

29. Cisco Technology Products

- Action:**
- A. Approve contracts for providing Cisco technology products and services for the term of five years in the estimated annual amount of \$2,000,000 to the following vendors:**
 - 1. CDW-Government**
 - 2. DISYS**
 - 3. NWN**
 - B. Authorize the City Manager to approve up to two, one-year renewal options with possible price adjustments as authorized by the contract.**

Staff Resource: Charles Robinson, Business Support Services

Explanation:

- Cisco products are used for the City's technology network infrastructure.
- Each live network jack in the City is powered by a Cisco switch. These switches connect to other Cisco switches, routers, wireless hotspots and firewalls to form the majority of the City network infrastructure.
- The infrastructure connects every City user to all of the applications and services that are used to complete their daily work, including but not limited to 911, 311, Charmeck.org, email and public safety radio.
- Recent additions to the network include the City traffic control system and environmental controls in buildings from CMGC to the Mint Museum of Art.
- Business Support Services issued a Request for Proposal (RFP) to provide Cisco Products and Services to the City of Charlotte on behalf of the Charlotte Cooperative Purchasing Alliance (CCPA).
- The CCPA is a cooperative purchasing group developed by BSS/PSD. The CCPA is designed to competitively solicit and secure contracts for the purchase of goods and services that may be used by other public agencies regionally and nationwide. The City will receive an administrative fee of 1% to 2% for all participating public agency sales volumes with the potential to generate \$100,000 in revenue.

Selection Process

- In response to the RFP, the City received eight proposals.
- The Evaluation Team, comprised of staff from Business Support Services, IT and Procurement Services evaluated service providers on the following criteria:
 - Background and experience of the company, including references
 - Operational qualifications of personnel
 - Customer service approach
 - Business processes
 - Insurance requirements
 - Willingness and ability to comply with the RFP and contract terms and conditions
 - Trade-in credits and
 - Cost of service provision, to include but not limited to, administrative fees
- After thorough evaluation, the Evaluation Team unanimously recommends CDW Government, DISYS Solutions, Inc., and NWN Corporation as the service providers that best met the established requirements.

Small Business Opportunity

No SBO goal was set for this contract because subcontracting opportunities are not anticipated (Part C; Section 2.4 of the SBO Policy).

Funding

Various KBU operating budgets on individual as needed basis

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

FIRST AMENDMENT TO THE CONTRACT TO PROVIDE
CISCO PRODUCTS AND SERVICES

THIS FIRST AMENDMENT TO THE CONTRACT TO PROVIDE CISCO PRODUCTS AND SERVICES (the "Master Contract") is made and entered into this 9th day of January, 2012 (the "Amendment Effective Date"), by and between NWN Corporation, a Delaware corporation doing business in North Carolina, (the "Company") and the City of Charlotte, a North Carolina municipal corporation (the "Lead Public Agency").

Statement of Background and Intent

- A. WHEREAS, the Lead Public Agency and the Company entered into a contract for the Company to provide Cisco Products and Services dated April 11, 2011; and
- B. WHEREAS, the Lead Public Agency has selected the Company to provide the Company's Hosted Cisco Unified Communications Solution with Contact Center Enterprise and nCare Managed Services (the "Hosted Services").

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the parties hereby agree to the following:

A G R E E M E N T

1. Defined terms used in this Amendment shall have the same meaning as are assigned to such terms in the Master Contract.
2. Changes to the Master Contract. In order to effectuate the intent of the parties, the Master Contract is hereby amended as follows:
3. This First Amendment Hereby modifies the Master Contract to incorporate **Exhibit F**: Statement of Work for Cisco Unified Workspace / Contact Center Implementation – Hosted, and **Exhibit G**: Confidentiality Agreement, both of which are attached hereto.
4. This First Amendment hereby appends the list of exhibits in **Section 1** of the Master Contract to add the following:
"Exhibit F: Statement of Work for Cisco Unified Workspace / Contact Center Implementation – Hosted
Exhibit G: Confidentiality Agreement"
5. Unless terminated in accordance with the terms of the Master Contract or **Exhibit F**, Statement of Work for Cisco Unified Workspace / Contact Center Implementation – Hosted, shall commence on the Amendment Effective Date and continue through March 31, 2015, with the Hosted Services commencing on April 1, 2012. The Lead Public Agency shall have an option to renew for two (2) additional one (1) year terms thereafter. If the Lead Public Agency does not exercise the first renewal option, the Lead Public Agency must give the Company notice of such intent at least ninety (90) days prior to the end of the original term and pay the Company a one-time termination fee of \$312,500. If the Lead Public Agency exercises the first renewal option but does not exercise the second renewal option, the Lead Public Agency must give the Company notice of such intent at least ninety (90) days prior to the end of the first renewal term and pay the Company a one-time termination fee of \$156,250.

