

Request for Proposal (RFP) for Design, Deployment, Integration, Operation, and Maintenance of an SD-WAN Overlay Solution over the existing GSWAN Hybrid WAN Architecture across the State of Gujarat (Tender ID 331499 on (n) procure portal dated 05-08-2026) (Pre-bid queries response)				
S.No	SECTION / Clause Ref	RFP Clause / Requirement	Change Requested by Bidder	Tenderer Response
1	SD-WAN HUB CPE Specification	The device should have minimum 64 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
2	(District HQ) CPE Specification	The device should have minimum 32 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
3	(Taluka HQ) CPE Specification	The device should have minimum 8 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
4	For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
5	SIM Based (For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
6	SD-WAN HUB CPE Specification	The device should have minimum 64 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
7	(District HQ) CPE Specification	The device should have minimum 32 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
8	(Taluka HQ) CPE Specification	The device should have minimum 8 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
9	For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
10	SIM Based (For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
11	SD-WAN HUB CPE Specification	The device should have minimum 64 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
12	(District HQ) CPE Specification	The device should have minimum 32 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
13	(Taluka HQ) CPE Specification	The device should have minimum 8 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
14	For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
15	SIM Based (For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
16	SD-WAN HUB CPE Specification	The device should have minimum 64 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
17	(District HQ) CPE Specification	The device should have minimum 32 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
18	(Taluka HQ) CPE Specification	The device should have minimum 8 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
19	For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
20	SIM Based (For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
21	SD-WAN HUB CPE Specification	The device should have minimum 64 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
22	(District HQ) CPE Specification	The device should have minimum 32 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
23	(Taluka HQ) CPE Specification	The device should have minimum 8 GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
24	For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum

25	SIM Based (For office location) CPE Specification	The device should have minimum 8GB RAM	The device should have sufficient memory to meet the RFP Requirement of SD-WAN throughput, IPsec performance, security throughput.	Pls. refer corrigendum
26	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
27	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN HUB and SPOKE appliance must be with native integrated NGFW security features including IPS, anti-malware, Malicious malware filtering, SSL inspection, DNS security, and application control without requiring separate security application hosting, additional virtualized security modules, or external security appliances and meet all the RFP specifications.	Pls. refer corrigendum
28	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 78 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 78 Gbps throughput from Day 1 with all required security services enabled.	Pls. refer corrigendum
29	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
30	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
31	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN HUB and SPOKE appliance must be with native integrated NGFW security features including IPS, anti-malware, Malicious malware filtering, SSL inspection, DNS security, and application control without requiring separate security application hosting, additional virtualized security modules, or external security appliances and meet all the RFP specifications.	Pls. refer corrigendum
32	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 78 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 78 Gbps throughput from Day 1 with all required security services enabled.	Pls. refer corrigendum
33	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN HUB and SPOKE appliance must be with native integrated NGFW security features including IPS, anti-malware, Malicious malware filtering, SSL inspection, DNS security, and application control without requiring separate security application hosting, additional virtualized security modules, or external security appliances and meet all the RFP specifications.	Pls. refer corrigendum

34	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 78 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 78 Gbps throughput from Day 1 with all required security services enabled.	Pls. refer corrigendum
35	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN HUB and SPOKE appliance must be with native integrated NGFW security features including IPS, anti-malware, Malicious malware filtering, SSL inspection, DNS security, and application control without requiring separate security application hosting, additional virtualized security modules, or external security appliances and meet all the RFP specifications.	Pls. refer corrigendum
36	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 78 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 78 Gbps throughput from Day 1 with all required security services enabled.	Pls. refer corrigendum
37	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
38	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN HUB and SPOKE appliance must be with native integrated NGFW security features including IPS, anti-malware, Malicious malware filtering, SSL inspection, DNS security, and application control without requiring separate security application hosting, additional virtualized security modules, or external security appliances and meet all the RFP specifications.	Pls. refer corrigendum
39	SD-WAN HUB CPE Specification	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	The SD-WAN appliance shall support 78 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 78 Gbps throughput from Day 1 with all required security services enabled.	Pls. refer corrigendum
40	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply and sufficient fan modules/fanless Air cooling.	No Change, as per RFP
41	(District HQ) CPE Specification	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules	The Device must have dual/redundant power supply and sufficient cooling as per OEM hardware design	No Change, as per RFP
42	(Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply	No Change, as per RFP
43	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply and sufficient fan modules/fanless Air cooling.	No Change, as per RFP
44	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply and sufficient fan modules/fanless Air cooling.	No Change, as per RFP
45	(District HQ) CPE Specification	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules	The Device must have dual/redundant power supply and sufficient cooling as per OEM hardware design	No Change, as per RFP
46	(Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply	No Change, as per RFP
47	(District HQ) CPE Specification	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules	The Device must have dual/redundant power supply and sufficient cooling as per OEM hardware design	No Change, as per RFP
48	(Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply	No Change, as per RFP
49	(District HQ) CPE Specification	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules	The Device must have dual/redundant power supply and sufficient cooling as per OEM hardware design	No Change, as per RFP

50	(Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply	No Change, as per RFP
51	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply and sufficient fan modules/fanless Air cooling.	No Change, as per RFP
52	(District HQ) CPE Specification	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules	The Device must have dual/redundant power supply and sufficient cooling as per OEM hardware design	No Change, as per RFP
53	(Taluka HQ) CPE Specification	The Device must have AC power supply and sufficient redundant cooling/fan modules	The Device must have AC power supply	No Change, as per RFP
54	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification #43	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Request to modify as follows : The device should have a minimum of 4x1G ports, out of which at least 1 port should be SFP based port. The SFP transceiver of this SFP type port will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should support cellular connectivity through either an inbuilt cellular module or an external/ODU-based solution compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules/ODU, SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum
55	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device shall have a minimum of 4 x 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award. Optionally, the bidder may provide cellular connectivity with an external ODU to ensure better cellular signal strength.	Pls. refer corrigendum
56	SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device should have a minimum of 4x1G RJ 45 ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum

57	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device shall have a minimum of 4 x 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award. Optionally, the bidder may provide cellular connectivity with an external ODU to ensure better cellular signal strength.	Pls. refer corrigendum
58	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device shall have a minimum of 4 x 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award. Optionally, the bidder may provide cellular connectivity with an external ODU to ensure better cellular signal strength.	Pls. refer corrigendum
59	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices - SIM Based (For office location) CPE Specification – Point 43	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Change Request: The device should have a minimum of 6 x 1G RJ45 Ethernet ports. Additionally, the solution shall support cellular connectivity through either inbuilt single SIM slot or USB supporting compatible 3G/4G/LTE/5G cellular dongles or 3G/4G/LTE/5G ODU with Ethernet handoff to SDWAN. SIM cards and recurring telecom charges shall be excluded unless explicitly specified. No additional hardware cost shall be admissible post-award. Justification: The existing requirement is hardware-specific and may restrict participation. The proposed change allows equivalent cellular connectivity options while meeting the intended WAN connectivity and backup requirements, ensuring technology neutrality, wider OEM participation, and cost-effective deployment.	Pls. refer corrigendum
60	SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device should have a minimum of 4x1G RJ 45 ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum

61	SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device should have a minimum of 4x1G RJ 45 ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum
62	SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device should have a minimum of 4x1G RJ 45 ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum
63	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device shall have a minimum of 4 x 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award. Optionally, the bidder may provide cellular connectivity with an external ODU to ensure better cellular signal strength.	Pls. refer corrigendum
64	SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	The device should have a minimum of 4x1G RJ 45 ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum

65	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	As per the specified requirement of 500 Mbps throughput, the current interface requirement appears to be on the higher side and may unnecessarily increase the overall solution complexity and cost. Further, the requirement specifies SFP-based interfaces for 2 ports. We request GIL to kindly review the interface requirement and consider a more flexible port configuration that adequately meets the required throughput and deployment requirements. We request GIL to amend the clause as follows: "The device should have a minimum of 4x1G ports. Additionally device should have inbuilt Dual SIM slots (2 x SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.	Pls. refer corrigendum
66	SD-WAN Edge Devices (Taluka HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
67	SD-WAN Edge Devices (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
68	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
69	SD-WAN Edge Devices (Taluka HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
70	SD-WAN Edge Devices (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
71	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
72	SD-WAN Edge Devices (Taluka HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
73	SD-WAN Edge Devices (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
74	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
75	SD-WAN Edge Devices (Taluka HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP

76	SD-WAN Edge Devices (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
77	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 50,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
78	5.2. SD-WAN SPECIFICATION: QoS & Traffic Engineering	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	Justification: Storm control is primarily a Layer-2 switching feature and is not a standard SD-WAN capability across most OEMs. Mandating it restricts wider OEM participation. Request to modify as follows Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR).	Pls. refer corrigendum
79	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps/QOS policy.	Pls. refer corrigendum
80	5.2. SD-WAN SPECIFICATION:	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps and interface rate limiting.	Pls. refer corrigendum
81	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps/QOS policy.	Pls. refer corrigendum
82	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps/QOS policy.	Pls. refer corrigendum
83	5.2. SD-WAN SPECIFICATION:	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps and interface rate limiting.	Pls. refer corrigendum
84	5.2. SD-WAN SPECIFICATION:	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps and interface rate limiting.	Pls. refer corrigendum
85	5.2. SD-WAN SPECIFICATION:	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps and interface rate limiting.	Pls. refer corrigendum
86	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps/QOS policy.	Pls. refer corrigendum
87	5.2. SD-WAN SPECIFICATION:	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.	QoS & Traffic Engineering : Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps and interface rate limiting.	Pls. refer corrigendum

88	SD-WAN HUB CPE Specification #5	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options . All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Justification: For DC-level SD-WAN platforms, high-speed interfaces are typically deployed as Layer-3 routed ports. Such interfaces can be utilized for either WAN or LAN connectivity based on the network design. Layer-2 switching capability on all ports is not standard across OEMs and restricts wider OEM participation. Request to modify as follows The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options. All ports can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
89	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	The device should have minimum 8X1/10GE SFP/SFP+ and 8x1 GE RJ45 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
90	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	We suggest the below revised clause to meet the real world requirement of the project. - The device should have minimum 12X1/10GE SFP+ and 4 X 40/100GE QSFP28/40GE QSFP with additional 4 x 25GE SFP28 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
91	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	The device should have minimum 8X1/10GE SFP/SFP+ and 8x1 GE RJ45 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
92	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	The device should have minimum 8X1/10GE SFP/SFP+ and 8x1 GE RJ45 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum

93	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	We suggest the below revised clause to meet the real world requirement of the project. - The device should have minimum 12X1/10GE SFP+ and 4 X 40/100GE QSFP28/40GE QSFP with additional 4 x 25GE SFP28 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
94	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	We suggest the below revised clause to meet the real world requirement of the project. - The device should have minimum 12X1/10GE SFP+ and 4 X 40/100GE QSFP28/40GE QSFP with additional 4 x 25GE SFP28 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
95	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	We suggest the below revised clause to meet the real world requirement of the project. - The device should have minimum 12X1/10GE SFP+ and 4 X 40/100GE QSFP28/40GE QSFP with additional 4 x 25GE SFP28 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
96	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	The device should have minimum 8X1/10GE SFP/SFP+ and 8x1 GE RJ45 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum
97	SD-WAN HUB CPE Specification	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	We suggest the below revised clause to meet the real world requirement of the project. The device should have minimum 12X1/10GE SFP+ and 4 X 40/100GE QSFP28/40GE QSFP with additional 4 x 25GE SFP28 ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Pls. refer corrigendum

98	SD-WAN Edge Devices (District HQ) CPE Specification #16	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Justification: For DHQ-level SD-WAN platforms, high-speed interfaces are typically deployed as Layer-3 routed ports. Such interfaces can still be utilized for either WAN or LAN connectivity based on the network design. Layer-2 switching capability on all ports is not standard across most OEMs and may restrict wider OEM participation. Request to modify as follows The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports can be used as both WAN and LAN ports.	Pls. refer corrigendum
99	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	The device should have minimum 8X1GE RJ45, 6x1/10GE SFP/SFP+. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Pls. refer corrigendum
100	(District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	We request to revise the clause as follow: The device should have minimum 8 X1GE SFP/RJ 45 , 4 x 10GE SFP+ and 4 X 25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	Pls. refer corrigendum
101	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	The device should have minimum 8X1GE RJ45, 6x1/10GE SFP/SFP+. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Pls. refer corrigendum
102	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	The device should have minimum 8X1GE RJ45, 6x1/10GE SFP/SFP+. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Pls. refer corrigendum
103	(District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	We request to revise the clause as follow: The device should have minimum 8 X1GE SFP/RJ 45 , 4 x 10GE SFP+ and 4 X 25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	Pls. refer corrigendum
104	(District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	We request to revise the clause as follow: The device should have minimum 8 X1GE SFP/RJ 45 , 4 x 10GE SFP+ and 4 X 25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	Pls. refer corrigendum
105	(District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	We request to revise the clause as follow: The device should have minimum 8 X1GE SFP/RJ 45 , 4 x 10GE SFP+ and 4 X 25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	Pls. refer corrigendum

106	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	The device should have minimum 8X1GE RJ45, 6x1/10GE SFP/SFP+. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Pls. refer corrigendum
107	(District HQ) CPE Specification	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	We request to revise the clause The device should have minimum 8 X1GE RJ 45 and 4 x 1G SFP/ 10GE SFP+ The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports	Pls. refer corrigendum
108	SD-WAN Edge Devices (Taluka HQ) CPE Specification # 25	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	Justification: Taluka HQ locations may serve as regional/aggregation sites and may require multiple WAN links along with additional LAN connectivity for local applications/services and future expansion. It is therefore recommended to provide higher WAN/LAN port density with at least two high-speed optical WAN interfaces for scalability. Request to modify as follows The device should have a minimum of 4 WAN ports and 6 LAN ports. Out of the 4 WAN ports, at least 2 ports should support both 1G/10G SFP/SFP+ options. The SFP transceivers will be provided by SI as per requirement from the same OEM/OEM Authorized Manufacturer of SFP's.	No Change, as per RFP
109	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Out of the 6 ports minimum 2 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	No Change, as per RFP
110	(Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 8x1G RJ45 ports from day 1. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. All ports WAN/LAN assignment should be configurable as per deployment requirement.	No Change, as per RFP
111	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Out of the 6 ports minimum 2 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	No Change, as per RFP
112	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Out of the 6 ports minimum 2 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	No Change, as per RFP
113	(Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 8x1G RJ45 ports from day 1. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. All ports WAN/LAN assignment should be configurable as per deployment requirement.	No Change, as per RFP

114	(Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 8x1G RJ45 ports from day 1. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. All ports WAN/LAN assignment should be configurable as per deployment requirement.	No Change, as per RFP
115	(Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 8x1G RJ45 ports from day 1. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. All ports WAN/LAN assignment should be configurable as per deployment requirement.	No Change, as per RFP
116	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Out of the 6 ports minimum 2 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	No Change, as per RFP
117	(Taluka HQ) CPE Specification	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	No Change, as per RFP
118	SD-WAN Edge Devices (For office location) CPE Specification	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
119	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
120	SD-WAN Edge Devices (For office location) CPE Specification	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
121	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
122	SD-WAN Edge Devices (For office location) CPE Specification	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
123	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum

124	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION SD-WAN Edge Devices (For office location) CPE Specification -- Point 31	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	Change Request: The device should have minimum 100 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 100 Mbps IPsec VPN encryption throughput from Day 1. Justification: As per Government capacity planning principles, infrastructure sizing should be based on current utilization, projected future requirements, expected growth and security/performance requirements. The existing WAN bandwidth requirement is below 20 Mbps. A minimum throughput of 100 Mbps provides more than 5 times the existing bandwidth requirement, offering sufficient headroom for future growth and reasonable capacity planning. The requirement of 500 Mbps, which is more than 25 times the existing bandwidth, appears disproportionate to the stated WAN requirement and may result in unnecessary overprovisioning and cost. Therefore, it is requested to revise the requirement to 100 Mbps while ensuring adequate scalability and performance.	Pls. refer corrigendum
125	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN Edge Devices - SIM Based (For office location) CPE Specification -- Point 40	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	Change Request: The device should have minimum 100 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 100 Mbps IPsec VPN encryption throughput from Day 1. Justification: As per Government capacity planning principles, infrastructure sizing should be based on current utilization, projected future requirements, expected growth and security/performance requirements. The existing WAN bandwidth requirement is below 20 Mbps. A minimum throughput of 100 Mbps provides more than 5 times the existing bandwidth requirement, offering sufficient headroom for future growth and reasonable capacity planning. The requirement of 500 Mbps, which is more than 25 times the existing bandwidth, appears disproportionate to the stated WAN requirement and may result in unnecessary overprovisioning and cost. Therefore, it is requested to revise the requirement to 100 Mbps while ensuring adequate scalability and performance.	Pls. refer corrigendum
126	SD-WAN Edge Devices (For office location) CPE Specification	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
127	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
128	SD-WAN Edge Devices (For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device shall have a minimum of 4 × 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface.	Pls. refer corrigendum
129	For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	Pls. refer corrigendum

130	SD-WAN Edge Devices (For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device shall have a minimum of 4 × 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface.	Pls. refer corrigendum
131	SD-WAN Edge Devices (For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device shall have a minimum of 4 × 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface.	Pls. refer corrigendum
132	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices (For office location) CPE Specification -- Point 34	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	Request changes: The device should have a minimum of 6x1G RJ45 ports configured as LAN/WAN. Justification: The proposed office-location SD-WAN Edge device requires flexible WAN/LAN connectivity based on the actual site deployment. Mandating a minimum of 4 WAN ports and 2 SFP-based ports may result in unnecessary interface over-provisioning, as WAN connectivity requirements may vary by location and can be adequately supported through RJ45 interfaces. Allowing a minimum of 6 × 1G RJ45 ports configurable as WAN or LAN will provide greater deployment flexibility, avoid unnecessary hardware and optical interface requirements, and improve cost competitiveness, while meeting the required connectivity and scalability needs of office locations.	Pls. refer corrigendum
133	For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	Pls. refer corrigendum
134	For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	Pls. refer corrigendum
135	For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	Pls. refer corrigendum
136	SD-WAN Edge Devices (For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device shall have a minimum of 4 × 1G RJ45 ports, each port should be configurable and usable as either a LAN or WAN interface.	Pls. refer corrigendum
137	For office location) CPE Specification	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.	The device should have a minimum of 4 x1G RJ45 ports from day 1. All ports WAN/LAN assignment should be configurable as per deployment requirement.	Pls. refer corrigendum
138	SECTION 2 Eligibility	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Allow OEM deployments of 5000+ SD-WAN devices across any large enterprise/public sector.	Pls. refer corrigendum

139	SECTION 2 Eligibility	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Allow OEM deployments of 5000+ SD-WAN devices across any large enterprise/public sector.	Pls. refer corrigendum
140	SECTION 2 Eligibility	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Allow OEM deployments of 5000+ SD-WAN devices across any large enterprise/public sector.	Pls. refer corrigendum
141	Eligibility Criteria:	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Request to kindly revised this clause and consider as below: The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 5,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Pls. refer corrigendum
142		The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	we request GIL to kindly review this criterion and consider aligning the minimum quantity with the scale of the proposed project, preferably to 6,300 sites or lower, in accordance with the applicable Government of India procurement principles and guidelines. This would facilitate participation from a wider range of technically qualified OEMs and encourage healthy competition. Further, we request GIL to kindly clarify the following aspects: Proof of OEM supply experience: Since OEMs generally supply the SD-WAN products through their authorized bidders/System Integrators, kindly clarify how the OEM is expected to independently establish that the supplied products were deployed/supplied specifically to State Government Organizations / Central Government / PSUs / Listed Companies / BFSI. Kindly specify the acceptable documentary evidence for establishing such experience. Supply versus implementation experience: The present clause appears to specify only the quantity of products supplied and does not explicitly consider the successful implementation/deployment of the solution. Since the objective of the requirement is to establish the OEM's capability for a project of this nature, we request GIL to kindly consider successful implementation/deployment experience in addition to supply experience. Equivalent treatment for bidder and OEM: The RFP	Pls. refer corrigendum
143	SECTION 2 Eligibility	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Allow OEM deployments of 5000+ SD-WAN devices across any large enterprise/public sector.	Pls. refer corrigendum
144	Eligibility Criteria:	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,00,00 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date. OR 15000 Qty in Single Work order	Pls. refer corrigendum

