SECTION VII.

TECHNICAL SPECIFICATIONS

Technical Specifications for Network Infrastructure

Bidders must indicate whether the goods and equipment offered are “Compliant” or “Non-Compliant” to the corresponding specifications prescribed by BCDA using this form.

RE-BIDDING FOR THE SUPPLY, DELIVERY, AND INSTALLATION OF NETWORK INFRASTRUCTURE FOR THE NATIONAL ACADEMY OF SPORTS (NAS) – PHASE 1 AT NEW CLARK CITY

TECHNICAL SPECIFICATIONS COMPLIANCE FORM

NO.	QTY.	UNIT	SPECIFICATIONS	COMPLIANCE	
				Compliant	Non-compliant
			NETWORK INFRASTRUCTURE		
			DATA CENTER FACILITY		
1	**1**	**unit**	**KVM SWITCH**		
			Must meet the following performance specifications: · Integrated LCD display, keyboard, mouse and switch · 18.5-inch LED energy-saving display · Scissors feet ultra-thin keyboard · The machine adapts the towline type protective design and signal cable design to avoid losses caused by repeated pumping · High quality dedicated slide rail · Overall 1U height, suitable for standard cabinet installation · No need for software installation, can be operated directly from the computer · Automatic power protection design. When device is not in use automatically enters in protected mode		
2	**8**	**units**	**POWER DISTRIBUTION UNIT**		
			Must meet the following performance specifications: · Managed PDU · Monitor and control power at the server level · Color-coded breaker & phase to better manage the load balancing · 60 deg C operating temperature · Thin Form Factor Chassis – 53mm deep, 52mm wide to safely remove servers · Extra Flat Breakers to avoid accidental tripping · Universal Mounting System including clip feet and flexible button, rear & side mounting system · eGrip system to secure standard IEC cables · +/- 1% IEC Class 1Billing Grade Accuracy		
3	**1**	**lot**	**INTER-RACK CABLING**		
4	**4**	**roll**	**UTP CAT6 CABLE**		
			Must meet the following performance specifications:		

			· 24AWG solid bare copper conductors, non-plenum, Polyolefin insulation, twisted pairs, central spline, rip cord, PVC jacket · NEC/(UL) Specification: CM · CEC/C(UL) Specification: CM · IEC Specification: 11801 Category 6 · EU RoHS Compliant (Y/N): Y · TIA Specification: 568 C .2 Category 6 · Suitable applications: Premise horizontal Cable, gigabit ethernet		
5	**6**	**units**	**UTP PATCH PANEL**		
			Must meet the following performance specifications: · Modular design, compatible with Shielded or Unshielded solution · Max. Capacity: 24 connectors · Front Connection: Flush · Termination Area: Rear · Material: Steel · Must include 1pc generic horizontal cable manager per patchpanel		
6	**144**	**units**	**UTP PATCH CORD**		
			Must meet the following performance specifications: · Stranded conductors improve Flexibility · Improved strain relief and a flexible boot for optimum protection in high-density installations · Exceeds TIA and ISO transmission and mechanical performance requirements · Patch panel patch cord must be 2meters in length and light blue in color compliant to TIA-606 color shade Workstation patch cord must be 3meters in length and light blue in color compliant to TIA-606 color shade		
			DATA CENTER INFRASTRUCTURE		
7	**2**	**units**	**TRADITIONAL VIRTUALIZATION NODE**		
			The Traditional Virtualization node must have the following minimum Specifications: · Form Factor: 1U rack server · Processor: One Intel® Xeon® Scalable processor, with at least 16 cores and 2.4GHz · Memory: Supports DDR4 RDIMM, with minimum of 384GB configured · Drive bays: Must support up to 8 x 2.5-inch SAS/SATA/NVMe (HDD/SSD) max 122.8 TB · Storage: 2 x 480GB SSD · Storage Controller: Must include support for RAID levels 0, 1, 5, 6, 10, 50, 60 · Network ports: Must have at least 2 x 1GbE, 2 x 10GbE SFP+, and 2 x 16Gb FC HBA · PSU: Must have hot-plug redundant power supply · Able to support the following Operating Systems: o VMware ESXi o Citrix o Microsoft Windows Server		

			o Red Hat Enterprise Linux o Ubuntu Server · Able to support the following security features: o TPM 1.2/2.0 o Cryptographically signed firmware o Secure Boot o System Lockdown o Secure erase o Silicon Root of Trust · Must include server warranty of at least 3 years 8x5 onsite support. · The proposed solution must have the necessary software license/s to ensure the operability of the solution			
8	**1**	**unit**	**TRADITIONAL VIRTUALIZATION STORAGE**			
			The Traditional Virtualization Storage must have the following minimum specifications: · Form Factor: 2U Rack · Drive Bays: 24 x 2.5” drive bays · Processor: Intel® Xeon Processor · Dual Controller with System Memory of 16Gb per Controller · Supports max raw capacity up to 5.22PB with expansion · Supports FC, iSCSI (optical or BaseT), SAS · Supports max 32Gb FC ports: 8 per array (support auto-negotiate to 16Gb) · Storage: at least 8TB usable (RAID 5), 10K RPM SAS Hot-plug Hard Drive · Supports auto-tiering up to 3 primary (media-based) tiers · Supports distributed erasure coding to reduce rebuild times when drive failures occur · Supports Thin provisioning · Supports Snapshots: 1024 maximum re-direct-on-write snapshots per array · Supports asynchronous replication via FC or iSCSI; Target/source relationships may be one-to-many or many-to-one · Supports Self-encrypting drives (SEDs) in SSD or HDD formats, Full Disk Encryption (FDE) based on AES-256, and Drives certified to FIPS 140-2 Level 2 · Supported host OS: o Windows o RHEL o SLES o VMware · Supports virtualization integration with: o VMware vSphere o vCenter o Microsoft Hyper-V · Power Supply: Must have at least 580W redundant power supply · Must include server warranty of at least 3 years 8x5 Onsite support.			

