# SUPPLEMENTAL/BID BULLETIN

| | |
|---|---|
| Name of Contract | Supply, Delivery, Installation, Testing and Configuration of Network Connectivity. |
| Addendum No. | Goods 0034-2021 |
| *This addendum is issued to modify or amend certain provisions in the bid documents. This shall form an integral part of the bid documents.* | |
| **PARTICULARS** | **Section VII. TECHNICAL SPECIFICATIONS** |
| **Note: This will be the final technical specifications** | |

| Item No. | Hardware Component | Specification | Statement of Compliance |
|---|---|---|---|
| 1. | Core Switch | • 24 x 10G SFP+, 6x 40G/100G QSFP28 fixed ports<br>• Dimensions of 43.6mm x 442.0mm x 420.0mm in H x W x D<br>• 1U Chassis Height<br>• Rated voltage range of 100V AC to 240V AC, 50/60 Hz<br>• Maximum voltage input of 90V AC to 290V AC, 45 Hz to 65 Hz<br>• Maximum input current of 8A at 600W AC<br>• Maximum power consumption of 254W<br>• Operating temperature of -5*C to +45*C at 0m – 1800m altitude<br>• Storage temperature of -40*C to +70*C<br>• Less than 65 dB(A) sound pressure at normal temperature<br>• Power Supply Surge protection of +/- 6kV in differential and / or common mode<br>• 1+1 power redundancy<br>• 4 Fan Modules<br>• Heat dissipation with fan<br>• Intelligent fan speed adjustment<br>• Up to 384K MAC address entries<br>• IEEE802.1d standards compliance<br>• MAC address learning and aging<br>• Static, dynamic and blackhole MAC address entries<br>• Packet filtering based on source MAC address<br>• 4K VLANs<br>• Guest VLANs and voice VLANs<br>• GVRP<br>• MUX VLAN<br>• VLAN assignment based on MAC addresses, protocols, IP subnets, policies and ports<br>• VLAN mapping<br>• Static ARP<br>• Dynamic ARP<br>• Static routing<br>• RIP v1, RIP v2, RIPng<br>• OSPF, OSPFv3<br>• IS-IS, IS-ISv6<br>• BGP, BGP4+<br>• ECMP<br>• Routing Policy<br>• Up to 256K FIBv4 entries<br>• Up to 80K FIBv6 entries | |

| | | | |
|---|---|---|---|
| | | • VLAN-Based Spanning Tree (VBST), working with PVST, PVST+ and RPVST<br>• Link-type Negotiation Protocol (LNP) similar to DTP<br>• VLAN Central Management Protocol (VCMP) similar to VTP<br>• Wireless Services:<br>o AP access control, AP domain management, and AP configuration template management<br>o Radio management, unified static configuration, and dynamic centralized management<br>o WLAN basic service, QoS, security and user management<br>o CAPWAP, tag/terminal location, and spectrum analysis<br>• RRPP ring topology and RRPP multi-instance<br>• Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover<br>• SEP<br>• ERPS<br>• BFD for OSPF, BFD for IS-IS for VRRP, and BFD for PIM<br>• STP, RSTP and MSTP<br>• BPDU protection, root protection and loop protection<br>• MPLS L3VPN<br>• MPLS L2VPN<br>• MPLS-TE<br>• MPLS QoS<br>• IPv6 Neighbor Discovery<br>• PMTU<br>• IPv6 Ping, IPv6 Tracert, IPv6 Telnet<br>• ACLS based on source IPv6 addresses, destination IPv6 Addresses, Layer 4 ports, or protocol types<br>• Multicast Listener Discover snooping (MLD v1/v2)<br>• IPV6 addresses configured for sub-interfaces<br>• VRRP6<br>• DHCPv6<br>• L3VPN<br>• IGMP v1/v2/v3 snooping and IGMP fast leave<br>• Multicast forwarding in a VLAN and multicast replication between VLANs<br>• Multicast load balancing among member ports of a trunk<br>• Controllable multicast<br>• Post-based multicast traffic statistics<br>• IGMP v1/v2/v3<br>• PIM-SM, PIM-DM and PIM-SSM<br>• MSDP<br>• Multicast VPN<br>• Rate limiting in the inbound and outbound directions of a port<br>• Packet redirection<br>• Port-based traffic policing and two-rate three-color CAR<br>• Eight queues on each port<br>• DRR, SP and DRR+SP queue scheduling algorithm<br>• WRED<br>• Re-marking of the 802.1p and DSCP field of packets | |

| | | | |
|---|---|---|---|
| | | • Packet filtering at Layer 2 to Layer 4<br>• Filtering out invalid frames based on the source MAC address, destination MAC address, Source IP address, destination IP address, TCP/UDP source, TCP/UDP destination, port number, protocol type and VLAN ID<br>• Queue-based rate limiting and shaping on ports<br>• Hierarchical user management and password protection<br>• DoS attack defense, ARP attack defense and ICMP attack defense<br>• Binding the IP address, MAC address, port number and VLAN ID<br>• Port Isolation, port security and sticky MAC<br>• MAC Forced Forwarding<br>• Blackhole MAC address entries<br>• Limit on the number of learned MAC addresses<br>• IEEE802.1X authentication and limit on the number of users on a port<br>• AAA authentication, RADIUS authentication and HWTACACS authentication<br>• NAC<br>• SSH V2.0<br>• HTTPS<br>• CPU protection<br>• Blacklist and whitelist<br>• Attack source and punishment for IPV6 packets such as ND, DHCPv6 and MLD packets<br>• IPsec for management packet encryption<br>• ECA<br>• Deception<br>• MACSec<br>• LACP<br>• E-Trunk<br>• Ethernet OAM<br>• ITU-Y.1731<br>• DLDP<br>• LLDP<br>• VXLAN L2 and L3 gateways<br>• Centralized and distributed gateway<br>• BGP-EVPN<br>• Configured through the NETCONF protocol<br>• Acting as the parent node to vertically virtualize downlink switches and APs as one device for management<br>• Two-layer client architecture<br>• SVF<br>• ASs can be independently configured. Services not supported by templates can be configured on the parent node<br>• Third-party devices allowed between SVF parent and clients<br>• Marking service packets to obtain the packet loss ratio and number of lost packets in real time<br>• Measurement of the number of lost packets and packet loss ratio on networks and devices<br>• Cloud-based management<br>• Virtual cable test<br>• SNMP v1/v2c/v3<br>• RMON<br>• Web-based NMS<br>• System logs and alarms of different severities | |

| | | | |
|---|---|---|---|
| | | • GVRP<br>• MUX VLAN<br>• Netstream<br>• Telemetry<br>• x8 Electrical Transceiver, SFP, GE, Electrical Interface Module (100m, RJ45)<br>• x22 Optical Transceiver, SFP+, 10G, Multi-mode Module (850nm, 0.3km, LC)<br>• x2 Stacking Cables<br>• x8 Wireless Access Controller AP Resource Licenses<br><br>* Will serve as Main Distribution Frame of the network | |
| 2. | Access Switch | • 24 10/100/1000Base-T ports, 4 X 10GE SFP+ ports<br>• Dimensions of 43.6mm x 442mm x 420mm in H x W x D<br>• 1U in Chassis Height<br>• 600W AC pluggable power supply type<br>• 100V AC to 240V AC, 50/60 Hz rated voltage range<br>• 90V to 290V, 45Hz to 65Hz maximum voltage range<br>• Maximum power consumption of 114W<br>• 47.5dB(A) of sound pressure under normal temperature<br>• -5*C to +45*C operating temperature at 0m-1800m altitude<br>• -40*C to +70*C storage temperature<br>• +/- 6kV common mode and/ or differential mode surge protection<br>• Air cooling heat dissipation,<br>• Intelligent speed adjustment<br>• Pluggable fans<br>• IEEE802.1d standards compliance<br>• 64K MAC address entries<br>• MAC address learning and aging<br>• Static, dynamic and blackhole MAC address entries<br>• Packet filtering based on source MAC address<br>• 4094 VLANs<br>• Guest VLANs and voice VLANs<br>• GVRP<br>• MUX VLAN<br>• VLAN assignment based on MAC addresses, protocols, IP subnets, policies and ports<br>• VLAN mapping<br>• RRPP ring topology and RRPP multi-instance<br>• Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover<br>• SEP<br>• ERPS<br>• BFD for OSPF, BFD for IS-IS for VRRP, and BFD for PIM<br>• STP, RSTP and MSTP<br>• BPDU protection, root protection and loop protection<br>• Static routing<br>• RIP v1, RIP v2, RIPng<br>• OSPF, OSPFv3<br>• IS-IS, IS-ISv6<br>• BGP, BGP4+<br>• ECMP<br>• Routing Policy<br>• Up to 16K FIBv4 entries<br>• Up to 8K FIBv6 entries | |

