements of make in India. Also OEM must have it's goods warehouse, R&D labs and service center with toll-free number in India.	Remains Unchanged

Eligibility criteria of OEM (Passive Components)	2	The OEM of passive components quoted by the bidder should have a presence in India for at least five years, ending on the previous day of the last day of submission of the tender. Supporting documents must be attached. The OEM should also have at least one manufacturing plant in India to comply with the Make in India initiative.		Kindly confirm if OEM should get these products manufactured/ sub contracted within India, to comply to requirements of make in India. Also OEM must have it's goods warehouse, R&D labs and service center with toll-free number in India.	Remains Unchanged
Eligibility criteria of OEM (Passive Components)	3	Passive network components: All passive network components (IO Ports, cat cables, fibres, patch panel, patch cord etc.) preferably be from one OEM.		Kindly confirm for OEM it should be mandatory to have atleast one RCDD on their payroll within India to support such a big project who can validate/certify the ICT designs & installations and provide furture support. This should be supported by a documents by OEM's HR Letter of appointment	Remains Unchanged
Eligibility criteria of OEM (Passive Components)	4	All fiber cables should be bent compliant with ITU-T G.657.A1, OS2.		Kindly consider G.652.D / G.657.A1 for fiber cable. Since G.657.A1 is basically a Bend Insensative Standard used specifically for Patch cords and high density application and majorly for Indoor application. For current application of Campus Networking this parameter would not essential which is increasing cost factor We recommand to use G.657.A2 for Fiber Patch cords	Remains Unchanged

Eligibility criteria of OEM (Passive Components)	9	Vendor/bidder should bring the sample of passive components and test reports (from any testing software/device) for evaluation by the technical evaluation committee.		Kindly confirm if OEM can submit the NABL accredited Lab test report instead of just "any" software/device for confirmation of authenticated reports	Remains Unchanged
Eligibility criteria of OEM (Passive Components)		New Point to be add for OEM's ISO Certifications		Kindly confirm if OEMs should be CE certified and must adhere to ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 27001:2022 , ISO 28000 and ESG Silver Rated. Valid certificates for all the above standards and ratings must be enclosed with the proposal to support compliance verification.	Not applicable
96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 3500 Meter)	4.1.12	Standards	AS/ACIF S008; AS/NZS 3080	kindly confirm if this shall be removed as these are Australian regulatory instrument which are non-applicable in India.	Please check the amendment (refer to Corrigendum - II)
96 Core OFC: Single Mode fiber 96 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 3500 Meter)	4.1.4	No of fibers:	96 core (6/8 Fiber per tube)	Kindly confirm for 96 Core would be required then it should be 12F/T & 8T or 8F/T & 12T combination)	Please check the amendment (refer to Corrigendum - II)

48 Core OFC: Single Mode fiber 48 core: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable Single Jacket. (Quantity: 2500 Meter)	4.2.12	Standards	AS/ACIF S008; AS/NZS 3080	kindly confirm if this shall be removed as these are Australian regulatory instruments which are non-applicable in India.	Please check the amendment (refer to Corrigendum - II)
24 Core OFC: Single Mode fiber 24: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable. (Quantity: 2200 Meter)	4.3.8	End to End Structured Cabling Products from Single Brand and Single OEM. OEMs should have once RCDD / CDCP in India.		Kindly confirm if the Employer can make RCDD as mandatory since CDCP and RCDD cannot be measured as equivalent. 1) CDCP is having preliminary & basic knowledge of Data center environment only whereas RCDD covers whole ICT Infrastructure Design 2) Typical deliverables from CDCP are basic understanding infrastructure environment and from RCDD one can expects ICT design, layouts, pathways, cable distribution, equipment rooms, telecom spaces designing	Please check the amendment (refer to Corrigendum - II)
12 Core OFC: Single Mode fiber 12: -Armored Multi-Tube, 9/125µm, OS 2 Type Optical Fiber Cable. (Quantity: 900 Meter)	4.4.8	End to End Structured Cabling Products from Single Brand and Single OEM. OEMs should have once RCDD / CDCP in India.		Kindly confirm if the Employer can make RCDD as mandatory since CDCP and RCDD cannot be measured as equivalent. 1) CDCP is having preliminary & basic knowledge of Data center environment only whereas RCDD covers whole ICT Infrastructure Design 2) Typical deliverables from CDCP are basic understanding infrastructure environment and from RCDD one can expects ICT design,	Please check the amendment (refer to Corrigendum - II)

				layouts, pathways, cable distribution, equipment rooms, telecom spaces designing	
LIU-24P: 24 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails (Quantity: 8 Number)				In order to further ensure product quality, compliance, and third-party validation, kindly confirm whether bidders may also be required to submit valid test report for Corrosion as per ASTM B117: 2019. (Relevant Document to be shared) by NABL Lab	Please check the amendment (refer to Corrigendum - II)
LIU-48P: 48 Port Fiber Optic Rack Mount LIU with Adaptors Plates, Splice, Tray and should come with standard fully populated Pigtails (Quantity: 75 Number)				In order to further ensure product quality, compliance, and third-party validation, kindly confirm whether bidders may also be required to submit valid test reports for Corrosion as per ASTM B117: 2019. (Relevant Document to be shared) by NABL Lab	Please check the amendment (refer to Corrigendum - II)
LC-LC Patch Cord-Type-1: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 0.5m (Quantity: 500 number)	4.7.1		9/125 µm, OS2, Duplex Zipcord.	Kindly confirm if OEM should be provide G.657.A2 type of Fiber for Patch cord which is Bend Insensitive and critical for applications	Please check the amendment (refer to Corrigendum - II)

LC-LC Patch Cord-Type-1: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 0.5m (Quantity: 500 number)	4.7.9	Certificate	ETL Tested	Kindly remove this clause since this is OEM specific, only one OEM has its Fiber product tested with ETL which is not essential as there will be no length standardization in FO connector Channel / link with respect to Single Mode Technology.	Remain unchanged
LC-LC Patch Cord-Type-2: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 1m (Quantity: 312 number)	4.8.1		9/125 µm, OS2, Duplex Zipcord.	Kindly confirm if OEM should be provide G.657.A2 type of Fiber for Patch cord which is Bend Insensative and critical for applications	Please check the amendment (refer to Corrigendum - II)
LC-LC Patch Cord-Type-2: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 1m (Quantity: 312 number)	4.8.9	Certificate	ETL Tested	Kindly remove this clause since this is OEM specific, only one OEM has its Fiber product tested with ETL which is not essential as there will be no length standardization in FO connector Channel / link with respect to Single Mode Technology.	Remain Unchanged
LC-LC Patch Cord-Type-3: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 2m (Quantity: 144 number)	4.9.1		9/125 µm, OS2, Duplex Zipcord.	Kindly confirm if OEM should be provide G.657.A2 type of Fiber for Patch cord which is Bend Insensative and critical for applications	Please check the amendment (refer to Corrigendum - II)
LC-LC Patch Cord-Type-3: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 2m (Quantity: 144 number)	4.9.9	Certificate	ETL Tested	Kindly remove this clause since this is OEM specific, only one OEM has its Fiber product tested with ETL which is not essential as there will be no length standardization in FO connector Channel / link with respect to Single Mode Technology.	Remain Unchanged

LC-LC Patch Cord-Type-4: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 5m (Quantity: 64 number)	4.10.1		9/125 µm, OS2, Duplex Zipcord.	Kindly confirm if OEM should be provide G.657.A2 type of Fiber for Patch cord which is Bend Insensative and critical for applications	Please check the amendment (refer to Corrigendum - II) .
LC-LC Patch Cord-Type-4: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 5m (Quantity: 64 number)	4.10.9	Certificate	ETL Tested	Kindly remove this clause since this is OEM specific, only one OEM has its Fiber product tested with ETL which is not essential as there will be no length standardization in FO connector Channel / link with respect to Single Mode Technology.	Remain unchanged
LC-LC Patch Cord-Type-5: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 10m (Quantity: 48 number)	4.11.1		9/125 µm, OS2, Duplex Zipcord.	Kindly confirm if OEM should be provide G.657.A2 type of Fiber for Patch cord which is Bend Insensative and critical for applications	Please check the amendment (refer to Corrigendum - II)
LC-LC Patch Cord-Type-5: LC-LC Type 9/125µm Singlemode OS2 Optical Fiber Patch Cords 10m (Quantity: 48 number)	4.11.9	Certificate	ETL Tested	Kindly remove this clause since this is OEM specific, only one OEM has its Fiber product tested with ETL which is not essential as there will be no length standardization in FO connector Channel / link with respect to Single Mode Technology.	Remain unchanged
CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity:80 Boxes)	4.21.3	TIA 568.2-D	ETL Verified & UL Listed & ETL 4 Connector Channel report (Certificates are mandatory)	Kindly confirm if it can be a mandatory to submit ETL 4 connector test report for 100mtr as well as for short distance i.e 15mtr 4 connector test report by ETL. Must include Zero Bit error Test report.	Please check the amendment (refer to Corrigendum - II)

CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity:80 Boxes)	4.21.3	TIA 568.2-D	ETL Verified & UL Listed & ETL 4 Connector Channel report (Certificates are mandatory)	Kindly confirm if the ETL testing should have been performed for characteristic upto 900Mhz	Please check the amendment (refer to Corrigendum - II)
CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity:80 Boxes)	4.21.9	Sheath Type	LSZH Complies to IEC 60332-1	Kindly confirm if OEM Should supply IEC 60332-3-22 as per mentioned in OEM criteria, "The Cat 6/Cat6A U/UTP cable should comply with IEC60332-3-22, IEC 61034-1 and -2, IEC 60754-1 and -2, UL 94, EN50575 features for environment safety"	Remain unchanged
CAT6 Cable type -1: CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity:80 Boxes)	4.21.9	Sheath Type	LSZH Complies to IEC 60332-1	Kindly confirm if LSZH Jacket must be tested by NABL/BIS Test lab	Remains unchanged
CAT6 Cable type -2: Metallic armour CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 5 Boxes)	4.22.3	Sheath Type(Inner & Outer)	Inner LSZH Outer UV Resistant PVC.	Kindly confirm if OEM should provide Outer sheath with Metallic Armoring inside the Outer Jacket which is ECCS Tape and PE/HDPE Jacket for more strength	Please check the amendment (refer to Corrigendum - II)

CAT6 Cable type -2: Metallic armour CAT6 cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 5 Boxes)	4.22.4	External OD	7. 0 ± 1. 0 mm	Kindly confirm if Metallic Armour CAT6 cable is required the OD of the cable shall be 10.0 ± 0.50 mm, since it has double sheath and armoring	Please check the amendment (refer to Corrigendum - II)
CAT6 Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 1000 number)	4.25.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	Kindly confirm if OEM should submit Anti-Bacterial test report at the time of bid and should comply to ISO: 22196:2011	Please check the amendment (refer to Corrigendum - II)
CAT6 Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 1000 number)	4.25.15	Verified	UL Listed & ETL Verified	Kindly confirm if Jacket must be tested by NABL/ BIS certified Lab	Please check the amendment (refer to Corrigendum - II)
CAT6 Patch Cord - type - 2: Patch Cords 1M (Quantity: 1000 number)	4.26.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	Kindly confirm if OEM should submit Anti-Bacterial test report at the time of bid and should comply to ISO: 22196:2011	Please check the amendment (refer to Corrigendum - II)
CAT6 Patch Cord - type - 2: Patch Cords 1M (Quantity: 1000 number)	4.26.15	Verified	UL Listed & ETL Verified	Kindly confirm if Jacket must be tested by NABL/ BIS certified Lab	Please check the amendment (refer to Corrigendum - II)

CAT6 Patch Cord - type - 3: Patch Cords 2M (Quantity: 500 number)	4.27.14	Commercial Standards	ISO/IEC 11801.1 2017 or Latest, ANSI/TIA-568.2-D-2018	Kindly confirm if OEM should submit Anti-Bacterial test report at the time of bid and should comply to ISO: 22196:2011	Please check the amendment (refer to Corrigendum - II)
CAT6 Patch Cord - type - 3: Patch Cords 2M (Quantity: 500 number)	4.27.15	Verified	UL Listed & ETL Verified	Kindly confirm if Jacket must be tested by NABL/ BIS certified Lab	Please check the amendment (refer to Corrigendum - II)
CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 20 Boxes)	4.28.4	Shall be 4-pair twisted pair with an isolator (+), i. e.4 pair cable should be individual screened pairs for electromagnetic interference (EMI) protection, meeting Category 6A tested to 500 MHz. (4 connector test report from ETL(Intertek) to be submitted with offer & must be available on Intertek site for verification).		Kindly confirm if U/UTP construction can be provided since for current environment shielded solution would not be required and CAT6 cables requested are also U/UTP construction only. Even the keystone outlets requested are with unshielded construction	Please check the amendment (refer to Corrigendum - II)
CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC requirements 305m each (Quantity: 20 Boxes)	4.28.10	Jacket/ Sheath type should be LS0H (Low Smoke Zero Halogen) as per IEC60332-I & IEC 60332-3-22		Kindly confirm if IEC 60332-3-22 can be optional to IEC60332-1 as mentioned in CAT6 as well even though CAT6 quantity is 4 times more.	Please check the amendment (refer to Corrigendum - II)
CAT6A Cable type - 1: CAT6A cable; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC	4.28.12	The screen should be each individual pair enclosed in laminated aluminium foil with drain wire		Kindly confirm if U/UTP construction will be considered this clause to be removed as it would not be available/ required.	Please check the amendment (refer to Corrigendum - II)

requirements 305m each (Quantity: 20 Boxes)					
CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each (Quantity: 8 Boxes)	4.29.1	Type	6A S/FTP 4-Pair Shielded- PVC+PE Sheath (Armored) Cable Category 6A ANSI/TIA 568.2-D ISO/IEC 11801 IEC 61156-5	Kindly confirm if Metallic Armour required as strong protection of Aluminium 0.8mm wires armouring should be provided between inner sheath and Outer sheath. S/FTP shielding is just to reduce EMI & proving earthing which is not essential for this outdoor application however U/UTP construction can very well works but strong armouring would be required	Please check the amendment (refer to Corrigendum - II)
CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each (Quantity: 8 Boxes)	4.29.3	Sheath Type(Inner & Outer)	Inner PVC Outer UV Resistant HDPE.	Kindly confirm as per OEM Criteria "The Cat 6/Cat6A U/UTP cable should comply with IEC60332-3-22, IEC 61034-1 and -2, IEC 60754-1 and -2, UL 94, EN50575 features for environment safety", this cable shall have inner sheath as LSZH and not PVC with at least IEC 60332-1-2 for Flammability test.	Please check the amendment (refer to Corrigendum - II)
CAT6A Cable type - 2: Metallic armor CAT6A cable for harsh outdoor environment; fire retardant; ISO/IEC 11801 Class EA; RoHS; BIS/TEC 305m each (Quantity: 8 Boxes)	4.29.8	Armour	Braided steel wires	Kindly confirm if Metallic Armour required as strong protection of Aluminium 0.8mm wires armouring should be provided between inner sheath and Outer sheath. braiding steel wires is nothing but thin shielding just to provide earthing which is not essential for this outdoor application however U/UTP construction can very well work but strong armouring would be required	Please check the amendment (refer to Corrigendum - II)

