STATE OF DELAWARE
EXECUTIVE DEPARTMENT
OFFICE OF MANAGEMENT AND BUDGET

June 13, 2014

TO: ALL STATE AGENCIES, SCHOOL DISTRICTS, MUNICIPALITIES, VOLUNTEER FIRE COMPANIES AND POLITICAL SUBDIVISIONS

FROM: WILLIAM W. PICKRUM
DEPUTY DIRECTOR, GOVERNMENT SUPPORT SERVICES
302-857-4501

SUBJECT: **AWARD NOTICE – Addendum #3, effective September 5, 2014**
CONTRACT NO. GSS14579-DATACOMM
Data Communications Products and Services

TABLE OF CONTENTS
OF
KEY CONTRACT INFORMATION

GOVERNMENT SUPPORT SERVICES – CONTRACTING
100 ENTERPRISE PLACE – SUITE 4 – DOVER, DE 19904-8202
PHONE: (302) 857-4550 – FAX: (302) 739-3779 – GSS.OMB.DELAWARE.GOV

KEY CONTRACT INFORMATION

1. MANDATORY USE CONTRACT

(Return to Table of Contents)

REF: Title 29, Chapter 6911(d) Delaware Code. Every state department and agency within the Executive Branch and Judicial Branch of the state government shall procure all material, equipment and nonprofessional services through the statewide contracts administered by Government Support Services, Office of Management and Budget. Delaware State University, Delaware Technical and Community College, the operations funded by Public School Districts, Delaware Transit Corporation, the Legislative Branch and the Board of Pension Trustees and their consultants are specifically exempted from the requirements of this subsection.

Under Title 29 §6933, The State of Delaware is authorized to participate in, sponsor, conduct or administer a cooperative purchasing agreement for the procurement of materiel or nonprofessional services with 1 or more public procurement units either within the State or within another state in accordance with an agreement entered into between the participants.

2. CONTRACT PERIOD

(Return to Table of Contents)

Each contractor's contract shall be valid for a five (5) year period from June 1, 2014 through May 31, 2019 unless terminated early or extended in accordance with the terms and conditions of the Utah Master Agreement.

3. VENDORS

(Return to Table of Contents)

GSS14579-DATACOMMV01 WSCA-NASPO Contract Number AR607 FSF Vendor ID: 0000214152 ADTRAN, Inc. Attn: Darrell Rogers 901 Explorer Blvd, NW Huntsville, AL 35806-2807 Phone: 970-482-2216 Fax: 256-963-6725 Email: darrell.rogers@adtran.com Website: www.adtran.com/sled See Attachment B – Scope of Work	**Approved Resellers:** Anixter, Inc. GSS14579-DATACOMMV14 FSF ID: 0000022076 1400 N Providence Rd Suite 410 Media, PA 19063-2057 Attn: Mark Staniszewski Phone: 610-627-3900 Fax: 610-627-3927 Email: mark.staniszewski@anixter.com Website: www.anixter.com
GSS14579-DATACOMMV02 WSCA-NASPO Contract Number AR214 FSF Vendor ID: 0000040269 Brocade Communications Systems, Inc. Attn: Tania Craythorne	**Approved Resellers** The Breaker Group, Inc. GSS14579-DATACOMMV15 FSF ID: 32 Mill St

