STATE OF UTAH "BEST VALUE" COOPERATIVE CONTRACT
CONTRACT NUMBER: AR229

November 17, 2015

Revision Number: Purchasing Agent: Spencer Hall
Phone #: 801-538-3307
Email: spencerh@utah.gov

Item: Data Communication Equipment and Services

Vendor: VC0000182225
Juniper Networks (US), Inc.
1194 Mathilda Avenue
Sunnyvale, CA 94089

Internet Homepage: www.juniper.net

General Contact: Roxanne Bieniek
Telephone: 978-589-0636
Fax number: 978-589-0142
Email: rbieniek@juniper.net

Usage Report Contact: Same

Reporting Type: Item-Line

Authorized Categories: 5.2.2 Networking Software
5.2.4 Optical Networking
5.2.5 Routers
5.2.6 Security
5.2.8 Switches
5.2.9 Wireless

Price: See Price on Website
Terms: Net 30
Effective dates: June 1, 2014 – May 31, 2019
Potential renewal options remaining: No Renewal Options
Days required for delivery: 30 Days ARO
Price guarantee period: Any price increase must be pre-approved by Utah
Freight: FOB Destination, Freight Prepaid
Minimum order: N/A
Min shipment without charges: N/A
Other conditions: None

Please note Tek-Hut, Inc. added to the Authorized Reseller.

Solicitation #: JP14001
The administrative fee for this contract is 0.25% and is already included in the contract price.

This contract covers only those procurement items listed. When placing orders, make sure to identify your organization as a government entity and provide the contract number. It is the responsibility of the ordering agency to ensure that the vendor is given the correct delivery and billing address. Agencies should return to the vendor any invoice which reflects incorrect pricing. Other items ordered that are not
listed on the contract must be invoiced separately.

State agencies are to place orders directly with the vendor creating a PRC in Finet.

This contract information sheet is subject to change. State Purchasing doesn’t recommend that you print a copy due to the potential to change. Always view contract information online at www.purchasing.utah.gov

Authorized Reseller list for Utah:

<table>
<thead>
<tr>
<th>Vendor #</th>
<th>Vendor Name</th>
<th>Contact</th>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>970009A</td>
<td>Accuvant</td>
<td>Brad LaVoie</td>
<td>(801) 571-0599</td>
<td></td>
<td><a href="mailto:blavoie@accuvant.com">blavoie@accuvant.com</a></td>
</tr>
<tr>
<td>VC000016088</td>
<td>Centurylink</td>
<td>Ken Romero</td>
<td>(801) 575-1025</td>
<td></td>
<td><a href="mailto:ken.romero@centurylink.com">ken.romero@centurylink.com</a></td>
</tr>
<tr>
<td>VC0000150941</td>
<td>Insight Public Sector, Inc</td>
<td>Lauren Bordlemay</td>
<td>(801) 575-1025</td>
<td></td>
<td><a href="mailto:lbordlemay@accuvant.com">lbordlemay@accuvant.com</a></td>
</tr>
<tr>
<td>121608A</td>
<td>Red Sky Solutions, LLC</td>
<td>Chris Barney</td>
<td>(801) 639-0532</td>
<td>(801) 553-1022</td>
<td><a href="mailto:cbarney@redskysol.com">cbarney@redskysol.com</a></td>
</tr>
<tr>
<td>55333I</td>
<td>Valcom Computer</td>
<td>Mike Linton</td>
<td>(801) 303-5317</td>
<td></td>
<td><a href="mailto:mlinton@vlcmtech.com">mlinton@vlcmtech.com</a></td>
</tr>
<tr>
<td>11462IB</td>
<td>CDW</td>
<td>Brett Johnson</td>
<td>(866) 465-9917</td>
<td></td>
<td>brejohn@ cdw.com</td>
</tr>
</tbody>
</table>
The following categories are authorized under this contract:

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.

5.2.4 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).

5.2.6 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

5.2.8 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
STATE OF UTAH "BEST VALUE" COOPERATIVE CONTRACT
CONTRACT NUMBER: AR229

November 17, 2015

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

Please contact the Purchasing Agent listed above if you have questions or concerns.

This is a multiple award contract. Please review all awarded contracts specific to your procurement needs and compare products and pricing before making your final purchase. The State of Utah may not sign a participating addendum (PA) with all vendors, despite issuing a master agreement contract award.

Only contracts appearing on the State Purchasing website have an active PA and are available for their specific awarded category use in the State of Utah. The awarded contracts resulting from the Data Communication solicitation are:

<table>
<thead>
<tr>
<th>Contractor</th>
<th>Contract Number</th>
<th>Contractor</th>
<th>Contract Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adtran</td>
<td>AR607</td>
<td>F5</td>
<td>AR615</td>
</tr>
<tr>
<td>Aruba Networks</td>
<td>AR608</td>
<td>Fujitsu Network</td>
<td>AR616</td>
</tr>
<tr>
<td>Avaya</td>
<td>AR603</td>
<td>Hewlett Packard</td>
<td>AR1464</td>
</tr>
<tr>
<td>Brocade</td>
<td>AR214</td>
<td>Huawei Enterprises</td>
<td>AR617</td>
</tr>
<tr>
<td>Ciena</td>
<td>AR612</td>
<td>IBM</td>
<td>AR618</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>AR233</td>
<td>Infoblox</td>
<td>AR619</td>
</tr>
</tbody>
</table>
STATE OF UTAH "BEST VALUE" COOPERATIVE CONTRACT

CONTRACT NUMBER: AR229

November 17, 2015

D-Link Systems AR613 Juniper Networks AR229
Dell AR602 Mitel Business Sys AR623
EMC AR620 Palo Alto Networks AR626
Enterasys/Extreme AR1470 Shore Tel AR627

FINET COMMODITY CODE(S):

20458 Modems, External, Data Communications
20464 Network Components: Adapter Cards, Bridges, Connectors, Expansion Modules/ports, Firewall Devices, Hubs, Line Drivers, Msaus, Routers, Transceivers, etc.
20621 Communication Control Units: Concentrators, Multiplexers, Couplers, etc.
20623 Communication Processors and Protocol Converters: Front-end Processor, Network Interface Module, Protocol Interchange, Switching Controls, etc.
20659 Modems, External Data Communications
83833 Communications: Networking, Linking, Fiber Modems, Power Over Ethernet, Wireless
88332 Computer Telephony Integration (cti) Systems
00000 Generic Commodity Code

REVISION HISTORY: