ATTACHMENT B – Scope of Work

The following categories are authorized under this contract:

5.2.4 OPTICAL NETWORKING — High capacity networks based on optical technology and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength based services.

5.2.4.1 Core DWDM (Dense Wavelength Division Multiplexing) Switches — Switches used in systems designed for long haul and ultra long-haul optical networking applications.

5.2.4.2 Edge Optical Switches — Provide entry points into the enterprise or service provider core networks.

5.2.4.3 Optical Network Management — Provides capabilities to manage the optical network and allows operators to execute end-to-end circuit creation.

5.2.4.4 IP over DWDM (IPoDWDM) — A device utilized to integrate IP Routers and Switches in the OTN (Optical Transport Network).

5.2.5 ROUTERS — A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keep the networks connected to the Internet.

5.2.5.1 Branch Routers — A multiservice router typically used in branch offices or locations with limited numbers of users and supports flexible configurations/feature. For example: security, VoIP, wan acceleration, etc.

5.2.5.2 Network Edge Routers — A specialized router residing at the edge or boundary of a network. This router ensures the connectivity of its network with external networks, a wide area network or the Internet. An edge router uses an External Border Gateway Protocol, which is used extensively over the Internet to provide connectivity with remote networks.

5.2.5.3 Core Routers - High performance, high speed, low latency routers that enable Enterprises to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV and Video on Demand (VoD), and Software as a Service (SaaS).

5.2.5.4 Service Aggregation Routers — Provides multiservice adaptation, aggregation and routing for Ethernet and IP/MPLS networks to enable service providers and enterprise edge networks simultaneously host resource-intensive integrated data, voice and video business and consumer services.

5.2.5.5 Carrier Ethernet Routers — High performance routers that enable service providers to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV, Video on Demand (VoD), and Software as a Service (SaaS).

5.2.8 SWITCHES — Layer 2/3 devices that are used to connect segments of a LAN (local area network) or multiple LANs and to filter and forward packets among them.

5.2.8.1 Campus LAN – Access Switches — Provides initial connectivity for devices to the network and controls user and workgroup access to internetwork resources.
The following are some of the features a campus LAN access switch should support:

**Security**
- SSHv2 (Secure Shell Version 2)
- 802.1X (Port Based Network Access Control)
- Port Security
- DHCP (Dynamic Host Configuration Protocol) Snooping

**VLANs**
- Fast Ethernet/Gigabit Ethernet
- PoE (Power over Ethernet)
- link aggregation
- 10 Gb support
- Port mirroring
- Span Taps
- Support of IPv6 and IPv4
- Standards-based rapid spanning tree
- Netflow Support (Optional).

**5.2.8.2 Campus LAN – Core Switches** — Campus core switches are generally used for the campus backbone and are responsible for transporting large amounts of traffic both reliably and quickly. Core switches should provide:

- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- Security
  - SSHv2
  - MacSec encryption
  - Role-Based Access Control Lists (ACL)
- Support of IPv6 and IPv4
- 1/10/40/100 Gbps support
- IGP (Interior Gateway Protocol) routing
- EGP (Exterior Gateway Protocol) routing
- VPLS (Virtual Private LAN Service) Support
- VRRP (Virtual Router Redundancy Protocol) Support
- Netflow Support.

**5.2.8.3 Campus Distribution Switches** — Collect the data from all the access layer switches and forward it to the core layer switches. Traffic that is generated at Layer 2 on a switched network needs to be managed, or segmented into Virtual Local Area Networks (VLANs), Distribution layer switches provides the inter-VLAN routing functions so that one VLAN can communicate with another on the network. Distribution layer switches provides advanced security policies that can be applied to network traffic using Access Control Lists (ACLs).