130 Holger Way San Jose, CA 95134-1376 Phone: 408-333-6226 Fax: 408-333-8101 Email: SLEDTeam@brocade.com Website: http://www.brocade.com/sales/sled/wsca.page See Attachment B – Scope of Work	Mount Holly, NJ 08060-1804 Attn: Randy Weaver Phone: 609-267-1330 Fax: 609-267-1433 Email: randy@breakergroup.com Website: www.breakergroup.com CDW Government, LLC GSS14579-DATACOMMV16 FSF ID: 0000044740 260 Industrial Way W Flr 1 Eatontown, NJ 077242262 Attn: Jon Mazella, Sales Manager Phone: 866-776-7415 or 732-982-0000 Fax: 203-899-2196 Email: jonathan.mazella@cdwg.com Website: www.cdw.com Glencom Systems, Inc. GSS14579-DATACOMMV17 FSF ID: 25 E Price St Linden, NJ 07036-3046 Attn: Glenn Falkowski Phone: 908-486-0420 Fax: 908-486-8621 Email: glennf@glen.com Website: www.glen.com SHI GSS14579-DATACOMMV17 FSF ID: 0000016884 290 Davidson Ave Somerset, NJ 08873 Attn: Bryan Rosenthal, Senior AE Phone: 908-692-4591 Fax: 888-896-8860 Email: bryan_rosenthal@shi.com Website: www.shi.com
GSS14579-DATACOMMV05 WSCA-NASPO Contract Number AR233 FSF Vendor ID: 0000035856 Cisco Systems, Inc. Attn: Angelene “Gigi” Feril 170 W Tasman Dr San Jose, CA 95134-1700 Phone: 408-424-0712 or 800-365-4578 Fax: 408-609-1729	**Approved Local Resellers** MTM Technologies, Inc. GSS14579-DATACOMMV18 FSF ID: 0000002776 Contact: Brian Shuba 1675 S State St Dover, DE 19901-5140 Phone: 302-744-2250 Fax: 302-735-3373

Email: aferil@cisco.com Website: http://www.cisco.com/web/strategy/government/wsca2014/delaware/index.html See Attachment B – Scope of Work	Email: bshuba@mtm.com Website: www.mtm.com NWN Corporation GSS14579-DATACOMMV19 FSF ID: 0000039535 Contact Jackie Bohn 303 Fellowship Rd, Suite 110 Mt. Laurel, NJ 08054-1212 Phone: 856-914-5618 Email: mnj-iss-team@nwnit.com Website: www.nwnit.com
GSS14579-DATACOMMV10 WSCA-NASPO Contract Number AR1464 FSF Vendor ID: 0000035207 Hewlett-Packard Company Attn: Erin Tank 355 Ledgelawn Dr Conway, AR 72034-9501 Phone: 501-428-8287 Fax: 501-339-2377 Email: erin.e.tank@hp.com Website: www.hp.com/buy/wscadata See Attachment B – Scope of Work	**Approved Local Resellers** http://gem.compaq.com/gemstore/sites/downloads/ApprovedDataComResellers07282014.xls
GSS14579-DATACOMMV12 WSCA-NASPO Contract Number AR229 FSF Vendor ID: 0000047993 Juniper Networks, Inc. Attn: Roxanne Bieniek 10 Technology Park Dr Westford, MA 01886-3140 Phone: 978 589 0636 Fax: 978 589 0800 Email: rbieniek@juniper.net Website: www.juniper.net See Attachment B – Scope of Work	**Approved Local Resellers** http://www.juniper.net/us/en/partners/locator/

4. SHIPPING TERMS

(Return to Table of Contents)

F.O.B. destination; freight pre-paid.

5. DELIVERY AND PICKUP

(Return to Table of Contents)

Delivery is 30 days ARO.

6. PRICING

(Return to Table of Contents)

Prices will remain firm for the term of the contract year. The discount rate shall remain in effect for the term of the Master Price Agreement.

IMPORTANT: The minimum discount percentage listed is for general informational purposes only and may not apply to every line item authorized under this contract. For specific item pricing, please refer to the contract price list weblink provided.

Contractor	Pricelist Link
Adtran	ar607pricelist.xls
Cisco	ar233pricelist.xls
Hewlett-Packard Company	ar1464pricelist.xlsx
Juniper Networks, Inc.	ar229pricelist.xls

7. AUTHORIZED CATEGORIES

(Return to Table of Contents)

Category	Service	Adtran	Cicso	Hewlett-Packard	Juniper Networks
a	Data Center Application Service		x	x	
b	Networking Software		x	x	X
c	Network Optimization and Acceleration		x	x	
d	Optical Networking	x	x	x	X
e	Routers	x	x	x	X
f	Security		x	x	X
g	Storage Networking		x	x	
h	Switches	x	x	x	X
i	Wireless	x	x	x	x
j	Unified Communications	x	x	x	

a. DATA CENTER APPLICATION SERVICES — Application networking solutions and technologies that enable the successful and secure delivery of applications within data centers to local, remote, and branch-office users using technology to accelerate, secure, and increase availability of both application traffic and computing resources.