6. Except to the extent specifically provided above, this First Amendment shall not be interpreted or construed as waiving any rights, obligations, remedies or claims the parties may otherwise have under the Master Contract.
7. In all other respects and except as modified herein, the terms of the Master Contract shall remain in full force and effect.

IN WITNESS WHEREOF, and in acknowledgement that the parties hereto have read and understood each and every provision hereof, the parties have caused this Amendment to be executed as of the date first written above.

NWN CORPORATION:

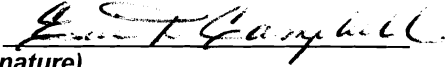
BY: 
(signature)

PRINT NAME: MICHAEL KANE

TITLE: REGIONAL SALES DIRECTOR

DATE: 1/6/12
dated by ACT with direction

CITY OF CHARLOTTE:

BY: 
(signature)

PRINT NAME: ERIC D. CAMPBELL

TITLE: ASSISTANT CITY MANAGER

DATE: 1/9/2012

ATTESTED:

CITY OF CHARLOTTE
CITY CLERK'S OFFICE

BY: 
(signature)

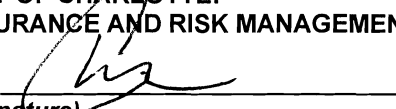
PRINT NAME: Ashleigh Price

TITLE: Deputy City Clerk

DATE: 1/9/12

CITY OF CHARLOTTE:

INSURANCE AND RISK MANAGEMENT

BY: 
(signature)

PRINT NAME: Christer Gibson

TITLE: Ins. Manager

DATE: 1/9/12

**EXHIBIT F
Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work**

CONTACT INFORMATION

CITY OF CHARLOTTE	OFFICE	MOBILE	EMAIL
Bellverie E. Ross	704.432.5627		bross@ci.charlotte.nc.us
Kimberly Laney	704.582.2057		kwlaney@ci.charlotte.nc.us
Greg Thomas	704.432.4070	704.507.3035	gtthomas@ci.charlotte.nc.us
Doug Symonds	704.432.8404	980.722.8401	dsymonds@ci.charlotte.nc.us
NWN CORPORATION & PARTNERS			
Rodger Bakken	704.496.6917	704.562.0835	rbakken@nwnit.com
Jeremy Maynard	919.653.4449		jmaynard@nwnit.com
Alvaro Riera	704.496.6906		ariera@nwnit.com
Greg Syer	919.653.4477		gsyer@nwnit.com
Chris Ludwig	919.653.4409		cludwig@nwnit.com
Wen-Kai Ho (SimpliCTI)	919.858.8898 x104		who@simplici.com
Steven Hollowell (SimpliCTI)	919.858.8898 x111	252.327.2651	shollowell@simplici.com
Amy Sanger (Cisco)	704.338.7340	704.724.3588	asanger@cisco.com
Perry Moon (Cisco)	336.931.4774	336.402.6683	pemoon@cisco.com

PROJECT OVERVIEW

The City of Charlotte (the "Lead Public Agency") has engaged NWN Corporation (the "Company" or "NWN") to perform the Professional Services defined in this document for the implementation of a Hosted Cisco Unified Communications System with nCare Managed Services aimed to support the Lead Public Agency's replacement of the existing Avaya platform for the Call Center and Customer Interaction System.

The scope of this project is split into two phases that will be executed in parallel to the extent feasible. The first phase covers the Hosted Unified Communications Manager ("UCM") and the customer premise equipment necessary to support the collaborative applications. The second phase covers the Hosted Unified Contact Center Enterprise ("UCCE") services and integration performed jointly with Company's partner SimpliCTI.

In the UCM phase, Company shall:

- Review the current configuration of the network infrastructure and provide recommendations for the implementation best practices for the support of the Unified Communications System.
- Implement an MPLS circuit between the City of Charlotte and the NWN hosted facility of Windstream in Raleigh, North Carolina.
- Provide Hosted Cisco Unified Communications Manager Cluster 8.6 as a service to the Lead Public Agency for three hundred (300) users.
- Integrate the Hosted Cisco Unified Communications Cluster with the Lead Public Agency's current Voicemail platform (AVST) using SIP.
- Install and Configure redundant Cisco ISR 2900 PRI Voice Gateways.

- Assist the Lead Public Agency's staff with the rollout and installation of Cisco IP Communicator 8.6 on the end users' desktop.
- Train the Lead Public Agency's staff on the use of the Cisco IP Communicator and the feature/functionality enabled in the system.
- Provide system documentation.

This platform will provide the Lead Public Agency with an enterprise-class hosted IP communications processing system for up to 30,000 users. In addition to traditional telephony features, it provides advanced capabilities, such as video, mobility, presence, preference, and full-featured conferencing services hosted services as needed.

The new Hosted Collaboration solution proposed by Company will allow the Lead Public Agency to cost-effectively access a wide range of Unified Communications applications and services, available in a comprehensive subscription based offering. It packages Lead Public Agency wide applications and client software subscriptions on a per-user basis.

In the UCCE phase, Company shall (This is explained in greater detail in Appendix 2): Design, install/configure, test (unit testing through User Acceptance Testing), and provide production cutover and knowledge transfer for:

- 200 concurrent UCCE licenses
- ICM scripting in support of call routing when calls are transferred from GetAbby to UCCE
- Out of the box standard Intelligence Center 8
- Historical Data Server and Administrative Workstation
- Roggers Side A and Side B
- PGs (Side A and Side B) for supporting 10 ports of GetAbby
- 200 IPIVR Queuing Ports (100 Side A, 100 Side B)
- Integration of the new Contact Center application with the existing GetAbby and Verint Impact 360 applications
- Integration of Verint Impact 360 to UCCE for Workforce Optimization
- Install and configure two Verint PGs (Side A and Side B)
- Configure and connect Verint PGs with Verint Impact360
- Configure and test failover between two Verint PGs
- Flow design and ICM scripts modification
- System regression testing and Cutover

Lead Public Agency Success Criteria

- Successful implementation of Hosted Collaboration subscription service.
- Integration of hosted Cisco Unified Communications Manager with AVST
- Successful implementation of Hosted Unified Contact Center Enterprise (UCCE)
- Successful integration of the Hosted UCCE with GetAbby
- Successful integration of the Hosted UCCE with Verint Impact 360
- Successful training of the Lead Public Agency's selected Trainers for the Hosted UC phones, Billing & Reporting application and UCCE application
- Successful implementation of the ICI Telemangement Application for Billing & Reporting

SCOPE DETAILS – WORK TO BE PERFORMED

Scope Summary

The Lead Public Agency has engaged Company for the implementation of a hosted Cisco-powered Unified Communications System. During this project Company will:

- Review the current configuration of the network infrastructure and provide recommendations for the implementation best practices for the support of hosted collaboration applications.
- Implementation of redundant 3MB MPLS WAN circuits between Company's Raleigh, NC hosted facility and the City of Charlotte, which Company will work with the Lead Public Agency and the MPLS vendor to ensure effective capacity management to meet the expectations of the Lead Public Agency.
- Provision a Cisco-powered Unified Communications Manager Cluster 8.6 dedicated to the Lead Public Agency.
- Integration of the hosted Unified Communications Cluster with the Lead Public Agency's current Voicemail platform (AVST) using SIP.
- Integration of the hosted Unified Contact Center Enterprise with the Lead Public Agency's GetAbby and Verint solutions.
- Installation and configuration of redundant Cisco ISR 2900 two port PRI voice gateways.
- Assist the Lead Public Agency's staff with the rollout and installation of the Cisco IP Communicator 8.6 software on the three hundred (300) end users' desktop.
- Validate operation of the hosted collaboration software and Integration with AVST.
- Coordinate with Service Providers the provisioning, installation and turn-up of any Data and Voice circuits required during the implementation.
- Train the Lead Public Agency's staff on the use of the Cisco IP Communicator and the feature/functionality enabled in the system.
- The Company Hosted Communications Solution will provide Billing and Reporting functionality for the Lead Public Agency via the ISI Telemanagement Solutions application.
- Provide system documentation.

