



# REQUEST FOR PROPOSAL

MIS – Equipment needed to Migrate to New  
Datacenter

December 1, 2015

MIS Department  
45 Courthouse Drive, Building E  
Bolivia, NC 28422

## **Brunswick County MIS – New Datacenter Virtual Environment, Firewalls, Switches, VMware Horizon View – RFP**

### **1. Introduction and General Information**

#### **1.1 Purpose**

Brunswick County Government invites experienced vendors to submit a proposal to provide a new virtual server environment and redundant firewalls. The virtual environment will consist of an EMC SAN and CISCO UCS for blade host servers. The firewalls are to be CISCO firewalls set up in a redundant fashion. A 50 user pilot of VMware Horizon View is also requested two 48 port CISCO switches, and various fiber patch cables.

#### **1.2 About Brunswick County / Project Overview**

Brunswick County, NC is located in southeastern North Carolina. The County seat is located in Bolivia, NC. We are one of the fastest growing counties in the state with a population of just over 115,000. Because of our fast growth, a new 911 Building is being built and almost complete. We will be moving our primary datacenter to that building. At the same time, we will be transitioning from an EMC NS-120 SAN that is at end of life.

#### **1.3 Original RFP Document**

All stated terms and conditions, exhibits and other attachments in the original form of the RFP are to remain unaltered in respondents' proposals. Each stated term and condition, exhibit and other attachments should be addressed in the response. Alternate proposals to the stated terms and conditions, exhibits and other attachments are to be stated in comparative relation to the original RFP requirements. Brunswick County reserves the right to reject any and all proposals.

#### **1.4 Timeframes**

The bid will end on January 14, 2016 at 2:00 PM. Work should be scheduled to begin within two weeks of bid acceptance with a project completion date before March 30, 2016. A walkthrough is scheduled for Monday January 4<sup>th</sup>, 2016 at 10:00 AM. The walkthrough is not required for submitting a proposal. Please RSVP to [Andrew.byron@brunswickcountync.gov](mailto:Andrew.byron@brunswickcountync.gov) before Thursday December 31, 2015 at 5:00 PM if you plan to attend the walkthrough.

#### **1.5 Professional Expectations**

The Contractor acknowledges that Brunswick County Government will rely on Contractor's ability, expertise and knowledge to provide a turn-key solution for Brunswick County's new datacenter. The contractor shall be obligated to exercise the highest standard of care in performing their obligation. Also the Contractor will direct its personnel to respect and abide by the authority of Brunswick County Government and/or its consultants on all matters related to

the Contractors operation at the Site, including but not limited to: Use of site resources such as elevators and loading docks, and the coordination of same; Connection to and use of utilities; Safety issues; Trash removal and site cleanliness; Site security.

## 2. Current Infrastructure

### 2.1 Current SAN

The current SAN consists of an EMC CX4/NS120. The SAN is physically expanded to the full 120 drive capacity. Total space is approximately 70TB. The SAN is connected to 5 VMWare host servers via Fiberchannel, using two Q-Logic fiber switches for speed and redundancy. The SAN also connects to the core network via iSCSI over copper, and serves as a NAS hosting CIFS shares. CIFS shares currently account for 2TB of total storage utilization, with the remainder used for VMWare data stores.

### 2.2 Current Host Servers

The virtual host environment consists of 5 HP ProLiant DL380 servers. Each host contains 8 dual core Xeon CPUs@2.53-2.66GHz, and 120GB of RAM. The hosts connect to the EMC NS120 SAN via fiber, as well as to the core data network via copper. Each host uses two fiber connections, as well as 5 copper connections for connectivity.

### 2.3 Current Core Network / Firewalls

Core network and firewalls consist of the following:

- (2) Nexus 5000 series switches. Each switch can house up to 32 SFP+ modules. Current connections include redundant 10GB links to (4) Nexus fabric extenders which serve the VMWare virtual hosts. The Nexus switches also serve as the core of the L2 and L3 network, providing redundant fiber links to the various switch stacks in each building on the complex. Links currently vary in speed, to include 1Gb-10Gb, based on fiber and distance limitations. The nexus core switches also connect to the County's firewall, a Cisco ASA5520.
- Cisco ASA 5520 firewall. The ASA controls the flow of traffic between the LAN, Internet, and DMZ traffic. Internet traffic flows out via a 100Mbps connection provided by Time Warner Cable.