CAT6A Patch Panel 24P: 24 port CAT 6A Patch Panel (Quantity: 4 number)	4.30.12	Should be certified by ETL/UL		Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remain unchanged
CAT6A Patch Panel 48P: 48 port CAT 6A Patch Panel (Quantity: 4 number)	4.31.12	Jack panel should be certified by ETL/UL.		Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remain Unchanged
CAT6A Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 100 number)	4.32.9	Screen material should be aluminum/polyester with tinned copper drain wire.		Kindly confirm if CAT6A Keystone Outlet can be unshielded, should OEM consider Patch cord also as U/UTP or Unshielded	Please check the amendment (refer to Corrigendum - II)
CAT6A Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 100 number)	4.32.12	Shall be RoHS Compliant		Kindly confirm if the Jacket must be tested by NABL / BIS certified Lab	Please check the amendment (refer to Corrigendum - II)
CAT6A Patch Cord - type - 1: Patch Cords 0.5M (Quantity: 100 number)	4.32.13	Should be certified by ETL/UL.		Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remains Unchanged
CAT6A Patch Cord - type - 2: Patch Cords 1M (Quantity: 100 number)	4.33.9	Screen material should be aluminum/polyester with tinned copper drain wire.		Kindly confirm if CAT6A Keystone Outlet can be unshielded, should OEM consider Patch cord also as U/UTP or Unshielded	Please check the amendment (refer to Corrigendum - II)
CAT6A Patch Cord - type - 2: Patch Cords 1M (Quantity: 100 number)	4.33.12	Shall be RoHS Compliant		Kindly confirm if the Jacket must be tested by NABL / BIS certified Lab	Please check the amendment (refer to Corrigendum - II)

CAT6A Patch Cord - type - 2: Patch Cords 1M (Quantity: 100 number)	4.33.13	Should be certified by ETL/UL.		Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remains Unchanged
CAT6A Patch Cord - type - 3: Patch Cords 2M (Quantity: 64 number)	4.34.9	Screen material should be aluminum/polyester with tinned copper drain wire.		Kindly confirm if CAT6A Keystone Outlet can be unshielded, should OEM consider Patch cord also as U/UTP or Unshielded	Remain Unchanged
CAT6A Patch Cord - type - 3: Patch Cords 2M (Quantity: 64 number)	4.34.12	Shall be RoHS Compliant		Kindly confirm if the Jacket must be tested by NABL / BIS certified Lab	Please check the amendment (refer to Corrigendum - II)
CAT6A Patch Cord - type - 3: Patch Cords 2M (Quantity: 64 number)	4.34.13	Should be certified by ETL/UL.		Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remains Unchanged
CAT6 IO Jacks: CAT6 IO jacks (RJ45 I/O modules) (Quantity: 500 Number)	7.16.18	Certification	Should be covered by UL/ETL certification.	Kindly confirm if OEM should submit ETL and UL separate as both are having different objective	Remains Unchanged
CAT6 Face Plates: CAT6 Face Plate (Single Port) (Quantity: 500 Number)	7.17.5	Shall be RoHS Compliant		Kindly confirm if OEM should submit Anti-Bacterial test report at the time of bid and should comply to ISO: 22196:2011	Please check the amendment (refer to Corrigendum - II)
CAT6 Face Plates: CAT6 Face Plate (Single Port) (Quantity: 500 Number)	7.17.3	Screw hole covers – to be supplied with plate, Plug in Icons – Icon tree – to be supplied with plate		Kindly confirm, instead of Screw holes covers, it should be of two plate design to fix the screws in inner plate and have professional aesthetic view with SUS304 Spring shutter on it to protect from Dust & Bug ingress	Please check the amendment (refer to Corrigendum - II)

CAT6A Face Plates: CAT6A Face Plate (Single Port) (Quantity: 100 Number)	7.20.3	Screw hole covers – to be supplied with plate, Plug in Icons – Icon tree – to be supplied with plate		Kindly confirm, instead of Screw holes covers, it should be of two plate design to fix the screws in inner plate and have professional aesthetic view with SUS304 Spring shutter on it to protect from Dust & Bug ingress	Please check the amendment (refer to Corrigendum - II)

Query - 15 (Palo Alto Networks on 05/10/2026)

Items No	**Technical Specifications**		**Response**
1.1.1.1	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall appliance should have minimum 20 core processing and management purposes along with minimum 48 GB RAM	Request to remove (SSD pair) since this is applicable in very high end applications. Usually a single SSD is sufficient for internal tasks, as all the logs can be hosted externally for redundancy.	Remains Unchanged
1.1.3.1	NGFW should have a 7 year subscription of Advanced Threat Prevention, Application Control/Identification, URL Filtering, Sandbox, DNS Security, IoT, SD-WAN, Client-based-VPN for Windows and Mac (If applicable). All updates, upgrades, and hotfixes should be applicable to a period of 7 years.	Request to change it to 5 or 6 years since hardware change and tech refresh will happen after that period in the cybersecurity space.	Please refer to the amendment (refer to Corrigendum - I) for warranty period
1.1.3.2	NGFW platform should have 24/7 OEM support via online/chat/telephone for a period of 7 years.		
1.1.3.3	NGFW hardware should have 7 years RMA warranty		

Query - 16 (iDream Networks on 12/10/2026)

				Response
1. Payment Schedule – Tender Payment Terms	Section-7: Payment Terms arrangement requires substantial financial commitment towards procurement of OEM equipment, materials, logistics and project deployment before completion of subsequent installation and commissioning activities.	Kindly review the payment terms in line with the suggested terms in the Manual for Procurement of Goods, Second Edition, 2024 pages no 141 & 142. Proposed structure for the supply component: 90% upon delivery, inspection and acceptance of goods at site with required documents, and 10% upon successful installation, configuration, commissioning, testing and acceptance. Separately identifiable installation/work components may be paid against suitable milestones determined by the procuring authority. (DOCUMENT ATTACHED) Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142.	Kindly consider suitably revising the payment terms to facilitate smooth procurement and timely execution of the project.	Remains Unchanged