Project Management

A Company Project Manager will be assigned to this project, utilizing the Company project methodology (see Appendix 1), to ensure the successful delivery of this initiative as defined in this scope. The following outlines the roles and responsibilities of the Company Project Manager:

- Act as a single point-of-contact between Company and the Lead Public Agency as well as coordinate all work between Company, Cisco, SimpliCTI, AVST, GetAbby & Verint.
- Ensure thorough project communication with project stakeholders and team members
- Develop & maintain detailed project plan, task plan, schedule & communications plan
- Prepare, distribute & communicate regular status, action item & related project reports
- Manage project scope and respond to change requests
- Define and manage the escalation process
- Conduct project kickoff, status, milestone and review/closure meetings
- Review all Project Documentation and Deliverables
- Oversee knowledge transfer

1 – Initiate Phase:

- Internal kickoff meeting – this meeting involves the Company Sales Team and the Company Implementation Team. At this meeting, the entire Company team is made aware of the Lead Public Agency's expectations that were set during the Sales process to ensure all communication is translated to the Implementation Team for the on-site work effort.
- External kickoff meeting – this meeting involves the Company team and the Lead Public Agency's Team and usually takes place at the Lead Public Agency's site. During this meeting, all aspects of the project will be reviewed and established. This includes, but is not limited to: logistics management, roles and responsibilities of all project team members, draft schedule, task plan and work breakdown structure (WBS), communications plan and design and implementation approaches.
- Scheduling for Design and status meetings – Company and Lead Public Agency will work together to identify resources for project and coordinate schedules for the Design and Status meetings.

Deliverables:

- External Kickoff Meeting
- Schedule for Design and Status Meetings
- Draft Roles & Responsibilities Matrix
- Draft Communications Plan
- Draft WBS

2 – Plan & Design Phase:

- Database Gathering – Company will provide the customer with a User Database form. This form will be completed by the client and reviewed at the Design Meeting.
- Network Configuration Review – Company will review the current configuration of the network infrastructure to be used to support the hosted collaboration applications to guarantee compliancy with Cisco and Company best practices and recommendations. Based on the status of the network Company will provide the Lead Public Agency with recommendations in regards to the corrective actions to be taken to bring the network into compliancy with the best practices and recommendations. These recommendations are then to be implemented by the Lead Public Agency in preparation to the deployment of the hosted collaboration services.
- Network Design Meeting - After the kick-off meeting, Company and the Lead Public Agency's team will hold a network design meeting to discuss the findings from the network configuration review and the technical aspects of the Network Infrastructure. Company expects the Lead Public Agency will come prepared with documentation and resources necessary to cover all topics. These topics will include:
 - Quality of Service (QoS) and security best practices
 - Hardware/software version review
 - IP Routing and IP Addressing
 - VLAN Layout
 - Redundant WAN circuit design
- Hosted Unified Communications Design Meeting – After the kick-off meeting, Company and the Lead Public Agency's team will hold a design meeting to discuss the technical aspects of the hosted Unified Communications services. Company expects the Lead Public Agency will come prepared with documentation and resources necessary to cover all topics. These topics will include:
 - Hosted Unified Communications best practices
 - Architecture and Software version features review
 - Unified Communications device compatibility check

- Unified Communications Upgrade Paths
- Migration strategies
- User database review
- Auto-Attendants and specialized voice-mail options
- Dial Plan
- Discussion of downtime and risks

Deliverables:

- *Design meeting and project plans for implementation of Unified Communications solution.*
- *Design meeting and project plans for implementation of Unified Contact Center Enterprise solution*
- *Agreed Upon Acceptance Plan and Process Document*
- *Agreed Upon Change Control Process Document*

3 – Execute Phase

- Hosted Application Provisioning – Company will provision two hosted Cisco Unified Communication Manager servers running version 8.6.1(a). This will provide call processing services for the Lead Public Agency's three hundred (300) softphone users utilizing the WAN connection between Company and the City of Charlotte.
- Equipment Staging – Company will configure the two (2) Cisco ISR 2921 Routers and Cisco WAN devices. The staging and configuration of the new servers will be performed at the local Company staging facility and will include:
 - Equipment inventory.
 - Equipment burn-in to validate proper operation and process any necessary replacements.
 - Complete configuration of two (2) Cisco 2921 routers as H.323 gateways with SRST feature set.
 - 0800202 CUCM System, Call Routing, Media Resources, Devices and Users Configuration.
 - Bulk Administration Tool Templates and files.
 - Cisco Unified Mobility (Single Number Reach) Configuration.
 - Company will ensure that database replication is functioning between the CUCM cluster.
 - Company will perform a complete system test and validate all functionality.
 - Company will perform a complete system test and validate all functionality paying special attention to the following features:
 - ANI preservation when transferring calls to and from GetAbby (NOTE: In order to preserve the ANI for each call, all calls will be routed by the ICM (Intelligent Call Module) component of UCC Enterprise. The ICM component then matches the ANI with a call that is being transferred back from GetAbby.)
 - Transfer of emergency calls from Contact Center agents
- Onsite Installation – After verifying all functionality, Company will pack the Cisco equipment and transport it to the hosting location where it will be again unpacked and installed for the completion of the following tasks:
 - Complete LDAP Integration with customer environment.
 - Installation and testing of WAN and PSTN circuits
 - Complete AVST (Voicemail) SIP Integration.
 - Validate all system configuration and functionality.

- Assist the Lead Public Agency's staff with the deployment of the Cisco IP Communicator software on the user's desktop.
 - SimpliCTI will perform installation and configuration on GetAbby and Verint Peripheral Gateways (PGs).
- Train the Trainer Training – The training to be provided as part of this project will be in the form of "train the trainers" for which Company will be responsible for:
 - Develop training plan and customize training material.
 - Deliver up to two (2) Phone User training session to a group of Lead Public Agency trainers not to exceed fifteen (15) trainers in each training session.
 - Provide the Lead Public Agency with the "end-user" training material in the form of Quick User Guides and Web Based Tutorial for future use in both electronic and master printed format.
 - Network, PSTN and Analog Connections – Company will provide the customer with requirements for all internal network connections. It is the Lead Public Agency's responsibility to provide any necessary cables, connections, panels and labor associated with bringing PSTN, internal network or internal analog cabling to the equipment. All connections must be identified prior to the start of the project. Company does not provide cabling services of any kind.
 - WAN Connectivity – Company will provide the customer premise equipment required for WAN connectivity back to Company's hosted facility. Connectivity will be through a 3MB MPLS circuit.
 - New System Migration – After the Lead Public Agency staff delivers training to the end users as per the training plan and as per the previously agreed upon implementation schedule Company will complete the system migration and remain onsite to provide First Day Support after the cut.
 - Network/System Troubleshooting – Company will troubleshoot and diagnose technical issues associated with this project. Any issues not related to the agreed upon SOW for Unified Communications will require a change order and may affect the schedule of events planned for this project. Company will work with the customer to isolate and identify network/system issues as well as provide assistance within reasonable boundaries. Any issues outside the scope of this project are the responsibility of the customer.
 - First Day in Service Support – Company will remain on site to help address and diagnose any problems that arise during the Unified Communications deployment within the scope of this project as each phase is brought onto the system. Company will troubleshoot configuration and integration issues arising from this project. First Day Support does not include additional Moves, Adds, or Changes. Company and the Lead Public Agency will formalize a detailed list of open items. Open items within the scope of this project will be addressed and resolved. Open items deferred due to Lead Public Agency availability will require a change order to complete.

To assist the Lead Public Agency with the implementation of HCS for users who have Virtual Desktop clients, Company agrees to provide the Lead Public Agency with up to three hundred (300) SIP enabled telephones at no additional cost. If the Lead Public Agency desires to use Softphones on Virtual Desktop clients at a future time, please refer to Appendix 3, "Concerns Regarding Implementation of Softphones on Virtual Desktops".