145	SECTION 2 - ELIGIBILITY CRITERIA	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	We request GIL to kindly review and amend the eligibility clause to enable wider participation from qualified SD-WAN OEMs and encourage participation of Make in India products. The existing clause may restrict participation to a limited number of OEMs. To promote healthy competition and provide an opportunity for capable Indian OEMs, we request that the experience requirement be suitably amended as follows: "The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 3,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date."	Pls. refer corrigendum
146	SECTION 2 > Eligibility Criteria	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	The OEM of the proposed product must have supplied SD-WAN Edge Device/Secure SD-WAN Appliance with a minimum quantity of 3,000 units in State Government Organizations, Central Government, PSUs, Listed Companies, or BFSI organizations during the last five (5) years prior to the bid opening date.	Pls. refer corrigendum
147	SECTION 2 Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	The OEM shall submit an undertaking letter confirming that all quoted items supplied under this bid shall be brand new, unused, and not refurbished or reconditioned.	No Change, as per RFP
148	Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	Kindly remove this clause to ensure a level playing field for all leading OEMs.	No Change, as per RFP
149	SECTION 2 Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	The OEM shall submit an undertaking letter confirming that all quoted items supplied under this bid shall be brand new, unused, and not refurbished or reconditioned.	No Change, as per RFP
150	SECTION 2 Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	The OEM shall submit an undertaking letter confirming that all quoted items supplied under this bid shall be brand new, unused, and not refurbished or reconditioned.	No Change, as per RFP
151	Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	Kindly remove this clause to ensure a level playing field for all leading OEMs.	No Change, as per RFP
152	Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	Kindly remove this clause to ensure a level playing field for all leading OEMs.	No Change, as per RFP
153	Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	Kindly remove this clause to ensure a level playing field for all leading OEMs.	No Change, as per RFP
154	SECTION 2 Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	The OEM shall submit an undertaking letter confirming that all quoted items supplied under this bid shall be brand new, unused, and not refurbished or reconditioned.	No Change, as per RFP
155	Eligibility Criteria:	OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.	Kindly remove this clause to ensure a level playing field for all leading OEMs.	No Change, as per RFP
156	SECTION 3 Scope of Work 3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography with readiness to support applicable PQC NIST standards and algorithms within one (1) year of award, subject to industry-standard maturity and availability	Pls. refer corrigendum
157	3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for threat monitoring, detection, prevention, troubleshooting & diagnostics.	Pls. refer corrigendum
158	SECTION 3 Scope of Work 3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography with readiness to support applicable PQC NIST standards and algorithms within one (1) year of award, subject to industry-standard maturity and availability	Pls. refer corrigendum

159	SECTION 3 Scope of Work 3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography with readiness to support applicable PQC NIST standards and algorithms within one (1) year of award, subject to industry-standard maturity and availability	Pls. refer corrigendum
160	3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for threat monitoring, detection , prevention, troubleshooting & diagnostics.	Pls. refer corrigendum
161	3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for threat monitoring, detection , prevention, troubleshooting & diagnostics.	Pls. refer corrigendum
162	3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for threat monitoring, detection , prevention, troubleshooting & diagnostics.	Pls. refer corrigendum
163	SECTION 3 Scope of Work 3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography with readiness to support applicable PQC NIST standards and algorithms within one (1) year of award, subject to industry-standard maturity and availability	Pls. refer corrigendum
164	3.4 Functional Requirement	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for threat monitoring, detection , prevention, troubleshooting & diagnostics.	Pls. refer corrigendum
165	SECTION 2 Eligibility Criteria:	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last Seven (7) years, as per any one of the following criteria: a) One (1) project covering 3,000 or more locations, or b) Two (2) projects, each covering 2,000 or more locations, or c) Three (3) projects, each covering 1,000 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture	Pls. refer corrigendum
166	SECTION 2 ELIGIBILT CRITERIA	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	The current experience requirement is restrictive and may limit wider participation. We request the Authority to kindly amend it to 3,000 sites across minimum 3 projects OR 4,000 sites across minimum 5 projects during the last 5 years.	Pls. refer corrigendum

167	Eligibility Criteria:	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 3,000 or more locations, or b) Two (2) projects, each covering 2,000 or more locations, or c) Three (3) projects, each covering 1,000 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture	Pls. refer corrigendum
168		The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	Kindly consider permitting the bidder to qualify through relevant WAN/SD-WAN implementation experience in Telecom/ISP organizations, in addition to the categories presently specified, considering the nature and scope of the proposed SD-WAN deployment.	Pls. refer corrigendum
169	SECTION 2 ELIGIBILITY CRITERIA	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	The current experience requirement is restrictive and may limit wider participation. We request the Authority to kindly amend it to 3,000 sites across minimum 3 projects OR 4,000 sites across minimum 5 projects during the last 5 years.	Pls. refer corrigendum
170	SECTION 2 ELIGIBILITY CRITERIA	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	The asked experience is too high and Blocking our participation; Please amend the same to 3000 Site with Min 3 Projects Or 4000 Sites with Min 5 Projects during last 5 Years.	Pls. refer corrigendum

171	Eligibility Criteria:	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	The bidder / OEM should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	Pls. refer corrigendum
172	SECTION 2 ELIGIBILITY CRITERIA	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	The DST / GSWAN Planning sites Phase wise; So please reduce the site experience by bidder. Kindly make it Single Experience of 2000, Two experience of 1000, or 3 Experience of 500.	Pls. refer corrigendum
173	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The proposed solution should support IPv4 and IPv6 dual stack from day one. The proposed solution or the product family should be IPv6 Ready logo and FIPS 140-2 or higher.	Pls. refer corrigendum
174	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT – Point 6	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	Request for Change: The solution should support IPv4 and IPv6 dual stack from day one. Request removal - The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher. Justification: FIPS 140-2 is a U.S. Government cryptographic module validation standard, and mandating Level 2 or higher may unnecessarily restrict participation of technically capable Indian OEMs and compliant solutions. The requirement should focus on the functional outcome— IPv4 and IPv6 dual stack support from Day 1—rather than mandating a specific certification/logo. This will avoid unnecessary restriction of technically compliant solutions while ensuring the required IPv6 capability, interoperability and future readiness of the SD-WAN deployment.	Pls. refer corrigendum
175	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The proposed solution should support IPv4 and IPv6 dual stack from day one. The proposed solution or the product family should be IPv6 Ready logo and FIPS 140-2 or higher.	Pls. refer corrigendum
176	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The proposed solution should support IPv4 and IPv6 dual stack from day one. The proposed solution or the product family should be IPv6 Ready logo and FIPS 140-2 or higher.	Pls. refer corrigendum
177	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The proposed solution should support IPv4 and IPv6 dual stack from day one. The proposed solution or the product family should be IPv6 Ready logo and FIPS 140-2 or higher.	Pls. refer corrigendum
178	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The proposed solution should support IPv4 and IPv6 dual stack from day one. The proposed solution or the product family should be IPv6 Ready logo and FIPS 140-2 or higher.	Pls. refer corrigendum

179	SECTION 5 - SPECIFICATIONS	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	As per TEC guidelines for SDWAN product they perform rigorous testing for IPV6. Kindly refer the government of India Ministry of Commerce DPIIT Office Memorandum dated December 20th , 2022 "Restrictive and discriminatory conditions against the local suppliers" and "Other conditions which make the bid noncompliant to PPP-Mli Order". The Office Memorandum dated December 20th , 2022 is attached for your kind reference. Therefore, we request GIL to kindly review this clause and consider accepting Indian standards or equivalent ISO certifications for compliance to PPP-MII Order. We request to amend the clause as "The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be TEC Certificate or IPv6 Ready logo and FIPS 140-2 or higher. "	Pls. refer corrigendum
180	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution should comply with applicable security and IPv6 interoperability requirements.	Pls. refer corrigendum
181	V.	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	"Due to industry wide ongoing supply chain constraint, AI Memory boom issue and geographical logistical issues and Forex volatility the final product/support/software prices are getting affected at faster pace. kind request you to Please modify as following: "The rates quoted shall remain valid for a period of 3 Months from the date of issuance of the Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates."	Pls. refer corrigendum
182	SECTION 6 (PRICE BID:)	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Kindly remove this clause.	Pls. refer corrigendum
183	Section 6: Price bid & validity	V. The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Considering the prevailing global supply chain volatility and fluctuations in the prices of memory, storage, and other critical IT hardware components, we request to revise this clause as V. The rates quoted shall remain valid for a period of Six (6) Months from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid during this validity period. Such repeat order shall be placed at the same unit prices and commercial terms as the original Purchase Order, provided that the INR–US Dollar (USD) exchange rate has not varied by more than ±5% compared to the RBI reference exchange rate prevailing on the date of the original Purchase Order. In the event the INR–USD exchange rate varies by more than ±5%, the prices applicable to the repeat order shall be adjusted by the Bank only to the extent of the exchange rate variation beyond the ±5% threshold. The applicable exchange rate shall be the RBI Reference Rate published on the Reserve Bank of India (RBI) website.	Pls. refer corrigendum
184	SECTION 6 (PRICE BID:)	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Kindly remove this clause.	Pls. refer corrigendum

185	SECTION 6 (PRICE BID:)	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the LoI/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Kindly remove this clause.	Pls. refer corrigendum
186	SECTION 6 (PRICE BID:)	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the LoI/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Kindly remove this clause.	Pls. refer corrigendum
187	SECTION 6 (PRICE BID:)	The rates quoted shall remain valid for a period of Five (5) years from the date of issuance of the LoI/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.	Kindly remove this clause.	Pls. refer corrigendum
188	SECTION 2 Eligibility Criteria:	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The quoted products of OEM should have an average annual related turnover of not less than Rs 150 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Pls. refer corrigendum
189	SECTION 2 Eligibility Criteria:	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The quoted products of OEM should have an average annual related turnover of not less than Rs 150 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Pls. refer corrigendum
190	SECTION 2 Eligibility Criteria:	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The quoted products of OEM should have an average annual related turnover of not less than Rs 150 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Pls. refer corrigendum
191	Eligibility Criteria:	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025	Request to kindly revised this clause and consider as below: The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025 for MSME an MII product.	Pls. refer corrigendum
192	SECTION 2 Eligibility Criteria:	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The quoted products of OEM should have an average annual related turnover of not less than Rs 150 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Pls. refer corrigendum
193	SECTION 2 - ELIGIBILTY CRITERIA	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Kindly refer clause 4.4.1 at page 10 of tender states that "GIL will follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) issued vide Central Vigilance Commission Order No.018/VGL/022- 377353 Date April 20, 2018 and basis of allotment will be done in terms of instructions on Public Procurement (Preference to Make In India), Order, 2017(PPP-MII Order), Order No. P- 45021/2/2017-B.E.-II Date 15.06.2017, as amended by Order No. P- 45021/2/2017-B.E.-II Date 28.05.2018; Order No. P- 45021/2/2017(BE-II) Date May 29, 2019, further revised on 04-06-2022 and 16-09-2020, 19.07.2024;and subsequent amendments as issued by GOI, Ministry of Commerce and Industry, Department of Promotion of Industry and Internal Trade(Public Procurement Section)." The CVC and DPIIT policy do not state such high OEMs average turnover even though the Project estimated value is around 40 Crore but OEM criteria has mentioned to be 500 Crore. Kindly refer Order No. P-45021/2/2017-PP (BE-II)-Part(4)Vol.II Government of India Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade (Public Procurement Section) dated 19/7/2024 clause no. 10 (b) states b. Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, production	Pls. refer corrigendum
194	SECTION 2 > Eligibility Criteria	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The OEM of the quoted products should have an average annual turnover from the relevant product/solution business of not less than ₹10 Crores during the last three financial years (FY 2022-23, FY 2023-24 and FY 2024-25). Eligible MSME Startup OEMs are allowed to participate with applicable relaxation in turnover criteria.	Pls. refer corrigendum

195	Eligibility Criteria:	The quoted product must be MTCTE certified.	The quoted product must be MTCTE certified on/or before supply of the material.	Pls. refer corrigendum
196	Eligibility Criteria:	The quoted product must be MTCTE certified.	The quoted product must be MTCTE certified on/or before supply of the material.	Pls. refer corrigendum
197	Eligibility Criteria:	The quoted product must be MTCTE certified.	The quoted product must be MTCTE certified on/or before supply of the material.	Pls. refer corrigendum
198		The quoted product must be MTCTE certified.	We requestwe request GIL to consider incorporating an appropriate MII declaration and applicable preference provisions in the RFP, as per the prevailing Government of India guidelines issues in October 2024, to ensure wider participation, fair competition and a level playing field for eligible bidders and OEMs.	Pls. refer corrigendum
199	Eligibility Criteria:	The quoted product must be MTCTE certified.	The quoted product must be MTCTE certified on/or before supply of the material.	Pls. refer corrigendum
200	Eligibility Criteria:	The quoted product must be MTCTE certified.	The quoted product must be MTCTE certified on/or before supply of the material.	Pls. refer corrigendum
201	SECTION 2 - ELIGIBLTY CRITERIA	The quoted product must be MTCTE certified.	To promote healthy competition and provide an opportunity for capable Indian OEMs, we request that the experience requirement be suitably amended as follows: "The quoted product must be MTCTE or TEC certified."	Pls. refer corrigendum
202	Key Features Required in the SD-WAN Solution #12	The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Justification : Secure Web Gateway (SWG), file upload/content control and Data Loss Prevention (DLP) are typically not core SD-WAN functionalities and generally require cloud-based SWG/SSE solutions. Since the current requirement is primarily for an on-premises SD-WAN solution, mandating these capabilities restricts wider OEM participation. Request to remove this clause.	Pls. refer corrigendum
203	SECTION 1 Key Features Required in the SD-WAN Solution	The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	The solution should support Secure Web Gateway/app-aware firewall capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Pls. refer corrigendum
204	SECTION 1 Key Features Required in the SD-WAN Solution	The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	The solution should support Secure Web Gateway/app-aware firewall capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Pls. refer corrigendum
205	SECTION 1 Key Features Required in the SD-WAN Solution	The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	The solution should support Secure Web Gateway/app-aware firewall capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Pls. refer corrigendum
206	SECTION 1 Key Features Required in the SD-WAN Solution	The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	The solution should support Secure Web Gateway/app-aware firewall capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Pls. refer corrigendum
207	3.4 Functional Requirement #42	The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	Request to modify as follows The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM/OEM Certified partner for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	Pls. refer corrigendum
208	SECTION 3 Scope of Work 3.4 Functional Requirement	The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	The Successful Bidder shall arrange training and training certification on the SD-WAN solution from the OEM/Bidder's technical expert for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL. Training can be conducted at GIL Premise.	Pls. refer corrigendum
209	SECTION 3 Scope of Work 3.4 Functional Requirement	The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	The Successful Bidder shall arrange training and training certification on the SD-WAN solution from the OEM/Bidder's technical expert for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL. Training can be conducted at GIL Premise.	Pls. refer corrigendum

210	SECTION 3 Scope of Work 3.4 Functional Requirement	The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	The Successful Bidder shall arrange training and training certification on the SD-WAN solution from the OEM/Bidder's technical expert for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL. Training can be conducted at GIL Premise.	Pls. refer corrigendum
211	SECTION 3 Scope of Work 3.4 Functional Requirement	The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	The Successful Bidder shall arrange training and training certification on the SD-WAN solution from the OEM/Bidder's technical expert for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL. Training can be conducted at GIL Premise.	Pls. refer corrigendum
212	5.1 SDWAN FUNCTIONAL SPECIFICATIONS #26	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g.,AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	Justification : User authentication, user-to-IP mapping, and integration with NAC/AAA/identity platforms such as AD/LDAP are typically not native SD-WAN functionalities and generally require dedicated identity/NAC solutions. Mandating these capabilities as part of the SD-WAN solution introduces additional components and restrict wider OEM participation. Request to remove this clause.	Pls. refer corrigendum
213	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g., AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with Third-party NAC/AAA/identity platforms (e.g., AD/LDAP).	Pls. refer corrigendum
214	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g., AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with Third-party NAC/AAA/identity platforms (e.g., AD/LDAP).	Pls. refer corrigendum
215	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g., AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with Third-party NAC/AAA/identity platforms (e.g., AD/LDAP).	Pls. refer corrigendum
216	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g., AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with Third-party NAC/AAA/identity platforms (e.g., AD/LDAP).	Pls. refer corrigendum

217	5.2. SD-WAN SPECIFICATION: Layer-2 Features	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Justification : Bridge Domains and Ethernet Virtual Connections (EVC) are predominantly switching/Layer-2 service-provider features and are generally not relevant to core SD-WAN CPE functionality. Mandating these features unnecessarily restricts wider OEM participation. Request to modify as follows Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; and Layer-3 Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
218	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge interface/domains; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
219	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge interface/domains; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
220	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge interface/domains; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
221	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge interface/domains; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
222	SD-WAN Edge Devices (Taluka HQ) CPE Specification #22	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	Justification: Taluka HQ locations may serve as regional aggregation points for sub-level sites and may also host or provide access to regional applications/services. Considering future traffic growth and aggregation requirements, 900 Mbps provides limited headroom. It is recommended to consider minimum 1.5 Gbps throughput capacity for better scalability. Request to modify as follows The device should have minimum 1.5 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 1.5 Gbps IPsec VPN encryption throughput from Day 1.	Pls. refer corrigendum
223	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
224	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
225	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum

226	SD-WAN Edge Devices (Taluka HQ) CPE Specification	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
227	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
228	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
229	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
230	SD-WAN Edge Devices (District HQ) CPE Specification	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. The appliance shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption and application-aware firewall, URLF, threat protection (anti-malware, IPS) etc.	Pls. refer corrigendum
231		The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1	The device should have minimum 5 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1	Pls. refer corrigendum
232	Central Orchestrator / Controller Specifications	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
233	Central Orchestrator / Controller Specifications	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
234	Central Orchestrator / Controller Specifications	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
235	Central Orchestrator / Controller Specifications	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
236	Central Orchestrator / Controller Specifications	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
237	Central Orchestrator / Controller Specifications	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	Requesting to delete this clause	Pls. refer corrigendum
238	Central Orchestrator / Controller Specifications	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	Requesting to delete this clause	Pls. refer corrigendum
239	Central Orchestrator / Controller Specifications	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	Requesting to delete this clause	Pls. refer corrigendum
240	Central Orchestrator / Controller Specifications	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	Requesting to delete this clause	Pls. refer corrigendum
241	Central Orchestrator / Controller Specifications	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	Requesting to delete this clause	Pls. refer corrigendum

242	3.4 Functional Requirement	In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period.The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	Requesting to delete this clause.	No Change, as per RFP
243	3.4 Functional Requirement	In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period.The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	Requesting to delete this clause.	No Change, as per RFP
244	3.4 Functional Requirement	In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period.The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	Requesting to delete this clause.	No Change, as per RFP
245	3.4 Functional Requirement	In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period.The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	Requesting to delete this clause.	No Change, as per RFP
246	3.4 Functional Requirement	In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period.The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	Requesting to delete this clause	No Change, as per RFP
247	3.4 Functional Requirement	All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.	Kindly confirm	No Change, as per RFP