2. Performance Bank Guarantee – Page 7, Clause 22	The tender specifies a Performance Bank Guarantee/Security Deposit of 5% of the supply order value.	Considering the substantial estimated project value and the comprehensive supply and implementation scope, we request the Competent Authority to kindly review the applicable PBG requirement with reference to the prevailing Ministry of Finance, Department of Expenditure procurement provisions and applicable Ministry of Education instructions.	Kindly consider a 3% as the Tender Estimated value is 14 Crore. Which is as per the Rule of Ministry of Finance, this may help reduce the financial burden on the successful bidder while retaining adequate contractual security for the Institute.	The Security Deposit/ PBG is in line with the notification of GOI. Please comply.
Liquidated Damages – Page 7, Clause 23	The existing provision stipulates liquidated damages at 0.5% per week, subject to a maximum of 10% of the order value.	Considering that the project comprises multiple equipment categories, supply activities, installation, configuration, integration and commissioning, delays in one particular component may not necessarily affect the entire project deliverables.	We kindly request the Institute to amend the Liquidated Damages (LD) clause and prescribe LD at 0.5% of the value of the delayed supply/work per week or part thereof, subject to a maximum of 5% of the total value of the order/contract, in line with the applicable	Remain Unchanged
4. EMD Exemption – Page 5, Clause 12	The scope of the tender includes supply, installation, configuration, integration, testing and commissioning of the proposed IT/network infrastructure.	Also, The Tender published under the Services Category for "Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure." (Screenshot of CPPP Portal Enclosed)	we request the Tender Inviting Authority to consider the provisions of Rule 170(i) of the General Financial Rules (GFR), 2017, read with the Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012, as amended, regarding exemption from payment of Earnest Money Deposit (EMD) for eligible MSEs.	

Query - 17 (Takyon Networks Limited on 12/10/2026)

Pre-Bid Queries – Section 5: General Conditions, Sl. No. 3 (Past Performance)	

Sl.	RFP Ref. (Page / Clause)	Existing Clause	Query / Clarification Requested	Justification	Response
1	Page 38, Section 5, Sl. No. 3-A, Table-1	Table-1 includes "Firewall/ADC – 2 Nos" as part of the quantities to be demonstrated in completed Campus Wide Network (LAN) projects.	We request that "Firewall/ADC – 2 Nos" be removed from Table-1. Alternatively, the bidder may be allowed to demonstrate Firewall/ADC experience through a separate Purchase Order / Completion Certificate from any of the eligible institutions listed in Clause 3. This need not be part of the LAN project(s) submitted under Clause 3-A.	In campus networks at IISERs, IITs, NITs, Institutes of National Importance and Government universities, perimeter security (Firewall/ADC) is usually procured under a separate tender or PO, often at a different time from the LAN work. LAN completion certificates therefore normally do not include Firewall/ADC, even when the same bidder supplied them. Linking security quantities to the LAN project would exclude experienced campus-network integrators for a reason unrelated to their LAN capability.	Remain Unchanged

2	Page 38, Section 5, Sl. No. 3-A, Table-1 (L3 Fibre Switches – 30 Nos; L2 Switches – 80 Nos)	Past performance is to be demonstrated through separate quantity thresholds for L3 Fibre Switches and L2 Switches, at 80%/60%/40% in one/two/three completed projects.	We request that past performance for network switching be assessed on either of the following, instead of separate quantities for each switch category: (a) Order value: completed campus network project(s) of value equal to 80% / 60% / 40% (for one / two / three projects respectively) of the estimated cost of the present work; or (b) Total number of managed switches: core, distribution and access switches taken together, with the 80% / 60% / 40% thresholds applied to the combined quantity (i.e. 110 Nos as per Table-1).	(a) The number of distribution or aggregation switches in a campus network depends on design choices: chassis-based versus fixed-configuration switches, collapsed-core designs, stacking and port density. A campus of the same scale may be designed with 5 high-density distribution switches or with 20 lower-density ones. A category-wise count therefore does not reflect the scale or complexity of the network the bidder has delivered. (b) Table-1 already captures network scale directly through “I/O ports as last-mile connection – 1000 Nos”. Assessing switching experience on order value or total switch count, together with the last-mile port count, gives a fair measure of comparable experience regardless of the design approach used. (c) Setting similar-work thresholds as a percentage of the estimated cost of the present work is the established practice in Government procurement.	Remains Unchanged

3	Page 38, Section 5, Sl. No. 3-A, Table-1 (L3 Fibre Switches – 30 Nos), read with Section 4: List of Materials	Table-1 specifies "L3 Fibre Switches – 30 Nos", to be demonstrated at 80%/60%/40% in one/two/three completed projects.	Without prejudice to Query No. 2, in case the category-wise quantities are retained, we request that the "L3 Fibre Switches" quantity in Table-1 be revised to match the quantity actually required under Section 4, i.e. 20 distribution switches [+ __ core switches], with the 80%/60%/40% thresholds applied to this revised quantity.	Section 4 requires only 20 distribution switches, but Table-1 sets the benchmark at 30 L3 fibre switches. Even at the 80% option, the bidder must show 24 such switches in one project, which is more than the quantity being procured in this tender. Under the standard 80%/60%/40% practice, past-performance thresholds are set as a percentage of the work being tendered, not above it.	Bidders shall refer to the Scope of Work, schematics, and system design documents for clarification regarding the different types of switches and their respective requirements. For the number of switches and type, please check the amendment (refer to Corrigendum - II)
4	Page 38, Section 5, Sl. No. 3-A, Table-1 (L3 Fibre Switches; L2 Switches)	The bidder shall satisfy any one of: one completed project with at least 80%, two completed projects each with at least 60%, or three completed projects each with at least 40% of the quantities listed in Table-1.	Without prejudice to Query No. 2, in case the category-wise quantities are retained, we request that the switch quantities in Table-1 be assessed item-wise and cumulatively across completed campus network projects / Purchase Orders executed in the eligible institutions listed in Clause 3 during the last seven years. Under this, the bidder may meet the L3 Fibre Switch quantity and the L2/Access Switch quantity through separate POs. It should not be necessary for both to appear in the same project.	(a) Campus networks in academic institutions are usually built and expanded in phases. The fibre backbone with core/distribution switches and the building-level access layer are often procured under different POs at different times. Requiring both quantities in the same project would exclude bidders with equal or larger cumulative campus experience. (b) Clause 3 already states that similar quantities shall be assessed on the cumulative deployment of comparable campus-wide networking equipment, such as managed switches, fibre backbone connectivity, structured cabling and network commissioning. Item-wise cumulative assessment applies this provision directly.	For the number of switches and type, please check the amendment (refer to Corrigendum - II)

5	Page 38, Section 5, Sl. No. 3-A, Table-1 (L3 Fibre Switches)	Table-1 refers to "L3 Fibre Switches" without defining which switch categories qualify.	Please confirm that "L3 Fibre Switches" includes core, distribution and aggregation switches with fibre ports, deployed in campus backbone networks.	Past campus orders describe backbone switches in different ways (core, distribution, aggregation, backbone). A clear definition will ensure all bidders' credentials are evaluated on the same basis during technical evaluation.	Experience of CS, DS and aggregations switches may be considered, provided they all are L3 fibres switches. For the number of switches and type, please check the amendment (refer to Corrigendum - II)
6	Page 38, Section 5, Sl. No. 3-A, Table-1 (L2 Switches – 80 Nos), read with Section 4, Item 2.8	Table-1 refers to "L2 Switches" as the access-layer quantity to be demonstrated.	Please confirm that "L2 Switches" includes managed access/edge switches, whether Layer-2 or Layer-3.	The access switches specified in Section 4 (e.g. Item 2.8, AS Type-5) are themselves Layer-3 managed switches. Counting only "L2 Switches" from past orders would exclude Layer-3 access switch deployments that match the present requirement better.	For the number of switches and type, please check the amendment (refer to Corrigendum - II) Experience in AS shall also be considered as relevant experience for L3 Base-T switches and L2 Base-T switches. However, the products offered shall strictly comply with the specifications prescribed in the tender document.