| | | | |
|---|---|---|---|
| | | • VLAN-Based Spanning Tree (VBST), working with PVST, PVST+ and RPVST<br>• Link-type Negotiation Protocol (LNP) similar to DTP<br>• VLAN Central Management Protocol (VCMP) similar to VTP<br>• IPv6 Neighbor Discovery, up to 8K ND entries<br>• PMTU<br>• IPv6 Ping, IPv6 Tracert, IPv6 Telnet<br>• ACLS based on source IPv6 addresses, destination IPv6 Addresses, Layer 4 ports, or protocol types<br>• Multicast Listener Discover snooping (MLD v1/v2)<br>• IPV6 addresses configured for sub-interfaces<br>• VRRP6<br>• DHCPv6<br>• L3VPN<br>• IGMP v1/v2/v3 snooping and IGMP fast leave<br>• Multicast forwarding in a VLAN and multicast replication between VLANs<br>• Multicast load balancing among member ports of a trunk<br>• Controllable multicast<br>• Post-based multicast traffic statistics<br>• IGMP v1/v2/v3<br>• PIM-SM, PIM-DM and PIM-SSM<br>• MSDP<br>• Multicast VPN<br>• Rate limiting in the inbound and outbound directions of a port<br>• Packet redirection<br>• Port-based traffic policing and two-rate three-color CAR<br>• Eight queues on each port<br>• DRR, SP and DRR+SP queue scheduling algorithm<br>• WRED<br>• Re-marking of the 802.1p and DSCP field of packets<br>• Packet filtering at Layer 2 to Layer 4<br>• Filtering out invalid frames based on the source MAC address, destination MAC address, Source IP address, destination IP address, TCP/UDP source, TCP/UDP destination, port number, protocol type and VLAN ID<br>• Queue-based rate limiting and shaping on ports<br>• Hierarchical user management and password protection<br>• DoS attack defense, ARP attack defense and ICMP attack defense<br>• Binding the IP address, MAC address, port number and VLAN ID<br>• Port Isolation, port security and sticky MAC<br>• MAC Forced Forwarding<br>• Blackhole MAC address entries<br>• Limit on the number of learned MAC addresses<br>• IEEE802.1X authentication and limit on the number of users on a port<br>• AAA authentication, RADIUS authentication and HWTACACS authentication<br>• NAC<br>• SSH V2.0<br>• HTTPS<br>• CPU protection<br>• Blacklist and whitelist<br>• Attack source and punishment for IPV6 packets such as ND, DHCPv6 and MLD packets | |

| | | | |
|---|---|---|---|
| | | • IPsec<br>• ECA<br>• Deception<br>• LACP<br>• E-Trunk<br>• Ethernet OAM<br>• ITU-Y.1731<br>• DLDP<br>• LLDP<br>• VXLAN L2 and L3 gateways<br>• Centralized and distributed gateway<br>• BGP-EVPN<br>• Configured through the NETCONF protocol<br>• SVF<br>• Two-layer client architecture<br>• IGMP snooping can be enabled on the access switches and the maximum number of access users on a port can be configured<br>• ASs can be independently configured. Services not supported by templates can be configured on the parent node<br>• Third-party devices allowed between SVF parent and clients<br>• Working as an SVF client that is plug-and-play with zero configuration<br>• Directly coloring service packets to collect real-time statistics on the number of lost packets and packet loss ratio<br>• Collection of statistics on the number of lost packets and packet loss ratio at network and device levels<br>• Two-way IP link performance measurement<br>• Measurement on two-way packet delay, one-way packet loss rate and one-way packet jitter<br>• Supported stacking for up to 9 members<br>• SNMP v1/v2c/v3<br>• RMON<br>• Smart Application Control<br>• Web-based NMS<br>• Systems logs and alarms of different levels<br>• GVRP<br>• MUX VLAN<br>• NetStream<br>• Intelligent O&M<br><br>Accessories:<br>• x20 Optical Transceiver, SFP+, 10G, Multi-mode Module (850nm, 0.3km, LC)<br><br>*Will serve as Intermediate Distribution Frame | |
| 3. | Access Points | • 47mm x 200mm x 200mm in H x W x D<br>• 1.05 kg in Weight<br>• x1 10/100/1000M self-adaptive Ethernet interface (RJ45 x 2)<br>• 1 x USB interface<br>• BLE5.0 Bult-in Bluetooth<br>• LED indicated that indicated power-on, startup, running, alarm and fault states of the system<br>• In compliance with 802.3at<br>• -10*C to +50*C operating temperature<br>• -40*C to +70*C storage temperature<br>• IP41 dustproof and waterproof grade | |

| | | | |
|---|---|---|---|
| | | • -60m to +5000 m operating altitude<br>• 53kPa to 106kPa operating atmospheric pressure<br>• Built-in adaptive array antennas<br>• 3.5dBi antenna gain at 2.4 GHz<br>• 5dBi antenna gain at 5GHz<br>• Less than or equal to 16 maximum number of SSIDs for each radio<br>• Less than or equal to 512 maximum number of users<br>• 25dBm maximum transmit power at 2.4GHz<br>• 25dBm maximum transmit power at 5GHz<br>• Power increment of 1dBm<br>• Can analyze the spectrum of no Wi-Fi interference sources and identify them<br>• WIDS/WIPS<br>• Monitor, identify, defend, counter and perform refined management on the rogue devices<br>• Compliance with IEEE 802.11a/b/g/n/ac/ac Wave 2/a<br>• Maximum rate of up to 1.775Gbps<br>• Maximum ratio combining (MRC)<br>• Space time block code (STBC)<br>• Cyclic Delay Diversity (CDD)/Cyclic Shift Diversity (CSD)<br>• Beamforming<br>• MU-MIMO<br>• DL OFDMA 1024QAM<br>• Low-density parity-check (LDPC)<br>• Maximum-likelihood detection (MLD)<br>• Frame aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx)<br>• 802.11 dynamic frequency selection (DFS)<br>• Short guard interval (GI) in 20 MHz, 40 MHz, 80 MHz, and 160 MHz modes<br>• Priority mapping and packet scheduling based on a Wi-Fi Multimedia (WMM) profile to implement priority-based data processing and forwarding<br>• Automatic and manual rate adjustment<br>• WLAN channel management and channel rate adjustment<br>• Automatic channel scanning and interference avoidance<br>• Service set identifier (SSID) hiding<br>• Signal sustain technology (SST) Unscheduled automatic power save delivery (U-APSD)<br>• Hotspot2.0 802.11k and 802.11v smart roaming<br>• 802.11r fast roaming (≤ 50 ms)<br>• WAN authentication escape<br>• Compliance with IEEE 802.3ab<br>• Auto-negotiation of the rate and duplex mode and automatic switchover between the Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)<br>• Compliance with IEEE 802.1q<br>• SSID-based VLAN assignment<br>• VLAN trunk on uplink Ethernet ports<br>• Management channel of the AP uplink port in tagged and untagged mode<br>• DHCP client, obtaining IP addresses through DHCP<br>• Tunnel data forwarding and direct data forwarding | |

| | | | |
|---|---|---|---|
| | | • Application identification and QoS classification when AP local forwarding (also called direct forwarding), which can significantly improve voice quality for applications such as Skype, QQ, and WeChat<br>• STA isolation in the same VLAN<br>• Access control lists (ACLs)<br>• Link Layer Discovery Protocol (LLDP)<br>• Soft Generic Routing Encapsulation (GRE)<br>• IPv6 Source Address Validation Improvements (SAVI)<br>• Multicast Domain Name Service (mDNS) gateway protocol<br>• Priority mapping and packet scheduling based on a Wi-Fi Multimedia (WMM) profile to implement priority-based data processing and forwarding<br>• WMM parameter management for each radio WMM power saving<br>• Priority mapping for upstream packets and flow-based mapping for downstream packets<br>• Queue mapping and scheduling<br>• User-based bandwidth limiting<br>• Adaptive bandwidth management (automatic bandwidth adjustment based on the user quantity and radio environment) to improve user experience<br>• Airtime scheduling<br>• Open system authentication<br>• WEP authentication/encryption using a 64-bit, 128-bit, or 152-bit encryption key<br>• WPA/WPA2-PSK authentication and encryption (WPA/WPA2 personal edition)<br>• WPA3-SAE authentication and encryption (WPA3* personal edition)<br>• WPA/WPA2-802.1x authentication and encryption (WPA/WPA2 enterprise edition)<br>• WPA3-802.1x authentication and encryption (WPA3* enterprise edition)<br>• WPA-WPA2 hybrid authentication<br>• WPA2-WPA3* hybrid authentication<br>• WAPI* authentication and encryption<br>• Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and countermeasure, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist<br>• 802.1x authentication, MAC address authentication, and Portal authentication<br>• DHCP snooping<br>• Dynamic ARP Inspection (DAI)<br>• IP Source Guard (IPSG)<br>• 802.11w Protected Management Frames (PMFs)<br>• Application identification<br>• Telnet<br>• STelnet using SSH v2<br>• SFTP using SSH v2<br>• SNMP v1/v2/v3<br>• Network Time Protocol (NTP)<br><br>Accessories:<br>• x30 PoE Injector | |

| | | | |
|---|---|---|---|
| | | Will serve as wireless connection to users using laptops | |
| 4. | Next-Generation Firewall | • Firewall Throughput –55,000 Mbps<br>• Firewall IMIX – 26,900 Mbps<br>• IPS Throughput – 10,800 Mbps<br>• NGFW Throughput – 10,000 Mbps<br>• Threat Protection Throughput – 2,200 Mbps<br>• IPsec VPN Throughput – 5000 Mbps<br>• The solution must support **13.6M** concurrent sessions.<br>• The solution must support **146,000** new connections/sec.<br><br>**I. Base Firewall Features**<br>**1. General Management**<br>• The solution must support two-factor authentication (one-time-password) support for administrator access, user portal, IPsec and SSL VPN.<br><br>• The solution must have a backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly.<br>• The solution must be able to support API for 3rd party integration.<br><br>**2. Firewall, Networking & Routing**<br>• The solution must support stateful deep packet inspection firewall.<br>• The solution must have a Network Flow FastPath acceleration for trusted traffic.<br>• The solution must have the capability of WAN link balancing like multiple internet connections, auto-link health check, automatic failover and weighted balancing, and granular multipath rules<br><br>**3. SD-WAN**<br>• The solution must support multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, and failover.<br>• The solution must have a feature which leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between managed endpoints and Firewall.<br>• The solution must have unique RED Layer 2 tunnel with routing.<br><br>**4. Base Traffic Shaping & Quotas**<br>• The solution must support flexible network or user-based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription).<br>• The solution must have a DSCP marking.<br><br>**5. Secure Wireless**<br>• The solution must have a central monitoring and management of APs and wireless clients through the built-in wireless controller. | |