9	**1**	**unit**	**NETWORK ATTACHED STORAGE (NAS)**		
			The Repository File Storage must have the following minimum specifications: · Form Factor: 3U rack server · HDD Bays: Must support up to 40 x 3.5inch HDD bays · Processors: Intel Xeon Processor with 8-core and up to 2.7GHz · Memory: Can Support up to 64GB, maximum of 64GB configured · Storage: Must have at least a total of 100TB usable capacity. Must support single volume size up to 200TB. · Network Interface Card: Must have at least 2x 10GB SFP+, ports 2x 10GbE RJ-45 and 4x 1GbE RJ-45 ports · Must support the following file systems: o BTRFS o Ext4 o Ext3 o FAT o NTFS o HFS+ o exFAT · Must include One (1) year warranty.		
10	**1**	**unit**	**ACTIVE DIRECTORY SERVER**		
			Specifications: · Form Factor: 1U Rack Server · Drive Bays: supports at least 8 x 2.5-inch SAS/SATA · CPU: Intel Xeon Processor, 8-Cores or Higher · Memory: 16Gb Memory · Storage: 2 x 600GB Hot-plug Hard Drive · RAID Controller: o 8-port 12Gbps Hardware RAID controller o Able to support RAID levels 0, 1, 5, 6, 10, & 50. o Can supports real-time RAID monitoring and hardware inventory · I/O & Ports: o Dual Port 1Gb LOM · Power Supply: 550W Power Supplies or Higher. · Supports Integration with third-party consoles. · Supports Connection for third-party consoles. · Supported Operating System: o Windows Server with Hyper-V o RHEL o SLES o Ubuntu Server o Citrix XenServer o VMwareESXi · Able to support the following security features: o TPM 1.2/2.0 optional o Secure Boot o Silicon Root of Trust		

			o Cryptographically signed firmware o System Lockdown o System Erase · Must include server warranty of at least 3 years 8x5 Onsite support. · The proposed solution must have the necessary software license/s to ensure the operability of the solution		
11	**5**	**unit**	**DG7GMGF0D5RK Windows Server 2022 Standard - 16 Core License Pack**		
12	**150**	**CAL**	**DG7GMGF0D5VX Windows Server 2022 - 1 User CAL**		
13	**150**	**CAL**	**DG7GMGF0D5VX Windows Server 2022 - 1 Device**		
14	**1**	**units**	**INTERNET ROUTER**		
			Specifications: · Must at least support forwarding performance of 1 Gbps · Must at least have the ff. ports: o 2x GE Combo WAN ports o 8x GE LAN ports which can be configured as WAN · Must support multi-core processors and non-blocking switching structure · Must support fault detection and determination in milliseconds, minimizing service interruption time · Must support Built-in firewall, IPS, URL filtering, and multiple VPN technologies, providing comprehensive security protection capabilities · Must support built-in SD-WAN solution · Must support traffic steering based on bandwidth and link quality · Must at least support memory of 2 GB · Must support 1U form factor · Must have built-in fan modules · Must at least support operating temperature of 0 º C to 45 º C · Must support the ff. features and protocols: o DHCP server/client/relay o PPPoE server/client o NAT o IEEE 802.1Q o IEEE 802.3 o VLAN management o MAC management o Routing policies o Static routes o RIP, RIPng o OSPF, OSPFv3 o IS-IS, IS-ISv6 o BGP, BGP4+ o MPLS o ACL o SNMP v1/v2c/v3 o Web-based network management o RMON		

15	**1**	**units**	**CORE SWITCH**		
			Specifications: · Must support maximum of 96 x 100GE, 96 x 40GE, 160 x 25GE or 192 x 10GE ports · Must support operating temperature of 0°C to +45°C · Must support relative humidity of 5% to 90% (non-condensing) · Must at least include dual AC power supplies · Must at least include the ff. interface cards: · 48-Port 10GE SFP+ interface card · 12-port 40GE QSFP+ interface card · Must at least include two switch fabric unit · Must include guide rails · Must include AP licenses with quantity equal or more than the quantity of proposed APs in this TOR · Must support the ff. Layer 2 functions: o ≥ 1M MAC address entries o Switching capacity ≥ 19.0 Tbps o Forwarding performance ≥14,200 Mpps o ≥ 4K VLANs o IEEE 802.1d o Automatic learning and aging of MAC addresses o IEEE 802.1w o IEEE 802.1s · Must support the ff. Layer 3 functions: o RIP and RIPng o OSPF and OSPFv3 o IS-IS and IS-ISv6 o BGP and BGP4+ · Must support the ff. multicast features: o Multicast traffic control o IGMPv1/v2/v3 snooping · Must support multicast ACL · Must support the ff. security features: o MACsec o NAC o IEEE 802.1X/MAC address/DHCP snooping-triggered authentication o 1K CPU hardware queues o RMON o DoS attack defense, TCP SYN flood attacks, UDP flood attacks · Must support the ff. features for reliability: o LACP and E-Trunk o VRRP and BFD-VRRP o High-speed Self Recovery · Must support the ff. integrated WLAN AC features: o WLAN terminal location o Locating of interference sources o Spectrum analysis function o 2.4G & 5G load balancing o ≥ 10K managed APs o Sets the AP access control mode		

			o Adjustable priority of traffic on wired interfaces of APs o 802.1x, portal and MAC address authentication o Dual-link load balancing for CAPWAP tunnels o Sets RF interference monitoring and avoidance o Automatically selects channels and power when APs go online o Rate limiting of upstream and downstream traffic on the air interface based on users o Configuration through NETCONF · Must support the ff. features for management and maintenance: o SNMPv1/v2/v3 o Hot patches o Streaming Telemetry o Console port login, Telnet, SSH		
16	**13**	**units**	**ACCESS SWITCH - ADMIN AND ACAD BLDG**		
			Specifications: · Must have the following switches: o 4 units of 24x10/100/1000BASE-T PoE+, 4 SFP+ o 9 units of 48x10/100/1000BASE-T, 4 SFP+ · Must have operating temperature of -5°C to +45°C, storage temperature of -40℃ to +70℃ and relative humidity of 5% to 90% (non-condensing). · Number of MAC address entries ≥ 16K · Must support switching capacity below: o At least 176 Gbps for 48 ports o At least 128 Gbps for 24 ports · PoE switches must at least support PoE power of 380W with built-in AC power module. · Must support the ff. Layer 2 functions: o ≥ 4K VLANs o IEEE 802.1d o learning and aging of MAC addresses o IEEE 802.1w o IEEE 802.1s · Must support the ff. Layer 3 functions: o ≥ 4K FIBv4 entries o ≥ 1K FIBv6 entries o Static routes o RIP v1/2 and RIPng o OSPF and OSPFv3 · Must support the ff. security features: o MFF o AAA authentication and RADIUS authentication o SSH V2.0/HTTPS · Must support the ff. management and maintenance features: o EFM o CFM o Y.1731 o SNMPv1/v2c/v3 o RMON · Must support ring protection protocol, RRPP.		
17	**1**	**units**	**ACCESS SWITCH - MULTI SPORT 48P PoE SWITCH**		