7	Page 38, Section 5, Sl. No. 3-B, read with Section 4, Item Nos. 3.1 to 3.3 and 3.7 (Pages 33–34)	The bidder should have supplied and deployed the software stack (Item Nos. 3.1 to 3.9 in Section 4: List of Materials).	We request that Clause 3-B be modified as follows: "The bidder should have supplied and deployed (i) a Network Access Control (NAC) solution with AAA/RADIUS (802.1X) based authentication, and (ii) a Network Management System (NMS), in IISERs, IITs, NITs, any other Institute of National Importance, or Central/State funded Government Universities and academic institutions during the last seven years. Each may be demonstrated through separate Purchase Orders / Completion Certificates, from the same or different institutions, and need not be part of the project(s) submitted under Clause 3-A."	(a) In education campuses, NAC and NMS are usually procured as separate orders or at different stages of the network lifecycle, often after the LAN is commissioned. Requiring the full software stack in a single order would exclude bidders who have deployed each of them in comparable institutions. (b) NAC functionally covers Items 3.1, 3.2 and 3.3. Item 3.2 itself requires NAC integration with AAA, and RADIUS/802.1X is the authentication mechanism NAC uses. Customers normally procure NAC as one solution, and AAA and RADIUS are rarely ordered or certified as separate line items. (c) Keeping the requirement to the education-sector institutions listed in Clause 3 preserves the intent of the criterion.	Remains unchanged

8	Page 38, Section 5, Sl. No. 3-B, read with Section 4, Item Nos. 3.4, 3.5, 3.6, 3.8 and 3.9 (Pages 33–34)	The bidder should have supplied and deployed the software stack (Item Nos. 3.1 to 3.9 in Section 4: List of Materials).	We request that, for Item 3.4 (LDAP), Items 3.5 and 3.6 (Internal and External DNS), Item 3.8 (Syslog) and Item 3.9 (Software Stack Deployment), the bidder's ability be accepted through a self-declaration / undertaking to deploy and commission these services as per the scope of work and acceptance tests. These items should not be part of the past-performance criterion.	(a) Item 3.9 is a deployment activity, not a supplied product. It requires DHCP, DNS, Directory (DC/ADC and LDAP), NTP, Syslog and User Access Log to be configured, preferably on open source. (b) Items 3.4, 3.5, 3.6 and 3.8 are repeated within Item 3.9. Open-source services are set up during commissioning and are not listed as separate line items in POs, so item-wise documentary proof does not normally exist for them. (c) Delivery of these services is better secured through the scope of work, acceptance testing and the performance security than through item-wise past orders.	Remains Unchanged

Query - 18 (Fortinet (2nd Representation) on 12/10/2026)

Clause Heading	**Spec. Number**	**Parameters**	**Sub Items No**	**Technical Specifications**	**Change Request**	**Justification**	**Response**
Corrigendum 1	Details of Specifications of the Stores	Warranty Period	2	The Warranty period is being amended from 7 Years to 5 Years. Now the bidder has to bid with 5 year warranty + 3 Years CAMC. The bidder has to quote the cost of year-wise CAMC separately. The cost of	Please clarify on CAMC.Does CAMC include back to back OEM support?		Yes CAMC required back-to-back OEM support

				additional three years CAMC will be included for evaluating the L1 bidder			
Annexure – 5: Check List to be submitted by Bidder/OEM	NA	NA	8	A letter of commitment for seven years from the date of installation, with respect to hardware and firmware support from OEM should be enclosed in the cover for a technical bid.	Please amend the clause to A letter of commitment for seven years from the date of **bid submission**, with respect to hardware and firmware support from OEM should be enclosed in the cover for technical bid.		The warranty period shall start as per the clause - 4, Annexure - 7: SLA.
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1	Hardware features and throughputs	1.1.1.1	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall appliance should have minimum **20** core processing and management	Not exceeding 2U, 19" standard rack hardware based NGFW along with inbuilt Trusted Platform Module (TPM) and Internal Storage of Min.480 GB SSD pair or higher. Proposed Network Firewall	Every OEM has its own architecture and methodology to process the traffic and restricting their participation specifically on cores does not allign with their performance capabilities and restricts their participation.	Remains Unchanged

				purposes along with minimum 48 GB RAM	appliance should have minimum **16** core processing and management purposes along with minimum 48 GB RAM		
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.2	Next Gen Firewall throughput measured with Application Control/Identification and logging enabled, utilizing L7 transactions should be 25 Gbps or higher |OR| 32 Gbps or higher standard NGFW performance as measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.	Please amend the clause to "Next Gen Firewall throughput measured with Application Control/Identification and logging enabled, utilizing **HTTP** transactions should be **35** Gbps or higher"	We request the authority to kindly consider defining a common and equivalent performance benchmark for all OEM's. A standardized benchmark will ensure fair comparison and wider OEM participation.As per our understanding all leading OEM measure Application Control throughput in HTTP transactions only.	Remains Unchanged
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.3	Threat Prevention throughput measured with Application Control/Identification, IPS, antivirus, antispyware, sandboxing, file blocking, and logging enabled, utilizing L7 transactions should be 15 Gbps or higher |OR| 30 Gbps or higher	Please amend the clause to threat protection throughput measured with Firewall, IPS, Application Control, and Malware Protection enabled	We request the authority to kindly consider defining a common and equivalent performance benchmark for all OEM's. A standardized benchmark will ensure fair comparison and wider OEM participation.As per our understanding all leading OEM measure threat	Remains unchanged

				standard Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic	(enterprise mix traffic) **should be 25 Gbps or higher**	protection throughput in enterprise mix traffic only.	
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.5	Max concurrent sessions are measured utilizing L7 transactions should be 2 million or higher |OR| Concurrent Sessions (TCP) should be minimum 40 million	Please amend the clause to Max concurrent sessions are measured utilizing **HTTP** transactions should be **10** million or higher |OR| Concurrent Sessions (TCP) should be minimum **20** million	We request the authority to kindly consider a common and equivalent methodology for evaluating concurrent sessions, as OEMs may publish session capacity using different traffic profiles and measurement methodologies. This will ensure a fair comparison and allow wider OEM participation. As per our understanding all leading OEM measure concurrent sessions in either HTTP or TCP sessions only	Remains Unchanged

Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.6	New sessions per second utilizing L7 transactions should be 200K or higher |OR| New Sessions/Second (TCP) should be minimum 600K	Please amend the clause to New sessions per second utilizing **HTTP** transactions should be **400K** or higher |OR| New Sessions/Second (TCP) should be minimum 600K	We request the authority to kindly consider a common and equivalent methodology for evaluating concurrent sessions, as OEMs may publish session capacity using different traffic profiles and measurement methodologies. This will ensure a fair comparison and allow wider OEM participation. As per our understanding all leading OEM measure new sessions per second in either HTTP or TCP sessions only	Remains Unchanged
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1 Page No. 69	Hardware features and throughputs	1.1.1.7	Minimum I/O Ports required from Day 1: Min.1G/2.5G/5G/10G (12 Nos.), 1G/10G SFP/SFP+ (10 Nos.), 25G SFP28 (4 Nos.), 40G/100G QSFP/QSFP28 (2 Nos.) For each NGFW: SFP+ I/O ports to be loaded with atleast 2 Nos. SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex	Please amend the clause to Minimum I/O Ports required from Day 1: Min.1G/10G RJ 45 Ports (12Nos.), 1G/10G SFP/SFP+ slots (10 Nos.), 25G SFP28 slots (4 Nos.), 40G/100G QSFP/QSFP28 slots (**4 Nos.**) For each NGFW:		Please check the amendment (refer to Corrigendum - II)

				LC, IEEE 802.3ae 10GBASE-SR compliant. QSFP28 I/O ports to be loaded with atleast 2 Nos. QSFP+ form factor, 40Gb SR4 optical transceiver, short reach 100m OM3, 8/12 strand MPO connector, IEEE 802.3ba 40GBASE-SR4 compliant	1. SFP+ I/O slots to be loaded with atleast 2 Nos. SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant. 2. QSFP28 I/O slots to be loaded with atleast 2 Nos. QSFP+ form factor, SR 25Gb optical transceiver, short reach 100m, MMF, duplex LC, IEEE 802.3ae 25GBASE-SR compliant. 3. QSFP+ I/O slots to be loaded with at least 2 Nos. QSFP+ form factor, 40Gb SR4 optical transceiver, short reach 100m OM3, 12 strand		

					MPO connector, IEEE 802.3ba 40GBASE-SR4 compliant		
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.1	Hardware features and throughputs	1.1.1.10	Power Supply: Redundant 100–240 VAC (50–60Hz) Operating temperature: 0°C to **50°C** Humidity tolerance: 10% to 90%	Power Supply: Redundant 100–240 VAC (50–60Hz) Operating temperature: 0°C to **40°C** Humidity tolerance: 10% to 90%	We request the authority to kindly consider this revision to avoid restricting participation based on a specific operating-temperature specification and to allow wider OEM participation. The appliance will be placed in the datacentre with enough cooling, please approve the change.	Remains Unchanged
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.7	IPsec **and** SSL VPN: Key exchange: manual key, **IKEv1**, and IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3des, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Secure access over IPsec or SSL VPN tunnels using VPN Gateway	Please amend the clause to IPsec **or** SSL VPN: Key exchange: manual key, IKEv2 (pre-shared key, certificate-based authentication) Encryption: 3des, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1,	Most global cybersecurity OEMs are dropping support for IKEv1 as it is legacy protocol. We request the authority to kindly consider this revision considering IKEv2 as the current-generation IPsec key-exchange protocol supporting the required authentication mechanisms. This will allow wider OEM participation while retaining the required IPsec VPN functionality.	Remains Unchanged

				and portals	SHA-256, SHA-384, SHA-512 Secure access over IPsec or SSL VPN tunnels using VPN Gateway and portals		
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.8	The proposed solution should support remote user based VPN clients for Windows. Module should be Common Criteria certified for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	Please amend the clause to "The proposed solution should support remote user based VPN clients for Windows"	Please allow the change to allow wider OEM participation, as most OEMs do not restrict their agent for VPN functionalities and offer a unified agent with more capabilities like EPP, ZTNA, VA on the same agent so this clause restrict the participation.	Please check the amendment (refer to Corrigendum - II)
Annexure – 9: Specifications - Next Generation	1.1.2	Software/OS/Platform features	1.1.2.13	Should provide visibility into TLS traffic, such as the amount of encrypted traffic, SSL/TLS versions, cipher suites, and more,	Please amend the clause to "Should provide visibility into TLS traffic, including SSL/TLS versions, cipher	We request the authority to kindly consider this revision to focus on the required visibility into TLS traffic and associated security parameters without	Remain unchanged

Firewall (NGWF)				without decrypting.	suites, without decrypting"	prescribing a specific reporting methodology. This will allow wider OEM participation while retaining the intended security objective.	
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.2	Software/OS/Platform features	1.1.2.17	Should prevent corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.	Please amend the clause to "Should help prevent corporate credentials from being submitted to malicious/unauthorized third-party websites and should support network-layer MFA for protected applications/access scenarios without requiring changes to the protected application"	We request the authority to kindly consider this revision to retain the intended security objective of credential protection and network-layer MFA while allowing equivalent technologies and architectures to participate. This will enable wider OEM participation.	Please check the amendment (refer to Corrigendum - II)
Annexure – 9: Specifications - Next Generation	1.1.4	Certifications	1.1.4.1	ISO 27001, ISO 27017, ISO 42001	Please amend the clause to "ISO 27001, ISO 27017"	Please allow this change, as this certificate is quite latest and most of the global NGFWs OEMs are still in the application process of this certificate, but they have	Please check the amendment (refer to Corrigendum - II)

Firewall (NGWF)						built their AI capabilities by keeping the standards of this certification in consideration.	
Annexure – 9: Specifications - Next Generation Firewall (NGWF)	1.1.4	Certifications	1.1.4.6	Following OEM certificates to be uploaded: a. Land Border Declaration b. Manufacturer Authorization Form for bidder c. Escalation Matrix and Toll Free Support Number d. SELF-CERTIFICATION for MII e. Non-Malicious Code Certificate f. Non-Blacklisting Declaration g. End of Life/Support of the Hardware h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625	Please amend the clause to Following OEM certificates to be uploaded: a. Land Border Declaration b. Manufacturer Authorization Form for bidder c. Escalation Matrix and Toll Free Support Number d. SELF-CERTIFICATION for MII e. Non-Malicious Code Certificate f. Non-Blacklisting Declaration g. End of Life/Support of the Hardware	Please allow the change to allow wider OEM participation, as most OEMs do not restrict their agent for VPN functionalities and offer a unified agent with more capabilities like EPP, ZTNA, VA on the same agent so this clause restricts the participation.	Please check the amendment (refer to Corrigendum - II)

				Functional Package for SSH Version 1. 0 PP-Module for Intrusion Prevention Systems (IPS), Version 1. 0 PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 Collaborative Protection Profile for Network Devices Version 3. 0e i. Common Criteria for VPN agent, following criteria must be validated: Functional Package for TLS Version 1.1 Protection Profile for Application Software Version 1.4	h. Common Criteria for NGFW, following criteria must be validated: collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 Functional Package for SSH Version 1. 0 PP-Module for Virtual Private Network (VPN) Gateways Version 1.3 Collaborative Protection Profile for Network Devices Version 3. 0e		