| | | | |
|---|---|---|---|
| | | • The solution must have bridge APs to LAN, VLAN, or a separate zone with client isolation options.<br>• The solution must support IEEE 802.1X (RADIUS authentication) with primary and secondary server support and also 802.11r (fast transition)<br>• The solution must have a wireless repeating and bridging meshed network mode with supported Aps.<br><br>**6. Authentication**<br>• The solution must have a server authentication agent for Active Directory SSO, STAS, and SATC.<br>• The solution must support the single sign-on with Active Directory, eDirectory and RADIUS Accounting<br>• The solution must have Radius Timeout with Two-Factor Authentication (2FA).<br>• The solution must support Browser SSO authentication via transparent, Proxy authentication (NTLM) and Kerberos.<br>• The solution must have Google Chromebook authentication support for environments with Active Directory and Google G Suite.<br><br>**7. Base VPN Options**<br>• The solution must be able to support site-to-site VPN like SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates and pre-shared key<br>• The solution must be able to support Remote Ethernet Device site-to-site VPN tunnel (robust and lightweight).<br>• The solution must be able to support IKEv2.<br><br>**8. IPSec VPN Client**<br>• The solution must be able to support authentication via pre-shared key (PSK), PKI (X.509), Token and XAUTH.<br>• The solution must have the ability to enable Synchronized Security and Security Heartbeat for remote connected users.<br>• The solution must have intelligent split-tunnelling for optimum traffic routing and NAT-traversal.<br><br>**b. Network Protection Subscription**<br>**1. Intrusion Prevention (IPS)**<br>• The solution must be able to support high-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection.<br>• The solution must be one of the top rated by NSS Labs.<br>• The solution must support custom IPS signatures.<br><br>**2. ATP**<br>• The solution must have advanced threat protection that detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall. | |

| | | | |
|---|---|---|---|
| | | • The solution must have a lateral movement protection that further isolates compromised systems by having healthy managed endpoints that reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain.<br><br>**3. SD-Remote Ethernet Device Management**<br>• The solution must have a central management of all SD-RED devices.<br>• The solution must the ability to compress tunnel traffic.<br><br>**4.Clientless VPN**<br>• The solution must support unique encrypted HTML5 self-service portal for RDP, HTTP, HTTPS, SSH, Telnet, and VNC.<br><br>**c. Web Protection Subscription**<br>**1. Web Protection and Control**<br>• The solution must be able to support full transparent proxy for anti-malware and web-filtering.<br>• The solution must have URL Filter database with millions of sites across 92 categories backed by OEMLabs.<br>• The solution must have advanced web malware protection with JavaScript emulation.<br>• The solution must have a second independent malware detection engine (Avira) for dual scanning.<br>• The solution must be capable of SafeSearch enforcement (DNS-based) for major search engines per policy (user/group).<br>**2. Cloud Application Visibility**<br>• The solution must have a control center widget that displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated.<br>• The solution must have the ability to drill down to obtain details on users, traffic, and data.<br>• The solution must be capable of filtering cloud application usage by category or volume.<br>**3. Application Protection and Control**<br>• The solution must have a Synchronized App Control that automatically identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall.<br>• The solution must have a signature-based application control with patterns for thousands of applications.<br>• The solution must have cloud application visibility and control to discover shadow IT.<br>**4. Web & App Traffic Shaping**<br>• The solution must have custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared | |

| | | | |
|---|---|---|---|
| | | **d. Email Protection Features**<br>**1. Email Protection and Control**<br>• The solution must have a reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology.<br>• The solution must have DKIM and BATV anti-spam protection.<br>• The solution must have spam grey listing and Sender Policy Framework (SPF) protection.<br>• The solution must Second independent malware detection engine (Avira) for dual scanning<br>• The solution must have a live protection real-time in-the-cloud lookups for the latest threat intelligence.<br>• The solution must be able to detect phishing URLs within e-mails.<br><br>**2. Email Quarantine Management**<br>• The solution must have a malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages.<br>**3. Email Encryption and DLP**<br>• The solution must have a patent-pending SPX encryption for one-way message encryption.<br>• The solution must have DLP engine with automatic scanning of emails and attachments for sensitive data.<br>• The solution must have a pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by OEMLabs.<br><br>**e. Web Server Protection Features**<br>**1. Web Application Firewall Protection**<br>• The solution must be capable of reverse proxy.<br>• The solution must be capable of URL hardening engine with deep-linking and directory traversal prevention.<br>• The solution must have dual-antivirus engines.<br>• The solution must be capable of HTTPS (TLS/SSL) encryption offloading.<br>• The solution must be able to support reverse authentication (offloading) for form-based and basic authentication for server access.<br>• The solution must be capable of skipping individual checks in a granular fashion as required.<br>• The solution must have an option to change Web Application Firewall performance parameters.<br>• The solution must be able support Wildcard for server paths and domains.<br>**f. On-box Reporting**<br>• The solution must have Current Activity Monitoring capability: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks. | |