248	3.4 Functional Requirement	All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.	Kindly confirm	No Change, as per RFP
249	3.4 Functional Requirement	All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.	Kindly confirm	No Change, as per RFP
250	3.4 Functional Requirement	All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.	Kindly confirm	No Change, as per RFP
251	3.4 Functional Requirement	All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.	Kindly confirm	No Change, as per RFP
252	3.5 Design Principles to be followed	The solution must support alert notifications via email, SMS, or WhatsApp upon crossing system or user-defined thresholds	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
253	3.5 Design Principles to be followed	The solution must support alert notifications via email, SMS, or WhatsApp upon crossing system or user-defined thresholds	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
254	3.5 Design Principles to be followed	The solution must support alert notifications via email, SMS, or WhatsApp upon crossing system or user-defined thresholds	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
255	3.5 Design Principles to be followed	The solution must support alert notifications via email, SMS, or WhatsApp upon crossing system or user-defined thresholds	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
256	3.5 Design Principles to be followed	The solution must support alert notifications via email, SMS, or WhatsApp upon crossing system or user-defined thresholds	The solution must support alert notifications via email or SMS or WhatsApp upon crossing system or user-defined thresholds	Pls. refer corrigendum
257	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	The branch devices must be able to identify and recover from a transit link failure within 50ms or less.	Pls. refer corrigendum
258	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	The branch devices must be able to identify and recover from a transit link failure within 50ms or less.	Pls. refer corrigendum
259	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	The branch devices must be able to identify and recover from a transit link failure within 50ms or less.	Pls. refer corrigendum
260	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	The branch devices must be able to identify and recover from a transit link failure within 50ms or less.	Pls. refer corrigendum
261	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	The branch devices must be able to identify and recover from a transit link failure within 50ms or less.	Pls. refer corrigendum
262	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	The solution should be able to define and identify Custom applications based on IP address, port numbers and FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	Pls. refer corrigendum
263	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	The solution should be able to define and identify Custom applications based on IP address, port numbers and FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	Pls. refer corrigendum
264	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	The solution should be able to define and identify Custom applications based on IP address, port numbers and FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	Pls. refer corrigendum
265	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	The solution should be able to define and identify Custom applications based on IP address, port numbers and FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	Pls. refer corrigendum

266	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	The solution should be able to define and identify Custom applications based on IP address, port numbers and FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	Pls. refer corrigendum
267	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	The data traffic from branch sites must not be impacted in case of failure to reach any controller/manager/orchestrator. The branch device shall continue forwarding traffic using locally stored configuration, routing, SD-WAN policies, VPN tunnels, and security policies shall be running until any configuration change is required.	Pls. refer corrigendum
268	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	The data traffic from branch sites must not be impacted in case of failure to reach any controller/manager/orchestrator. The branch device shall continue forwarding traffic using locally stored configuration, routing, SD-WAN policies, VPN tunnels, and security policies shall be running until any configuration change is required.	Pls. refer corrigendum
269	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	The data traffic from branch sites must not be impacted in case of failure to reach any controller/manager/orchestrator. The branch device shall continue forwarding traffic using locally stored configuration, routing, SD-WAN policies, VPN tunnels, and security policies shall be running until any configuration change is required.	Pls. refer corrigendum
270	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	The data traffic from branch sites must not be impacted in case of failure to reach any controller/manager/orchestrator. The branch device shall continue forwarding traffic using locally stored configuration, routing, SD-WAN policies, VPN tunnels, and security policies shall be running until any configuration change is required.	Pls. refer corrigendum
271	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	The data traffic from branch sites must not be impacted in case of failure to reach any controller/manager/orchestrator. The branch device shall continue forwarding traffic using locally stored configuration, routing, SD-WAN policies, VPN tunnels, and security policies shall be running until any configuration change is required.	Pls. refer corrigendum
272	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Should have Drill-down capabilities to follow the trail of sessions, trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	The solution should have drill-down capabilities to follow the trail of sessions, trace transactions, and provide log search capabilities based on Username and IP address, service, and applications.	Pls. refer corrigendum
273	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Should have Drill-down capabilities to follow the trail of sessions, trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	The solution should have drill-down capabilities to follow the trail of sessions, trace transactions, and provide log search capabilities based on Username and IP address, service, and applications.	Pls. refer corrigendum
274	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Should have Drill-down capabilities to follow the trail of sessions, trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	The solution should have drill-down capabilities to follow the trail of sessions, trace transactions, and provide log search capabilities based on Username and IP address, service, and applications.	Pls. refer corrigendum
275	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Should have Drill-down capabilities to follow the trail of sessions, trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	The solution should have drill-down capabilities to follow the trail of sessions, trace transactions, and provide log search capabilities based on Username and IP address, service, and applications.	Pls. refer corrigendum
276	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Should have Drill-down capabilities to follow the trail of sessions, trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	The solution should have drill-down capabilities to follow the trail of sessions, trace transactions, and provide log search capabilities based on Username and IP address, service, and applications.	Pls. refer corrigendum
277	5.2. SD-WAN SPECIFICATION:	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC) or equivalent ; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
278	5.2. SD-WAN SPECIFICATION:	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC) or equivalent ; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum

279	5.2. SD-WAN SPECIFICATION:	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC) or equivalent ; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
280	5.2. SD-WAN SPECIFICATION:	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Layer-2 Features - Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC) or equivalent ; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
281	5.2. SD-WAN SPECIFICATION:	Layer-2 Features Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Layer-2 Features Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC) or equivalent ; and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).	Pls. refer corrigendum
282	Price Bid	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	Clarification required	Pls. refer corrigendum
283	Price Bid	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	Clarification required	Pls. refer corrigendum
284	Price Bid	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	Clarification required	Pls. refer corrigendum
285	Price Bid	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	Clarification required	Pls. refer corrigendum
286	Price Bid	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	Clarification required	Pls. refer corrigendum
287	Essential & Critical Security Feature	Additional	Suggested Clause : Solution should support blocking known HTTPS based Botnet/Malware connections using fingerprint-based certificate blacklist.	No Change, as per RFP
288	Essential & Critical Security Feature	Additional	Suggested Clause : Solution should support blocking known HTTPS based Botnet/Malware connections using fingerprint-based certificate blacklist.	No Change, as per RFP
289	Essential & Critical Security Feature	Additional	Suggested Clause : Solution should support blocking known HTTPS based Botnet/Malware connections using fingerprint-based certificate blacklist.	No Change, as per RFP
290	Essential & Critical Security Feature	Additional	Suggested Clause : Solution should support blocking known HTTPS based Botnet/Malware connections using fingerprint-based certificate blacklist.	No Change, as per RFP
291	Essential & Critical Security Feature	Additional	Suggested Clause : Solution should support blocking known HTTPS based Botnet/Malware connections using fingerprint-based certificate blacklist.	No Change, as per RFP
292	Essential & Critical Security Feature	Additional	Suggested Clause : Should support Botnet server IP based blocking with global IP reputation database. It should also support Botnet Domain based blocking to filter known Botnet Domains	No Change, as per RFP
293	Essential & Critical Security Feature	Additional	Suggested Clause : Should support Botnet server IP based blocking with global IP reputation database. It should also support Botnet Domain based blocking to filter known Botnet Domains	No Change, as per RFP
294	Essential & Critical Security Feature	Additional	Suggested Clause : Should support Botnet server IP based blocking with global IP reputation database. It should also support Botnet Domain based blocking to filter known Botnet Domains	No Change, as per RFP

295	Essential & Critical Security Feature	Additional	Suggested Clause : Should support Botnet server IP based blocking with global IP reputation database. It should also support Botnet Domain based blocking to filter known Botnet Domains	No Change, as per RFP
296	Essential & Critical Security Feature	Additional	Suggested Clause : Should support Botnet server IP based blocking with global IP reputation database. It should also support Botnet Domain based blocking to filter known Botnet Domains	No Change, as per RFP
297	Essential & Critical Security Feature	Additional	The solution should have File Filter capabilities to block certain files, specifically the password-protected files from being uploaded/downloaded by users in the branches.	No Change, as per RFP
298	Essential & Critical Security Feature	Additional	The solution should have File Filter capabilities to block certain files, specifically the password-protected files from being uploaded/downloaded by users in the branches.	No Change, as per RFP
299	Essential & Critical Security Feature	Additional	The solution should have File Filter capabilities to block certain files, specifically the password-protected files from being uploaded/downloaded by users in the branches.	No Change, as per RFP
300	Essential & Critical Security Feature	Additional	The solution should have File Filter capabilities to block certain files, specifically the password-protected files from being uploaded/downloaded by users in the branches.	No Change, as per RFP
301	Essential & Critical Security Feature	Additional	The solution should have File Filter capabilities to block certain files, specifically the password-protected files from being uploaded/downloaded by users in the branches.	No Change, as per RFP
302	SECTION 1 Key Features Required in the SD-WAN Solution	Automated outage detection and correction	Automated outage detection and correction/failover	Pls. refer corrigendum
303	SECTION 1 Key Features Required in the SD-WAN Solution	Automated outage detection and correction	Automated outage detection and correction/failover	Pls. refer corrigendum
304	SECTION 1 Key Features Required in the SD-WAN Solution	Automated outage detection and correction	Automated outage detection and correction/failover	Pls. refer corrigendum
305	SECTION 1 Key Features Required in the SD-WAN Solution	Automated outage detection and correction	Automated outage detection and correction/failover	Pls. refer corrigendum
306	SECTION 3 Scope of Work 3.4 Functional Requirement	SDWAN solution should have packet level / policy level insight with the graphical representation ability to generate the synthetic traffic probes to check any and analyze the traffic flow.	SDWAN solution should have packet level / policy level insight with the graphical representation and ability to analyze the traffic flow.	Pls. refer corrigendum
307	SECTION 3 Scope of Work 3.4 Functional Requirement	SDWAN solution should have packet level / policy level insight with the graphical representation ability to generate the synthetic traffic probes to check any and analyze the traffic flow.	SDWAN solution should have packet level / policy level insight with the graphical representation and ability to analyze the traffic flow.	Pls. refer corrigendum
308	SECTION 3 Scope of Work 3.4 Functional Requirement	SDWAN solution should have packet level / policy level insight with the graphical representation ability to generate the synthetic traffic probes to check any and analyze the traffic flow.	SDWAN solution should have packet level / policy level insight with the graphical representation and ability to analyze the traffic flow.	Pls. refer corrigendum
309	SECTION 3 Scope of Work 3.4 Functional Requirement	SDWAN solution should have packet level / policy level insight with the graphical representation ability to generate the synthetic traffic probes to check any and analyze the traffic flow.	SDWAN solution should have packet level / policy level insight with the graphical representation and ability to analyze the traffic flow.	Pls. refer corrigendum
310	SECTION 3 Scope of Work 3.4 Functional Requirement	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behavior and must include the ability to generate synthetic traffic proactively verify application experience and WAN performance.	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behaviour.	Pls. refer corrigendum

311	SECTION 3 Scope of Work 3.4 Functional Requirement	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behavior and must include the ability to generate synthetic traffic proactively verify application experience and WAN performance.	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behaviour.	Pls. refer corrigendum
312	SECTION 3 Scope of Work 3.4 Functional Requirement	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behavior and must include the ability to generate synthetic traffic proactively verify application experience and WAN performance.	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behaviour.	Pls. refer corrigendum
313	SECTION 3 Scope of Work 3.4 Functional Requirement	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behavior and must include the ability to generate synthetic traffic proactively verify application experience and WAN performance.	The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behaviour.	Pls. refer corrigendum
314	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active Overlay tunnel support.	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active or single active Overlay tunnel support.	No Change, as per RFP
315	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active Overlay tunnel support.	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active or single active Overlay tunnel support.	No Change, as per RFP
316	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active Overlay tunnel support.	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active or single active Overlay tunnel support.	No Change, as per RFP
317	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active Overlay tunnel support.	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active or single active Overlay tunnel support.	No Change, as per RFP
318	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Access Control Lists (ACLs); prefix lists; route maps; and policy-based routing.	Support for Access Control Lists (ACLs); prefix lists; route maps/redistribution and policy-based routing.	Pls. refer corrigendum
319	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Access Control Lists (ACLs); prefix lists; route maps; and policy-based routing.	Support for Access Control Lists (ACLs); prefix lists; route maps/redistribution and policy-based routing.	Pls. refer corrigendum
320	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Access Control Lists (ACLs); prefix lists; route maps; and policy-based routing.	Support for Access Control Lists (ACLs); prefix lists; route maps/redistribution and policy-based routing.	Pls. refer corrigendum
321	Section – 5 5.2. SD-WAN SPECIFICATION:	Support for Access Control Lists (ACLs); prefix lists; route maps; and policy-based routing.	Support for Access Control Lists (ACLs); prefix lists; route maps/redistribution and policy-based routing.	Pls. refer corrigendum
322	Section – 5 Central Orchestrator / Controller Specifications	The solution shall support Multi-Factor Authentication (MFA) for administrative login.	The solution shall support integration with Multi-Factor Authentication (MFA) for administrative login.	No Change, as per RFP
323	Section – 5 Central Orchestrator / Controller Specifications	The solution shall support Multi-Factor Authentication (MFA) for administrative login.	The solution shall support integration with Multi-Factor Authentication (MFA) for administrative login.	No Change, as per RFP
324	Section – 5 Central Orchestrator / Controller Specifications	The solution shall support Multi-Factor Authentication (MFA) for administrative login.	The solution shall support integration with Multi-Factor Authentication (MFA) for administrative login.	No Change, as per RFP
325	Section – 5 Central Orchestrator / Controller Specifications	The solution shall support Multi-Factor Authentication (MFA) for administrative login.	The solution shall support integration with Multi-Factor Authentication (MFA) for administrative login.	No Change, as per RFP
326	Section – 5 Central Orchestrator / Controller Specifications	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access. The Management, Analytic, Control and Data plane must be multi-tenant/multi-domain with Role based access control and resource tagging integrated with Role-Based Access Control (RBAC). The proposed SDWAN device for Branch should support minimum 20 tenant/domain and DC/DR devices should support minimum 50 tenant/domain.	No Change, as per RFP

327	Section – 5 Central Orchestrator / Controller Specifications	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access. The Management, Analytic, Control and Data plane must be multi-tenant/multi-domain with Role based access control and resource tagging integrated with Role-Based Access Control (RBAC). The proposed SDWAN device for Branch should support minimum 20 tenant/domain and DC/DR devices should support minimum 50 tenant/domain.	No Change, as per RFP
328	Section – 5 Central Orchestrator / Controller Specifications	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access. The Management, Analytic, Control and Data plane must be multi-tenant/multi-domain with Role based access control and resource tagging integrated with Role-Based Access Control (RBAC). The proposed SDWAN device for Branch should support minimum 20 tenant/domain and DC/DR devices should support minimum 50 tenant/domain.	No Change, as per RFP
329	Section – 5 Central Orchestrator / Controller Specifications	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access. The Management, Analytic, Control and Data plane must be multi-tenant/multi-domain with Role based access control and resource tagging integrated with Role-Based Access Control (RBAC). The proposed SDWAN device for Branch should support minimum 20 tenant/domain and DC/DR devices should support minimum 50 tenant/domain.	No Change, as per RFP
330	SD-WAN HUB CPE Specification	Should support minimum 10000 overlay IPSec tunnels from day 1.	The solution single/cluster design, Should support minimum 10000 overlay IPSec tunnels from day 1.	Pls. refer corrigendum
331	SD-WAN HUB CPE Specification	Should support minimum 10000 overlay IPSec tunnels from day 1.	The solution single/cluster design, Should support minimum 10000 overlay IPSec tunnels from day 1.	Pls. refer corrigendum
332	SD-WAN HUB CPE Specification	Should support minimum 10000 overlay IPSec tunnels from day 1.	The solution single/cluster design, Should support minimum 10000 overlay IPSec tunnels from day 1.	Pls. refer corrigendum
333	SD-WAN HUB CPE Specification	Should support minimum 10000 overlay IPSec tunnels from day 1.	The solution single/cluster design, Should support minimum 10000 overlay IPSec tunnels from day 1.	Pls. refer corrigendum
334	Remote User Security and Access Management	additional query/Clarification	The Controller is a separate component of an SD-WAN solution. However, the terms **Controller** and **Orchestrator** are often used interchangeably, depending on the OEM's architecture and terminology. Therefore, we are considering either the Controller or Orchestrator component based on the specific functions and requirements defined in the RFP. Kindly confirm whether the Controller/Orchestrator can be considered in place of either Controller or Orchestrator, based on the functional requirements specified in the RFP.	No Change, as per RFP
335	Remote User Security and Access Management	additional query/Clarification	The Controller is a separate component of an SD-WAN solution. However, the terms **Controller** and **Orchestrator** are often used interchangeably, depending on the OEM's architecture and terminology. Therefore, we are considering either the Controller or Orchestrator component based on the specific functions and requirements defined in the RFP. Kindly confirm whether the Controller/Orchestrator can be considered in place of either Controller or Orchestrator, based on the functional requirements specified in the RFP.	No Change, as per RFP

336		additional query/Clarification	The Controller is a separate component of an SD-WAN solution. However, the terms **Controller** and **Orchestrator** are often used interchangeably, depending on the OEM's architecture and terminology. Therefore, we are considering either the Controller or Orchestrator component based on the specific functions and requirements defined in the RFP. Kindly confirm whether the Controller/Orchestrator can be considered in place of either Controller or Orchestrator, based on the functional requirements specified in the RFP.	No Change, as per RFP
337		additional query/Clarification	The Controller is a separate component of an SD-WAN solution. However, the terms **Controller** and **Orchestrator** are often used interchangeably, depending on the OEM's architecture and terminology. Therefore, we are considering either the Controller or Orchestrator component based on the specific functions and requirements defined in the RFP. Kindly confirm whether the Controller/Orchestrator can be considered in place of either Controller or Orchestrator, based on the functional requirements specified in the RFP.	No Change, as per RFP
338	SD-WAN HUB CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 5,00,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
339	SD-WAN HUB CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 5,00,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
340	SD-WAN HUB CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 5,00,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
341	SD-WAN HUB CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 5,00,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
342	SD-WAN Edge Devices (District HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 300,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
343	SD-WAN Edge Devices (District HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 300,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
344	SD-WAN Edge Devices (District HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 300,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
345	SD-WAN Edge Devices (District HQ) CPE Specification	Suggested Clause	The proposed SD-WAN appliance shall support a minimum of 300,000 IP routes in its routing table to meet current and future SD-WAN and non-SD-WAN routing requirements, ensuring adequate scalability and performance without degradation.	No Change, as per RFP
346	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support per-user QoS policy to restrict user traffic. restricting user traffic based on source-IP and user-id should be supported.	No Change, as per RFP
347	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support per-user QoS policy to restrict user traffic. restricting user traffic based on source-IP and user-id should be supported.	No Change, as per RFP
348	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support per-user QoS policy to restrict user traffic. restricting user traffic based on source-IP and user-id should be supported.	No Change, as per RFP
349	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support per-user QoS policy to restrict user traffic. restricting user traffic based on source-IP and user-id should be supported.	No Change, as per RFP

350	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support adaptive shaping capability that helps to avoid congestion at the Hub locations. Adaptive shaping allows a device (branch or hub), to enforce a dynamic egress shaping rate on any other device that is sending the traffic. On the sender, only the traffic destined to the device with adaptive shaping configured is shaped and doesn't affect other traffic.	No Change, as per RFP
351	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support adaptive shaping capability that helps to avoid congestion at the Hub locations. Adaptive shaping allows a device (branch or hub), to enforce a dynamic egress shaping rate on any other device that is sending the traffic. On the sender, only the traffic destined to the device with adaptive shaping configured is shaped and doesn't affect other traffic.	No Change, as per RFP
352	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support adaptive shaping capability that helps to avoid congestion at the Hub locations. Adaptive shaping allows a device (branch or hub), to enforce a dynamic egress shaping rate on any other device that is sending the traffic. On the sender, only the traffic destined to the device with adaptive shaping configured is shaped and doesn't affect other traffic.	No Change, as per RFP
353	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support adaptive shaping capability that helps to avoid congestion at the Hub locations. Adaptive shaping allows a device (branch or hub), to enforce a dynamic egress shaping rate on any other device that is sending the traffic. On the sender, only the traffic destined to the device with adaptive shaping configured is shaped and doesn't affect other traffic.	No Change, as per RFP
354	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support a way to manage flapping link i.e. remove a link from overlay for traffic forwarding if the link is frequently flapping with incremental times for example for first occurrence the link is out of the path for 1min , for next occurrence 3 mins or so on.	No Change, as per RFP
355	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support a way to manage flapping link i.e. remove a link from overlay for traffic forwarding if the link is frequently flapping with incremental times for example for first occurrence the link is out of the path for 1min , for next occurrence 3 mins or so on.	No Change, as per RFP
356	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support a way to manage flapping link i.e. remove a link from overlay for traffic forwarding if the link is frequently flapping with incremental times for example for first occurrence the link is out of the path for 1min , for next occurrence 3 mins or so on.	No Change, as per RFP
357	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support a way to manage flapping link i.e. remove a link from overlay for traffic forwarding if the link is frequently flapping with incremental times for example for first occurrence the link is out of the path for 1min , for next occurrence 3 mins or so on.	No Change, as per RFP
358	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support securing user traffic with threat protection by using flowing security features. SSL & TLS Proxy SSL Inspection for invalid, expired, untrusted certificates HTTPS Proxy SSL & TLS 1.2, 1.3 Proxy	No Change, as per RFP
359	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support securing user traffic with threat protection by using flowing security features. SSL & TLS Proxy SSL Inspection for invalid, expired, untrusted certificates HTTPS Proxy SSL & TLS 1.2, 1.3 Proxy	No Change, as per RFP
360	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support securing user traffic with threat protection by using flowing security features. SSL & TLS Proxy SSL Inspection for invalid, expired, untrusted certificates HTTPS Proxy SSL & TLS 1.2, 1.3 Proxy	No Change, as per RFP
361	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should support securing user traffic with threat protection by using flowing security features. SSL & TLS Proxy SSL Inspection for invalid, expired, untrusted certificates HTTPS Proxy SSL & TLS 1.2, 1.3 Proxy	No Change, as per RFP