- High bandwidth
- Low latency
Hot swappable power supplies and fans
Security (SSHv2 and/or 802.1X)
Support of IPv6 and IPv4
Jumbo Frames Support
Dynamic Trunking Protocol (DTP)
Per-VLAN Rapid Spanning Tree (PVRST+)
Switch-port auto recovery
NetFlow Support or equivalent

5.2.8.4 **Data Center Switches** — Data center switches, or Layer 2/3 switches, switch all packets in the data center by switching or routing good ones to their final destinations, and discard unwanted traffic using Access Control Lists (ACLs), all at Gigabit and 10 Gigabit speeds. High availability and modularity differentiates a typical Layer 2/3 switch from a data center switch. Capabilities should include:

- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- Ultra-low latency through wire-speed ports with nanosecond port-to-port latency and hardware-based Inter-Switch Link (ISL) trunking
- Load Balancing across Trunk group able to use packet based load balancing scheme
- Bridging of Fibre Channel SANs and Ethernet fabrics
- Jumbo Frame Support
- Plug and Play Fabric formation that allows a new switch that joins the fabric to automatically become a member
- Ability to remotely disable and enable individual ports
- Support NetFlow or equivalent

5.2.8.5 **Software Defined Networks (SDN) - Virtualized Switches and Routers** — Technology utilized to support software manipulation of hardware for specific use cases.

5.2.8.6 **Software Defined Networks (SDN)** — Controllers - is an application in software-defined networking (SDN) that manages flow control to enable intelligent networking. SDN controllers are based on protocols, such as OpenFlow, that allow servers to tell switches where to send packets. The SDN controller lies between network devices at one end and applications at the other end. Any communications between applications and devices have to go through the controller. The controller uses multiple routing protocols including OpenFlow to configure network devices and choose the optimal network path for application traffic.

5.2.8.7 **Carrier Aggregation Switches** — Carrier aggregation switches route traffic in addition to bridging (transmitted) Layer 2/Ethernet traffic. Carrier aggregation switches' major characteristics are:

- Designed for Metro Ethernet networks
- Designed for video and other high bandwidth applications
- Supports a variety of interface types, especially those commonly used by Service Providers
- Capabilities should include:
Redundant Processors
Redundant Power
IPv4 and IPv6 unicast and multicast
High bandwidth
Low latency
Hot swappable power supplies and fans
MPLS (Multiprotocol Label Switching)
BGP (Border Gateway Protocol)
Software router virtualization and/or multiple routing tables
Policy based routing
  • Layer 2 functionality
    Per VLAN Spanning Tree
    Rapid Spanning Tree
    VLAN IDs up to 4096
    Layer 2 Class of Service (IEEE 802.1p)
    Link Aggregation Control Protocol (LACP)
    QinQ (IEEE 802.1ad)
5.2.8.8 Carrier Ethernet Access Switches — A carrier Ethernet access switch can connect directly to the customer or be utilized as a network interface on the service side to provide layer 2 services.

  Hot-swappable and field-replaceable integrated power supply and fan tray
  AC or DC power supply with DC input ranging from 18V to 32 VDC and 36V to 72 VDC
  Ethernet and console port for manageability
  SD flash card slot for additional external storage
  Stratum 3 network clock
  Line-rate performance with a minimum of 62-million packets per second (MPPS) forwarding rate
  Support for dying gasp on loss of power
  Support for a variety of small form factor pluggable transceiver (SFP and SFP+) with support for Device Object Model (DOM)
  Timing services for a converged access network to support mobile solutions, including Radio Access Network (RAN) applications
  Support for Synchronous Ethernet (SyncE) services
  Supports Hierarchical Quality of Service (H-QoS) to provide granular traffic-shaping policies
  Supports Resilient Ethernet Protocol REP/G.8032 for rapid layer-two convergence

5.2.9 WIRELESS — Provides connectivity to wireless devices within a limited geographic area. System capabilities should include:

  Redundancy and automatic failover
  IPv6 compatibility
  NTP Support
5.2.9.1 Access Points — A wireless Access Point (AP) is a device that allows wireless
devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include:

802.11a/b/g/n
802.11n
802.11ac

Capable of controller discovery method via DHCP (onsite controller or offsite through Cloud Architecture)

UL2043 plenum rated for safe mounting in a variety of indoor environments

Support AES-CCMP (128-bit)

Provides real-time wireless intrusion monitoring and detection

5.2.9.2 Outdoor Wireless Access Points — Outdoor APs are rugged, with a metal cover and a DIN rail or other type of mount. During operations they can tolerate a wide temperature range, high humidity and exposure to water, dust, and oil. Capabilities should include:

Flexible Deployment Options

Provides real-time wireless intrusion monitoring and detection

Capable of controller discovery method via DHCP (onsite controller or offsite through Cloud Architecture)

5.2.9.3 Wireless LAN Controllers — An onsite or offsite solution utilized to manage lightweight access points in large quantities by the network administrator or network operations center. The WLAN controller automatically handles the configuration of wireless access-points. Capabilities should include:

Ability to monitor and mitigate RF interference/self-heal

Support seamless roaming from AP to AP without requiring re-authentication

Support configurable access control lists to filter traffic and denying wireless peer to peer traffic

System encrypts all management layer traffic and passes it through a secure tunnel

Policy management of users and devices provides ability to de-authorize or deny devices without denying the credentials of the user, nor disrupting other AP traffic

Support configurable access control lists to filter traffic and denying wireless peer to peer traffic

5.2.9.4 Wireless LAN Network Services and Management — Enables network administrators to quickly plan, configure and deploy a wireless network, as well as provide additional WLAN services. Some examples include wireless security, asset tracking, and location services. Capabilities should include:

Provide for redundancy and automatic failover

Historical trend and real time performance reporting is supported

Management access to wireless network components is secured

SNMPv3 enabled

RFC 1213 compliant

Automatically discover wireless network components

Capability to alert for outages and utilization threshold exceptions

Capability to support Apple’s Bonjour Protocol / mDNS

QoS / Application identification capability

5.2.9.5 Cloud-based services for Access Points — Cloud-based management of campus-wide WiFi deployments and distributed multi-site networks. Capabilities
include:

- Zero-touch access point provisioning
- Network-wide visibility and control
- RF optimization,
- Firmware updates

5.2.9.6 **Bring Your Own Device (BYOD)** — Mobile Data Management (MDM) technology utilized to allow employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged government information and applications in a secure manner. Capabilities should include:

  - Ability to apply corporate policy to new devices accessing the network resources, whether wired or wireless
  - Provide user and devices authentication to the network
  - Provide secure remote access capability
  - Support 802.1x
  - Network optimization for performance, scalability, and user experience

5.3.0 **UNIFIED COMMUNICATIONS (UC)** — A set of products that provides a consistent unified user interface and user experience across multiple devices and media types. Unified Communications that is able to provide services such as session management, voice, video, messaging, mobility, and web conferencing. It can provide the foundation for advanced unified communications capabilities of IM and presence-based services and extends telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications. Additional services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, are made possible through open telephony APIs. General UC solution capabilities should include:

  - High Availability for Call Processing
  - Hardware Platform High Availability
  - Network Connectivity High Availability
  - Call Processing Redundancy

5.3.0.1 **IP Telephony** — Solutions utilized to provide the delivery of the telephony application (for example, call setup and teardown, and telephony features) over IP, instead of using circuit-switched or other modalities. Capabilities should include:

  - Support for analog, digital, and IP endpoints
  - Centralized Management
  - Provide basic hunt group and call queuing capabilities
  - Flexibility to configure queue depth and hold time, play unique announcements and Music on Hold (MoH), log in and log out users from a queue and basic queue statistics (from the phone)
  - E911 Support

5.3.0.2 **Instant messaging/ Presence** — Solutions that allow communication over the Internet that offers quick transmission of text-based messages from sender to receiver. In push mode between two or more people using personal computers or other devices, along with shared clients, instant messaging basically offers real-time direct written language-based online chat. Instant messaging may also provide video calling, file sharing, PC-to-PC voice calling and PC-to-regular-
5.3.0.3 Unified messaging — Integration of different electronic messaging and communications media (e-mail, SMS, Fax, voicemail, video messaging, etc.) technologies into a single interface, accessible from a variety of different devices. Ability to access and manage voice messages in a variety of ways, using email inbox, Web browser, desktop client, VoIP phone, or mobile phone

Visual Voicemail Support (Optional)

5.3.0.4 Contact Center — A computer-based system that provides call and contact routing for high-volume telephony transactions, with specialist answering “agent” stations and a sophisticated real-time contact management system. The definition includes all contact center systems that provide inbound contact handling capabilities and automatic contact distribution, combined with a high degree of sophistication in terms of dynamic contact traffic management.