			Specifications: · Must support 48x10/100/1000BASE-T PoE+, 4 SFP+ · Must have operating temperature of -5°C to +45°C, storage temperature of -40℃ to +70℃ and relative humidity of 5% to 90% (non-condensing). · Number of MAC address entries ≥ 16K · Must support switching capacity of at least 176 Gbps · PoE switches must at least support PoE power of 380W with built-in AC power module. · Must support the ff. Layer 2 functions: o ≥ 4K VLANs o IEEE 802.1d o learning and aging of MAC addresses o IEEE 802.1w o IEEE 802.1s · Must support the ff. Layer 3 functions: o ≥ 4K FIBv4 entries o ≥ 1K FIBv6 entries o Static routes o RIP v1/2 and RIPng o OSPF and OSPFv3 · Must support the ff. security features: o MFF o AAA authentication and RADIUS authentication o SSH V2.0/HTTPS · Must support the ff. management and maintenance features: o EFM o CFM o Y.1731 o SNMPv1/v2c/v3 o RMON · Must support ring protection protocol, RRPP. RMON Must support ring protection protocol, RRPP.		
18	**1**	**unit**	**MANAGEMENT SWITCH (24-port Switch)**		
			Specifications: · Must support fixed ports of Twenty-Four 10/100/1000Base-T ports and four 10GE SFP+ ports · Must have operating temperature of -5°C to +45°C, storage temperature of -40℃ to +70℃ and relative humidity of 5% to 90% (non-condensing). · Number of MAC address entries ≥ 16K · Must at least support switching capacity of 128 Gbps · Must support the ff. Layer 2 functions: o ≥ 4K VLANs o IEEE 802.1d o learning and aging of MAC addresses o IEEE 802.1w o IEEE 802.1s · Must support the ff. Layer 3 functions: o ≥ 4K FIBv4 entries		

			o ≥ 1K FIBv6 entries o Static routes o RIP v1/2 and RIPng o OSPF and OSPFv3 · Must support the ff. security features: o MFF o AAA authentication and RADIUS authentication o SSH V2.0/HTTPS · Must support the ff. management and maintenance features: o EFM o CFM o Y.1731 o SNMPv1/v2c/v3 o RMON · Must support ring protection protocol, RRPP.			
19	**1**	**units**	**SERVER SWITCH**			
			Specifications: · Must at least support switching capacity of 3.6 Tbps · Must at least support forwarding performance of 940 Mpps · Must support front-to-back or back-to-front airflow. · Must at least support the ff. interfaces: o 6x 100G QSFP28 o 48x 25G SFP28 · Must support access, trunk, and hybrid interfaces to VLANs · Must support QinQ · Must support M-LAG technology · Must support DLDP. · Must support static, dynamic, and blackhole MAC address entries. · Must support IPv4 routing protocols, such as RIP, OSPF, ISIS, and BGP. · Must support IPv6 routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+. · Must support IP packet fragmentation and reassembly · Must support BFD for OSPF, BGP, IS-IS, and static route. · Must support IPv6 ND and PMTU discovery. · Must support queue scheduling modes such as PQ, DRR, PQ+DRR. · Must support ACL · Must support multicast traffic suppression · Must support traffic shaping. · Must support VRRP, VRRP load balancing, and BFD for VRRP. · Must support hardware-based BFD · Must support IGMP, PIM-SM, and MBGP · Must support MUX VLAN · Must support defense against DoS, ARP, and ICMP attacks.			

			· Must support port isolation, port security, and sticky MAC · Must support bindings of IP addresses, MAC addresses, port numbers, and VLAN IDs. · Must support RMON · Must support AAA, RADIUS, and HWTACACS authentication. · Must support IGMP snooping. · Must support IGMP proxy. · Must support ERSPAN+ · Must support Telemetry. · Must support SNMPv1/v2/v3, Telnet, and SSH. · Must support network-wide path detection. · Must support statistics on the buffer microburst status · Must support BootROM upgrade and remote upgrade. · Must support zero touch provisioning · Must support NetStream.		
20	**6**	**units**	**OUTDOOR ACCESS POINT**		
			Specifications: · Must support 5 GHz radio, 802.11ax 4x4 MU-MIMO. · Must support 2.4 GHz radio 802.11ax 4x4 MU-MIMO. · Must support total spatial streams: ≥ 8; device rate: ≥ 5 Gbps · Must at least have 1 x 5 GE, 1x GE and 1x 10GE SFP+ · Must support Bluetooth 5.0 · Must at least have antenna gain of 2.4GHz: 10dBi and 5GHz: 11dBi. · Must support maximum of 1024 number of users. · Must support IP68 dustproof and waterproof grade. · Must at least support 6 kA or 6 kV surge protection on Ethernet ports · Must support built-in smart antennas · Must support operating temperature of –40°C to +65°C · Must support the ff. WLAN features: o Beamforming o Priority mapping and scheduling o SSID hiding o 802.11k and 802.11v smart roaming · Must support the ff. network features: o IPv4/IPv6 Access control lists (ACLs) o Link Layer Discovery Protocol (LLDP) o SSID-based VLAN assignment o IEEE 802.1q o IEEE 802.3ab o DHCP client · Must support the QoS and Security features: o Queue mapping and scheduling o User-based bandwidth limiting o 802.1x authentication		

			o MAC-address authentication o Portal authentication o Rogue device detection and countermeasure o WPA/WPA2/WPA3 authentication · Must include PoE injector with at least the ff. specification: o Rated output voltage: 56 V o Rated output current: 1.61 A		
21	**2**	**units**	**POINT TO POINT ACCESS POINT**		
			Specifications: · Must support 5 GHz radio, 802.11ax 4x4 MU-MIMO. · Must support 2.4 GHz radio 802.11ax 4x4 MU-MIMO. · Must support total spatial streams: ≥ 8; device rate: ≥ 5 · Gbps · Must at least have 1 x 5 GE, 1x GE and 1x 10GE SFP+ · Must support Bluetooth 5.0 · Must support maximum of 1024 number of users. · Must support IP68 dustproof and waterproof grade. · Must at least support 6 kA or 6 kV surge protection on Ethernet ports · Must support operating temperature of –40°C to +65°C · Must support the ff. WLAN features: o Beamforming o Priority mapping and scheduling o SSID hiding o 802.11k and 802.11v smart roaming · Must support the ff. network features: o IPv4/IPv6 Access control lists (ACLs) o o Link Layer Discovery Protocol (LLDP) o SSID-based VLAN assignment o IEEE 802.1q o IEEE 802.3ab o DHCP client · Must support the QoS and Security features: o Queue mapping and scheduling o User-based bandwidth limiting o 802.1x authentication o MAC-address authentication o Portal authentication o Rogue device detection and countermeasure o WPA/WPA2/WPA3 authentication · Must include PoE injector with at least the ff. specification: o Rated output voltage: 56 V o Rated output current: 1.61 A		
22	**2**	**units**	**DIRECTIONAL ANTENNA 500M**		
			· Must have an external antenna with the ff. specifications: o Frequency (MHz): 2300-2700		

			o Gain (dBi): 18 o Coverage distance: 500 m o Maximum input power of the AP: 30 dBm o RSSI: -70 dBm, regardless of the local EIRP limit. o Downlink rate of a single STA: 10 Mbit/s o Horizontal lobe width (degrees): 60 o Vertical lobe width (degrees): 7 o Standing wave ratio (SWR) ≤ 1.5 o Polarization: Cross polarization o Connector: N-female x 4		
23	**1**	**units**	**DOOR ACCESS SYSTEM**		
			Must meet the following performance specifications: · Resolution: 120 x 160 · Frame Rate: 25 fps · Type: Touch Screen · Pixel: 2MP · Lens: Dual · Fast temperature measurement mode: Detects face and takes temperature without identity authentication · Multiple authentication modes are available: card and temperature, face and temperature, card and face and temperature · Face mask wearing alert: If the recognizing face does not wear a mask, the device will prompt a voice reminder. At the same time, the authentication or attendance is valid · Face mask wearing alert: If the recognizing face does not wear a mask, the device will prompt a voice reminder. At the same time, the authentication or attendance is valid · Face mask wearing alert: If the recognizing face does not wear a mask, the device will prompt a voice reminder. At the same time, the authentication or attendance is valid · Triggers voice prompt when detecting abnormal temperature · Configurable door status (open/close) when detecting abnormal temperature · Transmits online and offline temperature information to the client software via TCP/IP communication and saves the data on the client software · Face recognition duration ＜ 0.2 s/User; face recognition accuracy rate ≥ 99% · 6000 face capacity, 6000 card capacity, and 100,000 event capacity · Must have supporting floor stand brackets · Warranty: One (1) year		
24	**4**	**units**	**DATA RACK CABINET**		
			Must meet the following performance specifications: · W=800mm, D=1070mm, H= 1992mm (42U), black color, loading capacity:1500kgs · Adjustable EIA-310-E compliant mounting rails · Top panel with airflow or cable cover plates		

			· High-flow perforated steel front &rear doors · Swing handles with key lock · Lockable sides · Castors, leveling feet and anti-tip brackets · Quick-connect grounding · Color: Black (RAL9005) · Vertical air baffles with cable pass-thru · One (1) year warranty		
			CABLING		
25	**23**	**units**	**UTP Patch Panel**		
			Must meet the following performance specifications: · Modular design, compatible with Shielded or Unshielded solution · Max. Capacity: 24 connectors · Front Connection: Flush · Termination Area: Rear · Material: Steel · Must include 1pc generic horizontal cable manager per patch panel		
26	**954**	**units**	**UTP Patch cord**		
			Must meet the following performance specifications: · Stranded conductors improve Flexibility · Improved strain relief and a flexible boot for optimum protection in high-density installations · Exceeds TIA and ISO transmission and mechanical performance requirements · Patch panel patch cord must be 2meters in length and light blue in color compliant to TIA-606 color shade · Workstation patch cord must be 3meters in length and light blue in color compliant to TIA-606 color shade		
27	**10**	**units**	**Modular Connector**		
			Must meet the following performance specifications: · Plug housing: polycarbonate, UL 94V0-2 Rated · Conductor Type: solid; stranded · UL specification: UL1863 · EIA Specification: EIA - 364 · EU RoHS Compliant · Must have external boots		
28	**5**	**units**	**Power Distribution Unit**		
			Must meet the following performance specifications: · Shall have 6way C13 output ports · Shall be horizontally mounted · Power cord must be 2meters in length · Shall have a 10A ampere capacity and 220v input volts · Capable to mount directly to the rack or cabinet using cage nut		
29	**9**	**units**	**Uninterruptable Power Supply**		
			Must meet the following performance specifications:		

			· Advance digital control technology · Must have unity output power factor · Double Conversion technology · Wide input voltage and frequency window · Emergency shudown control through EPO · Wide input voltage and frequency window · Must be 2000va/1800W · Frequency range: 45hz - 65hz (auto sensing) · Output Receptacles: 6x IEC - C13 · Protection: overload, over temperature, short circuit, discharge, overcharge		
30	**8**	**units**	**Fiber Patch Panel**		
			Must meet the following performance specifications: · Fiber Patch Panel, that can accommodate SC duplex adapter and SC connectors · Fiber Patch Panel should be modular-type that can fit 2 fiber frames and can terminate up to 48-fiber in 1RU · Typically used in Server rooms, Network rooms, Data Centres and Small offices · Can be mounted directly on any 19" rack or cabinet · Must have 12-fiber SC duplex adapter as Load		
31	**120**	**units**	**Fiber Connector - Pigtail (SC – OM3)**		
			Must meet the following performance specifications: · Must have SC type Connector · Optical Characteristic: OM3 · Telecommunication Standards: TIA-568.3-D · Connector Standards: IEC 61754, TIA 604 · Flame Rating: PVC jacket: OFNR rating		
32	**44**	**units**	**Fiber Patch cord**		
			Must meet the following performance specifications: Standard Length: 3 meters Patch cords – 30 pcs · Conforms Standard: TIA/EIA 568 C.3 · Fiber type: OM3 · Connector 1: 30 pcs SC-LC and 14 pcs LC-LC · Cable Construction: duplex Patch cords – 14 pcs · Conforms Standard: TIA/EIA 568 C.3 · Fiber type: OM3 · Connector: LC - LC · Cable Construction: duplex		
33	**1**	**units**	**FIREWALL**		
			· The bidder must propose one (1) set appliance with license · The firewall must have the following hardware specifications: · Eight (8) port 1G Copper · Two (2) port 10G fiber (with 1 pc FSP+ SR Transceivers each firewall) **Performance Specifications**		

			· The proposed firewalls shall support at least 40 Gbps of Firewall Throughput. · The proposed firewalls shall support at least 24 Gbps of Firewall IMIX Throughput. · The proposed firewalls shall support at least 13 Gbps of IPS Throughput. · The proposed firewalls shall support at least 2.7 Gbps of Threat Protection Throughput. · The proposed firewalls shall support at least 13 million concurrent sessions. · The proposed firewalls shall support at least 250,000 new connections/sec. · The proposed firewalls shall support at least 21 Gbps of IPsec VPN Throughput. **General Management** · The proposed firewalls shall be purpose-built and shall have streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators. · The proposed firewalls shall have Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN · The proposed firewalls shall have advanced troubleshooting tools in GUI · The proposed firewalls shall have High Availability (HA) support in clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup · The proposed firewalls shall have automated firmware update notification with easy automated update process and rollback features. · The proposed firewalls shall have self-service user portal · The proposed firewalls shall have configuration change tracking · The proposed firewalls shall support Central Management via Cloud-based Unified Console · The proposed firewalls shall support API for 3rd party integration · The proposed firewalls shall have remote access option from the firewall vendor support. · The proposed firewalls shall have Cloud-based license management via Licensing Portal · The solution provider must have at least five (5) certified engineers of the proposed product. **Central Firewall Management** · The proposed firewalls shall include a centralized management and shall be a Cloud-based management and reporting for multiple firewalls, provides group policy management and a single console for all IT security products of the same brand. · The proposed central firewall management shall have Task Manager for providing a full historical audit trail and status monitoring of group policy changes			

			· The proposed central firewall management shall have Backup Firmware Management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access · The proposed central firewall management shall support firmware updates which offer one-click firmware updates to be applied to any device · The proposed central firewall management shall support Zero-touch deployment which enables the initial configuration to be performed in Cloud-based management and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to the central firewall management. **Firewall, Networking & Routing** · The proposed firewalls shall have Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing · The proposed firewall shall support DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine · The proposed firewalls shall support Network Flow which delivers policy-driven and intelligent acceleration of trusted traffic automatically · The proposed firewalls shall be able to enforce policy across zones, networks, or by service type · The proposed firewalls shall have Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi · The proposed firewalls shall support Custom zones on LAN or DMZ · The proposed firewalls shall support Flood protection: DoS, DDoS and ports can blocking · The proposed firewalls shall support Country blocking by Geo-IP · The proposed firewalls shall support Protocol independent multicast routing with IGMP snooping · The proposed firewalls shall support Bridging with STP support and ARP broadcast forwarding · The proposed firewalls shall have WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules · The proposed firewalls shall support 802.3ad interface link aggregation **SD-WAN** · The proposed firewalls SDWAN feature shall have Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, failover and fail-back · The proposed firewalls SDWAN feature shall support Application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP		

			· The proposed firewalls SDWAN feature shall support application identification that comes with the sharing of application control information between managed endpoints of the same brand which added clarity and reliability of identifying applications. · The proposed firewalls SDWAN feature shall support application routing over preferred links via firewall rules or policy-based routing · The proposed firewalls SDWAN feature shall have Centralized VPN orchestration · The proposed firewalls SDWAN feature shall support Unique Remote Ethernet Device Layer 2 tunnel with routing **Base Traffic Shaping & Quotas** · The proposed firewalls shall support Flexible network or user-based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)" · The proposed firewalls shall support Set user-based traffic quotas on upload/download or total traffic and cyclical or noncyclical · The proposed firewalls shall support Real-time VoIP optimization **Authentication** · The proposed firewalls shall support the sharing of currently · logged in Active Directory user ID between the managed endpoints of the same brand without an agent on the AD server or client. · The proposed firewalls shall support Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+ · The proposed firewalls shall support Single sign-on for Active directory, eDirectory, RADIUS Accounting · The proposed firewalls shall support Client authentication agents for Windows, Mac OS X, Linux 32/64 · The proposed firewalls shall support Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos · The proposed firewalls shall support Authentication certificates for iOS and Android · The proposed firewalls shall support Authentication services for IPSec, SSL, L2TP, PPTP · The proposed firewalls shall have Google Chromebook authentication support for environments with Active Directory and Google G Suite · The proposed firewalls shall support API-based authentication **User Self-Serve Portal** · The proposed firewalls shall have a self-serve portal to Download SSL remote access client (Windows) and configuration files (other OS) · The proposed firewalls shall have a self-serve portal for Hotspot access information · The proposed firewalls shall have a self-serve portal for Changing username and password		

			· The proposed firewalls shall have a self-serve portal to View personal internet usage **Base VPN Options** · The proposed firewalls shall support Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, preshared key · The proposed firewalls shall have Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Android VPN client support **VPN Client** · The proposed firewalls VPN client shall support · Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and · XAUTH · The proposed firewalls VPN client shall be able to enable the connection of FW and Endpoint security and Monitoring of the health status of the managed Endpoints for remote connected users · The proposed firewalls VPN client shall support Intelligent split-tunneling for optimum traffic routing · The proposed firewalls shall have Client-monitor for graphical overview of connection status · The VPN client shall have Mac and Windows Support **Network Protection Subscription** **Intrusion Prevention (IPS)** · The proposed firewalls shall have High-performance, NextGen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection · The proposed firewalls shall have Thousands of signatures · The proposed firewall shall have Support for custom IPS signatures · The proposed firewalls shall have IPS Policy Smart Filters which enable dynamic policies that automatically update as new patterns are added **ATP and Endpoint Health monitoring** · The proposed firewalls shall have Advanced Threat · Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall) · The proposed firewalls shall have automated policies that can limit access to network resources or completely isolate compromised systems until they are cleaned · The proposed firewalls shall have Lateral Movement Protection to further isolates compromised systems by having healthy managed endpoints, of the same brand, reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain **Clientless VPN**		

			· The proposed firewalls shall support Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC **Web Protection Subscription** **Web Protection and Control** · The proposed firewalls Web Protection and Control shall support Fully transparent proxy for anti-malware and web-filtering · The proposed firewalls Web Protection and Control shall have Enhanced Advanced Threat Protection · The proposed firewalls shall have URL Filter database with millions of sites across 92 categories backed by OEMLabs · The proposed firewalls Web Protection and Control shall have Advanced web malware protection with JavaScript emulation · The proposed firewalls Web Protection and Control shall have Live Protection real-time in-the-cloud lookups for the latest threat intelligence · The proposed firewalls Web Protection and Control shall have Second independent malware detection engine for dual scanning · The proposed firewalls Web Protection and Control shall have High performance web content caching · The proposed firewalls Web Protection and Control shall support Forced caching for Managed Endpoint (of the same brand) updates · The proposed firewalls Web Protection and Control shall support Safe Search enforcement (DNS-based) for major search engines per policy (user/group) · The proposed firewalls shall support Web policy override option to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users · The proposed firewalls Web Protection and Control shall support User/Group policy enforcement on Google Chromebooks **Cloud Application Visibility** · The proposed firewalls shall support Control Center widget which displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated · The proposed firewalls shall be able to Discover Shadow IT at a glance · The proposed firewalls shall be capable to Drill down to obtain details on users, traffic, and data · The proposed firewalls shall support One-click access to traffic shaping policies · The proposed firewalls shall be capable to Filter cloud application usage by category or volume · The proposed firewalls shall be able to provide Detailed customizable cloud application usage report for full historical reporting **Application Protection and Control**			

			· The proposed firewalls shall be able to automatically identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints of the same brand. · The proposed firewalls shall support Signature-based application control with patterns for thousands of applications · The proposed firewalls shall support Cloud Application Visibility and Control to discover Shadow IT · The proposed firewalls shall support App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added · The proposed firewalls shall support Micro app discovery and control · The proposed firewalls shall support Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g., P2P), and risk level Web & App Traffic Shaping · The proposed firewalls shall support 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 **Zero-Day Protection Subscription** **Dynamic Sandbox Analysis** · Dynamic Sandbox Analysis shall support Full integration into your security solution dashboard · Dynamic Sandbox Analysis shall be able to Inspect executables and documents containing executable content (Including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (Including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) · Dynamic Sandbox Analysis shall be able to Detect sandbox evasion behavior · Dynamic Sandbox Analysis shall support Machine Learning technology with Deep Learning scans all dropped executable files · Dynamic Sandbox Analysis shall include exploit prevention and Anti-ransomware Protection technology from endpoint security · Dynamic Sandbox Analysis shall be able to provide In-depth malicious file reports and dashboard file release capability · Dynamic Sandbox Analysis shall support one-time download links **Threat Intelligence Analysis** · All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) are automatically sent for Threat Intelligence Analysis			

			· Files are checked against massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware · Threat Intelligence Analysis shall be able to provide Extensive reporting including a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model. **Reporting** · Central Firewall Reporting · The proposed firewall must have a centralized management that shall have pre-defined reports with flexible customization options · The proposed firewall with centralized management shall be able to provide Report dashboard which has an at-a-glance view of events for at least the past 24 hours · The proposed firewall with centralized management shall be able to Easily identify network activities, trends, and potential attacks · The proposed firewall with centralized management shall have Easy backup of logs with quick retrieval for audit needs **Warranty and Support and Subscription** · The proposed solution shall have 8x5 support, feature updates, advanced replacement hardware warranty for term · The proposed solution shall have Machine Learning and Sandboxing File Analysis, reporting · The proposed solution shall have TLS and DPI engine, Web Security and Control, Application Control, reporting · The proposed solution must have Networking, Unlimited Remote Access VPN, Site-to-Site VPN, reporting · The Proposed solution shall provide One (1) year corrective / Remedial Maintenance and Annual health check visit from the date of acceptance.		
34	**40**	**lics**	**ENDPOINT SECURITY FOR WORKSTATIONS**		
			Integrated Management Must have: · A unified console for managing multiple products from the same vendor · The ability to manage security policies and administer multiple products from a single web interface. **Multi-Platform Management** · Windows, Mac, and Linux machines must be managed from one management console. **Updating and Deployment Options** Must be able to: · Configure the bandwidth limit for updating		

			· Must have the option to enable devices to get updates from the security vendor from a cache device and communicate all policy · Deploying the endpoint agent must support the following methodology: o Email setup link o Installer link o Scripted Installation o Inclusion on an Image **API & SIEM Integration** Must have the capability to: · Extract events and alerts information from the Cloud Dashboard to a local SIEM. · Allow integration with SIEM solutions Role Management Must have the capability: · To divide security administration by responsibility level and includes predefined roles including: o Super Admin o Admin o Help Desk o Read-Only o User **AD Synchronization** Must have the capability to: · Implement a service that maps users and groups from Active Directory to the security vendor cloud console and keeps them synced. · Synchronized with Azure Active Directory · Auto synchronization that happens every 6 hours for Azure AD **Tamper Protection** · Must have the capability to prevent the following actions on the endpoint protection solution: · Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or security vendor live protection · Disable tamper protection · Uninstall the security vendor agent software **Threat Protection** Must have the capability to: · Protect against malware, risky file types and websites, and malicious network traffic. · Have security vendor settings recommendation to provide best protection a computer can have without complex configuration · Check suspicious files against the latest information in security vendor database · Automatically submit malware samples to security vendor online for analysis · Do real-time scanning of local files and network shares the moment the user tries to access them. Access must be denied unless the file is clean. · Do real-time scanning internet resources as users attempt to access them. · Protect against threats by detecting suspicious or malicious behavior or traffic on endpoint computers:			

			· Documents from Ransomware · Critical functions in web browsers · Mitigate exploits in vulnerable applications · Application hijacking · Detect network traffic to command-and-control servers **Suspicious Behavior Detection** Must be able to: · Monitor the behavior of code to stop malware before a specific detection update is released · Have both pre-execution behavior analysis and runtime behavior analysis. · Have a technology that is used to identify specific characteristic of files before they run, to determine whether they have malicious intent **Advanced Deep Learning mechanism** · The system shall be light speed scanning; within 20 milliseconds, the model shall be able to extract millions of features from a file, conduct deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes. Must be able to: · Prevent both known and never-seen-before malware, likewise, must be able to block malware before it executes. · Protect the system even with offline and will not rely on signatures. · Classify files as malicious, potentially unwanted apps (PUA) or benign. · Should be able to process data through multiple analysis layers, each layer making the model considerably more powerful. · Should be able to process significantly more input, can accurately predict threats while continuing to stay up to date. · Model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance. · The deep learning model shall be trail and evaluate models end-to-end using advanced developed packages like Keras, TensorFlow, and Scikit-learn. Exploit Prevention/Mitigation must detect and stop the following known exploits: · Enforcement of Data Execution Protection (DEP) · Mandatory Address Space Layout Randomization (ASLR) · Bottom-up ASLR · Null Page (Null Dereference Protection) · Heap Spray Allocation · Dynamic Heap Spray · Stack Pivot · Stack Exec (MemProt) · Stack-based ROP Mitigations (Caller) · Branch-based ROP Mitigations (Hardware Augmented)		