## 3. New (Proposed) Infrastructure

### 3.1 New (Proposed) SAN

After carefully evaluating several SANs, Brunswick County has decided to stay with the current manufacturer, EMC. The VNX 5200 Build is below that includes the needed drive types and enclosures.

- Base System includes dual proc, (25) 600GB Flash, (2) 10GB and (4) 8GB FC
- (2) 15 Slot Disk Array Enclosures

- (1) 25 Slot Disk Array Enclosures
- (3) 200GB Fast SSD Cache
- (11) 100GB Fast SSD
- (25) 3TB NL-SAS
- Unified+Local+Fast Protection Suites
- 3-Year 24x7x4 Maintenance

### **3.1.2 EMC SAN Deliverables**

- 3.1.2.1 Provide final design and configuration worksheet to obtain Brunswick County approval before installation
- 3.1.2.2 Physically install EMC Storage System:
  - a. Install redundant Control Stations
  - b. Install Disk Processor Enclosure
  - c. Install (3) DAE(s)
  - d. Ensure proper disk placement within enclosures
- 3.1.2.3 Cable SAN for Fiber Channel and CIFS to Cisco UCS FI
- 3.1.2.4 Execute Unisphere Storage System Initialization software
- 3.1.2.5 Assign initial management IP
- 3.1.2.6 Setup Domain Name System (DNS)
- 3.1.2.7 Setup Network Time Protocol (NTP) via initialization software
- 3.1.2.8 Register and install licenses
- 3.1.2.9 Setup of ESRS and configure Connect Home
- 3.1.2.10 Evaluate current software/firmware versions and update if necessary
- 3.1.2.11 Configure Fast Cache for system
- 3.1.2.12 Configure storage connectivity for Vmware hosts FC protocol
- 3.1.2.13 Configure storage pool(s) utilizing Storage Tiering and best practice Raid configuration
- 3.1.2.14 Join to Active Directory and configure Common Internet File System, (CIFS)
- 3.1.2.15 Setup storage for CIFS and create share and snapshot schedule
- 3.1.2.16 Enable deduplication on CIFS volumes
- 3.1.2.17 Demonstrate basic functionality and assist Brunswick County with migration of current CIFS
- 3.1.2.18 Create and present a blank LUN for use with FCoE and boot from SAN on Cisco UCS servers
- 3.1.2.19 Integrate SAN with Vmware 6.X infrastructure
- 3.1.2.20 Assist Brunswick County with storage provisioning - LUN mapping and ensure proper integration with (6) new ESX hosts
- 3.1.2.21 Verify and test connectivity for redundancy
- 3.1.2.22 Configure tiering schedule
- 3.1.2.23 Configure CIFS snapshot scheduling
- 3.1.2.24 Provide high-level diagram (Visio)
- 3.1.2.25 Provide knowledge transfer to IT staff
- 3.1.2.26 Provide up to (6) additional hours of Day-2 support

## 3.2 New (Proposed) Host Servers – CISCO UCS

### 3.2.2 Configuration Requested

#### Cisco UCS Configuration

- (2) 5108 UCS Chassis
- (8) 2500W Power Supplies
- (6) B200M4 Blades with 2xE5-2660 256GB (16GB DDR4-2133-MHz)
- (4) UCS 6200 Series Fabric Interconnect Licenses - 1 Port
- (8) 8G FC SFP+ Modules
- (6) Fabric Interconnect License 1-Port
- (20) 1 Meter, 10GB SFP+ Cables
- (16) 3 Meter, 10GB SFP+ Cables
- (4) UCS 2208XP I/O Module
- 3 Year 24x7x4 Maintenance

### 3.2.3 CISCO UCS Deliverables

- 3.2.3.1 Provide vendor Project Management
- 3.2.3.2 Provide detailed deployment design using Cisco and industry best practices
- 3.2.3.3 Physically install (2) 5108 UCS B Series Chassis
- 3.2.3.4 Physically install (2) Fiber Interconnects
- 3.2.3.5 Physically connect and configure Fiber Interconnects and existing dual Nexus 5Ks using VPC and Cisco best practices
- 3.2.3.6 Physically install (6) Cisco Blade Servers
- 3.2.3.7 Physically install (4) PDU's in Brunswick County provided rack
- 3.2.3.8 Cable and label all equipment to Brunswick County standards
- 3.2.3.9 Configure Fabric Interconnects as a cluster:
- 3.2.3.10 Assign IP addresses to Fabric Interconnects and to the cluster
- 3.2.3.11 Configure global policies and settings
- 3.2.3.12 Assign port configurations and settings
- 3.2.3.13 Enable and configure Fiber Channel ports for storage integration
- 3.2.3.14 Configure equipment discovery policies
- 3.2.3.15 Configure DNS and NTP including Time Zone
- 3.2.3.16 Download and install recommend firmware packages from Cisco
- 3.2.3.17 Configure firmware policies and upgrade firmware on all components, if necessary
- 3.2.3.18 Configure and integrate new Fabric Interconnects with uplink to existing core - Dual Nexus 5K switches using industry best practices (Brunswick County will provide fiber between locations)
- 3.2.3.19 Configure two UCS chassis under single UCS management
- 3.2.3.20 Configure Kernel-based virtual machine (KVM) IP's
- 3.2.3.21 Develop naming and numbering scheme for the UCS deployment and obtain approval for design

- 3.2.3.22 Design and configure LAN settings on UCS Manager:
- 3.2.3.23 Configure media access control (MAC) address pools
- 3.2.3.24 Configure Port Channels to FI
- 3.2.3.25 Configure and assign VLANs
- 3.2.3.26 Configure vNIC Templates
- 3.2.3.27 Configure LAN Quality of Service (QoS) policies
- 3.2.3.28 Configure LAN connectivity policies
- 3.2.3.29 Design and configure SAN settings on UCS Manager (temp iSCSI for old and FC for new)
- 3.2.3.30 Configure World Wide Node Name(WWNN) Pools
- 3.2.3.31 Configure World Wide Port Name(WWPN) Pools
- 3.2.3.32 Configure WWN Pool
- 3.2.3.33 Create and configure VSANs
- 3.2.3.34 Configure virtual Host Bus Adapter (VHBA) templates
- 3.2.3.35 Configure Storage Connection Policies
- 3.2.3.36 Configure SAN Connection Policies
- 3.2.3.37 Create service profile template to best accommodate the intended customer use
- 3.2.3.38 Configure server policies and pools to best accommodate intended customer use
- 3.2.3.39 Associate service profiles to designated (6) blade servers
- 3.2.3.40 Setup Cisco blades to perform FCoE boots from designated SAN LUNs
- 3.2.3.41 Install VMware ESXi 6.X on each server
- 3.2.3.42 Test KVM access to each server
- 3.2.3.43 Test and verify boot of each server
- 3.2.3.44 Verify and test connectivity for redundancy
- 3.2.3.45 Configure Cisco Call Home
- 3.2.3.46 Configure UCS backup jobs to local target on Brunswick County provided SFTP server
- 3.2.3.47 Provide IT staff knowledge transfer on as-built UCS deployment
- 3.2.3.48 Provide IT staff knowledge transfer on UCS maintenance
- 3.2.3.49 Provide high level diagram (Microsoft Visio)
- 3.2.3.50 Document Cisco Maintenance contract information
- 3.2.3.51 Document hardware and serial numbers

### **3.3 New (Proposed) Firewalls**

#### **3.3.2 New Firewall Configuration**

##### **Cisco Redundant ASA 5525 with FirePower Configuration**

- (2) ASA 5525-X Firewalls
- Anyconnect Essentials for (750) Users
- FirePOWER IPS, AMP, URL Filtering (1 Year Subscription)
- FireSight Management Center for (2) devices
- 3 Year 24x7xNBD Support

### 3.3.3 New Firewall Deliverables

- 3.3.3.1 Working with Brunswick County MIS, document existing redundant Firewall connections. Convert to current syntax as needed and apply settings to new firewalls in a redundant configuration. Include specific documentation on the following:
  - 3.3.3.1.1 Interface settings
  - 3.3.3.1.2 Static mappings
  - 3.3.3.1.3 Allowed firewall port openings
  - 3.3.3.1.4 VPN site-to-site tunnels
  - 3.3.3.1.5 Remote client access
- 3.3.3.2 Configure and setup interfaces
- 3.3.3.3 Configure and setup routing
- 3.3.3.4 Configure and setup the hostname
- 3.3.3.5 Configure and setup the system time
- 3.3.3.6 Configure and setup management access
- 3.3.3.7 Configure and setup licensing
- 3.3.3.8 Configure and setup logging
- 3.3.3.9 Configure and setup users/AAA
- 3.3.3.10 Configure and setup certificates (Brunswick County will provide required certificates)
- 3.3.3.11 Configure and setup DHCP (for VPN pools)
- 3.3.3.12 Configure and setup DNS
- 3.3.3.13 Configure and setup advanced settings
- 3.3.3.14 Update boot image
- 3.3.3.15 Update ASDM image
- 3.3.3.16 Configure and setup access rules
- 3.3.3.17 Configure and setup NAT rules
- 3.3.3.18 Configure and setup service policy rules
- 3.3.3.19 Configure and setup objects
- 3.3.3.20 Configure and setup advanced firewall rules
- 3.3.3.21 Configure and setup AnyConnect
- 3.3.3.22 Configure and setup IPsec tunnels
- 3.3.3.23 Configure and setup Clientless SSL
- 3.3.3.24 Configure and setup NAT rules
- 3.3.3.25 Configure and setup Advanced Policy settings
- 3.3.3.26 Configure and setup connection profiles
- 3.3.3.27 Configure and setup group policies
- 3.3.3.28 Configure and setup Advanced peer to peer policies
- 3.3.3.29 Rack Redundant ASAs
- 3.3.3.30 Cable Redundant ASAs
- 3.3.3.31 Schedule and perform after-hours cutover
- 3.3.3.32 Test and remediate issues
- 3.3.3.33 Provide drawing of network with NAT and Firewall translations
- 3.3.3.34 Determine FireSight deployment location
- 3.3.3.35 Deploy OVF Template(VMware)
- 3.3.3.36 Configure initial set up
- 3.3.3.37 Configure system settings

- 3.3.3.38 Configure FireSight manager
- 3.3.3.39 Configure traffic redirection on ASA
- 3.3.3.40 Configure health monitoring
- 3.3.3.41 Configure health policies
- 3.3.3.42 Configure health events
- 3.3.3.43 Configure health blacklist
- 3.3.3.44 Configure local FireSight system
- 3.3.3.45 Configure local registration
- 3.3.3.46 Configure user management
- 3.3.3.47 Configure system policies
- 3.3.3.48 Configure product updates
- 3.3.3.49 Configure rule updates
- 3.3.3.50 Configure geolocation updates
- 3.3.3.51 Ensure licenses are correctly applied
- 3.3.3.52 Configure backup management
- 3.3.3.53 Configure task scheduling
- 3.3.3.54 Configure FirePower Networks
- 3.3.3.55 Configure FirePower security intelligence
- 3.3.3.56 Configure FirePower Ports
- 3.3.3.57 Configure FirePower URL's
- 3.3.3.58 Configure FirePower application filters
- 3.3.3.59 Configure FirePower security zones
- 3.3.3.60 Configure FirePower distinguished names
- 3.3.3.61 Configure FirePower PKI's
- 3.3.3.62 Configure access control policies
- 3.3.3.63 Configure intrusion policies
- 3.3.3.64 Configure file control policies
- 3.3.3.65 Configure SSL Policies
- 3.3.3.66 Configure application detector policies
- 3.3.3.67 Configure User policies
- 3.3.3.68 Configure correlation policies
- 3.3.3.69 Configure response and remediation policies
- 3.3.3.70 Configure Malware protection policies
- 3.3.3.71 Configure active scanning policies
- 3.3.3.72 Configure scheduled task policies
- 3.3.3.73 Provide up to (10) hours of Policy Configurations after Go Live
- 3.3.3.74 Provide up to (2) hours of knowledge transfer

### **3.4 VMware Horizon View Configuration**

#### **3.4.2 Requested Configuration** -(50) VMware Horizon View Licenses with 3 Year Support

#### **3.4.3 VMware Horizon View SOW**

- 3.4.3.1 Review and design a pilot View deployment with Brunswick County
- 3.4.3.2 Set up the required administrator users and groups in Active Directory.
- 3.4.3.3 Install View Composer on existing vCenter 6.X Server
  - 3.4.3.3.1 Install the View Composer database per best practices with SQL Express
- 3.4.3.4 Create Server 2012 VM
- 3.4.3.5 Install View Connection Server
- 3.4.3.6 Install the Events database.
- 3.4.3.7 Create Server 2012 VM
- 3.4.3.8 Install View Security Server
- 3.4.3.9 Assist Brunswick County with Firewall configuration for View server access remotely (Brunswick County will provide static IP and external DNS)
- 3.4.3.10 Install Licenses for View environment
- 3.4.3.11 Create up to (2) virtual machines that can be used as a parent for linked-clone desktop pools
- 3.4.3.12 Create up to (2) desktop pools
- 3.4.3.13 Assign pools to test user
- 3.4.3.14 Install Horizon Client on (1) end users machine and test access
- 3.4.3.15 Assist in applying SSL cert for view environment (Brunswick County will provide SSL Certificate)
- 3.4.3.16 Assist in accessing view from outside environment/remotely
- 3.4.3.17 Demonstrate basic functionality of admin console and day to day tasks
- 3.4.3.18 High level diagram (Visio)
- 3.4.3.19 Knowledge transfer to IT staff

#### **3.4.4 Redundant PDUs for UCS Configuration**

- (2) APC PDU's-24 Outlets, Rack Mountable (AP8941)

#### **3.4.5 Datacenter to Core Connectivity Configuration**

- (14) SFP 10G Base LR Transceiver Modules
- (14) 1 Meter, LC-LC Cables, Single mode

#### **3.4.6 Datacenter to Core Connectivity SOW**

- 3.4.6.1 Relocate (2) existing Nexus 2K top of rack to new data center and reconfigure for connectivity to Nexus 5K core
- 3.4.6.2 Setup and configure (2) 2960XR stacks and connect to Nexus 5K core

### **3.4.7 2960 XR Switches Configuration**

- (2) Cisco 48 Port, 2960XR PoE Switches, 2x10G SFP+
- (2) 6ft USB Console Cables
- (2) Cisco FlexStack Plus Stacking Modules
- (2) 3 Meter, Cisco FlexStack Stacking Cables
- (2) Cisco 1.02kW Power Supplies
- 3 Year 8x5xNBD Support

### **3.5 New Hardware Requirements**

All hardware needs to be new. Refurbished hardware will not be accepted. Also, no third-party hardware will be accepted.

### **3.6 New Hardware Support and Services Requirements**

Services must be completed by the organization bidding. Outsourcing of configuration and installation is strictly prohibited. The use of sub-contractors is strictly prohibited. All engineers must be full-time employees of the bidding organization. The bidding organization must be partnered with EMC and CISCO on the basis of solution design, configuration, and installation. Onsite support must be capable within two hours of reporting an issue. Remote only support is not acceptable.

### **3.7 New Hardware Assumptions**

The new SAN and hosts will be going to a new building. Racks, cooling, and power will be included. PDUs will be provided except for the PDUs required for the Cisco UCS mentioned above.

## **4 Proposal Preparation Guidelines**

### **4.1 Vendor's Understanding of the RFP**

In responding to this RFP, the vendor accepts the responsibility fully to understand the RFP in its entirety, and in detail, including making any inquiries to Brunswick County as necessary to gain such understanding. Brunswick County reserves the right to determine, at its sole discretion, whether the vendor has demonstrated such understanding. That right extends to cancellation of award if award has been made. Such disqualification and/or cancellation shall be at no fault, cost, or liability whatsoever to Brunswick County.

## 4.2 Guidelines

Configure and price your system design to satisfy all stated RFP requirements, including any and all system hardware and software elements necessary to satisfy a requirement. Where possible, break apart costs so that Brunswick County may select items for inclusion or exclusion. All products and solutions proposed for this RFP must be included at time the completed RFP is returned to Brunswick County. Omissions will be deemed nonresponsive. Do not provide material or information unrelated or not relevant to a specific RFP clause requirement. Alternate solutions, however, if presented in contrast to specifically stated requirements are acceptable.

## 4.3 Inquiries

After the RFP issue date, all communications between vendors and Brunswick County must be submitted in writing. No oral questions will be accepted. Any inquiries, requests concerning interpretation, technical questions, clarification, or additional information pertaining to functionality shall be directed to:

Brunswick County MIS Department  
P.O. Box 249  
Bolivia, NC 28422  
Attention: Andrew Byron, Server and Communications Administrator II  
E-mail: [andrew.byron@brunswickcountync.gov](mailto:andrew.byron@brunswickcountync.gov)

Vendors should not ask questions of other Brunswick County personnel, as information gathered from other sources may not be reliable or official. All questions concerning the RFP must reference the RFP page number, section heading, and paragraph. The question(s) must be concisely stated and be numbered in sequential order. Answers will be returned as soon as possible. Questions and responses affecting the content of this RFP will be provided to all vendors via a posting on the [brunswickcountync.gov](http://brunswickcountync.gov) website under the RFP section.

## 4.4 Proposal Submission

A written proposal specifying services and materials compliant with the requirements in this document should be mailed or hand delivered to Andrew Byron. Please include four copies for review

Mail:	Andrew Byron Brunswick County MIS P.O. Box 249 Bolivia, NC 28422
Hand Delivered:	Andrew Byron 45 Courthouse Drive Building E Bolivia, NC 28422

with the following sections:

#### 4.4.2 Company Overview

Provide a brief overview of your company and the services offered including:

- A) Full legal name of the company
- B) Year the business was established
- C) Years your organization has been a partner with EMC and CISCO and what level if applicable (gold, silver, etc.)
- D) Number of employees
- E) How many engineers in your company are technically certified to support
  - a. EMC
  - b. CISCO
- F) An outline of your current financial status
- G) An outline of your current partnerships
- H) List the qualifications and experience of the project manager(s) and engineer(s) that will be working on the project

#### 4.4.3 Vendor References

Please provide information about your current clients, including:

- A) Total number of current clients
- B) A list of clients that you have either implemented an EMC SAN or CISCO UCS
- C) A list of clients in the public sector
- D) Evidence of successful completion of a project of a similar size and complexity
- E) References: Please provide a client reference list consisting of three customers presently using the proposed system. The referenced clients should be local, and references from other governmental organizations using equipment similar to what is being proposed are preferred. The list should include organization name, name of

contact with address and telephone number, and a brief description of the system, platform, length of time using the system and number of users.

#### **4.4.4 Pricing**

Price and discount schedules submitted by vendor will be valid for a period of not fewer than 90 days following the date of submission of their proposal. Vendors are required to state this guarantee or better in their proposal.

If pricing includes any promotional pricing, please include the expiration date of the promotion allowing Brunswick County an opportunity to take advantage of the promotional pricing if possible.

All Services for Cisco products must be 3 years of 24x7x4. All services for EMC must be 3 years of Premium Hardware & Software support

If the vendor identifies anything that they must add to any of the deliverables sections above to successfully complete the project, please add that to your proposal along with pricing and explanation(s).

#### **4.4.5 Selection**

Proposals will be reviewed by a selection committee. The committee may request additional information from proposers or request personal interviews with one or more proposers. Final evaluation and selection may be based on, but not limited to, any or all of the following:

- Delivery Time
- Information presented in the proposal
- Flexibility and capability of proposed system
- Qualifications and experience of the proposer
- Quality
- Reference Checks
- Technical Support
- Total Cost

#### **4.4.6 Payment**

The vendor will charge no more than the price agreed to unless a change in the scope of work. The schedule and price are to be agreed upon by the vendor and Brunswick County.

## 5 Terms and Conditions

**5.1 BRUNSWICK COUNTY MINIMUM INSURANCE COVERAGE REQUIREMENTS** -At contractor's expense, contractor shall procure and maintain the following recommended lines of insurance according to the scope of work. The County may choose to elect higher or lower coverages according to the work performed. Contractors must be insured by a licensed agent in North Carolina and rated A-VII or better by A.M. Best.

**5.1.2 A. COMMERCIAL GENERAL LIABILITY** Covering all operations involved in this Agreement.

\$2,000,000 General Aggregate  
 \$2,000,000 Products/Completed Operations Aggregate  
 \$1,000,000 Each Occurrence  
 \$1,000,000 Personal and Advertising Injury Limit  
 \$ 5,000 Medical Expense Limit

**5.1.3 WORKERS' COMPENSATION**

Statutory limits covering all employees, including Employer's Liability with limits of:  
 \$500,000 Each Accident  
 \$500,000 Disease - Each Employee  
 \$500,000 Disease - Policy Limit

**5.1.4 COMMERCIAL AUTOMOBILE LIABILITY**

\$1,000,000 Combined Single Limit – Any Auto

**5.1.5 PROFESSIONAL LIABILITY**

\$1,000,000 Per Occurrence

**5.2 ADDITIONAL INSURANCE AND INDEMNIFICATION REQUIREMENTS**

**5.2.2** Contractor agrees to defend, indemnify, and hold harmless Brunswick County, its officers, employees, and agents from and against any and all losses, penalties, damages, settlements, costs, charges, professional fees, or other expenses or liabilities of every kind and character arising out of or relating to any and all claims, liens, demands, obligations, actions, proceedings, or causes of action of every kind in connection with or arising out of this Agreement and/or the performance hereof that are due in part or in the entirety of Contractor, its employees or agents. Contractor further agrees to investigate, handle, respond to, defend and dispose of same at its sole expense and agrees to bear all other costs and expenses related thereto.

**5.2.3** Before commencement of any work or event, Contractor shall provide a Certificate of Insurance in satisfactory form as evidence of the insurances required above.

**5.2.4** Contractor shall have no right of recovery or subrogation against Brunswick County (including its officers, agents and employees), it being the intention of the parties that the insurance policies so affected shall protect both parties and be primary coverage for any and all losses covered by the above-described insurance.

- 5.2.5** Brunswick County shall have no liability with respect to Contractor's personal property whether insured or not insured. Any deductible or self-insured retention is the sole responsibility of Contractor.
- 5.2.6** All certificates of insurance must provide that the policy or policies shall not be changed or cancelled without at least thirty (30) days prior written notice.  
The Certificate of Insurance should note in the Description of Operations the following:  
Department: \_\_\_\_\_  
Contract #: \_\_\_\_\_
- 5.2.7** Insurance procured by Contractor shall not reduce nor limit Contractor's contractual obligation to indemnify, hold harmless and defend Brunswick County for claims made or suits brought which result from or are in connection with the performance of this Agreement.
- 5.2.8** In the event Contractor receives Notice of Cancellation of Insurance required pursuant to this Agreement, Contractor shall immediately cease performance of all services and shall provide Notice to Brunswick County's Legal/Risk Management personnel within twenty-four (24) hours.
- 5.2.9** Certificate Holder shall be listed as follows;  
ATTENTION: Brunswick County Risk Manager  
30 Government Center Dr. NE  
P.O. Box 249  
Bolivia, NC 28422
- 5.2.10** If Contractor is authorized to assign or subcontract any of its rights or duties hereunder and in fact does so, Contractor shall ensure that the assignee or subcontractor satisfies all requirements of this Agreement, including, but not limited to, maintenance of the required insurances coverage and provision of certificate(s) of insurance and additional insured endorsement(s), in proper form prior to commencement of services.

# New Datacenter Acceptance of Terms

Company Name: \_\_\_\_\_

Contact Person: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Proposed Price: \_\_\_\_\_

I certify that all above listed information is correct and that I and my company will agree to meet or exceed all requirements as outlined in the Request for Proposal.

\_\_\_\_\_  
Name, Title (Print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date