Corrigendum-3				
SUPPLY, INSTALLATION, TESTING, CONFIGURATION AND MAINTENANCE OF SOFTWARE-DEFINED WIDE AREA NETWORK (SD-WAN) CONNECTIONS ACROSS VARIOUS OFFICES OF BYPL NIT: CMC/BY/24-25/RS/SkS/APT/44				
S. No.	**NIT Pdf Page No.**	**NIT Clause No.**	**NIT Clause Descriptions**	**BYPL Response**
1	73	1	Solution must be implemented as true software defined network architecture with a complete separation of Control, management, orchestration and Data plane and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic	Solution must be implemented as software defined network architecture On premises with a Physical/Logical separation of Control/Data Plane, management/orchestration and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic
2	73	2	System shall be implemented as true software-defined network architecture with a complete separation of Control and Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.	System shall be implemented as software-defined network architecture on premises with a physical/logical of Control/Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic
3	**73**	**3**	The solution shall comprise of following components: The solution must allow management of networks as software-defined network (SDN). The proposed solution should have separate Centralized Network Orchestrator /Management/Controller along with compatible head end and Branch devices. **Centralized Management-** Shall be a separate component that provides single point of entry for Configuration and Monitoring. Shall be securely accessed and capable of configuration policies, monitoring and troubleshooting of multiple WAN Edge devices in the branches, data-centres or remote locations. This management engine shall be available in either physical/virtual form factor and should provide high availability. **Controller/HeadEnd** - Control plane must be secured using DTLS/TLS/IPSec encryption and shall be a separate/in-built component that abstracts all the routing information from the edge devices and distributes route prefixes, encryption key/Certificate to all Edges. The controller/HeadEnd shall maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instructs data plane to change traffic flow as per the defined policy. Controller/head-end shall be available in either physical/virtual form factor and should provide Active-Active instances across DC and DR. **Orchestrator/Authentication** Gateway shall be used to authenticate the on boarding edge devices using Certificates and serial number of the edge devices. Data Plane: Data plane is responsible to forward traffic in encrypted tunnels, apply local policy like QoS, ACL etc.	The solution shall comprise of following components: The solution must allow management of networks as software-defined network (SDN). The proposed solution should have separate Centralized Network Orchestrator /Management/Controller along with compatible head end and Branch devices. Centralized Management- Shall be a separate component that provides single point of entry for Configuration and Monitoring. Shall be securely accessed and capable of configuration policies, monitoring and troubleshooting of multiple WAN Edge devices in the branches, data-centers or remote locations. This management engine shall be available in either physical/virtual form factor and should provide high availability. Controller/HeadEnd - Control plane must be secured using DTLS/TLS/IPSec encryption and shall be a separate/in-built component that abstracts all the routing information from the edge devices and distributes route prefixes, encryption key/Certificate to all Edges. The controller/HeadEnd shall maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instructs data plane to change traffic flow as per the defined policy. Controller/head-end shall be available in either physical/virtual form factor and should provide Active-Active instances across DC and DR. Orchestrator/Authentication Gateway shall be used to authenticate the onboarding edge devices using Certificates and serial number of the edge devices. Data Plane: Data plane is responsible to forward traffic in encrypted tunnels, apply local policy like QoS, ACL etc.
4	74	13	All SD-WAN solution components including hardware and software for controller/centralized manager/orchestrator/hub and edge router shall be from the same OEM	The proposed SDWAN components (hardware and software) will be from the same OEM at the edge location however, the software for centralized manager/orchestrator requires VM instances which can be deployed on Third-Party hardware.

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	BYPL Response
5	74	21	Solution must be implemented as true software defined network architecture with a complete separation of Control, management, orchestration and Data plane and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic	Solution must be implemented as software defined network architecture On premises with a Physical/Logical separation of Control/Data Plane, management/orchestration and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic
6	74	5	The overlay paths established amongst the edge devices shall support transport of unicast & multicast	The overlay paths established amongst the edge devices shall support transport of unicast/multicast.
7	75	22	System shall be implemented as true software-defined network architecture with a complete separation of Control and Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.	System shall be implemented as software-defined network architecture on premises with a physical/logical of Control/Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic
8	**76**	**38**	The SD-WAN solution should be STQC certified/ BIS certified for IS 13252(PART 1):2010/ IEC 60950-1: 2005/ TEC Certified/MEF 3.0 / SOC2 / FCC Part 15B / Class A / CE / RCM / VCCI / UL/cUL / CB/ BSM and MTCT certified or similar certification which required for Indian standard Security .	The SD-WAN solution should be STQC certified/ BIS certified / IS 13252(PART 1):2010/ IEC 60950-1: 2005/ TEC Certified/MEF 3.0 / SOC2 / FCC Part 15B / Class A / CE / RCM / VCCI / UL/cUL / CB/**NDPP/NDcPP/**BSM and MTCT certified, similar certification which required for Indian standard Security
9	76	39	The solution shall have functionality to protect the edge devices from traffic flooding from Day1 without any additional hardware requirement	As per Tender. required DDoS features
10	76	41	The Device should support IP, FQDN, Device based /**MAC based**, and User/Group based policies	The Device should support IP, FQDN, Device based /MAC based, and User/Group based policie
11	**76**	**43**	The Proposed SDWAN CPE solution should support serial number/ UID based device authentication	The Proposed SDWAN CPE solution should support integration with central and Branches using serial number/ UID or Higher security mechanism based device authentication
12	77	63	SD WAN solution should be able to load balance across multiple links simultaneously and leverage all the available links to carry traffic in the flow & Packet based forwarding method	SD WAN solution should be able to load balance across multiple links simultaneously and leverage all the available links to carry traffic in the flow/ Packet based forwarding method.
13	**76**	**48**	SDWAN Solution should have capabilities to define VRF/Tenant and service information/VRF Tag are propagated network wide within an organization for application driven architecture with inherent security.	SDWAN Solution should have capabilities to define VRF/Tenant.
14	**76**	**51**	SDWAN should support SLA Dampening/Equivalent for a smoother transition and prevent disruptions and instabilities.	SDWAN should support SLA Dampening/Equivalent/ (latency and Jitter) for a smoother transition and prevent disruptions and instabilities.
15	**76**	**54**	SDWAN should support inline data measurements/Equivalent and inspected directly at the edge of the network for App-Route Detection and SLA Enforcement during app aware routing.	SDWAN should support inline data measurements/Equivalent or inspected directly at the edge of the network for App-Route Detection and SLA Enforcement during app aware routing.

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	BYPL Response
16	**76**	**55**	Link SLA management should have fall-back mechanism in place i.e. the traffic should flow to best path when all links cannot serve SLA to continue traffic flow. Solution should have the capability to define priority levels or ranks to links and route traffic based on them	Link SLA management should have fall-back mechanism in place i.e. the traffic or should flow to best path when all links cannot serve SLA to continue traffic flow.
17	**77**		Solution should have the capability to define priority levels or ranks to links and route traffic based on them	Solution should have the capability to define priority levels or ranks to links or route traffic based on them
18	77	66	The solution should be able to support LTE primary and LTE aggregation where wired WAN links may not be a feasible option	The proposed solution of LTE (4G/5G) should be utilized as active/active or (And) active/passive for data traffic
19	78	81	The centralized management solution shall have NMS capabilities and shall support network wide device and network visibility for all the devices in the terminated on the devices irrespective of the type of link (MPLS, broadband, FTTH, ILL, SIM etc.). The NMS /SDWAN Monitoring solution shall have capabilities including but not limited to TCP dump or equivalent ping and trace route. Device should be equipped with the features like Visualize in real-time, graphs and reports, WAN Link utilization, Detailed bandwidth usage of applications, Link wise WAN Link Latency, jitter and packet loss, SLA monitoring and compliance, Appliance utilization, Alert for high resource utilization. All types of alarms, Application performance monitoring. In case of performing any troubleshoot, the solution should have trouble tracking tools such as TCP dump or equivalent, ping, trace route etc.	The centralized management solution shall have NMS capabilities and shall support network wide device and network visibility for all the devices in the terminated on the devices irrespective of the type of link (MPLS, broadband, FTTH, ILL, SIM etc.). The NMS /SDWAN Monitoring solution shall have capabilities including but not limited to TCP dump or equivalent ping and trace route. Device should be equipped with the features like Visualize in real-time, graphs and reports, WAN Link utilization, Detailed bandwidth usage of applications, Link wise WAN Link Latency, jitter and packet loss, SLA monitoring and compliance, Appliance utilization, Alert for high resource utilization. All types of alarms, Application/Network performance monitoring. In case of performing any troubleshoot, the solution should have trouble tracking tools such as TCP dump or equivalent, ping, trace route etc.
20	79	83	The solution shall support email-based alarm to notify the administrators when any device/link fault,auth,data,encryption,threat,traffic, tunnel,url or network performance degradation happens. The recipient of the alerts should be deployed per site.	The solution shall support email-based alarm to notify the administrators when any device/link fault or network performance degradation happens. The recipient of the alerts should be Deployed/configurable per site.
21	79	87	The Centralized management solution shall provide a single, unified platform for network service provisioning, device configuration, software updates, monitoring and assurance, change and compliance management.	The Centralized management solution shall provide a single, unified platform for network service provisioning, device configuration, software updates, monitoring and assurance management.
22	80,92	8,8	Solution should have the features site-Site, DVPN and Remote VPN, (SSL, IPSec and Client VPN)	Solution should have the features site-Site, DVPN (Dynamic VPN) , (SSL, and IPSec)
23	**80**	(Category A), Point 9	Proposed device should have Ethernet 802.1Q VLAN capability	Proposed device should have Ethernet 802.1Q VLAN capability/Layer2 supportive or Equivalent
24	**80**	(Category A), Point 10	Proposed device should have Multicast, PIM, IGMPv3 capability	"Proposed device should have Multicast, PIM, IGMPv3 capability or Equivalent solution" which comly the Requirment
25	80,81,82, 92	22,4,22	**OT Protocol Support:** IEC 101-104, IEC 61850, Modbus, MQTT, MMS, Goose etc.	OT Protocol Support: IEC 104, IEC 61850, Modbus, MQTT, MMS, Goose etc.
26	81,82,92, 93	(Category B) \ Pt No. 4	OT Protocol Support and Visibility: IEC 101-104, IEC 61850, Modbus MQTT, MMS, Goose etc. Comply with IEC 62443, Cyber security for OT and Compliance to various standards for IT & OT security.	OT Protocol Support and visibility: IEC 104, IEC 61850, Modbus, MQTT, MMS, Goose etc. Comply with IEC 62443, Cyber security for OT and Compliance to various standards for IT & OT security.
27	86	**Functional Requirements for SDWAN Device** - 1	Solution must be implemented as true software defined network architecture with a complete separation of Control, management, orchestration and Data plane and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic	Solution must be implemented as software defined network architecture On premises with a Physical/Logical separation of Control/Data Plane, management/orchestration and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	BYPL Response
28	86	2	System shall be implemented as true software-defined network architecture with a complete separation of Control and Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.	System shall be implemented as software-defined network architecture on premises with a physical/logical of Control/Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.
29	87	13	All SD-WAN solution components including hardware and software for controller/centralized manager/orchestrator/hub and edge router shall be from the same OEM	The proposed SDWAN components (hardware and software) will be from the same OEM at the edge location however, the software for centralized manager/orchestrator requires VM instances which can be deployed on Third-Party hardware
30	87	21	Solution must be implemented as true software defined network architecture with a complete separation of Control, management, orchestration and Data plane and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic	Solution must be implemented as true software defined network architecture with a complete separation of Control/Data plane, management/orchestration and integrate the WAN and branch networks into a single, end-to-end framework that uses policies to manage traffic
31	87	**Functional Requirements for SDWAN Device** - 22	System shall be implemented as true software-defined network architecture with a complete separation of Control and Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.	System shall be implemented as software-defined network architecture with a complete separation of Control/Data plane. It shall integrate different types of connectivity (MPLS, ILL, FTTH, Broadband, LTE) into a single, end-to-end framework that uses policies to manage traffic.
32	90	81	The centralized management solution shall have NMS capabilities and shall support network wide device and network visibility for all the devices in the terminated on the devices irrespective of the type of link (MPLS, broadband, FTTH, ILL, SIM etc.). The NMS /SDWAN monitoring solution shall have capabilities including but not limited to TCP dump or equivalent ping and trace route. Device should be equipped with the features like Visualize in real-time, graphs and reports, WAN Link utilization, Detailed bandwidth usage of applications, Link wise WAN Link Latency, jitter and packet loss, SLA monitoring and compliance, Appliance utilization, Alert for high resource utilization. All types of alarms, Application performance monitoring. In case of performing any troubleshoot, the solution should have trouble tracking tools such as TCP dump or equivalent, ping, trace route etc.	The centralized management solution shall have NMS capabilities and shall support network wide device and network visibility for all the devices in the terminated on the devices irrespective of the type of link (MPLS, broadband, FTTH, ILL, SIM etc). The NMS /SDWAN monitoring solution shall have capabilities including but not limited to TCP dump or equivalent ping and trace route. Device should be equipped with the features like Visualize in real-time, graphs and reports, WAN Link utilization, Detailed bandwidth usage of applications, Link wise WAN Link Latency, jitter and packet loss, SLA monitoring and compliance, Appliance utilization, Alert for high resource utilization. All types of alarms, Application/Network performance monitoring. In case of performing any troubleshoot, the solution should have trouble tracking tools such as TCP dump or equivalent, ping, trace route etc.
33	81	18	Compliance to various Indian and International standards for OT security Power supply: DC 48-220V/10A VDC.	DC Supply as per Indian Standard
34	82	19	Compliance to various Indian and International standards for OT security Power supply: DC 48-220V/10A VDC.	DC Supply as per Indian Standard
35	56	BILL OF MATERIAL AND OFFICE CATEGORIZATION - 1	**BYPL OT SCADA DC Core Router (SRD) - Qty - 4** Divided ISP link based on Services, we are using 10 types of ISP Services (MPLS and P2P) In High Availability consider as a primary and secondary -	BYPL OT SCADA DC Core Router (SRD) - Qty - 6 (2 Pair for DC and one Pair for DR)
36	76 & 78	53 & 75	The SDWAN solution must be able to apply QoS policies for all traffic types including TCP, UDP traffic types other non-TCP traffic types is additional benefits	The SDWAN solution must be able to apply QoS policies for all traffic types including TCP, UDP traffic types / other non-TCP traffic types is additional benefits
37	79	93	Site wise Reports: All Sources, All Destinations, Site based Application usage analysis report, All sites, All Sites over time, Site availability over time, Total Availability etc.	Currently Number of OT Sites are 65 currently, in future it will enhance.
38	**80**	(Category A), Point 9	Proposed device should have Ethernet 802.1Q VLAN capability	Proposed device should have Ethernet 802.1Q VLAN capability or Equivalent

S. No.	NIT Pdf Page No.	NIT Clause No.	NIT Clause Descriptions	BYPL Response
39	81	12	Device shall have minimum **4 X 1G RJ-45 ports with flexibility to configure any port as L2 and L3, 1 X Mgmt., 1 X Console.** ***** Aggregated device **throughput requirement minimum 500 Mbps** from day one, **Threat Protection and SSL Inspection**. * All ports should be populated to be used from day-1 with required SFP's if required	Device shall have minimum **4 X 1G RJ-45 ports with flexibility to configure any port as L2 and L3, 1 X Mgmt., 1 X Console.** ***** Aggregated device **throughput requirement minimum 500 Mbps** from day one with Threat Protection and HTTPS/SSL Inspection for entire traffic. * All ports should be populated to be used from day-1 with required SFP's if required
40	18	81	Compliance to various Indian and International standards for OT security Power supply: DC 48-220V/10A VDC.	DC Supply as per Indian Standard
41	12	82	Device shall have **minimum 4 X 1G RJ-45 ports with flexibility to configure any port as L2 and L3, 1 X Mgmt., 1 X Console**. Device should have capability of 4G, 5G, LTE, NB-IOT * Aggregated **device throughput requirement minimum 500 Mbps** from day one with **Threat Protection and SSL Inspection** * All ports should be populated to be used from day-1 with required SFP's if required	Device shall have **minimum 4 X 1G RJ-45 ports with flexibility to configure any port as L2 and L3, 1 X Mgmt., 1 X Console**. Device should have capability of 4G, 5G, LTE, NB-IOT * Aggregated **device throughput requirement minimum 500 Mbps** from day one with **Threat Protection and HTTPS/SSL Inspection for entire traffic.** * All ports should be populated to be used from day-1 with required SFP's if required
42	19	82	Compliance to various Indian and International standards for OT security Power supply: 100-220 VAC 10A	DC Supply as per Indian Standard
43	9	83	**Power supply**: 48-220V/10A VDC	DC Supply as per Indian Standard