			· Structured Exception Handler Overwrite Protection (SEHOP) · Import Address Table Access Filtering (IAF) (Hardware Augmented) · Load Library API calls · Reflective DLL Injection · Shellcode monitoring · VBScript God Mode · WoW64 · Syscall · Hollow Process Protection · DLL Hijacking · Application Lockdown · Java Lockdown · Squiblydoo AppLocker Bypass **Policies** · Selected policies should be able to be applied to either users or devices. · Policies must have the capability to be enforced and whether it expires. **Data Loss Prevention (DLP)** Must be able to: · Monitor and restrict the transfer of files containing sensitive data. · Specify conditions for data loss prevention to detect, action to be taken if the rules are matched, any files to be excluded from scanning · Must have two types of rules: File & Content **Peripheral Control** Must be able to: · Control access to peripherals and removable media · Exempt individual peripherals from that control · Application Control · Must be able to: · Detect and block applications that are not a security threat but lets the administrator decide if its unsuitable for office use. **Web Control** Must be able to: · Block by category of the site · Block specific file types or specific websites · Prevent access to sites that increase the risk to the organization · Help improve productivity and potentially limit bandwidth **Root cause analysis** Must be able to: · Allow investigation on the chain of events surrounding a malware infection and pinpoint areas where you can improve security · Must have the following list for each case that is being created: o Priority o Summary o Status o Time Created			

			o User o Device **Remediation** · Detected malware are cleaned up automatically · If a cleanup is successful, the malware detected is deleted from the Alerts list. The malware detection and cleanup are shown in the "Events" list **Synchronized Security** · Security products of the same vendor actively work together, responding automatically to incidents and delivering enhanced security insights. **Endpoint Security + Firewall** · Automatically isolate infected endpoints on the public and local area networks · Identify all apps on the network · Link threats to individual users and computers		
35	**6**	**lics**	**ENDPOINT SECURITY FOR SERVER**		
			Must have the capability to: · Enable computers to get updates from a cache on a server on the network, rather than directly from internet or security vendor. · Only applications you have approved can run on a server. · File Integrity Monitoring · Secure cloud, on-premises, and virtual server deployments. · Be managed via the security vendor cloud management platform for all the same security vendor solutions		
36	**213**	**lics**	**MOBILE DEVICE MANAGEMENT**		
			Admin User Interface · Must support the following devices o Android 7.x or later o iOS 12.x or later o Windows 10 version 1803 or later (desktop OS) o macOS 10.14 (Mojave) or later o Chrome OS 77 or later · Must have an easy-to-use cloud-hosted management console · Must have a flexible Dashboard with different user-selectable widgets and filter mechanism · The management console must have role-based access · Must support the following push notification services · The management console must have a customizable administrator user interface **Self-Service Portal** Must have a self-service portal that has the following capabilities: · Register new device · Device wipe · Device lock · Device locate · Passcode reset for Device		

			· App Protection · Application Container · Trigger device check-in · Decommission device · Delete decommissioned device from inventory · Monitor device status and compliance information · Show acceptable use policy with new device registration · Display post-enrollment message · Control registration by OS type · Configure maximum number of devices per user · Company-specific configuration of commands available to users · Customizable branding **User Directory and Management** · Must have comprehensive password policies. · Must be capable of Active Directory integration. **Device Compliance Enforcement Rules** · Must have the following Device Compliance Enforcement Rules: o Group assignment or ownership-based compliance rules o Compliance violations analytics o Device under management o Jailbreak or rooting detection o Encryption required o Passcode required o Minimum OS version required o Maximum OS version allowed o Last synchronization of the device o Last synchronization of the MDM app o Blacklisted apps o Whitelisted apps o Mandatory apps o Block installation from unknown sources (side-loading) o Data roaming setting o USB debugging setting o MDM client version o Malware detection (classical AV plus machine learning) o System Integrity Protection required o Firewall required (macOS) o Suspicious apps detection o Side-loaded apps detection o Unmanaged configuration profile detection o Potentially unwanted apps detection o Last malware scan o Locate app-enabled Compliance rule templates for HIPAA and PCI o Administrator guidance to resolve compliance issues o Man-in-the-middle attack detection **Security** · Must have the following security features: o Encrypted connection to the cloud-based management console			

			o Encrypted communication with devices o Control email access by compliance state (Exchange gateway, Office 365 access control) o 2FA device authentication at the Exchange gateway (password, certificate) o Define allowed email clients at the Exchange gateway o Control network access by compliance (Generic NAC interface, Sophos UTM or Wireless, - ---Cisco ISE, Check Point) o Text message phishing detection o Protection from malicious websites (web filtering) o Protect corporate apps with additional authentication (App Protection) o Web productivity filtering by 14 categories + allow/deny lists by IP address, DNS name, and IP range o Manage and store passwords using KeePass format o Must have the security for USSD code protection **Inventory** · Must have the capability to create device groups. · Must have a user-oriented device view · Must be able to automatically transfer unique device ID and further device data. · Must have automatic OS version detection. · Must have automatic device model resolution into a user-friendly name. · Must be able to use the actual device name for device inventory. · Must have a marker for company-owned and privately-owned devices. · Must have customer-defined device properties with template support. · Must have the capability to import/export device information. · Must have savable extended filters for devices. **Provisioning / Device Enrollment** · Must have the following provisioning/device enrollment capabilities: o Device management (MDM) enrollment o Container-only Management enrollment o Device enrollment wizard for admins o Device enrollment by emails o Online registration from the device o Bulk provisioning o Apple Configurator deployment o Apple DEP enrollment (Device Enrollment Program) o Android Zero-touch device enrollment o Samsung Knox Mobile Enrollment o Admin enrollment w/o installed app o Definition of standard rollout packages for personal or corporate devices o Automatic assignment of initial policies and groups based on user directory group membership o Enrollment using provisioning package files **Task Management** · Must be able to generate scheduled tasks.			