i. Virtualized Load Balancers — Virtual devices that act like a reverse proxy to distribute network and/or application traffic across multiple servers to improve the concurrent user capacity and overall reliability of applications. Capabilities should include:
SSL (Secure Sockets Layer) Off-loading
Caching capabilities
Layer 4 Load Balancing
Layer 7 Load Balancing
Detailed Reporting

Supports multiple load balancers in the same system for multiple groups
Supports TLS1.2

ii. WAN Optimization — An appliance utilizing a collection of techniques for increasing data-transfer efficiencies across wide-area networks (WAN). Capabilities should include:
CIFS (Common Internet File System) acceleration
Data Compression
SSL encryption/decryption for acceleration (Optional)
Layer 4-7 visibility
Application Specific optimization

b. NETWORKING SOFTWARE — Software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. Networking software capabilities should include:
Restartable Process
High availability options
Targeted operating systems, i.e. DC, campus, core, wan, etc.
Operating System Efficiencies

i. Network Management and Automation — Software products and solutions for data center automation, cloud computing, and IT systems management.
ii. Data Center Management and Automation — Software products and solutions that capture and automate manual tasks across servers, network, applications, and virtualized infrastructure.
iii. Cloud Portal and Automation — Software products and solutions for cloud management with policy-based controls for provisioning virtual and physical resources.
iv. Branch Office Management and Automation — Software products and solutions for management of branch offices. Capabilities include remote troubleshooting, device management, WAN performance monitoring.

c. NETWORK OPTIMIZATION AND ACCELERATION — Devices and tools for increasing data-transfer efficiencies across wide-area networks.

i. Dynamic Load Balancing — An appliance that performs a series of checks and calculations to determine which server can best service each client request in order to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.
ii. WAN Acceleration — Appliance that optimizes bandwidth to improve the end user's experience on a wide area network (WAN). Capabilities should include:
CIFS acceleration
Data Compression
SSL encryption/decryption for acceleration (Optional)
Layer 4-7 visibility
Application Specific optimization
iii. High Availability and Redundancy — Limits any disruption to network uptime should an appliance face unforeseen performance issues. Transparently redistributes workloads to surviving cluster appliances without impacting communication throughout the cluster.

d. 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.
   i. Core DWDM (Dense Wavelength Division Multiplexing) Switches — Switches used in systems designed for long haul and ultra-long-haul optical networking applications.
   ii. Edge Optical Switches — Provide entry points into the enterprise or service provider core networks.
   iii. Optical Network Management — Provides capabilities to manage the optical network and allows operators to execute end-to-end circuit creation.
   iv. IP over DWDM (IPoDWDM) — A device utilized to integrate IP Routers and Switches in the OTN (Optical Transport Network).

e. 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.
   i. 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.
   ii. 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.
   iii. 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).
   iv. 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.
   v. 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).

f. SECURITY
   i. Data Center and Virtualization Security Products and Appliances — Products designed to protect high-value data and data center resources with threat defense and policy control.
   ii. Intrusion Detection/Protection and Firewall Appliances — Provide comprehensive inline network firewall security from worms, Trojans, spyware, key loggers, and other malware. This includes Next-Generation Firewalls (NGFW), which offer a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. Intrusion Detection/Protection and Firewall Appliances should provide: Non-disruptive in-line bump-in-the-wire configuration Standard first-generation firewall capabilities, e.g., network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc. Application

awareness, full stack visibility and granular control Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc. Upgrade path to include future information feeds and security threats SSL decryption to enable identifying undesirable encrypted applications (Optional).

iii. Logging Appliances and Analysis Tools — Solutions utilized to collect, classify, analyze, and securely store log messages.

iv. Secure Edge and Branch Integrated Security Products — Network security, VPN, and intrusion prevention for branches and the network edge. Products typically consist of appliances or routers.

v. Secure Mobility Products — Delivers secure, scalable access to corporate applications across multiple mobile devices.

vi. Encryption Appliances — A network security device that applies crypto services at the network transfer layer - above the data link level, but below the application level.

vii. On-premise and Cloud-based services for Web and/or Email Security — Solutions that provide threat protection, data loss prevention, message level encryption, acceptable use and application control capabilities to secure web and email communications.

viii. Secure Access — Products that provide secure access to the network for any device, including personally owned mobile devices (laptops, tablets, and smart phones). Capabilities should include:
   a) Management visibility for device access Self-service on-boarding, Centralized policy enforcement
   b) Differentiated access and services, Device Management

g. STORAGE NETWORKING — High-speed network of shared storage devices connecting different types of storage devices with data servers.

i. Director Class SAN (Storage Area Network) Switches and Modules — A scalable, high-performance, and protocol-independent designed primarily to fulfill the role of core switch in a core-edge Fibre Channel (FC), FCOE or similar SAN topology. A Fibre Channel director is, by current convention, a switch with at least 128 ports. It does not differ from a switch in core FC protocol functionality. Fibre Channel directors provide the most reliable, scalable, high-performance foundation for private cloud storage and highly virtualized environments.

ii. Fabric and Blade Server Switches — A Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, which is currently the core component of most SANs. The fabric is a network of Fibre Channel devices, which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning; a mechanism that disables unwanted traffic between certain fabric nodes.

iii. Enterprise and Data Center SAN and VSAN (Virtual Storage Area Network) Management — Management tools to provisions, monitors, troubleshoot, and administers SANs and VSANs.

iv. SAN Optimization — Tools to help optimize and secure SAN performance (ie. Encryption of data-at-rest, data migration, capacity optimization, data reduction, etc.

h. 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.

i. 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:
   a) SSHv2 (Secure Shell Version 2)
   b) 802.1X (Port Based Network Access Control)
   c) Port Security
   d) 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).

ii. 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
   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.

iii. 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

iv. 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

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

vi. 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 Open Flow, 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 Open Flow to configure network devices and choose the optimal network path for application traffic.

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

viii. 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.

i. WIRELESS — Provides connectivity to wireless devices within a limited geographic area. System capabilities should include:
Redundancy and automatic failover
IPv6 compatibility
NTP Support

i. 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

ii. 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)

iii. 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

iv. 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.

v. 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

vi. 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

j. 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

i. 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

ii. 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 realtime direct written language-based online chat. Instant messaging may also provide video calling, file sharing, PC-to-PC voice calling and PC-to-regular phone calling.

iii. 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)

iv. 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.

v. Communications End Points and Applications Attendant Consoles IP Phones

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

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

viii. 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 provide call control that enables intelligent video bandwidth management.

a) 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.

b) Physical Security — Technology utilized to restricting physical access by unauthorized people to controlled facilities. Technologies include:

i. Access control systems

ii. Detection/Identification systems, such as surveillance systems, closed circuit television cameras, or IP camera networks and the associated monitoring systems.

iii. Response systems such as alert systems, desktop monitoring systems, radios, mobile phones, IP phones, and digital signage

iv. Building and energy controls.

ADDITIONAL TERMS AND CONDITIONS

(Return to Table of Contents)

8. BILLING

The successful vendor is required to "Bill as Shipped" to the respective ordering agency(s). Ordering agencies shall provide at a minimum the contract number, ship to and bill to address, contract name and phone number.

9. PAYMENT

The agencies or school districts involved will authorize and process for payment each invoice within thirty (30) days after the date of receipt. The contractor or vendor must accept full payment by procurement (credit) card and/or conventional check and/or other electronic means at the State's option, without imposing any additional fees, costs or conditions.

10. PRODUCT SUBSTITUTION

All items delivered during the life of the contract shall be of the same type and manufacture as specified unless specific approval is given by Government Support Services to do otherwise. Substitutions may require the submission of written specifications and product evaluation prior to any approvals being granted.

11. ORDERING PROCEDURE

Successful contractors are required to have either a local telephone number within the (302) area code, a toll free (800) number, or agree to accept collect calls. Each agency is responsible for placing their orders and may be accomplished by written purchase order, telephone, fax or computer on-line systems. The contractor or vendor must accept full payment by procurement (credit) card and/or conventional check and/or other electronic means at the State's option, without imposing any additional fees, costs or conditions.

All dealers and resellers authorized in the State of Delaware are approved to provide sales and service support under the WSCA-NASP Master Price Agreement.

12. PURCHASE ORDERS

Agencies are required to identify the contract number **GSS14579-DATACOMM** on all Purchase Orders (P.O.) and shall complete the same when entering P.O. information in the state's financial reporting system.

13. REQUIREMENTS

For a complete list of contract specifications please refer to the original bid solicitation document(s). Any contract specific documentation will be accessible through the hyperlink(s) provided on this contract's details page.

14. HOLD HARMLESS

The contractor agrees that it shall indemnify and hold the State of Delaware and all its agencies harmless from and against any and all claims for injury, loss of life, or damage to or loss of use of property caused or alleged to be caused, by acts or omissions of the

contractor, its employees, and invitees on or about the premises and which arise out of the contractor's performance, or failure to perform as specified in the Agreement.

15. NON-PERFORMANCE

In the event the contractor does not fulfill its obligations under the terms and conditions of this contract, the ordering agency may purchase equivalent product on the open market. Any difference in cost between the contract prices herein and the price of open market product shall be the responsibility of the contractor. Under no circumstances shall monies be due the contractor in the event open market products can be obtained below contract cost. Any monies charged to the contractor may be deducted from an open invoice.

16. FORCE MAJEURE

Neither the contractor nor the ordering agency shall be held liable for non-performance under the terms and conditions of this contract due, but not limited to, government restriction, strike, flood, fire, or unforeseen catastrophe beyond either party's control. Each party shall notify the other in writing of any situation that may prevent performance under the terms and conditions of this contract.

17. AGENCY'S RESPONSIBILITIES

The Agency shall:

a. Examine and review in detail all letters, reports, drawings and other documents presented by the Contractor to the Agency and render to the Contractor in writing, findings and decisions pertaining thereto within a reasonable time so as not to delay the services of Contractor.

b. Give prompt written notice to the Contractor whenever the Agency observes or otherwise becomes aware of any development that affects the scope or timing of the Contractor's services.

c. When an ordering agency first experiences a relatively minor problem or difficulty with a vendor, the agency will contact the vendor directly and attempt to informally resolve the problem. This includes failure to perform by the date specified and any unacceptable difference(s) between the purchase order and the merchandise received. Ordering agencies should stress to vendors that they should expedite correction of the differences because failure to reply may result in an unfavorable rating in the execution of the awarded contract.

d. The state has several remedies available to resolve non-performance issues with the contractor. The Agency should refer to the Contract Terms and Conditions to view these remedies. When a default occurs, the Agency should first review the contract to confirm that the issue is a part of the contract. If the issue is not covered by the contract, the state cannot expect the contractor to perform outside the agreement. If the issue is a part of the contract, the Agency or GSS - Contracting must then contact the contractor, discuss the reasons surrounding the default and establish a date when the contractor will resolve the non-performance

issue.

e. If there is a performance deficiency, a Corrective Action Report (CAR) may be used. Complete this form to report concerns with vendors or commodities. Be sure to furnish as much detail as possible. http://gss.omb.delaware.gov/divisionwide/forms.shtml.

1 PRICING

Vendor Name: **ADTRAN**

RFP Product Categories (ADTRAN)	Minimum Discount Percentage
5.2.4 Optical Networking	Discount 13%
5.2.5 Routers	Discount 10%
5.2.8 Switches	Discount 10%
5.2.9 Wireless	Discount 10%
5.3.0 Unified Communications (UC)	Discount 10%

Current ADTRAN pricing sheets, approved by the State of Utah, can be found at the following web link:

Vendor Name: **Brocade Communications**

RFP Product Categories (Brocade)	Minimum Discount Percentage
5.2.1 Data Center Application Services	Discount 44%
5.2.2 Networking Software	Discount 44%
5.2.3 Network Optimization and Acceleration	Discount 44%
5.2.5 Routers	Discount 44%
5.2.6 Security	Discount 44%
5.2.7 Storage Networking	Discount 44%
5.2.8 Switches	Discount 44%
5.2.9 Wireless	Discount 44%

Current Brocade pricing sheets, approved by the State of Utah, can be found at the following web link:
http://www.brocade.com/sales/sled/wsca.page

IMPORTANT: The minimum discount percentage listed is for general informational purposes only and may not apply to every line item authorized under this contract. For specific item pricing, please refer to the contract price list web link provided.

Vendors are required to post state specific pricing on their hosted website or through the WSCA-NASPO eMarket center. The State of Utah vendor pricing sheets will serve as the approved base price.