362	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support real-time monitoring at interval of every 3-5 seconds, for parameters like latency, packet loss, jitter, utilization, etc. Historical data with granularity of 5-15 mins minimum interval should also be stored in Analytics engine for forensic analysis later	Pls. refer corrigendum
363	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support real-time monitoring at interval of every 3-5 seconds, for parameters like latency, packet loss, jitter, utilization, etc. Historical data with granularity of 5-15 mins minimum interval should also be stored in Analytics engine for forensic analysis later	Pls. refer corrigendum
364	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support real-time monitoring at interval of every 3-5 seconds, for parameters like latency, packet loss, jitter, utilization, etc. Historical data with granularity of 5-15 mins minimum interval should also be stored in Analytics engine for forensic analysis later	Pls. refer corrigendum
365	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution must support real-time monitoring at interval of every 3-5 seconds, for parameters like latency, packet loss, jitter, utilization, etc. Historical data with granularity of 5-15 mins minimum interval should also be stored in Analytics engine for forensic analysis later	Pls. refer corrigendum
366	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like: Statistic bandwidth usage of available links Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization	No Change, as per RFP
367	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like: Statistic bandwidth usage of available links Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization	No Change, as per RFP
368	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like: Statistic bandwidth usage of available links Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization	No Change, as per RFP
369	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like: Statistic bandwidth usage of available links Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization	No Change, as per RFP
370	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The Proposed SDWAN Solution should provide the Application performance Monitoring dashboard (GUI) in a single pane for each branch offering real-time and historical visibility into application and network performance. The data stored and processed must be GSWAN datacenter no data/telemetry data must go outside the designated GSWAN datacenters.	Pls. refer corrigendum
371	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The Proposed SDWAN Solution should provide the Application performance Monitoring dashboard (GUI) in a single pane for each branch offering real-time and historical visibility into application and network performance. The data stored and processed must be GSWAN datacenter no data/telemetry data must go outside the designated GSWAN datacenters.	Pls. refer corrigendum
372	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The Proposed SDWAN Solution should provide the Application performance Monitoring dashboard (GUI) in a single pane for each branch offering real-time and historical visibility into application and network performance. The data stored and processed must be GSWAN datacenter no data/telemetry data must go outside the designated GSWAN datacenters.	Pls. refer corrigendum

373	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The Proposed SDWAN Solution should provide the Application performance Monitoring dashboard (GUI) in a single pane for each branch offering real-time and historical visibility into application and network performance. The data stored and processed must be GSWAN datacenter no data/telemetry data must go outside the designated GSWAN datacenters.	Pls. refer corrigendum
374	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a built-in security dashboard that provides insight into Top Application Usage base done session, Bandwidth, Risk score and Productivity score. Top URL based on categories reputation	No Change, as per RFP
375	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a built-in security dashboard that provides insight into Top Application Usage base done session, Bandwidth, Risk score and Productivity score. Top URL based on categories reputation	No Change, as per RFP
376	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a built-in security dashboard that provides insight into Top Application Usage base done session, Bandwidth, Risk score and Productivity score. Top URL based on categories reputation	No Change, as per RFP
377	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a built-in security dashboard that provides insight into Top Application Usage base done session, Bandwidth, Risk score and Productivity score. Top URL based on categories reputation	No Change, as per RFP
378	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a granular reporting for application performance behaviour and reports, must display, network level, DNS, HTTP, TCP level response time and QOE of the application from branch to HQ/DC/DR applications	No Change, as per RFP
379	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a granular reporting for application performance behaviour and reports, must display, network level, DNS, HTTP, TCP level response time and QOE of the application from branch to HQ/DC/DR applications	No Change, as per RFP
380	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a granular reporting for application performance behaviour and reports, must display, network level, DNS, HTTP, TCP level response time and QOE of the application from branch to HQ/DC/DR applications	No Change, as per RFP
381	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The solution should have a granular reporting for application performance behaviour and reports, must display, network level, DNS, HTTP, TCP level response time and QOE of the application from branch to HQ/DC/DR applications	No Change, as per RFP
382	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The deployed SDWAN solution should comply with Class-1 categorised Make in India govt. orders by DPII (including latest amendments).	No Change, as per RFP
383	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The deployed SDWAN solution should comply with Class-1 categorised Make in India govt. orders by DPII (including latest amendments).	No Change, as per RFP
384	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The deployed SDWAN solution should comply with Class-1 categorised Make in India govt. orders by DPII (including latest amendments).	No Change, as per RFP
385	Section – 5 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	Suggested Clause	The deployed SDWAN solution should comply with Class-1 categorised Make in India govt. orders by DPII (including latest amendments).	No Change, as per RFP
386	ANNEXURE - II	We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s_____ (SI / Bidder)	Kindly allow the bidder to submit the MAF as per the OEM's standard format.	Pls. refer corrigendum
387	ANNEXURE - II	We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s_____ (SI / Bidder)	Kindly allow the bidder to submit the MAF as per the OEM's standard format.	Pls. refer corrigendum

388	ANNEXURE - II	We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s _____ (SI / Bidder)	Kindly allow the bidder to submit the MAF as per the OEM's standard format.	Pls. refer corrigendum
389	ANNEXURE - II	We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s _____ (SI / Bidder)	Kindly allow the bidder to submit the MAF as per the OEM's standard format.	Pls. refer corrigendum
390	Delivery Milestone:	Delay penalty 0.15% per week up to 20% TCV	The proposed penalty of 0.15% per week, capped at 20% of TCV, is relatively high. We request a reasonable penalty cap to ensure it remains proportionate to the actual impact of delay and does not create an excessive financial burden on the bidder.	No Change, as per RFP
391	Delivery Milestone:	Delay penalty 0.15% per week up to 20% TCV	Please Cap implementation delay penalties at 10% of delayed milestone value.	No Change, as per RFP
392	Delivery Milestone:	Delay penalty 0.15% per week up to 20% TCV	Please Cap implementation delay penalties at 10% of delayed milestone value.	No Change, as per RFP
393	SLA	Incident penalties per breach plus availability penalties	Multiple penalties for the same incident may result in double penalization. We request that incident and availability penalties be mutually exclusive and capped at a reasonable limit, ensuring penalties remain proportionate to the actual service impact.	Pls. refer corrigendum
394	SLA	Incident penalties per breach plus availability penalties	Aggregate penalties with overall cap of 10% of quarterly value.	Pls. refer corrigendum
395	SLA	Incident penalties per breach plus availability penalties	Aggregate penalties with overall cap of 10% of quarterly value.	Pls. refer corrigendum
396	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT -- Point 55	The proposed solution components or its Operating System should be IPv6 logo and USGv6 certified	Request for Change: The proposed solution components or their Operating System shall support IPv6 from Day 1 of deployment. Justification: The requirement should focus on the functional objective of IPv6 support from Day 1, rather than mandating specific certification/logo requirements. Certification-specific requirements such as IPv6 Ready Logo or USGv6 may unnecessarily restrict technically compliant solutions. The proposed change will enable technology-neutral and wider participation while ensuring the required IPv6 capability, interoperability and future readiness of the SD-WAN deployment.	Pls. refer corrigendum
397	SECTION 5 - SPECIFICATIONS - Compliance Point no 55	The proposed solution components or its Operating System should be IPv6 logo and USGv6 certified	As per TEC guidelines for SDWAN product they perform rigorous testing for IPV6. Kindly refer the government of India Ministry of Commerce DPIIT Office Memorandum dated December 20th , 2022 "Restrictive and discriminatory conditions against the local suppliers" and "Other conditions which make the bid noncompliant to PPP-MII Order". The Office Memorandum dated December 20th , 2022 is attached for your kind reference. Therefore, we request GIL to kindly review this clause and consider accepting Indian standards or equivalent ISO certifications for compliance to PPP-MII Order. We request to amend the clause as "The proposed solution components or its Operating System should be TEC Certificate or IPv6 logo and USGv6 certified. "	Pls. refer corrigendum
398	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The proposed solution components or its Operating System should be IPv6 logo and USGv6 certified.	The proposed solution should support IPv4/IPv6 dual-stack functionality and comply with applicable IPv6 interoperability requirements.	Pls. refer corrigendum

399	3.10 Delivery Milestone:	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad. T1 = T + 45 calendar days	Due to industry wide ongoing supply chain constraint, AI Memory boom issue and geographical logistical issues Please modify as following: "Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad. T1 = T + 120 calendar days"	Pls. refer corrigendum
400		Delivery of all components (Hardware, Software, Licenses, etc. at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad - T1 = T + 45 calendar days	Considering the present OEM challenges, we request to revise this clause as Delivery of all components (Hardware, Software, Licenses, etc. at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad - T1 = T + 90 calendar days	Pls. refer corrigendum
401	5.1 SDWAN FUNCTIONAL SPECIFICATIONS #22	The solution should support extension of L2 network across sites over the SD-WAN fabric. It should also support MP-BGP EVPN with VXLAN.	Justification: EVPN/VXLAN is one particular architecture/mechanism for providing Layer-2/Layer-3 overlay services and is commonly associated with data-center fabric deployments. It should not necessarily be mandated where the functional requirement is only to extend Layer-2 connectivity across an SD-WAN network. Most OEMs may provide the required Layer-2 extension using their own native mechanisms. To allow wider OEM participation, it is recommended to retain the functional requirement without mandating a specific overlay technology. Request to modify as follows The solution should support extension of L2 network across sites over the SD-WAN fabric.	Pls. refer corrigendum
402	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT -- Point 22	The solution should support extension of L2 network across sites over the SD WAN fabric. It should also support MP-BGP EVPN with VXLAN.	Request for Change :- The solution shall support Layer-2 network extension across sites over the SD-WAN fabric using standards-based mechanisms such as MP-BGP EVPN with VXLAN or equivalent technologies. Justification - The customer may utilize multiple WAN underlays such as MPLS, Internet and P2P connectivity. L2 extension across sites is a functional requirement, whereas MP-BGP EVPN with VXLAN represents a specific implementation technology. Mandating a particular technology may unnecessarily restrict otherwise compliant SD-WAN solutions that provide equivalent L2 extension capabilities using other standards-based mechanisms. Therefore, it is requested that the requirement be made technology-neutral by permitting MP-BGP EVPN with VXLAN or equivalent mechanisms, while retaining the required L2 extension functionality.	Pls. refer corrigendum
403	SD-WAN Edge Devices (For office location) CPE Specification #32	The device should have minimum 8GB RAM	Justification: Adequate bootflash/storage is required for storing system software images, configuration files, logs, crash information and supporting software upgrade/rollback operations. Specifying minimum bootflash capacity along with RAM helps ensure sufficient local storage for reliable operations and future software lifecycle requirements. Request to modify as follows The device should have minimum 8 GB RAM and minimum 8 GB Bootflash.	Pls. refer corrigendum

404	SD-WAN Edge Devices - SIM Based (For office location) CPE Specification #41	The device should have minimum 8GB RAM	Justification: Adequate bootflash/storage is required for storing system software images, configuration files, logs, crash information and supporting software upgrade/rollback operations. Specifying minimum bootflash capacity along with RAM helps ensure sufficient local storage for reliable operations and future software lifecycle requirements. Request to modify as follows The device should have minimum 8 GB RAM and minimum 8 GB Bootflash.	Pls. refer corrigendum
405	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria:a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations.The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	Details of such projects undertaken along with work order/purchase order copy/clients' completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.	Bidder should have at least 1 order of SDWAN as a Managed Services Partner (MSP) from any Govt/Public Sector Undertaking (PSU) or Commercial Bank in India with a minimum of 250 locations/devices.	Pls. refer corrigendum
406	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Details of such projects undertaken along with work order/purchase order copy/clients' on-going or completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.	Bidder should have at least 1 order of SDWAN as a Managed Services Partner (MSP) from any Govt/Public Sector Undertaking (PSU) or Commercial Bank in India with a minimum of 250 locations/devices	No Change, as per RFP
407	The bidder must have average annual turnover of Rs. 200 Crore (Minimum) in the last three financial years as on 31st March 2025.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2025 shall be attached along with the bid.	•The Bidder should have a minimum annual turnover of Rs. 200 Crores	No Change, as per RFP
408	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2025 shall be attached along with the bid.	•The Bidder should have a minimum annual turnover of Rs. 200 Crores	No Change, as per RFP
409	Remote User Security and Access Management	Suggested Clause	The proposed solution should perform security inspection all traffic coming from the remote user's machine to the private applications irrespective of port and protocol and should at least perform the following security checks : SSL decryption, Anti-Virus/Anti- Malware for any file upload/download to and from the private application.	No Change, as per RFP
410	Remote User Security and Access Management	Suggested Clause	The proposed solution should perform security inspection all traffic coming from the remote user's machine to the private applications irrespective of port and protocol and should at least perform the following security checks : SSL decryption, Anti-Virus/Anti- Malware for any file upload/download to and from the private application.	No Change, as per RFP

411	Remote User Security and Access Management	Suggested Clause	The solution should have device posture validation across multiple parameters like Registry Check, Process Check, AD Domain Check, and Certificates etc to provide specific URL or Internet Access based on granular policy controls. The solution must be able to enforce the device posture check irrespective of whether the user is accessing Internet applications or private applications. The solution also must be able to detect not only whether a specific software is installed or not but also whether it is actually running and is configured.	No Change, as per RFP
412	Remote User Security and Access Management	Suggested Clause	The solution should have device posture validation across multiple parameters like Registry Check, Process Check, AD Domain Check, and Certificates etc to provide specific URL or Internet Access based on granular policy controls. The solution must be able to enforce the device posture check irrespective of whether the user is accessing Internet applications or private applications. The solution also must be able to detect not only whether a specific software is installed or not but also whether it is actually running and is configured.	No Change, as per RFP
413	Remote User Security and Access Management	Suggested Clause	The agent should support both Fail-open and Fail-safe configuration and should be tamperproof i.e. not allow the uninstallation of the agent even with admin credentials till the uninstall password is provided	The agent can be provided with this functionalities to meet the solution if required
414	Remote User Security and Access Management	Suggested Clause	The agent should support both Fail-open and Fail-safe configuration and should be tamperproof i.e. not allow the uninstallation of the agent even with admin credentials till the uninstall password is provided	The agent can be provided with this functionalities to meet the solution if required
415	Remote User Security and Access Management	Suggested Clause	The should follow the least-privilege access approach for connected users. The solution should support multi factor authentication using TOTP, Email.	No Change, as per RFP
416	Remote User Security and Access Management	Suggested Clause	The should follow the least-privilege access approach for connected users. The solution should support multi factor authentication using TOTP, Email.	No Change, as per RFP
417	Remote User Security and Access Management	Suggested Clause	Dedicated hardware appliances shall be deployed for ZTNA functionality at both the DC and DR sites to ensure high availability and seamless DC-DR resilience. The bidder may propose either an integrated or a dedicated solution, provided it fully meets the required ZTNA functionality and high-availability requirements. Solution should be scalable to support 1000 remotes user without replacing or upgrade ZTNA gateway. Tenderer/GIL would pay for license subscription only to add more remote users in future.	No Change, as per RFP
418	Remote User Security and Access Management	Suggested Clause	Dedicated hardware appliances shall be deployed for ZTNA functionality at both the DC and DR sites to ensure high availability and seamless DC-DR resilience. The bidder may propose either an integrated or a dedicated solution, provided it fully meets the required ZTNA functionality and high-availability requirements. Solution should be scalable to support 1000 remotes user without replacing or upgrade ZTNA gateway. Tenderer/GIL would pay for license subscription only to add more remote users in future.	No Change, as per RFP

419	3.10 Delivery Milestone:	2. Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad T1 = T + 45 calendar days	Considering the project requirement involving multi-location deployment across numerous sites, the stipulated delivery timeline appears to be very stringent and may not be sufficient for procurement, manufacturing, logistics, and coordinated deployment activities. We kindly request the Authority to consider revising the delivery timeline as follows: T1 = T + 90 Calendar Days Further, we request the Authority to suitably align the timelines for Installation & Commissioning and Factory Acceptance Testing (FAT) with the above revised delivery schedule to ensure adequate time for procurement, delivery, installation, configuration, testing, and successful commissioning across multiple locations.	Pls. refer corrigendum
420	SECTION 3 Scope of Work	2. Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad: T1 = T + 45 calendar days	Request to change as "T1 = T + 90 calendar days" considering current logistics challenges on chipsets. Timelines for subsequent milestones need to be increased accordingly.	Pls. refer corrigendum
421	SECTION 2 ELIGIBILITY CRITERIA	Managed WAN	Clarification: Managed WAN shall mean the SITC (Supply, Installation, Testing & Commissioning) of WAN devices at the customer premises.	No Change, as per RFP
422	SECTION 2 ELIGIBILITY CRITERIA	Managed WAN	Clarification: Managed WAN shall mean the SITC (Supply, Installation, Testing & Commissioning) of WAN devices at the customer premises.	No Change, as per RFP
423	Scope 3.3	Any item, activity, software, hardware, license, service, or component reasonably required for achieving the intended functionality, performance, interoperability, security, scalability, availability, compliance, or successful operation of the solution shall be deemed to be included in the Bidder's scope and quoted price. No additional payment, change request, variation order, or financial claim shall be admissible on account of omission, oversight, misunderstanding, or interpretation of the RFP.	Limit to items reasonably inferable from RFP/BoQ; changes outside scope through mutually agreed change request.	The scope is limited to the RFP and to complete the solution as defined in scope of work
424	Scope 3.3	Any item, activity, software, hardware, license, service, or component reasonably required for achieving the intended functionality, performance, interoperability, security, scalability, availability, compliance, or successful operation of the solution shall be deemed to be included in the Bidder's scope and quoted price. No additional payment, change request, variation order, or financial claim shall be admissible on account of omission, oversight, misunderstanding, or interpretation of the RFP.	Limit to items reasonably inferable from RFP/BoQ; changes outside scope through mutually agreed change request.	The scope is limited to the RFP and to complete the solution as defined in scope of work
425	Delivery Milestone:	In case, the selected bidder does not supply the ordered items for any reason, the bidder will be liable to pay the difference amount to the purchaser, over and above the performance guarantee.	Limit total liability to contract value/PBG except fraud.	No Change, as per RFP
426	Delivery Milestone:	In case, the selected bidder does not supply the ordered items for any reason, the bidder will be liable to pay the difference amount to the purchaser, over and above the performance guarantee.	Limit total liability to contract value/PBG except fraud.	No Change, as per RFP
427	Payment	In case of delay, manpower support shall continue at no additional cost until successful handover.	Extension support to be mutually agreed where delay attributable to purchaser/third parties.	No Change, as per RFP
428	Payment	In case of delay, manpower support shall continue at no additional cost until successful handover.	Extension support to be mutually agreed where delay attributable to purchaser/third parties.	No Change, as per RFP
429	Termination	Termination, risk purchase, PBG forfeiture largely at Tenderer discretion	Please Include cure period, bidder representation rights, and liability cap.	Pls. refer corrigendum
430	Termination	Termination, risk purchase, PBG forfeiture largely at Tenderer discretion	Please Include cure period, bidder representation rights, and liability cap.	Pls. refer corrigendum