Deliverables:

- *Delivery of the detailed Bill of Materials (BOM) equipment &/or software components as identified in the Reference Materials section of this document.*
- *Installation and Configuration of the following based on parameters referenced in the approved Design Document:*
 - *Provisioning of a hosted two server Cisco Unified Communications Manager version 8.6 cluster dedicated for the Lead Public Agency*
 - *Installation of Cisco ISR 2921 voice gateways with SRST services*
 - *Installation of Cisco MPLS WAN gateway*
 - *Integration of CUCM with AVST*
 - *Integration of UCCE with GetAbby & Verint*
 - *Strategy for the deployment of Cisco IP Communicator 8.6*
 - *Go Live*
- *First Day Support*

4 – Close Phase

In this phase, on site engineering is complete. Engineers will be focused on completing technical documentation and a review with project team. The Company Project Manager will verify approval for final billing and schedule and complete Project Review and Closure meetings with the Lead Public Agency.

Deliverables:

- *Technical documentation, to include:*
 - *Technical workbook including site specific configuration information*
 - *Quick Reference Guides, Admin & configurations guides from manufacturer*
 - *All manufacturer's manuals and documents received with products*
- *Project documentation, to include:*
 - *Project plan &/or task list, including work schedules*
 - *Status reports (written and/or verbal)*
 - *Action item list & Issues reports*
 - *Roles & Responsibilities Matrix for ALL Parties, including Company Help Desk & Third Party Applications*

Out of Scope

Any area not specifically presented in the Scope section of this proposal is considered outside the scope of this project. Changes to the scope as detailed in this proposal require an estimate review and must be approved by mutual agreement. Additional (or lower) charges may apply to incorporate the requested changes. Changes will not become effective until agreed upon in writing by both the Lead Public Agency and Company.

CUSTOMER REQUIREMENTS & ASSUMPTIONS

Technical requirements/ assumptions:

- 1) Lead Public Agency will perform and/or provide the following design/technical components as part of the delivery of this project:
 - a) Provide current network design.
 - b) Provide IP address schema and design specs.
 - c) Participate in all design and planning sessions and be prepared to sign off on all milestones.
 - d) Third party delays are recognized and accounted for
 - e) Lead Public Agency provided information is correct and current
- 2) Lead Public Agency must provide an acceptable workspace, an outside phone and Internet access, at no additional charge, for all Company staff when onsite as required to assist the Lead Public Agency throughout this project.
- 3) Lead Public Agency will ensure LAN Infrastructure is in place and configured to support Cisco Unified Communications. In the event Company is asked to assist the client with LAN configurations, a Change Order will be issued for additional services
- 4) Lead Public Agency is responsible for all hardware, software, licensing, maintenance or other required resources not explicitly listed on the Bill of Materials and subsequent Purchase Order.
- 5) Company is not responsible for configuration changes on any equipment not specifically stated in the above Statement of Work. This includes IOS upgrades on existing equipment.
- 6) Company is not responsible for any unknown hardware or software that may not be compatible with Unified Communications version 8.
- 7) Lead Public Agency is responsible for all LAN and WAN configuration work effort to establish proper internal network connectivity in this scope of work.
- 8) Lead Public Agency is responsible for all existing switch and router configuration work needed to establish proper connectivity in this Scope of Work unless otherwise noted in this Scope of Work.
- 9) The Lead Public Agency will ensure that all structured wiring and structured wiring components are in place and operational to support the efforts in this project.
- 10) The Lead Public Agency will ensure that adequate electrical power, UPS, and surge protection are in place and operational to support hardware and software listed on this project.
- 11) Equipment racks, shelves, and environmental requirements such as heating and cooling are the responsibility of the customer. Company will provide the Lead Public Agency with these requirements upon request.
- 12) The Lead Public Agency is responsible for existing switch, router, and firewall configurations that may be required to complete this project. If Company assistance is requested a change order will be required.
- 13) The work effort in this proposal assumes a continuous work effort that is established at the beginning of the project based on a project plan. If delays occur in the installation process due to Lead Public Agency related issues, then a change order will need to address any additional costs that arise due to this delay.
- 14) Company is not responsible for configuration changes on any equipment not specifically stated in this Statement of Work.
- 15) Lead Public Agency will install and configure any IOS upgrades and/or maintenance patches to existing hardware such as voice gateways, analog interface devices, etc. that may be required.