| | | | |
|---|---|---|---|
| | | • The solution must have the ability of report scheduling to multiple recipients by report group with flexible frequency options.<br>• The solution must be capable of exporting reports as HTML, PDF, Excel (XLS).<br>**g. Central Firewall Reporting**<br>• The solution must have a pre-defined report with flexible customization options.<br>• The solution must have a report dashboard that provides an at-a-glance view of events over the past 24 hours.<br><br>*Will serve as control panel for the client | |
| 5 | Active Directory Server | • Form Factor: Rack Server<br>• Drive Bays: Up to 4 x 3.5" Hot-Plug drives.<br>• CPU: Intel Xeon E-2226G 3.4GHz, 12M cache, 6C/6T, 80W<br>• Memory: 2 x 16GB 2666MT/s UDIMM.<br>• Storage:<br>  ○ 2 x 960GB SSD SATA Mixed Used 6Gbps 512e Hot Plug<br>• RAID Controller:<br>  ○ 8-port 12Gbps Hardware RAID controller<br>  ○ Able to support RAID levels 0, 1, 5, 6, 10, & 50.<br>  ○ Can supports real-time RAID monitoring and hardware inventory<br>• I/O & Ports:<br>  ○ Dual Port 1Gb LOM<br>• Power Supply: Dual 350W Redundant Hot Plug Power Supplies.<br>• Supports Integration with third-party consoles.<br>• Supports Connection for third-party consoles.<br>• Supported Operating System:<br>  ○ Windows Server with Hyper-V<br>  ○ RHEL<br>  ○ SLES<br>  ○ Ubuntu Server<br>  ○ Citrix XenServer<br>  ○ VMware ESXi<br>• Able to support the following security features:<br>  ○ TPM 1.2/2.0 optional<br>  ○ Secure Boot<br>  ○ Silicon Root of Trust<br>  ○ Cryptographically signed firmware<br>  ○ System Lockdown<br>  ○ System Erase<br>• Must include server warranty of 3-years 24x7 Onsite support.<br><br>*Will serve as domain controller for client computers | |
| 6 | Application Server | • Form Factor: Rack Server<br>• Drive Bays: Up to 8 x 2.5" Hot-Plug drives.<br>• CPU: Intel Xeon Gold 6238 2.1GHz, 30.25M cache, 22C/44T, 140W<br>• Memory: 2 x 16GB 3200MT/s RDIMM Dual Rank.<br>• Storage:<br>  ○ x 480GB SSD SATA Mixed Used 6Gbps 512e Hot Plug<br>  ○ 4 x 1.92TB SSD SATA Mixed Used 6Gbps 512e Hot Plug<br>• RAID Controller: | |

| | | | |
|---|---|---|---|
| | | ○ 8-port 12Gbps Hardware RAID controller<br>○ Able to support RAID levels 0, 1, 5, 6, 10, & 50.<br>○ Can supports real-time RAID monitoring and hardware inventory<br>• I/O & Ports:<br>○ Dual Port 1Gb LOM<br>○ Quad Port 10GbE SFP+Power Supply: Dual 550W Redundant Hot Plug Power Supplies.<br>• Supports Integration with third-party consoles.<br>• Supports Connection for third-party consoles.<br>• Supported Operating System:<br>○ Windows Server with Hyper-V<br>○ RHEL<br>○ SLES<br>○ Ubuntu Server<br>○ Citrix XenServer<br>○ VMware ESXi<br>• Able to support the following security features:<br>○ TPM 1.2/2.0 optional<br>○ Secure Boot<br>○ Silicon Root of Trust<br>○ Cryptographically signed firmware<br>○ System Lockdown<br>○ System Erase<br>• Must include server warranty of 3-years 24x7 Onsite support.<br><br>*Will serve as a server to run specific applications needed by the Provincial Government of Cagayan | |
| 7 | 6 Core Fiber Optic Cable (1lot) | • Opti-Core Fiber Optic Distribution Cable shall be used.<br>• The Contractor shall supply and install multi-core fiber optic cables as the vertical/horizontal backbone cables as noted in this specification and in the drawings/SLD.<br>• The Contractor shall observe the bending radius and pulling strength requirements of all backbone cables during handling and installation.<br>• Each optical fiber shall be buffered with color-coded PVC for identification of multi-core fiber optics cable. The connector type shall be SC connector.<br>• The fiber optic cable shall meet the NEC requirements for OFNR or OFNP and comply with Bell core, FDDI, TIA/EIA-568-C.3, IEC and ICEA standards.<br>• All Multimode optical fiber cables shall be graded index with core/cladding construction of 50/125 m; the fiber shall be compliant to the performance specifications for OM3 Multimode fiber detailed in ISO11801.<br>• The fiber optic cable shall be protected by means of either a cable tray or a dedicated fiber routing system at all times. Each end of the fiber optic cable shall contain a slack storage box with approximately three (3) meters of cable slack.<br>• OM3 Maximum Cable Attenuation Performance<br>○ Transmission Wavelength: 850nm – 1300nm<br>○ Maximum Attenuation: 3.5 – 1.5<br><br>*Will serve as a fast connection from MDF to IDF | |