431	3.1 Scope Overview 3.4 Functional Requirement point 19	The proposed SD WAN solution component should be IPv6 ready logo or USGv6 certified. Must support IPv4 and IPv6 protocols from day 1.	Request for Change: The proposed SD WAN solution component must support IPv4 and IPv6 from day 1. Justification: The requirement should focus on the functional outcome—full IPv4 and IPv6 support from Day 1—rather than mandating a specific certification/logo. This will avoid unnecessary restriction of technically compliant solutions while ensuring the required IPv6 capability, interoperability and future readiness of the SD-WAN deployment.	Pls. refer corrigendum
432	3.4 Functional Requirement	The proposed SD WAN solution component should be IPv6 ready logo or USGv6 certified. Must support IPv4 and IPv6 protocols from day 1.	As per TEC guidelines for SDWAN product they perform rigorous testing for IPV6. Kindly refer the government of India Ministry of Commerce DPIIT Office Memorandum dated December 20th , 2022 "Restrictive and discriminatory conditions against the local suppliers" and "Other conditions which make the bid noncompliant to PPP-MII Order". The Office Memorandum dated December 20th , 2022 is attached for your kind reference. Therefore, we request GIL to kindly review this clause and consider accepting Indian standards or equivalent ISO certifications for compliance to PPP-MII Order. We request to amend the clause as "The proposed SD WAN solution component should be IPv6 ready logo or USGv6 certified or TEC certified. Must support IPv4 and IPv6 protocols from day 1. "	Pls. refer corrigendum
433	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT -- Point 53	The proposed solution shall use cryptographic modules certified under FIPS 140-2 Level 2 or higher,	Request for Removal: Kindly consider removing the mandatory requirement for FIPS 140-2 Level 2 or higher certification for the proposed solution and instead require compliance with applicable Government of India/DoT/TEC security and certification requirements. Justification: FIPS 140-2 is a U.S. Government cryptographic module validation standard, and mandating Level 2 or higher may unnecessarily restrict participation of technically capable Indian OEMs and compliant solutions. The security objective can be addressed through applicable Government of India/DoT/TEC requirements and recognized security standards. Hence, removal of the mandatory FIPS 140-2 Level 2 or higher requirement is requested to ensure technology-neutral and wider participation without compromising security requirements.	No Change, as per RFP
434	SECTION 5 - SPECIFICATIONS - Compliance Point no 53	The proposed solution shall use cryptographic modules certified under FIPS 140-2 Level 2 or higher,	As per TEC guidelines for SDWAN product they perform rigorous testing for SD-WAN Product. Kindly refer the government of India Ministry of Commerce DPIIT Office Memorandum dated December 20th , 2022 "Restrictive and discriminatory conditions against the local suppliers" and "Other conditions which make the bid noncompliant to PPP-MII Order". The Office Memorandum dated December 20th , 2022 is attached for your kind reference. Therefore, we request GIL to kindly review this clause and consider accepting Indian standards or equivalent ISO certifications for compliance to PPP-MII Order. We request to amend the clause as "The proposed solution shall use cryptographic modules certified under TEC Certificate or FIPS 140-2 Level 2 or higher,."	No Change, as per RFP

435	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices (District HQ) CPE Specification Point 16	16.The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	Request for Clarification / Changes: Kindly review the requirement of 20 port requirement -- 8x1GE SFP, 8x1/10GE SFP+ and 4x10/25GE SFP28 ports and consider an appropriate port configuration based on the actual WAN/LAN connectivity and projected bandwidth requirements. Justification The specified 20-port configuration may result in unnecessary over-provisioning if the actual WAN/LAN connectivity, aggregate bandwidth and future scalability requirements do not justify the stated interface density. Port requirements should therefore be aligned with the actual deployment architecture, current connectivity and projected bandwidth growth of the proposed solution. Accordingly, allowing an appropriate and equivalent port configuration based on the required throughput and connectivity will provide greater solution flexibility, avoid unnecessary hardware cost and over-provisioning, and promote wider participation and price competitiveness, while ensuring that all required performance and scalability requirements are met.	Pls. refer corrigendum
436	SD-WAN Edge Devices (District HQ) CPE Specification	16 - The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.	As per the specified requirement of 10 Gbps throughput, the current interface requirement appears to be on the higher side and may unnecessarily increase the overall solution complexity and cost. Further, the requirement specifies SFP-based interfaces for all ports. We request GIL to kindly review the interface requirement and consider a more flexible port configuration that adequately meets the required throughput and deployment requirements. We request GIL to amend the clause as follows: The device should have minimum 8X1GE , 12 x1/10GE SFP+	Pls. refer corrigendum
437	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices (Taluka HQ) CPE Specification -- Point 25	25.The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's	Change Request: The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Justification: The LAN is connect through Switch and only one or two ports will be used. For Taluka HQ there are only 2 links, additional one port can be fiber or copper can be utilized.	No Change, as per RFP
438	SD-WAN Edge Devices (Taluka HQ) CPE Specification	25 .The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's	As per the specified requirement of 900 Mbps throughput, the current interface requirement appears to be on the higher side and may unnecessarily increase the overall solution complexity and cost. We request GIL to kindly review the interface requirement and consider a more flexible port configuration that adequately meets the required throughput and deployment requirements. We request GIL to amend the clause as follows: "The device should have a minimum of 6x1G ports, out of which at least 2 ports should be SFP based. Out of the 6 ports minimum 3 WAN and 3 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's"	No Change, as per RFP

439	SECTION 5 - SPECIFICATIONS - Compliance Point no 54	The proposed solution shall be Common Criteria (CC) certified against the relevant Network Device Protection Profiles (NDPP). The Common Criteria certification shall be issued either by an internationally recognized Common Criteria Certification Scheme or by the Indian Common Criteria Certification Scheme (IC3S), established by the Ministry of Electronics and Information Technology (MeitY). Valid Common Criteria certification details shall be submitted along with the technical bid.	As per TEC guidelines for SDWAN product they perform rigorous testing for SD-WAN Product. Kindly refer the government of India Ministry of Commerce DPIIT Office Memorandum dated December 20th , 2022 "Restrictive and discriminatory conditions against the local suppliers" and "Other conditions which make the bid noncompliant to PPP-MII Order". The Office Memorandum dated December 20th , 2022 is attached for your kind reference. Therefore, we request GIL to kindly review this clause and consider accepting Indian standards or equivalent ISO certifications for compliance to PPP-MII Order. We request to amend the clause as " The Common Criteria certification shall be issued either by an internationally recognized Common Criteria Certification Scheme or by the Indian Common Criteria Certification Scheme (IC3S), established by the Ministry of Electronics and Information Technology (MeitY) or TEC (Telecommunication Engineering Centre), Department of Telecommunications (DoT).. Valid certification details shall be submitted along with the technical bid.. "	No Change, as per RFP
440	5.1. SD-WAN – FUNCTIONAL – REQUIREMENT	The proposed solution shall be Common Criteria (CC) certified against the relevant Network Device Protection Profiles (NDPP). The Common Criteria certification shall be issued either by an internationally recognized Common Criteria Certification Scheme or by the Indian Common Criteria Certification Scheme (IC3S), established by the Ministry of Electronics and Information Technology (MeitY). Valid Common Criteria certification details shall be submitted along with the technical bid.	The clause may be removed from the tender requirement.	No Change, as per RFP
441	3.4 Functional Requirement #5	The solution should be capable of utilizing a combination of two or more links in any of the following scenarios: a) Point-to-Point links, L2 MPLS,L3 MPLS, Internet Leased Line, 3G/4G/5G/LTE, Broadband Internet, etc.	Remark: Since the SD-WAN router operates on Layer-3/IP connectivity, we understand that in case of L2 MPLS connectivity, appropriate IP connectivity/reachability shall be extended up to the SD-WAN router for establishing the SD-WAN overlay. Please clarify if otherwise.	No Change, as per RFP
442	3.4 Functional Requirement #9	The bidder is required to design, supply, and provision hardware, software, and licenses for the SD-WAN core infrastructure capable of supporting a minimum of 6,000 SD-WAN devices/sites with minimum two link termination at each location from Day-1 of commissioning. The solution must also support an additional 30% scalability (1,800 devices), making the total capacity 7,800 devices, without any augmentation or upgrade of hardware, software, or licenses. The bidder should ensure that this scalability is built-in within the proposed architecture, and no additional cost should be payable by the Department for enabling or utilizing this additional capacity during the contract period.	Remark: We understand that the SD-WAN core infrastructure shall be sized to support 6,000 devices/sites from Day-1 with scalability up to 7,800 devices/sites without augmentation of the proposed core infrastructure. We understand that licenses/subscriptions associated with additional SD-WAN edge devices/sites beyond the initial 6,000 shall be procured as and when such additional devices/sites are deployed. Please clarify if otherwise.	The understanding is correct. However the licenses (6000 device/sites) supplied shall be with 10 years validity and support period as mentioned in the RFP.
443	3.4 Functional Requirement #12	The SD-WAN OEM shall provide professional services for the design, validation, and initial implementation of the SD-WAN solution. The OEM shall be responsible for designing, validating, and implementing the SD-WAN Controller and SD-WAN Hub at the State Headquarters (SHQ). Further, as part of OEM professional services, the OEM shall directly design and implement a minimum 100 sites to establish the reference architecture, validate performance, and ensure correct deployment standards. Thereafter, the remaining site implementations may be carried out by the Bidder under the guidance, validation, and certification of the OEM.	The SD-WAN OEM shall provide professional services for the design, validation, and initial implementation of the SD-WAN solution. The OEM shall be responsible for designing, validating, and implementing the SD-WAN Controller and SD-WAN Hub at the State Headquarters (SHQ). Further, as part of OEM professional services, the OEM shall directly provide design and configuration templet for each type of site to establish the reference architecture, validate performance, and ensure correct deployment standards. Thereafter, the remaining site implementations may be carried out by the Bidder as per the shared template and standard operating procedure documents. The OEM should provide project manager during the OEM implemetation duration.	Pls. refer corrigendum

444	3.4 Functional Requirement #15	All components of the proposed SD-WAN solution must be on-premises.	We understand that the requirement for all components to be deployed on-premises is intended specifically for the core SD-WAN solution and associated control/management components, and is not applicable to Remote User Security and Access Management solutions. Kindly clarify if our understanding is otherwise.	Complete solution needs to be on-premises.
445	3.4 Functional Requirement #20	The proposed SD-WAN branch appliance shall be quoted with maximum supported license tier by the hardware platform. The appliance should meet the requirements specified in the RFP while also supporting future scalability without hardware replacement.	Justification: Mandating the maximum supported license tier may include features and capabilities that are not required under the RFP or relevant to the architecture, providing no functional benefit while unnecessarily increasing the solution cost. The appropriate license tier supporting all features specified in the RFP should therefore be considered. Further, "future scalability without hardware replacement" is open-ended and cannot be assured without a defined future capacity or throughput requirement, as the appliance would be sized based on the requirements specified in the RFP. Request to modify as follows The proposed SD-WAN branch appliance shall be quoted with the appropriate license tier supporting all features specified in the RFP. The appliance should meet the requirements specified in the RFP.	Pls. refer corrigendum
446	3.4 Functional Requirement #45	All SD-WAN device, software, routing, security, security signature updates, orchestration, analytics, subscription services and management licenses shall be perpetual or subscription (with 10 years license to be supplied from day 1) in nature from the Go-Live of the project. No feature reduction, throttling, or license expiry shall occur after completion of the mentioned period.	Justification: The typical lifecycle of enterprise networking hardware is around 5- 7 years, and most SD-WAN OEMs follow subscription-based licensing models. Active licenses/subscriptions are required to continue using the applicable features and functionality. Request to align the license period with the hardware lifecycle and consider 5 years instead of 10 years as per the contract terms. Request to modify as follows All SD-WAN device, software, routing, security, security signature updates, orchestration, analytics, subscription services and management licenses shall be perpetual or subscription (with 5 years license to be supplied from day 1 in line with contract duration) in nature from the Go-Live of the project. Applicable subscription licenses shall be renewed as required to continue using the respective features and functionality after completion of the mentioned period.	Pls. refer corrigendum
447	3.4 Functional Requirement #53	The solution shall comply with all applicable CERT-In, DoT, and TRAI guidelines, including, but not limited to, log retention and secure maintenance of records. The successful bidder shall implement all necessary measures to ensure compliance as part of the solution including all network device configuration files shall be securely backed up within India, version-controlled, encrypted, and retained for a minimum of 2 years, ensuring availability for audit, recovery, and compliance verification. Bidder has to provide the necessary logs whenever asked by GIL / competent authority. Bidder should deploy any tool / solution for ip address management / syslog to ensure necessary compliance and retention for 2 years as asked above	The 2-year retention requirement appears excessive and may result in significant storage and operational overhead. For reference, CERT-In requires applicable ICT system logs to be retained for a minimum of 180 days (6 months). Accordingly, request to consider reducing the retention period to 6 months.	Pls. refer corrigendum
448	3.4 Functional Requirement #53	Configuration backups of the Central Orchestrator shall be encrypted, version controlled and replicated between DC and DR with automated scheduled backup.	Request to modify as follows for wider OEM participation Configuration backups of the Central Orchestrator shall be encrypted, version controlled/incremental and replicated between DC and DR with manual/ automated scheduled backup as supported by OEM architecture.	No Change, as per RFP

449	3.5 Design Principles to be followed.	b) Security policies must be configured for all devices and controllers to prevent unwanted intrusions, including IPS, Malicious URL filtering, and detection of known and unknown malware.	Justification: SD-WAN controllers are management/control-plane components and are typically deployed behind dedicated firewall/security infrastructure rather than providing IPS, Malicious URL filtering or malware inspection natively. These security features can be enabled on the SD-WAN edge devices as applicable, while Hub/DC/DR and controller infrastructure can be protected through the proposed firewall/security architecture. Request to modify as follows Security policies must be configured for all SD-WAN edge devices to prevent unwanted intrusions, including IPS, Malicious URL filtering, and malware detection . Controllers and Hub/DC/DR infrastructure may be protected through the proposed firewall/security infrastructure as supported by OEM architecture.	No Change, as per RFP
450	Final Acceptance Testing (FAT) & Go-Live 6 PERFORMANCE	Throughput Test Measure SD-WAN throughput with security enabled	Justification: Throughput validation during FAT will be constrained by the bandwidth provisioned at the respective site and may not reflect the rated throughput capability of the proposed appliance. For example, a device sized for 100 Mbps cannot be validated for its rated throughput over a 10 Mbps WAN link. Additionally such testing would require dedicated traffic-generation tools and test infrastructure. The supported throughput should instead be validated through OEM-published datasheet/documentation. Request to remove this clause.	No Change, as per RFP
451	Final Acceptance Testing (FAT) & Go-Live High Availability 7	7 High Availability Edge Device HA Primary appliance failure Secondary appliance assumes operation without session interruption	We understand that the requirement is intended for Hub locations where HA is required, and that depending on the nature of the session, existing sessions should remain established during failover even though brief packet loss may occur during convergence. Kindly confirm if our understanding is correct.	Yes, the understanding is correct.
452	Final Acceptance Testing (FAT) & Go-Live 39 Management	39 Management Configuration Version Control Multiple configuration revisions Version history maintained and rollback available	Justification: Maintaining complete configuration version history with rollback for every change across all managed devices is not a standard or scalable capability across most SD-WAN OEMs. Configuration changes and administrative activities are typically captured through centralized audit logs for traceability. Mandating configuration version history and rollback as part of FAT may therefore restrict wider OEM participation. Request to remove this clause.	No Change, as per RFP

453	5.13. Alignment with GSWAN / Hybrid MPLS–Internet Architecture Traffic Steering	The dynamic path selection rules should allow traffic steering based on following parameters: ☑ Source IP address ☑ Source MAC address ☑ User identity and user groups (where identity integration is available) ☑ Destination IP address, route attributes/tags, and Type of Service (ToS) / DSCP values ☑ Application identification, application groups, or application categories ☑ Protocol type and QoS markings ☑ Link quality parameters or service level agreement (SLA) metrics such as latency, jitter, packet loss, or other defined performance thresholds.	Justification: Source MAC address is a Layer-2 attribute whose visibility depends on the LAN topology and may not be available to the SD-WAN CPE when intermediate Layer-3 devices are present. Dynamic WAN path selection is typically performed using Layer-3/Layer-7 parameters such as IP addresses, applications, QoS markings and SLA metrics. Request to remove this parameter for wider OEM participation. Request to modify as follows The dynamic path selection rules should allow traffic steering based on following parameters: ☐ Source IP address ☐ User identity and user groups (where identity integration is available) ☐ Destination IP address, route attributes/tags, and Type of Service (ToS) / DSCP values ☐ Application identification, application groups, or application categories ☐ Protocol type and QoS markings ☐ Link quality parameters or service level agreement (SLA) metrics such as latency, jitter, packet loss, or other defined performance thresholds.	Pls. refer corrigendum
454	5.1 SDWAN FUNCTIONAL SPECIFICATIONS #32	The proposed solution must support IP and User and User group-aware SD-WAN policies to prioritize traffic of VIP users, Ministers, and higher officials at any site.	Justification: Support for both IP and User/User group-aware SD-WAN policies is not standard across all OEMs and may restrict wider OEM participation. The intended traffic prioritization can be achieved using either IP-based or User/User group-based policy mechanisms. Request to modify as follows The proposed solution must support IP or User or User group-aware SD-WAN policies to prioritize traffic of VIP users, Ministers, and higher officials at any site.	Pls. refer corrigendum
455	5.1 SDWAN FUNCTIONAL SPECIFICATIONS #34	SD-WAN solution should support all advanced SD-WAN features without any restriction, more than 1000 VRF, unlimited topologies, Per Packet / Session base Load balancing, Advanced QoS, FEC, Bandwidth Detection, Packet Duplication, Per Packet/Session base Steering, Unlimited topologies.	Justification: The requirement for more than 1000 VRFs is excessive for the envisaged deployment, where typically 3–4 VRFs/segments would be required. Scalability of minimum 10 VRFs with corresponding logical topologies for each VRF/segment should provide sufficient headroom. Further, “Advanced QoS” is not quantifiable; QoS capabilities should be considered as per the specifications defined in the RFP. Request to modify as follows SD-WAN solution should support SD-WAN features as required in the specifications, minimum 10 VRF, corresponding logical topologies for each VRF/Segment, Per Packet /Session base Load balancing, QoS as per specifications, FEC, Bandwidth Detection, Packet Duplication, Per Packet/Session base Steering, corresponding logical topologies for each VRF/Segment.	Pls. refer corrigendum
456	5.1 SDWAN FUNCTIONAL SPECIFICATIONS #35	All Hub devices /solutions (Central infrastructure including software and license and accessories) should be in HA with N+N set up with all SD-WAN features mentioned in this RFP at DC & DR location	Remark: We understand that the N+N HA requirement is applicable to the Hub SD-WAN routers/Firewalls/Switches at DC & DR locations, while HA for the SD-WAN control and management components shall be provided across DC and DR as per the OEM-supported solution architecture. Please clarify if otherwise.	Pls. refer corrigendum

457	Standards Compliance	All features shall be supported using open standards and non-proprietary implementations	Justification: SD-WAN solutions inherently use OEM-specific control-plane, orchestration, policy and management mechanisms, while supporting industry-standard protocols where applicable. Mandating that all features be based only on open standards and non-proprietary implementations is not practical and restricts wider OEM participation. Request to remove the clause.	Please consider omitted
458	Central Orchestrator / Controller Specifications #2	The complete management, orchestration, analytics, reporting, policy management and monitoring platform shall be supplied by the same OEM as the SD-WAN solution.	Justification: While core SD-WAN management, orchestration and policy management should be provided by the same OEM, certain advanced reporting, logging and analytics capabilities may be delivered through an integrated third-party platform. Allowing this flexibility will enable bidders to meet the overall functional requirement without restricting wider OEM participation. Request to modify as follows The complete management, orchestration, analytics, reporting, policy management and monitoring platform shall be supplied by the same OEM as the SD-WAN solution. For certain advanced reporting, logging and analytics capabilities, an integrated third-party tool may be proposed to meet the overall requirement.	No Change, as per RFP
459	Central Orchestrator / Controller Specifications #10	Configuration version history with rollback capability shall be available for all managed devices.	Justification: Maintaining complete configuration version history with rollback for every change across all managed devices is not a standard or scalable capability across most SD-WAN OEMs. Configuration changes and administrative activities are typically captured through centralized audit logs for traceability. Mandating full per-device configuration versioning and rollback may therefore restrict wider OEM participation. Request to modify as follows Configuration changes and administrative activities shall be captured through centralized audit logs for traceability.	No Change, as per RFP
460	Central Orchestrator / Controller Specifications #29	The bidder shall provide perpetual/subsorption licenses valid for ten (10) years for the complete Orchestrator platform.	Justification: The typical lifecycle of enterprise networking hardware is around 5-7 years, and most SD-WAN OEMs follow subscription-based licensing models. Active licenses/subscriptions are required to continue using the applicable features and functionality. Request to align the license period with the hardware lifecycle and consider 5 years instead of 10 years. Request to modify as follows The bidder shall provide perpetual/subsorption licenses valid for 5 years	Pls. refer corrigendum
461	SD-WAN Edge Devices (Taluka HQ) CPE Specification # 27	Should support minimum 250 overlay IPSec tunnels from day 1.	Justification: Taluka HQ locations potentially serve as regional aggregation points for sub-level sites and may host or provide access to regional applications/services. To provide sufficient scalability and headroom for such use cases, it is recommended that the platform support a minimum of 500 overlay IPSec tunnels. Request to modify as follows Should support minimum 500 overlay IPSec tunnels from day 1.	No Change, as per RFP

462	General Clarification	Please provide details of the existing P2P connectivity across the different site categories, including: Number of P2P links terminating at site category. Any Routing protocol currently used over the P2P links (Static/OSPF/BGP, etc.) How these links are physically terminated today — directly on the WAN router or through an intermediate aggregation switch/router Whether all existing P2P links are expected to be retained and integrated as SD-WAN underlay transports during migration. This information will be required for appropriate network planning and migration.		For detailed design, you may visit GSWAN / GIL and confirm the requirements.
463	Section 6: Price Bid	Quantities to be ordered on 1st day is not defined.	our understanding is to supply the notional quantity mentioned on page 43 as a day 1 supply. Kind request you to please clarify if this is correct?	Minimum Quantity required for deployment including Complete central architecture and DC, TC locations will be given on Day -1. However the actual quantity may defer from the notional quantity.
464	Additional Clause	As advanced AI frontier models reshape the threat landscape, proposed SD-WAN must evolve to provide deeper visibility and predictive threat analysis. we suggest to include following points mentioned in Justification column, these will allows GIL/DST to proactively manage attack surface and secure the network against emerging threats, fulfilling the critical security requirements for such critical statewide deployment."	The proposed solution must deliver a single, AI-native digital experience that unifies asset visibility, security & configuration assessments, proactive risk insights, and support-case management within one interface - not a collection of separate portals or point dashboards."	No Change, as per RFP
465			"The solution must include a natural-language generative-AI assistant capable of answering environment-specific questions, summarizing risk exposure, and generating custom reports on demand - grounded in both the customer's own telemetry and the OEM's engineering/support knowledge base. "	No Change, as per RFP
466			"The solution must continuously assess the core installed base and prioritize findings using an automated device-criticality model that weights each device by its role and impact in the network topology (e.g., WAN aggregation/hub routers vs. low-impact branch edge), rather than presenting a flat, unprioritized list."	No Change, as per RFP
467			"The solution must provide configuration best-practice and security-hardening assessments derived from the OEM's own validated intellectual capital, and identify misconfigurations across core SDWAN devices."	No Change, as per RFP
468			"The solution must ingest telemetry natively from the OEM's WAN/SD-WAN controller, campus controller, and compute/cloud controllers through a single collection architecture."	No Change, as per RFP
469			"The solution must provide visibility and assessment for devices that are NOT managed by any controller, including standalone and end-of-life devices."	No Change, as per RFP
470			"The proactive insights/AI platform must be included within the standard support entitlement at no additional license cost."	No Change, as per RFP
471	The OEM & bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2025.	The copies of CA Certified Statement for last three financial years as on 31st March 2025 shall be attached along with the bid.	•The Bidder should report positive EBITDA or Positive Net profit during each of the last 3 financial years.	Pls. refer corrigendum
472	Section 3.4 Clause 9 & 10	SD-WAN Controller/Orchestrator to support 7,800 devices from Day-1 without augmentation	Kindly clarify whether scalability up to 7,800 sites can be achieved through software/license expansion without hardware replacement during the contract period.	Yes, the understanding is correct.

473	Section 5.1 Clause 42	Alerting through Email, SMS and WhatsApp	Kindly clarify whether SMS/WhatsApp gateway infrastructure will be provided by GSWAN or needs to be supplied by the bidder as part of the proposed solution.	Will be provided by GIL / GOG.
474	Section 7 (POC)	Successful demonstration of all mandatory requirements during POC	Request customer to share detailed POC test cases, acceptance criteria, and testing methodology.	Already mentioned in RFP.
475	Clause 40	Migration with Near Zero Downtime	Kindly clarify existing routing architecture (OSPF/BGP/Static), migration methodology expectations	Will be provided to L1 bidder.
476	Throughout RFP	Secure Web Gateway capability required	Kindly clarify whether on-prem Secure Web Gateway is mandatory or cloud-delivered SWG/SASE service from OEM shall be acceptable.	Complete solution needs to be on-premises.
477	Scalability	10-Year License requirement	Kindly confirm whether subscription licenses valid for 10 years are acceptable in lieu of perpetual licenses.	Yes, the understanding is correct.
478	Section 2 - Eligibility Criteria	Section 2 - Eligibility Criteria	We request addition of this clause : If the bidder is a wholly owned parent company of a subsidiary, the experience, technical capability, financial capability, project references, and other eligibility criteria may be fulfilled by either the Bidder or its wholly-owned subsidiary, and such credentials shall be considered for the purpose of qualification and evaluation of the Bidder. Reason/ Justification : The proposed amendment is requested to ensure wider participation and fair competition by recognizing the credentials of wholly owned parent companies and subsidiaries operating within the same corporate group. Large organizations often execute projects, maintain financial records, and hold technical capabilities through different group entities. Allowing the experience, technical capability, financial strength, and project references of a wholly owned parent company or subsidiary to be considered will enable qualified bidders to participate without compromising the intent of the eligibility criteria, while ensuring the customer benefits from the combined expertise and resources of the corporate group.	No Change, as per RFP
479	Section 2 - Eligibility Criteria	10. The quoted product must be MTCTE certified	Request amendment to: The quoted product must be MTCTE certified. In case the bidder has applied for MTCTE certification, the bidder must submit the proof that he has applied for. Bidder will also need to provide an undertaking that within three months of bid award, the bidder will submit MTCTE certificate document to the buyer.	No Change, as per RFP
480	3.4 Functional Requirement	2. SD-WAN Orchestrator and Controllers shall be deployed on premise within Government Data Centre / designated location. Public cloud-only orchestration shall not be acceptable.	Kindly accept SD-WAN orchestrator or controller deployment in bidder / OEM cloud also.	No Change, as per RFP
481	3.4 Functional Requirement	15. All components of the proposed SD-WAN solution must be on-premises.	Kindly accept SD-WAN orchestrator or controller deployment in bidder / OEM cloud also.	No Change, as per RFP
482	3.4 Functional Requirement	16. The Hub and Branch CPE Appliance should have the Hardware/virtual appliance. In case of virtual appliance all required hardware, software, license etc. shall be provided by the bidder as part of the solution.	Virtual appliance degrades the throughput. In addition, for virtual appliance, there is an additional requirement of a license for the SDWAN application, either perpetual or subscription-based. Therefore, kindly allow only hardware-based appliance for head end and branch locations. Only SD-WAN orchestrator or controller can be a virtual appliance based.	No Change, as per RFP
483	40 Interoperability Existing NMS/SIEM Integration	Verify integration with existing GSWAN tools Successful event and log exchange	Pls provide details of existing SIEM (OEM Name, model, Software Version etc)	Will be provided to L1 bidder.
484	3.10 Delivery Milestone:	3 Installation, and Commissioning of SD-WAN solution at Hub / Central Locations T2 = T1 + 60 calendar days	SDWAN hardware supply is severely affected on account of supply chain disruptions. Therefore, kindly allow up to 90 to 105 days for the SDWAN hardware supply and installation.	No Change, as per RFP
485	3.10 Delivery Milestone:	4 Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations T3 = T2 + 15 calendar days	kindly allow up to 105 days for the SDWAN hardware supply and installation.	Pls. refer corrigendum

486	3.10 Delivery Milestone:	5 Installation, Commissioning, and FAT of SD-WAN Edge Devices at Individual Office Locations	kindly allow up to 120 days for the SDWAN hardware supply and installation.	Pls. refer corrigendum
487	3.10 Delivery Milestone:	6 Installation, and Commissioning of SD-WAN solution at District Locations, Taluka and PoP Locations T5 = T1 + 100 calendar days	kindly allow up to 120 days for the SDWAN hardware supply and installation.	Pls. refer corrigendum
488	3.10 Delivery Milestone:	7 Final Acceptance Testing (FAT) and Go-Live of the SD-WAN solution for District, Taluka and PoP Locations T6 = T5 + 15 calendar days	kindly allow up to 135 days for the clause	No Change, as per RFP
489	3.8 Manpower Deployment, Knowledge Transfer & Handover	A. Scope & Duration of Manpower Deployment: 1. The bidder shall deploy the required SD-WAN manpower only for a period of one (1) year post Go-Live. 2. The objective of manpower deployment shall be: a) Stabilization of the SD-WAN solution b) Advanced troubleshooting and root cause analysis c) Configuration and policy support d) Knowledge transfer and operational handover to GSWAN operation team 3. Post completion of the one-year period, no dedicated manpower deployment by the bidder shall be mandatory, except for obligations under SLA, warranty, OEM support, or AMC. B. Minimum Manpower Requirement: Role Minimum Count Key Responsibilities SD-WAN L3 / Solution Architect 1 Architecture oversight, policy design, RCA, upgrades SD-WAN L2 Engineer 1 Configuration support, fault isolation, coordination SD-WAN Orchestrator / NMS Specialist 1 Monitoring, analytics, reporting, NMS integration Service Delivery Manager 1 SLA tracking, reporting, coordination with GSWAN & TPA	We observe that Section 6 – Price Bid does not provide any separate line item/provision for quoting the cost towards the above manpower resources. We request the Authority to kindly clarify under which line item/head the bidder should quote the cost of the manpower resources specified under Clause 3.8.	It will be part of overall solution, bidder may quote accordingly.
490	SECTION 6 PRICE BID:		We request the Authority to include a separate line item in the Price Bid/BOQ for the manpower deployment for one (1) year, to ensure uniform and transparent commercial evaluation across all bidders.	No Change, as per RFP
491	Limitation of Liability	Not mentioned	It is recommended that the RFP include a Limited Liability clause specifying that the maximum liability shall be capped at 10% of the Total Contract Value (TCV)	No Change, as per RFP
492	Payment Terms	As per table	Payments shall be released within 30 days of invoice acceptance; delayed payments shall carry interest at 12% per annum	No Change, as per RFP
493	Section 1 : Earnest Money Deposit	EMD as mentioned above, shall be submitted in the form of Demand Draft OR in the form of an unconditional Bank Guarantee (which should be valid up to validity of 9 months from the date of bid submission) of any Nationalized Bank (operating in India having branch at Ahmedabad/ Gandhinagar) in the name of "Gujarat Informatics Ltd." payable at Gandhinagar and must be submitted along with the covering letter.	As per the amendment in GFR 2017 dated 02-02-2022 (Rule 170 of GFR 2017), Bid security may be obtained in the form of insurance surety bonds, account payee demand draft, banker's cheque, or bank guarantee (including e-BG) from any of the commercial banks or payment online in an acceptable form. Therefore, we request to accept the EMD in the form of Insurance Surety Bond also.	No Change, as per RFP
494	Section 1: Performance Bank Guarantee	The PBG shall: ☑ Be denominated in Indian Rupees. ☑ Be in the form of an unconditional Bank Guarantee. ☑ Be issued by any Nationalized Bank / Public Sector Bank / Private Sector Bank / Commercial Bank / Co-operative Bank / Rural Bank operating in India having a branch at Ahmedabad or Gandhinagar.	As per the latest amendment in GFR 2017 dated 02-02-2022 (Rule 171 of GFR 2017), Performance Security may be obtained in the form of insurance surety bonds, account payee demand draft, banker's cheque, or bank guarantee. Therefore, we request you accept the Insurance Surety Bonds / Bank Guarantee towards Performance Security.	No Change, as per RFP
495	Section 3: Delivery Milestone	Submission of Performance Bank Guarantee (PBG) and conduct of Project Kick-off Meeting - T + 15 calendar days	Submission of Performance Bank Guarantee (PBG) and conduct of Project Kick-off Meeting - T + 30 calendar days	No Change, as per RFP
496		Installation, and Commissioning of SD WAN solution at Hub / Central Locations - T2 = T1 + 60 calendar days	Installation, and Commissioning of SD WAN solution at Hub / Central Locations - T2 = T1 + 60 calendar days	No Change, as per RFP

497		Installation, Commissioning, and FAT of SD-WAN Edge Devices at Individual Office Locations - T4 = T1 + 90 calendar days	Installation, Commissioning, and FAT of SD-WAN Edge Devices at Individual Office Locations - T4 = T1 + 120 calendar days	No Change, as per RFP
498		Installation, and Commissioning of SD WAN solution at District Locations, Taluka and PoP Locations - T5 = T1 + 100 calendar days	Installation, and Commissioning of SD WAN solution at District Locations, Taluka and PoP Locations - T5 = T1 + 240 calendar days	No Change, as per RFP
499	Section 4: SLA-wise Penalty Mapping (Overlay SLAs Only)	Total SLA penalties (availability + incident penalties) are capped at the overall maximum per quarter (e.g., 25% of QCV)	As a standard RFP clause, Total SLA penalties (availability + incident penalties) are capped at the overall maximum per quarter, i.e. 10% of QCV.	No Change, as per RFP
500	5.9. Penalty and Termination	Quarterly SLA Penalty Cap - 25% of quarterly contract value	As a standard RFP clause, Quarterly SLA Penalty Cap should be 10% of quarterly contract value.	No Change, as per RFP
501	Section 4 : Payment Schedule	M1 : Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad - 30% of total Contract Value	To reduce finance cost, we request you to revise payment term as mentioned below. M1 : Delivery of all components (Hardware, Software, Licenses, etc. at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad - 60% of total Contract Value	Pls. refer corrigendum
502		M2 : Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations - 20% of total Contract Value	M2 : Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations - 15% of total Contract Value	No Change, as per RFP
503		M3 : Installation, Commissioning, and FAT of SD-WAN Edge Devices at Office Locations (site-wise) - 20% of total Contract Value (Pro-rata based on sites completed)	M3 : Installation, Commissioning, and FAT of SD-WAN Edge Devices at Office Locations (site-wise) - 10% of total Contract Value (Pro-rata based on sites completed)	No Change, as per RFP
504		M4 : Final Acceptance Testing (FAT) of the SD-WAN solution for District, Taluka and PoP Locations. - 20% of total Contract Value	M4 : Final Acceptance Testing (FAT) of the SD-WAN solution for District, Taluka and PoP Locations. - 5% of total Contract Value	No Change, as per RFP
505		M5 : Deployment of SD-WAN SI Manpower and provision of stabilization, knowledge transfer, operational support, and handover services for one (1) year from Go-Live - 10% of the Total Contract Value, payable in four (4) equal quarterly instalments (2.5% each), subject to successful deployment of the required manpower, satisfactory service delivery, submission of quarterly reports, and compliance with the applicable SLA.	M5 : Deployment of SD-WAN SI Manpower and provision of stabilization, knowledge transfer, operational support, and handover services for one (1) year from Go-Live - 10% of the Total Contract Value, payable in four (4) equal quarterly instalments (2.5% each), subject to successful deployment of the required manpower, satisfactory service delivery, submission of quarterly reports, and compliance with the applicable SLA.	No Change, as per RFP
506	3.4 Functional Requirement	Kindly provide the detailed network topology and connectivity details, including the site-wise connectivity architecture, number of locations/sites, bandwidth requirement, primary and secondary links, fiber/OFC connectivity, WAN/LAN connectivity, connectivity between sites and the Central/NOC/Cloud/DC/DR infrastructure, and the required network devices/interfaces.	Justification: The above details are essential for accurately understanding the network architecture, sizing the required bandwidth and network equipment, and preparing the technical and commercial proposal. It will also help bidders ensure appropriate redundancy, scalability and end-to-end connectivity as per the project requirements.	Will be provided to L1 bidder.
507	3.4 Functional Requirement	Kindly provide the detailed SD-WAN Hub/Aggregation topology and connectivity details, including the number and location of SD-WAN Hubs, aggregation architecture, bandwidth at each Hub, number and type of WAN links, primary/secondary connectivity, Internet/MPLS connectivity, required SD-WAN devices, HA requirements, and connectivity towards the Central NOC/DC/Cloud/DR infrastructure	Justification: These details are required to accurately size the SD-WAN Hub devices, bandwidth, licenses, interfaces and redundancy, and to prepare the technical and commercial proposal based on the actual network architecture.	Will be provided to L1 bidder.
508	3.4 Functional Requirement	13. The SD-WAN solution must be implemented in such a way that incoming and outgoing traffic is automatically loadbalanced across network links at branches, even when the primary link is not fully utilized. Traffic should be distributed across network links even when the links are not congested.	Please clarify the requirement for "incoming traffic load balancing." As inbound traffic is controlled by ISP/upstream routing	No Change, as per RFP
509	3.4 Functional Requirement	28. The Successful Bidder will be responsible for integrating Log Analysis and Reporting solutions with the existing solution of GSWAN/GSDC (NMS/SIEM/SOAR).	Kindly share the existing details of NMS/SIEM/SOAR along with make,model and version	Will be provided to L1 bidder.

510	3.3 Key Responsibilities of the Bidder	The Bidder shall provide all hardware, software, firmware, licenses, subscriptions, accessories, transceivers, passive components, cables, connectors, racks, mounting accessories, tools, utilities, documentation, professional services, OEM services, manpower, security components, integration services, third-party interfaces, testing equipment, consumables, and any other item or service required for successful implementation and operation of the complete solution, irrespective of whether specifically mentioned in the RFP.	Kindly confirm whether the Bidder is required to provide racks only for the SD-WAN Hub, Regional Hub, and Controller infrastructure, or whether racks are also required at all branch locations. If new racks are required at the branch locations, kindly specify the required rack size and quantity per location.	Not required for branch locations
511	Payment Schedule	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad 30% of total Contract Value Payment under M1 shall be released only after successful inspection of the material.	Kindly increase the M1 payment from 30% to 60% upon successful delivery and inspection of all materials. Justification: This will support timely procurement and ensure smooth project execution by improving the bidder's cash flow.	No Change, as per RFP
512	SECTION 2-Eligibility Criteria:	Additional Clause	In line with the Government of India's flagship "Make in India" initiative and the Public Procurement (Preference to Make in India) Order, 2017, issued by the Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce & Industry, under Rule 153(iii) of the General Financial Rules (GFR), 2017, as amended from time to time, it is requested that preference/eligibility be extended to products offered by Class-I Local Suppliers with a minimum local content of 60%. This will promote indigenous manufacturing, domestic value addition and participation of Indian OEMs in the project.	No Change, as per RFP
513	SECTION 2-Eligibility Criteria:	4.The OEM & bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2025.	request to allow relaxation of positive Net worth or Profit making criteria for eligible MSMEs registered under MSMED Act, 2006. Proposed Clause: "For MSME bidders/OEMs registered under the MSMED Act, 2006, the requirement of positive Net Worth or for the last three financial years shall stand relaxed in accordance with Clause 10 of the Public Procurement Policy for MSEs, 2012 and Ministry of Finance OM dated 28.01.2014, subject to submission of valid MSME certificate and proof of technical competence." Justification: 1. Clause restricts participation of technically capable MSMEs, contrary to Government of India's MSME procurement policy. 2. As per Public Procurement Policy for MSEs, 2012 (Clause 10), Ministries/Departments must relax turnover, experience, and financial criteria for eligible MSMEs. 3. Ministry of Finance OM dated 28.01.2014 permits relaxation of financial norms including EBITDA, turnover, solvency, past performance for MSMEs. 4. Tender conditions should not be restrictive or discriminatory against MSMEs as per government procurement guidelines. 5. Lavelle Networks is a registered MSME with proven technical capabilities and successful SD-WAN deployments.	No Change, as per RFP

514	SECTION 2-Eligibility Criteria:	5.The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	Request to allow relaxation or average annual related turnover criteria for eligible MSMEs registered under MSMED Act, 2006. Proposed Clause: "For MSME bidders/OEMs registered under the MSMED Act, 2006, the requirement of average annual related turnover of not less than Rs 500 Crores in last three financial years shall stand relaxed in accordance with Clause 10 of the Public Procurement Policy for MSEs, 2012 and Ministry of Finance OM dated 28.01.2014, subject to submission of valid MSME certificate and proof of technical competence." Justification: 1. Clause restricts participation of technically capable MSMEs, contrary to Government of India's MSME procurement policy. 2. As per Public Procurement Policy for MSEs, 2012 (Clause 10), Ministries/Departments must relax turnover, experience, and financial criteria for eligible MSMEs. 3. Ministry of Finance OM dated 28.01.2014 permits relaxation of financial norms including EBITDA, turnover, solvency, past performance for MSMEs. 4. Tender conditions should not be restrictive or discriminatory against MSMEs as per government procurement guidelines. 5. Lavells Networks is a registered MSME with proven	No Change, as per RFP
515	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT – Point 23	Bidirectional Forwarding Detection (BFD) features should be supported	Request for Change :Bidirectional Forwarding Detection (BFD) or equivalent path monitoring and rapid failure detection mechanisms should be supported. Justification : To ensure technology neutrality and wider OEM participation, it is recommended that the requirement permit BFD or an equivalent path monitoring mechanism. The objective of the requirement is rapid detection of WAN/path failures and timely traffic failover, rather than the use of a specific protocol. Different SD-WAN solutions may achieve the same or better operational outcome using alternative mechanisms. The proposed change will avoid vendor/protocol-specific dependency while ensuring that the required resiliency and failover capability is maintained.	No Change, as per RFP
516	Section – 5 SPECIFICATIONS 5.1. SD-WAN – FUNCTIONAL – REQUIREMENT – Point 54	54.The proposed solution shall be Common Criteria (CC) certified against the relevant Network Device Protection Profiles (NDPP). The Common Criteria certification shall be issued either by an internationally recognized Common Criteria Certification Scheme or by the Indian Common Criteria Certification Scheme (IC3S), established by the Ministry of Electronics and Information Technology (MeitY). Valid Common Criteria certification details shall be submitted along with the technical bid.	Request for Change: Kindly remove the mandatory requirement for Common Criteria (CC) against NDPP / IC3S certification and accept applicable MTCTE (TEC/DoT) certification as the mandatory regulatory compliance requirement for the proposed SD-WAN solution. Since the RFP already recognizes applicable MTCTE (TEC/DoT) certification under the Eligibility Criteria, kindly extend the same compliance approach to this clause . Justification: 1. Common Criteria NDPP certifications are foreign/private commercial certification frameworks and are not mandated under any Government of India Act, 2.MTCTE is a statutory certification framework notified by TEC/DoT under the Indian telecom regulatory regime and already validates core security, interoperability, and performance requirements for SD-WAN / NGFW equipment. 3. As per Rule 149 of GFR 2017 and CVC procurement guidelines, tender specifications should remain generic, non-restrictive, and should not unnecessarily limit fair competition through proprietary or non-mandatory certification conditions. Request: In view of the above, we respectfully request that: 1. Common Criteria (CC), NDPP / IC3S certification be removed 2. MTCTE (TEC/DoT) be retained as the sole mandatory	No Change, as per RFP

517	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION -- Routing Protocols	The proposed SD-WAN solution shall support Static Routing, OSPFv2/v3, BGP (including MP-BGP and Route Reflector functionality where applicable), and Bidirectional Forwarding Detection (BFD) for fast convergence. Support for IS-IS shall be optional for interoperability with service provider networks. Legacy protocols such as RIP/RIPv2 are not required. The SD-WAN edge devices shall support Static Routing, OSPF, BGP, and BFD for branch connectivity and fast failover.	Request for Change: The proposed SD-WAN solution shall support Static Routing, OSPFv2/v3 and BGP. BFD or an equivalent path-monitoring and fast-failover mechanism shall be supported for rapid convergence and traffic failover. Justification:MP-BGP, Route Reflector and IS-IS are architecture-dependent and are not universally required for SD-WAN branch connectivity. Mandating these capabilities may unnecessarily restrict technically compliant solutions. Hence, the requirement may be limited to Static Routing, OSPFv2/v3 and BGP, with BFD or an equivalent fast-failover mechanism accepted.	No Change, as per RFP
518	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN HUB CPE Specification) -- Point 5	5.The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports. The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable.	Request for Clarification / Changes: Kindly clarify the design basis for the specified 12x1/10GE SFP+ and 2x40GE QSFP+ port requirements, including the expected number of WAN/LAN connections, aggregate bandwidth/throughput, current port utilization and projected scalability requirements. This will enable bidders to propose an appropriately sized Hub CPE aligned with the actual deployment requirements. Justification: The port density should be aligned with the actual connectivity, traffic and scalability requirements of the Hub. A clearly defined interface requirement will help avoid unnecessary over-provisioning while ensuring adequate capacity for the intended deployment. Allowing equivalent interface configurations, including OEM-supported breakout options and compatible industry-standard optics, will provide greater solution flexibility, reduce unnecessary vendor dependency and improve price competitiveness, while the prime OEM remains responsible for interoperability, performance, warranty and end-to-end support.	No Change, as per RFP
519	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices (District HQ) CPE Specification Point 12	12.The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.	Request for Clarification: Kindly provide the design basis for specifying 10 Gbps SD-WAN traffic throughput and 10 Gbps IPsec VPN encryption throughput from Day 1, including existing WAN bandwidth, current utilization, proposed bandwidth, projected traffic growth, and expected encrypted/security-inspected traffic. This will enable bidders to propose appropriately sized and scalable appliances based on the actual traffic requirement.	Pls. refer corrigendum
520	Section – 5 SPECIFICATIONS 5.2. SD-WAN SPECIFICATION (SD-WAN SD-WAN Edge Devices (Taluka HQ) CPE Specification Point 22	22.The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.	Change Request / Clarification: Kindly consider revising the minimum SD-WAN Traffic Throughput and IPsec VPN Encryption Throughput from 900 Mbps to 500 Mbps, subject to the proposed CPE meeting all required SD-WAN, security and performance requirements. Further, kindly provide the existing and projected/future WAN bandwidth requirements for Taluka HQ locations, including the expected bandwidth growth, so that the CPE throughput requirement can be appropriately sized against the actual deployment needs. Justification: The throughput requirement should be aligned with the actual and projected WAN bandwidth of the locations. A 500 Mbps requirement will provide adequate headroom for the intended deployment while avoiding unnecessary over-sizing of the CPE.	Pls. refer corrigendum

521	5.2. SD-WAN SPECIFICATION: SD-WAN General Specification: Central Orchestrator / Controller Specifications -- Point 3	3.The solution shall support deployment in High Availability (HA) mode without any single point of failure using Active-Active and Active-Standby architecture as supported by OEM with minimum two independent controller nodes with N+N redundancy, deployed across DC and DR, with automatic failover and no single point of failure	Clarification Requested: Kindly clarify whether the requirement mandates: a) Local N+N HA of the SD-WAN Orchestrator/Controllers at both DC and DR, in addition to geographical HA/failover between DC and DR; or b) Geographical HA between DC and DR with redundancy across the two locations.	Pls. refer corrigendum
522	SECTION 1 KEY INFORMATION	Key Features Required in the SD-WAN Solution 12. The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.	Please clarify whether there are any internet links at the remote locations which require local break-out to internet to understand the SWG use case	Local breakout is required. Internet will be provided by GOG.
523	SECTION 3 Scope of Work	3.4 Functional Requirement 28. The Successful Bidder will be responsible for integrating Log Analysis and Reporting solutions with the existing solution of GSWAN/GSDC (NMS/SIEM/SOAR).	Request to share the make, model & version of NMS, SIEM, SOAR to check the integration capability of the proposed SDWAN solution	Will be provided to L1 bidder.
524	SECTION 3 Scope of Work	3.4 Functional Requirement 39. The Successful Bidder must appoint and depute a dedicated resource for device deployment and support services, who will act as a Single Point of Contact (SPOC) for the entire project.	While the subsequent section of RFP asks for resource deployment for 1 year, this clause mentions dedicated SPOC for entire project. Please clarify whether the resource required is for 1 year or for full contract period.	1 Year only post project go-live
525	SECTION 3 Scope of Work	3.4 Functional Requirement 42. The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.	Request to provide the size of the batch to be trained on the SDWAN solution.	10-20 People.
526	SECTION 3 Scope of Work	3.4 Functional Requirement 45. All SD-WAN device, software, routing, security, security signature updates, orchestration, analytics, subscription services and management licenses shall be perpetual or subscription (with 10 years license to be supplied from day 1) in nature from the Go-Live of the project. No feature reduction, throttling, or license expiry shall occur after completion of the mentioned period.	Please clarify whether the SDWAN subscription license is required for 10Years	Pls. refer corrigendum
527	SECTION 3 Scope of Work	3.4 Functional Requirement 50. The solution shall support standard IPsec-based interoperability for underlay connectivity and shall not restrict migration or coexistence with future WAN technologies.	Does this refer to static site-to-site IPsec tunnels from SDWAN CPEs to existing traditional CPEs? If yes, request to remove this clause as centralized operations will be nullified with this approach. Instead traffic between SDWAN site to non-SDWAN site can be routed through DC / DR	No Change, as per RFP
528	SECTION 3 Scope of Work	3.4 Functional Requirement 52. The proposed solution shall support centralized logging and shall store all logs in compliance with the policies and guidelines issued by Department of Telecommunications, Telecom Regulatory Authority of India, and Indian Computer Emergency Response Team for the specified retention period as mandated from time to time.	Requesting clarification on the scope of storage supply & retention period	As per CERT-IN/DoT/TRAI compliance and any other GOI guidelines. The storage calculation to be done by the bidder and supplied along with solution.
529	SECTION 3 Scope of Work	3.4 Functional Requirement 53. The solution shall comply with all applicable CERT-In, DoT, and TRAI guidelines, including, but not limited to, log retention and secure maintenance of records. The successful bidder shall implement all necessary measures to ensure compliance as part of the solution including all network device configuration files shall be securely backed up within India, version-controlled, encrypted, and retained for a minimum of 2 years, ensuring availability for audit, recovery, and compliance verification. Bidder has to provide the necessary logs whenever asked by GIL / competent authority. Bidder should deploy any tool / solution for ip address management / syslog to ensure necessary compliance and retention for 2 years as asked above.	Since this deployment is captive, requesting to clarify whether bidder can provide remote NOC services to collect & storage the logs for 2years as per this clause. If no, requesting GIL to provision storage within DC/DR for log storage for the duration of 2 years.	Pls. refer corrigendum
530	SECTION 3 Scope of Work	1. The bidder shall deploy the required SD-WAN manpower only for a period of one (1) year post Go-Live.	While the SLA spreads across overall contract period, resource requirement is mentioned only for 1 year. Please clarify on the support model for the remaining contract period.	The existing O&M agency will handle the devices for the remaining period.

531	SECTION 4 Service Level Agreement, Penalties & Payment Terms	1. State Data Centre (SDC) / Hub Availability/SD-WAN Controller/Central Infrastructure: ≥ 99.99%	Since the deployment is done at GIL premises, requesting to change the availability as 99.95%	No Change, as per RFP
532	SECTION 4 Service Level Agreement, Penalties & Payment Terms	2. District Availability: ≥ 99.99%	Since the deployment is done at GIL premises, requesting to change the availability as 99.5%	No Change, as per RFP
533	SECTION 4 Service Level Agreement, Penalties & Payment Terms	3. Taluka / PoP / Customer_Edge Site Availability: ≥ 99.50%	Since the deployment is done at GIL premises, requesting to change the availability as 99.0%	No Change, as per RFP
534	A. SLA Measurement – System of Record	1. All SLA parameters including availability, downtime, incident occurrence, incident resolution time, SLA compliance, and penalty calculation shall be measured, recorded, and reported exclusively through the following authorized systems: o GSWAN Helpdesk System, and/or o GSWAN Network Monitoring System (NMS), and/or o Authorized SD-WAN Monitoring / Orchestration System integrated with GSWAN NMS.	While onsite resource is requested only for 1 year, please clarify on the support model & SLA visibility for subsequent years of the contract period. Also clarify whether bidder NOC will have access to GSWAN system for logging, tracking, updates & closure of the incident tickets.	The bidder has to log complaint in NOC / helpdesk / anyother tool provided by GOG.
535	B. Incident Management & Measurement	1. All incidents shall be logged, tracked, and closed through the GSWAN Helpdesk System.	While onsite resource is requested only for 1 year, please clarify on the support model & SLA visibility for subsequent years of the contract period. Also clarify whether bidder NOC will have access to GSWAN helpdesk system for logging, tracking, updates & closure of the incident tickets.	The existing O&M agency will handle the devices for the remaining period.
536	5.10. SD-WAN Overlay Accountability	The Bidder shall be responsible for meeting the defined SLAs for the SD-WAN overlay solution only, including SD-WAN CPE, centralized controllers, orchestration, policy enforcement, monitoring, and integration with the existing GSWAN underlay network. The Bidder shall coordinate with the underlay connectivity service provider for fault isolation and resolution; however, SLA accountability for underlay connectivity shall remain outside the scope of this RFP.	Please clarify on the coordination with underlay connectivity service provider as this part of the network is owned by GIL. Further with no resources or visibility into the network, please clarify on how the access to GSWAN SDWAN overlay will be extended to bidder's operations team.	Will be provided to L1 bidder.
537		General Query	Please confirm whether the bid is L1 submission or Reverse Auction	L1 submission
538	Payment Terms	M1 - Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad 30% of total contract value M2 - Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations 20% of total contract value M3 - Installation, Commissioning, and FAT of SD-WAN Edge Devices at Office Locations (site-wise) 20% of total contract value M4 - Final Acceptance Testing (FAT) of the SD-WAN solution for District, Taluka and PoP Locations 20% of total contract value M5 - Deployment of SD-WAN SI Manpower and provision of stabilization, knowledge transfer, operational support, and handover services for one (1) year from Go-Live 10% of the Total Contract Value, payable in four (4) equal quarterly installments (2.5% each)	Please amend the payment terms as mentioned below. M1 - Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad 60% of total contract value M2 - Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations 10% of total contract value M3 - Installation, Commissioning, and FAT of SD-WAN Edge Devices at Office Locations (site-wise) 10% of total contract value M4 - Final Acceptance Testing (FAT) of the SD-WAN solution for District, Taluka and PoP Locations 10% of total contract value M5 - Deployment of SD-WAN SI Manpower and provision of stabilization, knowledge transfer, operational support, and handover services for one (1) year from Go-Live 10% of the Total Contract Value, payable in four (4) equal	No Change, as per RFP
539	Eligibility Criteria	9. Bidder and OEM should not be blacklisted/debarred by any state government / central government / PSU in last three years as on last date of bid submission.	Please amend the clause as mentioned below. 9. Bidder and OEM should not be blacklisted/debarred by any state government / central government / PSU as on last date of bid submission.	No Change, as per RFP

540		General Query	Please share Gujarat Informatics Limited below mentioned details for internal documentation for the opportunity GST No. PAN No. Registered Address:	Will be provided to L1 bidder.
541	Payment Terms / Delivery	Milestone payment linked to successful delivery and inspection of materials	Kindly clarify whether the delivery milestone shall be considered on a location-wise basis or only after delivery of the complete quantity across all designated locations.	Already mentioned in RFP.
542	Payment Terms / Delivery	Inspection of delivered materials	Kindly clarify the timeline within which the Purchaser shall complete inspection and acceptance of the delivered materials after receipt at the designated location.	No Change, as per RFP
543	Delivery	Delivery of equipment	Kindly clarify whether site readiness (rack space, power availability and access permissions) shall be ensured by the Purchaser prior to scheduling deliveries at respective locations.	All the locations are currently active and GSWAN is operational through P2P links and traditional routers.
544	Delivery	Delivery timeline	Kindly clarify whether the delivery timeline shall be extended in cases where delays are attributable to site readiness, access restrictions or dependencies beyond the bidder's control.	Yes.
545	Delivery	Delivery milestone	Kindly confirm whether partial deliveries against the Purchase Order, if accepted by the Purchaser, shall be eligible for corresponding milestone payments.	No Change, as per RFP
546	Payment Terms	Future expansion	Kindly clarify the payment mechanism for additional sites/hardware/licenses added during the contract period. Will the same commercial terms and milestone structure apply?	Yes, the understanding is correct.
547	Payment Terms	Acceptance Certificate	Kindly confirm whether the respective milestone payment shall be released upon issuance of the Acceptance Certificate by GIL/authorized agency.	Already mentioned in RFP.
548	Delivery	Project implementation	Kindly clarify whether phased deliveries aligned with the implementation schedule shall be acceptable instead of a single consolidated delivery.	No Change, as per RFP
549	Delivery	Site readiness	Kindly confirm that all implementation sites will be made ready (rack space, power, network connectivity and access permissions) by GIL/User Department prior to scheduling deliveries.	Yes, the understanding is correct.
550	Delivery	Material Acceptance	Kindly clarify the timeline within which GIL/User Department shall complete inspection and acceptance of delivered materials after delivery at the designated location.	Already mentioned in RFP.
551	Delivery	Delivery Documentation	Kindly confirm the list of documents required for successful delivery acceptance (Delivery Challan, OEM Serial Numbers, Packing List, Warranty Certificate, etc.).	Will be provided to L1 bidder.
552	Delivery	Delivery Completion	Kindly clarify whether partial deliveries, if accepted by GIL, shall be considered as completed delivery for the corresponding locations and eligible for milestone completion.	No Change, as per RFP
553	Delivery	Project Rollout	Kindly confirm whether GIL will provide a location-wise delivery and implementation schedule after award of contract to facilitate procurement and logistics planning.	Yes. However the logistics has to be done by the bidder after inspection as mentioned in the RFP

554		The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY 2022-23, 2023-24, 2024-25.	We request GIL to kindly consider revising the clause as follows: "The OEM should have an average annual turnover of not less than Rs. 200 Crores during the last three financial years FY 2022-23, FY 2023-24 and FY 2024-25." In this regard, we request GIL to kindly consider the following aspects: Turnover threshold: The stipulated OEM turnover requirement of Rs. 500 Crores appears relatively high in comparison with the estimated value of the project. We request GIL to kindly review the threshold and consider a more proportionate financial criterion in accordance with applicable Government of India procurement guidelines. Role of the bidder: Since the project implementation, deployment, operations and service delivery are primarily to be undertaken by the selected bidder, we request GIL to kindly review whether such a high turnover criterion specifically for the OEM is necessary for establishing the overall capability to execute the project successfully. Encouraging wider participation: The proposed criterion, particularly when linked specifically to the turnover of the proposed product, may limit participation by technically capable OEMs, including established Indian OEMs. A product-neutral and proportionate turnover criterion would facilitate wider participation, encourage healthy	No Change, as per RFP
555		The OEM shall comply with the Government of India guidelines regarding restrictions on procurement from bidders/OEMs of countries sharing land borders with India, as applicable and amended from time to time. Necessary declarations and supporting documents, if required, shall be submitted in accordance with the applicable Government of India orders	Kindly confirm the specific declaration and supporting documentation required from the bidder and OEM at the time of bid submission for compliance with the applicable Government of India procurement guidelines concerning restrictions on procurement from bidders/OEMs of countries sharing land borders with India.	Pls. refer annexure B&C
556		Bidder should be IT/ITeS Company registered under Indian Companies Act 1956/2013.	Kindly consider permitting Telecom/ISP companies also to participate, subject to meeting all other eligibility, technical and financial requirements, considering the nature of the proposed SD-WAN deployment and managed WAN services.	Pls. refer corrigendum
557		Headless Resilience: Data traffic at branches must continue uninterrupted if controllers are unreachable. Headless data forwarding must persist for at least 5 days.	Request GIL to amend the period as "Headless data forwarding must persist for at least 24 hours".	Pls. refer corrigendum
558		Secure TPM chips for storing cryptographic keys; support encryption standards AES, DES, ESP, and Diffie-Hellman (DH) groups.	Request GIL to relax the TPM chip requirement for wider participation of industry OEMs and not restrict to select few.	No Change, as per RFP
559		Cryptographic modules must be certified under FIPS 140-2 Level 2 or higher.	We request to relax on the FIPS compliance for maximum participation, it is specific to one OEM	No Change, as per RFP
560		Common Criteria (CC) certified against Network Device Protection Profiles (NDPP) by internationally recognized scheme or Indian IC3S (MeitY).	We request the Common Criteria NDPP Cert to be relaxed for maximum participation	No Change, as per RFP
561		Proposed solution components or operating systems must be IPv6 Ready Logo and USGv6 certified.	We request IPv6 / USGv6 Certified requirement be removed for maximum participation	Pls. refer corrigendum
562		Orchestrator, Controller, Analytics, and Security must be supplied by the same SD-WAN OEM.	We request "security by the same OEM" to be relaxed. As per present ask, it favours only specific OEMs and limits the industry participation to select few vendors.	No Change, as per RFP
563		Support quantum-resistant cryptography standards and AI/ML-based predictive diagnostics and monitoring.	The RFP mandates quantum-resistant cryptography and AI/ML-based capabilities. Kindly specify the applicable standards/algorithms and minimum functional requirements against these provisions, including the acceptable NIST/PQC standards, so that compliance can be evaluated objectively and uniformly across OEMs."	Pls. refer corrigendum
564		Secure TPM Hardware chip	We request GIL to remove/relax the TPM requirement	No Change, as per RFP
565		Compliance with Gujarat State Data Centre (GSDC) security hardening and successful VAPT remediation.	GSDC Security VAPT – What is this? Should understand the process and whether this is required before bidding	Any security gaps identified during the VAPT should be closed. Also the same is required after becoming L1.
566		Certification related to NDPP and FIPS	To be removed.	No Change, as per RFP

567	SECTION 2 ELIGIBILITY CRITERIA	Managed WAN	Clarification : Managed WAN means SITC of WAN Devices to Customer.	No Change, as per RFP
568	Eligibility Criteria:	Payment terms : 30 % on Delivery	Payment terms : 50 % on Delivery	No Change, as per RFP
569	Timelines	120 Days for Core and 160 Days for Remote sites	180 Days for Core and 210 Days for Remote sites	No Change, as per RFP
570	Introduction / Bid Submission Guidelines, Clause (a) & (b)	Bid Processing Fee: ₹17,700/- (non-refundable). EMD: ₹2 Crore (refundable).	Whether the Bid Processing Fee of ₹17,700/- and EMD of ₹2 Crore shall be exempted/waived for eligible Government/PSU entities as per the Gujarat Government Procurement Policy, 2024, vide Resolution No. SPO-102021-188460-CH dated 14/03/2024, Section 4(A)(d) and 4(A)(g). Therefore, It is requested to exempt BSNL for the Tender Fee and EMD	We may allow as per as per GeM GTC and Gujarat State Procurement Policy 2024 for the EMD.
571	section 3	With reference to Clause No. 3.3 12 under section 3 of the tender, it is mentioned that 100 sites shall be implemented by OEM and rest of the sites shall be completed by the bidder.	Kindly clarify whether the implementation of the remaining sites can be jointly done by bidder and its partner.	Consortium / Subcontracting is not allowed.
572	section 2	As per our understanding of the clause at Sr. No. 9 under section 2, bidder and OEM both should meet the requirement separately, it is pertinent to mention that the facilities of either OEM or bidder should be sufficient to provide the customer support 24x7x365. Therefore, you are kindly requested to amend the clause as follows	The Bidder OR OEM should have a Customer Support Center which operates 24x7x365 and is capable of troubleshooting 24x7x365 days	Support center of OEM is required, however the bidder has to ensure the complaints are addressed within the SLA.
573			Ports, Memory, IPSec Tunnels, Throughput The combination of throughput, memory, tunnel capacity and exact interface density appears to prescribe a particular hardware architecture. We request that equivalent or superior solutions be evaluated on aggregate forwarding/security performance, concurrent tunnel capacity and required interface capacity, while permitting different physical interface combinations supported by the OEM.	No Change, as per RFP
574			Dual SIM slots We request that OEM-supported integrated or externally connected cellular WAN architectures be accepted, provided that dual-SIM/dual-carrier resiliency, 4G/5G connectivity, SD-WAN failover and the prescribed performance requirements are met.	Pls. refer corrigendum
575			Ports requirements Minimum aggregate interface capacity and required interface speeds/types may be specified, but equivalent combinations of native interfaces, breakout, aggregation or OEM-supported interface configurations must be allowed.	No Change, as per RFP
576			SASE Ready architecture The proposed SD-WAN architecture must support a phased transition toward a Secure Access Service Edge architecture without requiring replacement of the deployed branch infrastructure. The architecture should support integration between branch-based secure SD-WAN/NGFW capabilities and cloud-delivered security services for internet, SaaS, private applications and remote users. This enables the Government to progressively adopt SASE/SSE capabilities as its cloud and application landscape evolves. The architecture should support progressive integration with cloud-delivered SSE/SASE capabilities for users, branches, internet, SaaS and private applications, without requiring replacement of the underlying SD-WAN infrastructure.	No Change, as per RFP
577			Eligibility criteria: The OEM eligibility criteria may be demonstrated through established industry recognition in relevant analyst research. Accordingly, an OEM positioned in the latest applicable Gartner Magic Quadrant for SD-WAN, Security Service Edge (SSE), or Single-Vendor SASE, as relevant to the proposed architecture, shall be considered as meeting the intent of established technology capability, subject to fulfillment of the functional, performance, security, deployment and support requirements of the RFP.	No Change, as per RFP

578	2, Eligibility criteria (2)	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations.	The credential of parent company or group companies should be allowed if the parent is a telecom or IT company and the bidder is wholly owned subsidiary of parent	No Change, as per RFP
579	2, Eligibility criteria (6)	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	The credential of parent company or group companies should be allowed	Pls. refer corrigendum
580	3.2, Overlay Vs Underlay responsibility	The OEM shall be responsible for designing the complete overlay and underlay network architecture required for the proposed SD-WAN solution across all locations. The design shall include selection and sizing of appropriate transport technologies such as P2P links, L2/L3 MPLS, ILL, Broadband, and wireless connectivity options including 3G/4G/LTE/5G, ensuring optimal performance, redundancy, high availability, and scalability for the SD-WAN overlay. c) The OEM shall provide detailed underlay design recommendations including bandwidth sizing, link redundancy model, routing architecture, failover mechanisms, QoS considerations, and integration with the SD-WAN overlay policies.	The bidder shall be responsible for designing the complete overlay and underlay network architecture required for the proposed SD-WAN solution across all locations. The design shall include selection and sizing of appropriate transport technologies such as P2P links, L2/L3 MPLS, ILL, Broadband, and wireless connectivity options including 3G/4G/LTE/5G, ensuring optimal performance, redundancy, high availability, and scalability for the SD-WAN overlay. c) The OEM shall validate the design while bidder provides underlay design recommendations including bandwidth sizing, link redundancy model, routing architecture, failover mechanisms, QoS considerations, and integration with the SD-WAN overlay policies.	No Change, as per RFP
581	3.4, Functional requirement (12)	The SD-WAN OEM shall provide professional services for the design, validation, and initial implementation of the SD-WAN solution. The OEM shall be responsible for designing, validating, and implementing the SD-WAN Controller and SD-WAN Hub at the State Headquarters (SHQ). Further, as part of OEM professional services, the OEM shall directly design and implement a minimum 100 sites to establish the reference architecture, validate performance, and ensure correct deployment standards.	The SD-WAN OEM shall provide professional services for the design, validation, and initial implementation of the SD-WAN solution. The OEM shall be responsible for designing and validating the configuration of SD-WAN Controller and SD-WAN Hub at the State Headquarters (SHQ). Further, as part of OEM professional services, the OEM shall directly design and validate configuration of minimum 100 sites to establish the reference architecture, validate performance, and ensure correct deployment standards.	No Change, as per RFP
582	3.10, Delivery Milestone	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad	T + 90 days	Pls. refer corrigendum
583	8, Contract cancellation & termination clause (8)	Partial termination	The Tenderer may terminate specific sites / locations / components without affecting the entire contract.	No Change, as per RFP
584	Additional clause	Limitation of liability	Successful bidder's cumulative liability for its obligations under the contract shall not exceed the value of the charges payable by the DST/GIL within the remaining duration of the contract term from the day claim is raised and selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.	No Change, as per RFP
585	5.14, Payment schedule		Payment shall be made within 30 days from the date of receipt of the valid invoice, submitted upon completion and acceptance of the applicable milestone.	No Change, as per RFP
586	Section – 5.1 Functional Requirement – Failover SLA	RFP specifies failover time between 300–800 ms	Confirm if measurement is at overlay tunnel level only or also at application session level without TCP/UDP reset	Already mentioned in RFP.
587	Section – 5.1 Functional Requirement – Traffic Steering	Traffic steering based on latency, jitter, packet loss, SLA	Clarify if user identity-based steering (AD/LDAP) is mandatory from Day 1 or optional	The clause of the RFP mentioned is for traffic steering based on latency, jitter, packet loss and SLA and does not mention User Identity based steering.

588	Section – 5.2 Security Features – IPS/Firewall/Malware	IPS, malware detection, botnet prevention, SWG features	Should these be natively integrated into SD-WAN appliance or via OEM-supported modules	Pls. refer corrigendum
589	Section – 5.2 Certification Requirement – FIPS/IPv6 Logo	MTCTE, FIPS 140-2, Common Criteria, IPv6 logo	Confirm if all certifications must be available at bid submission or OEM undertaking is acceptable	Certifications must be available before the material delivery.
590	Section – 5.2 Controller Deployment – Orchestrator Specs	Orchestrator on-premises with N+N redundancy	Is Active-Active deployment across DC & DR mandatory, or will Active-Standby suffice	Pls. refer corrigendum
591	Section 3.4 Software Upgrades – Partial Upgrade	Partial upgrades at specific sites	Clarify if downgrade rollback is also required as part of configuration rollback	Yes, the understanding is correct.
592	Section 3.9 Integration – GSWAN NMS/SIEM	Integration with NMS/SIEM/SOAR	Confirm if API-level integration is mandatory or syslog/SNMPv3 export suffices	Need to confirm with GSDC.
593	High Availability – Edge Devices	Edge devices Active-Active / Active-Passive	Clarify if dual-hub redundancy at SDC is mandatory for all sites or only central hubs	Only for central site.
594	Section – 5.2 Training & Certification – OEM-led	OEM-led training for DST/GIL officers	Confirm if certification exams are mandatory or OEM-issued participation certificates are acceptable	OEM Certification exams are mandatory.
595	Section 7 Proof of Concept – POC Requirements	POC requires ZTP, failover, QoS, RBAC	Clarify if remote demonstration is acceptable or must be conducted physically at GIL premises	Remote demonstration is acceptable.
596	Section 7 Proof of Concept – POC Requirements	demonstration of features like Zero Touch Provisioning	RFP document mentions demonstration of features like Zero Touch Provisioning, application-aware routing, and security features. Is there a predefined test environment or specific network topology that the OEM must adhere to during the POC?	GSWAN topology will be discussed and similar use case must be deployed for POC.
597	Section 3.4 The proposed SD WAN solution component should be IPv6 ready logo or USGv6 certified. Must support IPv4 and IPv6 protocols from day 1.	On the requirement for IPv6 readiness,	The RFP states the solution should be IPv6 ready from Day-1 with USGv6 certification. Is there a preferred or certified vendor for IPv6 support, or is compliance with IPv6 standards sufficient?	Already mentioned in RFP.
598	Section 3.4 Concerning the scalability of the SD-WAN infrastructure	Infrastructure Requirement	The document mentions a minimum support for 7,800 devices from Day-1 with 30% scalability. Could you please specify if the existing Data Centre infrastructure (for hosting the orchestrator and controllers) is already equipped to support this scale, or will additional infrastructure provisioning be required?	Premises will be provided by GSWAN / GSDC
599	Section 3.9 Interoperability	Regarding the integration with existing GSWAN underlay network,	are there any specific protocols or configurations (e.g., BGP, OSPF, MPLS) that the SD-WAN overlay must support or be compatible with?	Already mentioned in RFP.
600	Section 5.1 SD-WAN – FUNCTIONAL – REQUIREMENT	IPv4 and IPv6 dual-stack support	The RFP document specifies the need for IPv4 and IPv6 dual-stack support, along with FIPS 140-2 certification. Is there a preference for certain OEMs or certifications beyond the stated standards?	Already mentioned in RFP.
601	Section 3.10 Penalty Clause – Delayed Site/Location	RFP states: "A penalty of 0.15% per week or part thereof per delayed site/location shall be levied for delays beyond the specified timeline, subject to an overall maximum of 20% of the TCV."	Request amendment to cap maximum penalty at 10% of the product value instead of 20% of the Total Contract Value (TCV), to align with industry practice and ensure fairness.	No Change, as per RFP
602	Section 3.10 Delivery Timeline	RFP provides only indicative quantity (6234 Nos.) without product-wise breakup	Kindly quantify the exact quantity of each product and propose phased delivery schedule for practical execution	Notional quantity mentioned in the RFP, however the bidder may provide additional material to complete the functional scope of work. Also it will be bottom up approach for execution and implementation with central site to be deployed in parallel.
603	Section 3.10 Penalty Clause	Maximum penalty capping mentioned as 20%	Request amendment to cap maximum penalty at 10% to align with industry norms and OEM feasibility	No Change, as per RFP

604	Section 3.4	Clause 45 : All SD-WAN device, software, routing, security, security signature updates, orchestration, analytics, subscription services and management licenses shall be perpetual or subscription (with 10 years license to be supplied from day 1) in nature from the Go-Live of the project. No feature reduction, throttling, or license expiry shall occur after completion of the mentioned period.	We request to align the license duration with the contract period of 5 years (as per Section 6 Price Bid validity and 5-year warranty), with provision to extend licenses for subsequent years if contract is extended.	Pls. refer corrigendum
605	Section 5.1	Clause 25: The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	We request clarification that sub-second failover (300-800 ms) applies to overlay BFD / tunnel link failure detection when secondary link is in active-active hot standby state. Please clarify whether 300–800 ms is a target range or maximum threshold, and whether measurement is at tunnel, application or end-user level for FAT.	This is maximum permissible limit
606	Section 3.4	Clause 11: In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period. The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.	We request to add: 'Provided the high resource utilization (>85% sustained for 24 hrs) is due to specified RFP traffic scope and not due to un-contracted feature additions or bandwidth expansion beyond 30% baseline.'	No Change, as per RFP
607	Sec. 3.4(2)	SD-WAN Orchestrator and Controllers shall be deployed on premise within Government Data Centre / designated location. Public cloud-only orchestration shall not be acceptable.	Please clarify whether a solution using an on-premises controller/orchestrator with optional cloud-based security intelligence, licensing portal or telemetry services is acceptable, provided all management/control functions required by the RFP remain on-premises.	The complete solution should be On premise only.
608	Sec. 3.4(3)	The SD-WAN Central Orchestrator shall be deployed in High Availability mode across Primary Data Centre and Disaster Recovery Data Centre with automated database replication, policy synchronization and controller failover. There shall be no single point of failure in the management infrastructure.	Please clarify whether active-standby or N+1 controller architecture is acceptable in addition to active-active, provided there is no single point of failure and automatic failover is demonstrated. Please define maximum acceptable RPO/RTO for controller database and policy synchronization.	Pls. refer corrigendum
609	Sec. 5.1 Functional 6	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	Please clarify whether FIPS 140-2/140-3 certification is required for the exact quoted appliance model or whether validated cryptographic modules within the product are acceptable.	Pls. refer corrigendum
610	Sec. 5.1 Functional 19	The solution must support Certificate management. Solution to support all versions SSL/TLS Inspection for inspection of invalid, expired, untrusted certificates.	Please clarify whether SSL/TLS inspection is required on all branch appliances or only on security-enabled models at hub/district sites.	On all the SDWAN appliances.
611	Sec. 5.1 Functional 22	The solution should support extension of L2 network across sites over the SD-WAN fabric. It should also support MP-BGP EVPN with VXLAN.	Please clarify whether MP-BGP EVPN/VXLAN must be supported natively on the SD-WAN edge itself or may be provided through an integrated/adjacent OEM switching platform.	Pls. refer corrigendum
612	Key Features Required in the SD-WAN Solution	Integrated IPS, anti-malware, botnet, application control, URL filtering, DoS protection. The SD-WAN solution deployed at hub and branch locations shall support integrated security capabilities such as Intrusion Prevention System (IPS), anti-malware protection, botnet detection and prevention, application control, and malicious URL/web filtering, DoS protection available from the initial deployment	Please clarify whether all security functions must run concurrently at the stated throughput, and whether separate integrated OEM security appliances are acceptable where SD-WAN remains centrally orchestrated.	The bidder may quote same or different device.
613	Sec. 3.5 / 3.6 (General)	Security features must be native or tightly integrated without additional third-party products.	Please clarify whether additional licenses from the same OEM for security/analytics/SWG are acceptable or whether all functions must be included in the base SD-WAN license.	No change, as per RFP

614	Sec. 3.4 / requirement 51	The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.	Please clarify the required standard/algorithm (e.g., NIST post-quantum cryptography) and whether roadmap support or current production support is required on Day-1.	Pls. refer corrigendum
615	Sec. 3.4 / requirements 52, 53	52. The proposed solution shall support centralized logging and shall store all logs in compliance with the policies and guidelines issued by Department of Telecommunications, Telecom Regulatory Authority of India, and Indian Computer Emergency Response Team for the specified retention period as mandated from time to time. 53. The solution shall comply with all applicable CERT-In, DoT, and TRAI guidelines, including, but not limited to, log retention and secure maintenance of records. The successful bidder shall implement all necessary measures to ensure compliance as part of the solution including all network device configuration files shall be securely backed up within India, version-controlled, encrypted, and retained for a minimum of 2 years, ensuring availability for audit, recovery, and compliance verification. Bidder has to provide the necessary logs whenever asked by GIL / competent authority. Bidder should deploy any tool / solution for ip address management / syslog to ensure necessary compliance and retention for 2 years as asked above.	Please clarify whether the 2-year retention applies to all raw device logs, security logs, audit logs and configuration backups, and whether GSWAN/GSDC existing SIEM/syslog storage can be used.	Pls. refer corrigendum
616	Sec. 3.4 / 60	The Bidder shall configure and demonstrate automated and/or manual failover and fallback mechanisms between DC and DR locations. In the event of failure of the Primary (DC) site, traffic shall be seamlessly redirected to the DR site with minimal disruption. The solution shall support automated failover within 30 seconds and manual failover within 5 minutes.	Please clarify whether the 30-second automatic failover is for management/control-plane availability only or must also include traffic redirection and application recovery.	Complete failover with traffic diversion and system up and running from DR Site.
617	Hub CPE Specification (2)	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	Please define the exact traffic/security test profile and packet size used to establish 20 Gbps throughput during FAT.	Will be provided to L1 bidder.
618	Hub CPE Specification (8)	Should support minimum 10000 overlay IPsec tunnels from day 1.	Please clarify whether 10,000 means configured tunnels, simultaneously established tunnels, or supported maximum, and whether the number is measured per appliance or HA pair.	Pls. refer corrigendum
619	Central Orchestrator / Controller Specifications (16)	The solution shall support REST API for integration with NMS, SIEM, SOAR, ITSM and third-party applications.	We understand that required licenses of NMS is already in place to monitor SD WAN devices, please clarify.	No Change, as per RFP
620	Section 3.10 (2)	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad	Please clarify whether all 6,000 devices must be delivered by T+45 or phased delivery is allowed	Pls. refer corrigendum
621	Section 3.8 (A)-(1)	The bidder shall deploy the required SD-WAN manpower only for a period of one (1) year post Go-Live.	Please clarify whether manpower support is required only for one year post Go-Live or if resources must continue to be deployed for the entire 5-year O&M contract period. If limited to one year, kindly confirm how operations and SLA compliance will be managed thereafter.	Manpower required for 1 year period. Existing O&M agency will take over after 1 year period.