5.3.0.5 Communications End Points and Applications
   Attendant Consoles
   IP Phones

5.3.0.6 UC Network Management — Provides end-to-end service management for Unified Communications. Capabilities include testing, performance monitoring, configuration management, and business intelligence reporting.

5.3.0.7 Collaboration — Voice, video, and web conferencing; messaging; mobile applications; and enterprise social software.

5.3.0.8 Collaborative Video — A set of immersive video technologies that enable people to feel or appear as if they were present in a location that they are not physically in. Immersive video consists of a multiple codec video system, where each meeting attendee uses an immersive video room to “dial in” and can see/talk to every other member on a screen (or screens) as if they were in the same room and provides call control that enables intelligent video bandwidth management.

5.3.0.8.1 Content Delivery Systems (CDS) — A large distributed system of servers deployed in multiple data centers connected by the Internet. The purpose of the content delivery system is to serve content to end-users with high availability and high performance. CDSs serve content over the Internet, including web objects (text, graphics, URLs, and scripts), downloadable objects (media files, software, documents), applications (e-commerce, portals), live streaming media, on-demand streaming media, and social networks.

5.3.0.8.2 Physical Security — Technology utilized to restricting physical access by unauthorized people to controlled facilities. Technologies include:
   a. Access control systems
   b. Detection/Identification systems, such as surveillance systems, closed circuit television cameras, or IP camera networks and the associated monitoring systems.
   c. Response systems such as alert systems, desktop monitoring systems, radios, mobile phones, IP phones, and digital signage
   d. Building and energy controls

5.3.1 SERVICES — For each Category above (5.21-5.30), the following services should be
available for procurement as well at the time of product purchase or anytime afterwards.

5.3.1.1 Maintenance Services — Capability to provide technical support, flexible hardware coverage, and smart, proactive device diagnostics for hardware.

5.3.1.2 Professional Services

Deployment Services
  Survey/Design Services — Includes, but not limited to, discovery, design, architecture review/validation, and readiness assessment.
  Implementation Services — Includes, but not limited to, basic installation and configuration or end-to-end integration and deployment.
  Optimization — Includes, but not limited to, assessing operational environment readiness, identify ways to increase efficiencies throughout the network, and optimize Customer’s infrastructure, applications and service management.

Remote Management Services — Includes, but not limited to, continuous monitoring, incident management, problem management, change management, and utilization and performance reporting that may be on a subscription basis.

Consulting/Advisory Services — Includes, but not limited to, assessing the availability, reliability, security and performance of Customer’s existing solutions.

Data Communications Architectural Design Services — Developing architectural strategies and roadmaps for transforming Customer’s existing network architecture and operations management.

Statement of Work (SOW) Services — Customer-specific tasks to be accomplished and/or services to be delivered based on Customer’s business and technical requirements.

5.3.1.3 Partner Services — Provided by Contractor’s Authorized Partners/Resellers.

Subject to Contractor’s approval and the certifications held by its Partners/Resellers, many Partners/Resellers can also offer and provide some or all of the Services as listed above at competitive pricing, along with local presence and support. As the prime, Contractor is still ultimately responsible for the performance of its Partners/Resellers. Customers can have the option to purchase the Services to be directly delivered by Contractor (OEM) or its certified Partners/Resellers.

5.3.1.4 Training — Learning offerings for IT professionals on networking technologies, including but not limited to designing, implementing, operating, configuring, and troubleshooting network systems pertaining to items provided under the master agreement.