| | | | |
|---|---|---|---|
| 8 | Pigtail SC Type OM3 (SC Connector) | • TIA/EIA-604-3[SC]<br>• Ferrule type: Zirconia ceramic ferrule with a pre-polished fiber stub.<br>• Insertion Loss: 0.3dB average (multimode).<br>• Return Loss: >50dB (multimode)<br>• No special fiber termination tools required.<br>• Translucent inner housing assembly facilitates inspection of the fiber termination quality, results in rapid installations, improved termination yields, and lower installed costs.<br>• Mechanical cable retention consistently provides higher than industry standard cable retention; requires no adhesive, speeding installation.<br>• Allow up to ten (10) re-terminations.<br><br>*Will serve as link from fibre panel to Switches | |
| 9 | Fiber Optic Patch Cord Duplex OM3 | • Pass all TIA/EIA-568-C.3 performance requirements<br>• Insertion loss per connection: 0.10dB<br>• Return loss: 20dB min. (multimode); 26dB min. (10Gig multimode)<br>• 100% factory terminated and tested for insertion loss<br>• Meets UL1666 (OFNR) flame ratings<br>• Lifetime traceability of test data to a Q.C. number on each patch cord<br>• Duplex Patch Cords include Duplex Clips to maintain polarity<br>• "The Contractor shall supply and install multi-core fiber optic cables with patch panel 1U as the vertical/horizontal backbone cables as noted in this specification and in the drawings/SLD."<br>• The type of fiber optic patch cords to be used shall be selected to suit the type of fiber optic connector that is installed in the corresponding fiber termination tray.<br><br>&Will serve as link from Switch to Switch | |
| 10 | Horizontal Cabling | **1. Category 6 UTP Cable**<br>• The Contractor shall supply and install horizontal cables to connect each TO to the FD termination hardware for the respective floor.<br>• The type of horizontal cables used for each work location shall be 4 pair Category 6 unshielded twisted pair UTP construction.<br>• The Cat6 UTP cable shall be constructed of 24 AWG copper conductors with HDPE insulation.<br>• The copper conductors shall be twisted into pairs, separated by a cross-divider; crosstalk cancellation spiral in the form of a cross that maintains constant distance between all the 4 pairs. This will ensure that even under torsion during installation, the crosstalk should be constant over the whole cable.<br>• The copper conductors shall be covered in a flame retard PVC jacket.<br>• The Cat6 UTP cable shall be Underwriter's Laboratories (UL) listed type CM.<br>• The Cat6 UTP cable must exceed TIA/EIA-568 C.2 Category 6 requirements. It must be tested to Class E to ensure performance for any application up to and including 1000Mbps.<br>• The Cat6 UTP cable must meet requirement specified for current applications such as IEEE 802.3, 10/100/1000 BASE T; | |

| | | | |
|---|---|---|---|
| | | IEEE 802.5, 4/16/100Mbps; ATM Forum 52/155/622/1200 Mbps, 1 Gigabit Networking.<br>• The horizontal cables shall be run using a star topology format from the TR on each floor to every individual TO. All cable routes must follow the routes and directions described on the drawings/SLD.<br>• The length of each individual run of horizontal cable from the TR to the TO shall not exceed 90m.<br>• The Contractor shall observe the bending radius and pulling strength requirements of the horizontal cable during handling and installation.<br>• Each run of cable between the TR and the TO shall be continuous without any joints or splices, except where consolidation points are required. Installation practice shall comply to manufacturer best practices.<br>• The cable manufacturer shall be ISO 9001 and 14001 registered.<br><br>**2. Equipment Patch Cords**<br>• All Category 6 patch cords shall be factory terminated and supported by the system manufacturer with modular plugs featuring EASY CONTROL BY TURNING BOOT to support easy moves, adds and changes.<br>• The type of cable used for station cords shall be 4 pair Category 6 unshielded twisted pair UTP of a stranded construction. Each patch cord shall be QC, 100% performance tested at the factory in a channel test to the proposed TIA/EIA-568-C.2 Category 6 standard.<br>• All patch cord shall contain a molded strain relief for the cable termination.<br>• All patch cord shall consist of round, 32 AWG tinned copper, stranded conductors insulated with solid polyolefin, tightly twisted into individual pairs and jacketed with flame retardant PVC. The patch cord shall come in standard lengths of one meter for Switch to Patch Panel and 3 meters for TO to Desktop, IP Phone and AP.<br>• All patch cord shall be UL rated 1863 and meets IEC 60603-7.<br>• All patch cord shall be dual rated to meet CM and LSZH flame ratings.<br>• All patch cord shall meet ANSI/TIA-968-A and FCC Part 68 Subpart F; contacts plated with 50 micro-inches of gold.<br>• The length of each station patch cord in Work Area shall be 3 meters.<br>• All patch cord shall have Labels on it to provide identification of performance level, length, and quality control number.<br>• All patch cord shall compatible with optional RJ45 plug lock-in device to prevent unauthorized removal of cable, IP phone, other networking equipment, or critical connection.<br><br>**3. Copper Patch Panel**<br>• The patch panel shall be modular with snap-in modular jack, and allow front access.<br>• • Modular patch panels shall consist of a metal panel with molded snap-in faceplates which can be front releasable. | |