1. Pricing Structure: Pricing for the Master Agreements shall be based on the Percent Discount off the current global MSRP Schedule applicable to United States customers.
2. Price Guarantee Period: The Data Communication Provider's Discount rate shall remain in effect for the term of the WSCA-NASPO Master Price Agreement.
3. Price Escalation
   Equipment, Supplies and Services: Data Communications provider may update the pricing on their MSRP price list one time every year after the first year of the original contract term.
4. Price Reductions: In the event of a price decrease in any category of product at any time during the contract in a Provider's Price Schedule, including renewal options, the WSCA-NASPO Contract Administrator shall be notified immediately. All Price Schedule price reductions shall be effective upon the notification provided to the WSCA-NASPO Master Agreement Administrator.
5. Adding Products: The ability to add new equipment and services is for the convenience and benefit of WSCA-NASPO, the State of Delaware, and all the Authorized Purchasers. The intent of this process is to promote "one-stop shopping" and convenience for the customers and equally important, to make the contract flexible in keeping up with rapid technological advances. The option to add new product or service categories and/items will expedite the delivery and implementation of new technology solutions for the benefit of the Authorized Purchasers.

   After the contracts are awarded, additional IT product categories and/or items may be added per the request of the Contractor, the State, an Authorized Purchaser or WSCA-NASPO. Additions may be ad hoc and temporary in nature or permanent. All ADDITIONS TO AN AWARDED Contractor of Manufacturer's offerings must be products, services, software, or solutions that are commercially available at the time they are added to the contract award and fall within the original scope and intent of the RFP (i.e., converged technologies, value adds to manufacturer's solution offerings, etc.).
6. New Product from Contractors – If Contractor, the State, an Authorized Purchaser or WSCA-NASPO itself requests to add new product categories permanently, then all awarded Contractors (Manufacturers) will be notified of the proposed change and will have the opportunity to work with WSCA to determine applicability, introduction, etc. Any new products or services must be reviewed and approved by the State of Utah WSCA-NASPO Contract Administrator.
7. Pricelist Updates – As part of each Contractor's ongoing updates to its pricelists throughout the contract term, Contractor can add new SKUs to its awarded product categories that may have been developed in-house or obtained through mergers, acquisitions or joint ventures; provided, however, that such new SKUs fall within the Contractor's awarded product categories. Updated price lists will be reviewed and approved by the State of Utah WSCA-NASPO Contract Administrator before the revised price list is considered valid.

2 ADTRAN, Inc. Scope of Work

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

i. SSHv2 (Secure Shell Version 2)
ii. 802.1X (Port Based Network Access Control)
iii. Port Security
iv. 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 light-weight 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-

phone calling.

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.

3 Brocade Communications Systems, Inc. Scope of Work

State of Utah Contract Number: AR613

ATTACHMENT B – Scope of Work

The following categories are authorized under this contract:

5.2.1 DATA CENTER APPLICATION SERVICES — Application networking solutions and technologies that enable the successful and secure delivery of applications within data centers to local, remote, and branch-office users using technology to accelerate, secure, and increase availability of both application traffic and computing resources.

5.2.1.1 Virtualized Load Balancers — Virtual devices that act like a reverse proxy to distribute network and/or application traffic across multiple servers to improve the concurrent user capacity and overall reliability of applications. Capabilities should include:

- SSL (Secure Sockets Layer) Off-loading
- Caching capabilities
- Layer 4 Load Balancing
- Layer 7 Load Balancing
- Detailed Reporting
- Supports multiple load balancers in the same system for multiple groups
- Supports TLS1.2

5.2.1.2 WAN Optimization — An appliance utilizing a collection of techniques for increasing data-transfer efficiencies across wide-area networks (WAN). Capabilities should include:

- CIFS (Common Internet File System) acceleration
- Data Compression
- SSL encryption/decryption for acceleration (Optional)
- Layer 4-7 visibility
- Application Specific optimization

5.2.2 NETWORKING SOFTWARE — Software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. Networking software capabilities should include:

- Restartable Process
- High availability options
- Targeted operating systems, i.e. DC, campus, core, wan, etc.
- Operating System Efficiencies

5.2.2.1 Network Management and Automation — Software products and solutions for data center automation, cloud computing, and IT systems management.

5.2.2.2 Data Center Management and Automation — Software products and solutions that capture and automate manual tasks across servers, network, applications, and virtualized infrastructure.