Annexure – 9: Specifications - Next Generation Firewall (NGWF)	NA	NA	NA	New Suggestion	The proposed firewall shall support SSL inspection (including TLS 1.3) and shall provide a minimum SSL Inspection throughput of 20 Gbps and support at least 2 million SSL Inspection concurrent sessions.	SSL/TLS inspection is essential with the increasing use of HTTPS encrypted traffic and threats such as malware, malicious downloads and unauthorized application activity can be concealed within encrypted sessions. Without SSL/TLS decryption and inspection, critical NGFW security controls such as IPS, Anti-Malware, Application Control and URL Filtering may have limited visibility into the actual content of the traffic. Therefore, defining minimum SSL Inspection throughput and concurrent SSL/TLS session capacity is necessary to ensure that encrypted traffic can be inspected at the required scale without creating a security or performance gap.	Not Applicable

Annexure – 9: Specifications - AAA Server:	3.1.1.	Make	3.1.1.2	The offered solution shall be ON Premises Virtual appliance to be provided in High Availability with all the necessary Operating system, required RAM, CPUs to cater the required number of devices mentioned in the subsequent clause. Licenses/subscriptions should be provided to 5000 users with 3 devices each from day 1.	The offered solution shall be ON Premises Virtual appliance to be provided in High Availability with all the necessary Operating system, required RAM, CPUs to cater the required number of devices mentioned in the subsequent clause. **Perpetual licenses** shall be provided for 5000 users with 3 devices each from day 1.		Remains Unchanged
Annexure – 9: Specifications - AAA Server:	3.1.2	Functionality	3.1.2.3	Solution should support up to 5000 users with 3 devices each from day 1. Licenses/Subscription to be considered accordingly. The solution should be scalable to support 20000 users or more in future.	The solution should support a minimum 5000 users with 3 devices each from day 1. **Perpetual licenses** to be considered accordingly. The solution should be		Remains Unchanged

					scalable to support 20000 users or more in future.		
Annexure – 9: Specifications - AAA Server:	3.1.2	Functionality	3.1.2.6	Solution should have device profiling functionality	It's a NAC feature. Please put this clause under NAC		Remains Unchanged
Annexure – 9: Specifications - AAA Server:	3.1.5	Licenses/Subscription & support	3.1.5.1	Perpetual license with 7 Year OEM TAC and OS support for all licenses and Software. All software and Hardware should be included in the solution for 20000 users.	Perpetual license with 7 Year OEM TAC and OS support for all licenses and Software. All software and Hardware should be included in the solution for **5000** users **from day 1**		Remains Unchanged
Annexure – 9: Specifications - AAA Server:	3.1.6	Mandatory compliance	3.1.6.1	All switches, NMS, Transceivers, AAA should be from the same OEM for better inter operatability, management and support.	Please remove AAA from this clause for wider OEM participation.		Please check the amendment (refer to Corrigendum - II)

Annexure – 9: Specifications - Network Access Control (NAC)	3.2	Network Access Control (NAC)	3.2	Network Access Control (NAC): Supply, installation, configuration, integration, testing, and commissioning of a Network Access Control (NAC) solution for device authentication, endpoint posture assessment, policy-based network access enforcement, guest/BYOD management, and integration with AAA, LDAP/Active Directory, and network Infrastructure.	Please clarify the total number of endpoints/devices, maximum concurrent endpoints, number of switches, number of access points, other network infrastructure devices requiring NAC integration to be supported by the NAC solution		The number of users, devices, and other relevant infrastructure parameters are already indicated at appropriate places in the tender document.
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.1	GENERAL	1.2.1.5	The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects and shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	Please amend the clause to The Controller/Container Plugin shall support orchestration to dynamically create and manage WAF objects.	For wider OEM participation please allow this change	The requirement for per-namespace operations is intended to provide granular WAF policy and service management in containerized environments. Remain unchanged
Annexure – 9: Specifications -	1.2.1	GENERAL	1.2.1.6	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should	Please amend the clause to Controller/Container Plugin should	For wider OEM participation please allow this change	Remain unchanged

Application Delivery Controllers (ADC)				register to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource Queue maintained by the controller.	use Custom resources extensions of the Kubernetes API. It should register to the Kubernetes using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to and maintained by the controller.		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.3	Load Balancing Features	1.2.3.3	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2	Please amend the clause to Server Load Balancer should support for the following databases for health checks: • Oracle • MSSQL • MySQL •	For wider OEM participation please allow this change	Remain unchanged

Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.3	Load Balancing Features	1.2.3.4	The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, Nagle Algorithm, delay window control, packet loss ignore rate, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of traffic compression processing to improve page load times and reduce bandwidth utilization.	Please amend the clause to The proposed solution must provide below application optimization features: 1) TCP Optimization: Should be able to modify TCP parameters like keep alive interval, maximum RTO, window size, delay window control, flow control, congestion control speed etc. on the fly to improve application performance 2) Hardware based Compression: Solution should be able to provide cost-effective offloading of	For wider OEM participation please allow this change	Remain unchanged

				3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance	traffic compression processing to improve page load times and reduce bandwidth utilization. 3) Caching: Solution should be able to do caching to reduce network traffic and increase application performance		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.3	A given user must be enforced to follow a sequence of pages while accessing without any script and should have provision to apply the restriction to the application or part of the application based on Geo Location	Please amend the clause to A given user must be enforced to follow and should have provision to apply the restriction to the application	For wider OEM participation please allow this change	Remain unchanged

Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.4	The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.	Please amend the clause to The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including and. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated	For wider OEM participation please allow this change	Remain unchanged

					for audit and compliance.		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.6	The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	Please amend the clause to The solution should have pre-built templates for well-known applications attack signatures.	For wider OEM participation please allow this change	Remain unchanged
Annexure – 9: Specifications - Application Delivery	1.2.4	WAF FEATURES	1.2.4.8	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for	Please amend the clause to The WAF Solution should have mechanism to block	For wider OEM participation please allow this change	Remain unchanged

Controllers (ADC)				set amount of time (Tarpit action)	bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.9	System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.10	The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance (without accessing the internet/cloud service) to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCI DSS compliance requirements for web application servers. Necessary logs to be generated for audit and compliance.	Please amend the clause to The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting. The Solution should have inbuilt ability within the appliance to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCI DSS compliance requirements for web application servers.	For wider OEM participation please allow this change	Remain unchanged

					Necessary logs to be generated for audit and compliance.		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.15	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.16	The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.	Please amend the clause to The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including	For wider OEM participation please allow this change	Remain unchanged

Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.17	The WAF must provide BOT mitigation functionality (including CAPTCHA) without having to go on internet for some cloud based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc.	The WAF must provide BOT mitigation functionality (including CAPTCHA) and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc.	For wider OEM participation please allow this change	Remain unchanged
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.20	The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation • Backend application parser protection against XML DOS • XML Encryption and XML Signatures • Granular WSDL methods selection	Please amend the clause to The solution should be able to protect web applications that include Web services (XML) content like: • Full Schema/WSDL validation	For wider OEM participation please allow this change	Remain unchanged

					• XML Encryption and XML Signatures		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.4	WAF FEATURES	1.2.4.21	The proposed solution must support SSL VPN and Single Sign On functionality on the same hardware solution running on the same OS version from the same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups:	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

				* Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and the same should be configurable. * Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken			
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.7	MONITORING, LOGGING AND REPORTING	1.2.7.1	The proposed solution should have the capability to create a granular logging policy per application. The system shall have the ability to customize logging. The proposed solution should have the capability	Please amend the clause to The proposed solution should have the capability to create a granular logging policy per application. The	For wider OEM participation please allow this change	Remain unchanged

				to define a customized log format for each application.	system shall have the ability to customize logging.		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.7	MONITORING, LOGGING AND REPORTING	1.2.7.2	The proposed solution should have the capability to define multiple log destinations for each application	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.8.2	ADMINISTRATION	1.2.8.2	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used	Please amend the clause to The solution must support the following password management capabilities without relying on any external system: b. Password length (minimum required number of	For wider OEM participation please allow this change	Remain unchanged

				d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)	characters in the password.) d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not. (Password Complexity)		
Annexure – 9: Specifications - Application Delivery Controllers (ADC)	1.2.9	Product / OEM Evaluation Criteria	1.2.9.1	WAF / WAF's Operating System should be tested and certified for NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged
Annexure – 9: Specifications - Application Delivery	1.2.9	Product / OEM Evaluation Criteria	1.2.9.2	The WAF solution should be in the Gartner's/Kpingercole/ SecureIQ Magic Quadrant of Latest published Report Web Application and	Please delete this clause	For wider OEM participation please allow this change	Remain unchanged

Controllers (ADC)				API Protection/WAF.			

Query - 19 (Momentum Techsys Private Limited on 13/10/2026)

						Response
1	Liquidated Damages	Page 7, Clause 23.	The existing provision stipulates liquidated damages at 0.5% per week, subject to a maximum of 10% of the order value. Considering that the project comprises\multiple equipment categories, supply activities, installation, configuration, integration and commissioning, delays in one particular component may not necessarily affect the entire project deliverables.		Request: We kindly request the Institute to amend the Liquidated Damages (LD) clause and prescribe LD at 0.5% of the value of the delayed supply/work per week or part thereof, subject to a maximum of 5% of the total value of the order/contract, in line with the applicable	Remain Unchanged

2	Payment Schedule – Tender Payment Terms.		The existing milestone-based payment as per Section-7: Payment Terms arrangement requires substantial financial commitment towards procurement of OEM equipment, materials, logistics and project deployment before completion of subsequent installation and commissioning activities.	Considering the significant supply component involved in the project, we request that the payment terms may kindly be considered as follows. 90% payment upon delivery, inspection and acceptance of the supplied equipment/materials at site and 10% payment upon successful installation, configuration, commissioning, testing and final acceptance. Therefore, Kindly review the payment terms in line with the suggested terms in the Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142. Proposed structure for the supply component: 90% upon delivery, inspection and acceptance of goods at site with required documents, and 10% upon successful installation, configuration, commissioning, testing and acceptance. (DOCUMENT ATTACHED) Manual for Procurement of Goods, Second Edition, 2024 page no 141 & 142.	Request: Kindly consider suitably revising the payment terms to facilitate smooth procurement and timely execution of the project.	Remain Unchanged

3	EMD Exemption	Page 5, Clause 12	The scope of the tender includes supply, installation, configuration, integration, testing and commissioning of the proposed IT/network infrastructure. Also, The Tender published under the Services Category for "Design, Supply, Installation, Testing, Commissioning, Integration & Support of Core Network Infrastructure." (Screenshot of CPPP Portal Enclosed)	In this regard, we request the Tender Inviting Authority to consider the provisions of Rule 170(i) of the General Financial Rules (GFR), 2017, read with the Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012, as amended, regarding exemption from payment of Earnest Money Deposit (EMD) for eligible MSEs. Accordingly, we request that the EMD clause be suitably amended to extend the applicable exemption to eligible Micro and Small Enterprise service providers holding valid Udyam/MSME and/or NSIC registration under the relevant service category/NIC Code, subject to the applicable Government of India procurement rules and eligibility conditions.	We therefore request Competent Authority to issue a suitable clarification/corrigendum permitting eligible MSE service providers to claim EMD exemption wherever admissible under the prevailing rules, thereby ensuring fair competition and wider participation of eligible MSEs in Government procurement.	The EMD applicable as per procurement rules has been mentioned in the tender document. As per the bid estimation the majority of the bid value comprises of the equipment. Hence, bidders are requested to comply with the rules.
4	Performance Bank Guarantee	Page 7, Clause 22		The tender specifies a Performance Bank Guarantee/Security Deposit of 5% of the supply order value. Considering the substantial estimated project value and the comprehensive supply and implementation scope, we request the Competent Authority to kindly review the applicable PBG requirement with reference to the prevailing Ministry of Finance, Department of Expenditure procurement provisions and applicable Ministry of Education instructions.	Request: Kindly consider a 3% as the Tender Estimated value is 14 Crore. Which is as per the Rule of Ministry of Finance, this may help reduce the financial burden on the successful bidder while retaining adequate contractual security for the Institute.	The Security Deposit/ PBG is in line with the notification of GOI. Please comply.

5	Next Generation Firewall (NGFW)	Annexure 9, Section 4, Page 69, Clause 1.1.		The NGFW heading specifies port configurations that differ from the detailed technical specifications.	Request: We request that the heading be aligned with the detailed requirements for minimum Day-1 I/O ports: 12 × 1G/2.5G/5G/10G ports, 10 × 1G/10G SFP/SFP+ ports, 4 × 25G SFP28 ports and 2 × 40G/100G QSFP/QSFP28 ports. Each firewall shall include at least 2 × 10G SFP+ SR optical transceivers supporting 300 m over OM3 multimode fibre, duplex LC, compliant with IEEE 802.3ae 10GBASE-SR	Please check the amendment (refer to Corrigendum - II)
6	Access Switch Type 2	Page 91, Clause 2.5			We request that the heading be aligned with the detailed specification to clearly specify 48 × 10/100/1000Base-T RJ45 ports and 4 × 10/25G SFP28 uplink ports, operational from Day 1. as these are not explicitly mentioned in the detailed specifications.	Please check the amendment (refer to Corrigendum - II)

7	Access Switch Type 3	Page 93, Clause 2.6			We request that the heading be aligned with the detailed specification to specify 24 × 10/100/1000Base-T RJ45 ports and 4 × 10/25G SFP28 uplink ports, operational from Day 1, while retaining the stipulated Layer 3 capabilities and minimum switching capacity.	Please check the amendment (refer to Corrigendum - II)
8	Access Switch Type 4	Page 96, Clause 2.7			We request that the heading be amended to specify 16 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplink ports, operational from Day 1.	Please check the amendment (refer to Corrigendum - II)
9	Access Switch Type 5	Page 97, Clause 2.8			We request that the heading be amended to specify 8 × 10/100/1000Base-T PoE+ RJ45 ports and 2 × 1G/10G SFP+ uplink ports, operational from Day 1.	Please check the amendment (refer to Corrigendum - II)

Query - 20 (CSK Information Technology Pvt. Ltd. on 12/10/2026)

S No	**RFP clauses**	**RFP specs as per bid**	**request amendments**	**Response**
1	General	General	As per the latest Make in India guidelines (attached) dated 11 September 2025, the minimum local content requirement is 60% for switches and 65% for firewalls. Kindly confirm whether these minimum local content requirements are applicable to the switches and firewalls covered under this tender	The attachment provided is “Notice for inviting Stakeholders Comments”, only. Please comply with the guidelines notified by GoI through orders/OMs in regard to MII.