| | | | |
|---|---|---|---|
| | | • The modular patch panel shall support the appropriate Category 6 cabling and shall facilitate cross-connection and inter-connection using RJ45 8 position 8 conductors modular plug patch cords.<br>• Patch panels shall accept all Mini-Com modules for UTP, STP, fiber, or A/V applications and shall mount to standard 19" racks<br>• The modular patch panel shall be able to accommodate 24 AWG cable conductors.<br>• The modular patch panel shall be Underwriter's Laboratories (UL▪) listed.<br>• The modular patch panel shall be of 1RU 24-port for 19" rack mounting.<br>• High density 1RU 48-port or 2RU 72-port configuration might be used if rack space is limited.<br>• Separate modular patch panel shall be used for the termination of voice and data.<br><br>**4. Horizontal Cable Manager**<br>• Horizontal cable manager must be used with patch panel.<br>• The horizontal cable manager shall be capable of managing cables on the front, of any 19" Data rack.<br>• The horizontal cable manager shall consist of a 1-piece construction that is molded out of plastic.<br>• The horizontal cable manager shall have pass through holes that incorporate integral bend radius control as well as finger with rounded edges.<br>• The horizontal cable manager shall have rigid end fingers that incorporate integral bend radius control.<br>• The horizontal cable manager shall be available in 1RU, front only. | |
| 11 | Scope of Work – Cabling | • Supply and Delivery of Materials and Components<br>• Underground/burial works for the fiber backbone which includes excavation, trenching, backfilling, and other necessary works.<br>• Fiber cable pulling and layout on the designated areas.<br>• Installation of data cabinets in designated areas.<br>• Installation of fiber patch panel and termination.<br>• Installation of roughing-ins with proper hangers and supports.<br>• UTP cable pulling and layout on the designated areas.<br>• Installation of patch panels, cable managers, faceplates and patch cords.<br>• End to end testing, tagging and harnessing of all installed cables.<br>• Restoration of affected areas.<br>• Testing, commissioning and documentation.<br>• Turn-over and Acceptance." | |
| 12 | Implementation Services of Switches and Access Points | • Configuration of Basic and Advanced Settings<br>• Configuration of VLAN & Other Protocols<br>• Testing & Verification of Configuration & Connectivity<br>• Knowledge Transfer | |
| 13 | Support – One (1) Year | Unlimited 8x5 Helpdesk Support (no onsite)<br>• Phone Support<br>• Email Support<br>• Remote Support | |

All works shall be directly supervised by the Information Systems unit.

**A. Manpower Requirement**

The bidder shall include in his quotation a statement of manpower requirement for the project for evaluation.

**B. Deliverables**

| No. | Particulars | Unit | Qty |
|---|---|---|---|
| 1 | Access Points | unit | 30 |
| 2 | Access Switch | unit | 10 |
| 3 | Core Switch | unit | 2 |
| 4 | FIREWALL | unit | 1 |
| 5 | Active Directory Server | unit | 1 |
| 6 | Application Server | unit | 1 |

**C. Training/Aftersales Service/Parts Warranty**

Users Training for at least 4 personnel is required. Warranty period shall be for a period of One (1) year on parts and service. Technical Support shall be provided within 24 hours upon receipt of communication thereof via email or phone call. In case of latent manufacturing defects, the supplier shall replace the defective components within 7 days upon receipt of communication letter/request.

## VII. PAYMENT TERMS

The ABC is inclusive of all applicable government taxes and charges, professional fees, and other incidental and administrative costs. Any extension of contract time shall not involve any additional cost to the Government. Payment shall be made in cheque within 30 days following the completion and final acceptance of the project.

## VIII. LIQUIDATED DAMAGES

If the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance.

For guidance and information of all concerned.

July 27, 2021

**ATTY. ROGELIO R. TALIPING, JR.**
Chairperson, PBAC Goods and Services