5.2.2.3 Cloud Portal and Automation — Software products and solutions for cloud management with policy-based controls for provisioning virtual and physical resources.

5.2.2.4 Branch Office Management and Automation — Software products and solutions for management of branch offices. Capabilities include remote troubleshooting, device management, WAN performance monitoring.

5.2.3 NETWORK OPTIMIZATION AND ACCELERATION — Devices and tools for increasing data-transfer efficiencies across wide-area networks.

5.2.3.1 Dynamic Load Balancing — An appliance that performs a series of checks and calculations to determine which server can best service each client request in order to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

5.2.3.2 WAN Acceleration — Appliance that optimizes bandwidth to improve the end user's experience on a wide area network (WAN). Capabilities should include:

CIFS acceleration

Data Compression

SSL encryption/decryption for acceleration (Optional)

Layer 4-7 visibility

Application Specific optimization

5.2.3.3 High Availability and Redundancy — Limits any disruption to network uptime should an appliance face unforeseen performance issues. Transparently redistributes workloads to surviving cluster appliances without impacting communication throughout the cluster.

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).

5.2.6 SECURITY

5.2.6.1 **Data Center and Virtualization Security Products and Appliances** — Products designed to protect high-value data and data center resources with threat defense and policy control.

5.2.6.2 **Intrusion Detection/Protection and Firewall Appliances** — Provide comprehensive inline network firewall security from worms, Trojans, spyware, key loggers, and other malware. This includes Next-Generation Firewalls (NGFW), which offer a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. Intrusion Detection/Protection and Firewall Appliances should provide:

- Non-disruptive in-line bump-in-the-wire configuration
- Standard first-generation firewall capabilities, e.g., network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc.
- Application awareness, full stack visibility and granular control
- Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc.
- Upgrade path to include future information feeds and security threats
- SSL decryption to enable identifying undesirable encrypted applications (Optional)

5.2.6.3 **Logging Appliances and Analysis Tools** — Solutions utilized to collect, classify, analyze, and securely store log messages.

5.2.6.4 **Secure Edge and Branch Integrated Security Products** — Network security, VPN, and intrusion prevention for branches and the network edge. Products typically consist of appliances or routers.

5.2.6.5 **Secure Mobility Products** — Delivers secure, scalable access to corporate applications across multiple mobile devices.

5.2.6.6 **Encryption Appliances** — A network security device that applies crypto services at the network transfer layer - above the data link level, but below the application level.

5.2.6.7 **On-premise and Cloud-based services for Web and/or Email Security** — Solutions that provide threat protection, data loss prevention, message level encryption, acceptable use and application control capabilities to secure web and email communications.

5.2.6.8 **Secure Access** — Products that provide secure access to the network for any device, including personally owned mobile devices (laptops, tablets, and smart phones). Capabilities should include:

- Management visibility for device access
- Self-service on-boarding
- Centralized policy enforcement
- Differentiated access and services
- Device Management

5.2.7 STORAGE NETWORKING — High-speed network of shared storage devices connecting different types of storage devices with data servers.

5.2.7.1 **Director Class SAN (Storage Area Network) Switches and Modules** — A scalable, high-performance, and protocol-independent designed primarily to fulfill the role of core switch in a core-edge Fibre Channel (FC), FCOE or similar SAN topology. A Fibre Channel director is, by current convention, a switch with at

least 128 ports. It does not differ from a switch in core FC protocol functionality. Fibre Channel directors provide the most reliable, scalable, high-performance foundation for private cloud storage and highly virtualized environments.

5.2.7.2 Fabric and Blade Server Switches — A Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, which is currently the core component of most SANs. The fabric is a network of Fibre Channel devices, which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning; a mechanism that disables unwanted traffic between certain fabric nodes.

5.2.7.3 Enterprise and Data Center SAN and VSAN (Virtual Storage Area Network) Management — Management tools to provisions, monitors, troubleshoot, and administers SANs and VSANs.

5.2.7.4 SAN Optimization — Tools to help optimize and secure SAN performance (ie. Encryption of data-at-rest, data migration, capacity optimization, data reduction, etc.

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

i. SSHv2 (Secure Shell Version 2)
ii. 802.1X (Port Based Network Access Control)
iii. Port Security
iv. 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 light-weight 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

5.3.1 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.