			· Must be able to generate tasks for a single device or group of devices. · Must have detailed status tracking for each task. · Must have intelligent strategies for task repetition. **Reporting** · Must have the capability to export inventory using applied filters. · Must have the capability to export all reports as XLS or CSV. · Must have the following reports available: o A compliance log of all administrator activities o A detailed Alert log o Malware reports o Compliance violation reports o Device reports o App reports o Certificate reports **MDM App Functionality** · Must have the capability to create an Enterprise App Store. · Must be able to show compliance violations (including help for the end-user to fix reported compliance issues). · Must be able to show server messages. · Must be able to show technical contact. · Must have the capability to trigger device synchronization. · Must be able to show privacy information. **Application Management** · Must have the capability to install apps (with or without user interaction, including managed apps on iOS). · Must have the capability to uninstall apps (with or without user interaction). · Must be able to list all installed apps. · Must be able to support Apple Volume Purchasing Program (VPP). · Must have the capability to Allow/forbid the installation of apps. · Must have the capability to Block app uninstallation. **Device Configuration** · Must have the following device configuration settings: o Microsoft Exchange settings for email o IMAP or POP settings for email o LDAP, CardDAV and CalDAV settings o Configuration of access points o Proxy settings o Wi-Fi settings o VPN settings o Install root certificates o Install client certificates o Per-app VPN o Single sign-on (SSO) for 3rd party apps (app protection) and company webpages o Distribution of bookmarks (Web Clips)			

			o Force iOS update on supervised devices (and display pending iOS updates) o Configure the iOS lock screen and home screen o Automatically receive Wi-Fi and VPN settings from Sophos UTM appliances o Managed domains o Firewall configuration o Kernal Extension policy o Kiosk Mode o App permissions o Enable iOS Lost Mode o Configure Google Accounts o Android enterprise: Configure password policy (workspace) o Android enterprise: Configure password policy (device) o Android enterprise: Configure restrictions o Android enterprise: Configure Wi-Fi o Android enterprise: Configure app protection o Android enterprise: Configure app control o Android enterprise: Configure app permissions o Android enterprise: Configure Exchange o Android enterprise: Install the root certificate o Android enterprise: Install a client certificate o Android enterprise: Install client certificate via SCEP o Samsung Knox: Container handling (create, lock, decommission) o Samsung Knox: Configure restrictions o Samsung Knox: Configure Exchange o Samsung Knox: Manage container password o Samsung Knox: Allow/block data and file sync between Knox Workspace and personal area o Samsung Knox: Allow/block Iris scan authentication for Knox Workspace o Configure devices to use AirPrint printers **Device Information** · Must be able to show the following device information: o Internal memory utilization (free/used) o Battery charge level o IMSI (unique identification number) of SIM card o Currently used cellular network o Roaming mode o OS version o List of installed profiles o List of installed certificates o Malware detected on device · Must have the capability to do remote screen sharing (via TeamViewer or AirPlay device) **Secure Email** · Must have an email app that's fully featured, secure, and containerized personal information management (PIM) app for Android and iOS that lets you isolate information like business email, calendars, and contacts from private data on the mobile device. · Email app must have the following features:		

			o Sync email with Microsoft Exchange or any other ActiveSync compatible email service. o Geo-fencing / Time-fencing / Wi-Fi fencing o Control cut and copy o Control screenshot o Show event details o Export contacts to device o Define out of office message in the email app o Unified calendar view o Anti-phishing protection for links in emails **Corporate Browser** · Must have a Corporate Browser feature for secure access to intranets or corporate websites. · Corporate Browser feature must have the following capabilities: o Browsing restricted to predefined corporate domains o Preconfigured corporate bookmarks o Password manager o Client or user certificates to authenticate against corporate websites o Root certificates o Restricted cut, copy, and paste **Content Management** · Must have a containerized mobile Content Management app for iOS and Android that provides a secure way to manage, distribute, and edit business documents and view web content. · Must have the capability to edit Office format documents without leaving the container environment to ensure encrypted content remains secure. · Must be able to store documents securely with AES-256 encryption · Must support the following storage providers: o Dropbox o Google Drive o Microsoft OneDrive personal and business o Box o Telekom MagentaCloud o Egnyte o OwnCloud o WebDAV · Must have the capability to control data leaving the container · Must have the following capabilities: o Geo-fencing / Time-fencing / Wi-Fi fencing o Lock container access on non-compliant devices o Request call home based on time or by unlocking count o Edit or create Word, Excel, PowerPoint, and text format files o Annotate PDF files o Fill PDF forms o View Sophos SafeGuard format password protected HTML5 files o Share documents as password protected HTML5 files o Anti-phishing protection for links in documents			

			o View with Secure Workspace access to encrypted documents from other apps o Unlock app via a fingerprint reader o View, manage and create Zip and 7z compressed archives o Manage and store passwords securely using KeePass format **Telecom Cost Control** · Must have a Telecom Expense Management (TEM) feature that can monitor cellular data usage of individual devices. · Must have the following capabilities: o Disable data while roaming o Disable voice while roaming o Control sync while roaming o Configure APN or Carrier settings o Define data usage upper limit per device o Compare data usage against limit o Per app network usage rules		
			IP TELEPHONY AND UNIFIED COMMUNICATIONS		
37	**6**	**units**	**Conference Phone**		
			· Must support up to 6 lines, 6 SIP accounts or higher · Must support Android 4.4 or higher and offers access to the Google Play Store · Must support 7-way conference bridge or higher · Must at least support 4.3" (800x480) or higher capacitive touch screen · Must have an auto-sensing Gigabit Ethernet port with integrated PoE+ · Must support Bluetooth for audio pairing and data syncing with mobile devices and Wi-Fi for wireless calling/conferencing. · Must support HD audio to maximize voice quality and must offer daisy chain support · Must support TLS and SRTP security encryption		
38	**3**	**lot**	**IMPLEMENTATION, DEPLOYMENT and CONFIGURATION SERVICES**		
			Implementation and configuration services for the major components o MAJOR PRODUCT #2 : Data Center Infrastructure o MAJOR PRODUCT #3 : Network Components · MAJOR PRODUCT #4 : Security		
39	**1**	**lot**	**PROJECT MANAGEMENT SERVICES**		
			· Project Management for all the components of ICT Equipment · The winning bidder will appoint a project manager as a SINGLE POINT OF CONTACT · Tracks and monitors the progress of the project from component delivery, installation, configuration, testing, deployment, acceptance and turn over		

			· Adopts project management methodology and practices for regular reporting, incident reporting and change management		
40	**3**	**lot**	**ONSITE ENGINEER (for 3 months)**		
			· One (1) on-site engineer for three (3) months per major product after project acceptance. o MAJOR PRODUCT #1 : Desktops and Laptops o MAJOR PRODUCT #2 : Data Center Infrastructure o Traditional Virtualization o Network Attached Storage o Active Directory Server o MAJOR PRODUCT #3 : Network Components o Internet Router o Core Switch o Access Switch o Management Switch o Server Switch o Access Points · MAJOR PRODUCT #4 : Security o Firewall o Endpoint Security and Server Protection o Mobile Device Management		
41	**2**	**lot**	**TRAINING**		
			· Solution Knowledge Transfer Training for Major products with certification from the winning bidder · One (1) Data Center Facilities Training from CDCP Trainor · One (1) official training with certification for ITIL.		

Bidder's Authorized Representative

Signature over Printed Name **Principal Bidder / Supplier**