Operational requirements/ assumptions:

- The Lead Public Agency will assign a representative to this project, who will coordinate the installation activity with the Company Project Manager.
- The Lead Public Agency will provide access to all work locations along with safety, access, security & emergency protocols.
- As needed, the Lead Public Agency will provide a work area for Company to use during on-site activities to include Internet and public phone network access.
- The work effort in this proposal assumes a continuous work effort that is established at the beginning of the project based on a project plan. If delays occur in the installation process due to Lead Public

Agency related issues, then a change order will need to address any additional costs that arise due to this delay.

- Lead Public Agency and Company will mutually agree upon downtime prior to any installation and ensure this downtime is scheduled in advance so the Lead Public Agency can make appropriate preparations at the facility.
- The Lead Public Agency will provide parking passes and adequate parking for the Company project team at the CGMC Parking facility ONLY.
- When applicable the Lead Public Agency will provide the best possible prints and floor plans for use during the installation. These prints and floor plans will become the property of Company.

TERMS & CONDITIONS

1. If the project is put on hold due to customer delays for a period over sixty (60) days the Lead Public Agency and Company will work together to address closure of the existing project. A Project Change Request will be provided that addresses how to handle remaining billing on the project as well as how the remaining tasks will be completed. Re-scheduling the project is subject to existing Company workload and will be scheduled accordingly.
2. The Contract to Provide Cisco Products and Services dated April 11, 2010 in place between Company and the Lead Public Agency (the "Master Contract") serves as the general terms and conditions of these services. This Statement of Work presents the specific details of this project under that Master Contract. These terms are supplemental to the Master Contract; any point of conflict defaults to the terms and conditions presented in the Master Contract.
3. Prices do not include State sales tax or freight which is billed to the Lead Public Agency. Any additional shipping required is not included in the presented pricing.
4. Quotation for Services does not include travel and expenses, which will be billed at actual cost. Any travel and/or expenses must be approved by the Lead Public Agency prior to being incurred or billed. If the Lead Public Agency approves such travel and/or expenses, this section will apply. As used in this Statement of Work the term "Out-of-Pocket Expenses" shall mean the following expenses which are actually incurred by employees of the Company or its subcontractors who live outside of a 100 mile radius of Charlotte, North Carolina and who travel to Charlotte in the performance of the Services, provided that such expenses shall not exceed the limits set forth in the then current version of IRS Publication 1542.
 - Lodging at a local hotel;
 - A per diem meals reimbursement as permitted in the then current version of IRS Publication 1542;
 - Parking, tolls, or rental car; and
 - Reasonable travel costs to and from the City locations.

For Company or subcontractor employees who stay in Charlotte over extended time periods, the Company will rent an apartment in the Charlotte area if doing so proves to be more economical on a monthly average. Otherwise, the Company will attempt to obtain accommodations at the same rates as those applicable for federal government employees. The Company will attempt to minimize travel costs by obtaining the lowest fares reasonably practicable under the circumstances.

All Out-of-Pocket Expenses must be invoiced separate from the Hosted Services and shall detail all services performed and shall itemize in detail and provide documentation and actual receipts for all Out-of-Pocket Expenses for which the Company seeks reimbursement. The parties acknowledge that the Out-of-Pocket Expenses will only be paid based on the Company submitting the actual receipts along with the required invoice.

5. Unless other specified, working hours for engineering services are normal business hours (8:00 am to 5:00 pm), Monday through Friday with no limitations of access to the workplace. Work performed after normal business hours will be billed at an additional charge.

6. Professional Services will be invoiced per the terms specified in Project Financials below.

7. Termination Clause(s)

a. TERMINATION FOR DEFAULT BY EITHER PARTY.

By giving written notice to the other party, either party may terminate this Statement of Work upon the occurrence of one or more of the following events with no penalty or buyout:

- The other party violates or fails to perform any covenant, provision, obligation, term or condition contained in the Master Contract or this Statement of Work, provided that, unless otherwise stated in the Master Contract or this Statement of Work, such failure or violation shall not be cause for termination if both of the following conditions are satisfied: (i) such default is reasonably susceptible to cure; and (ii) the other party cures such default within thirty (30) days of receipt of written notice of default from the non-defaulting party; or
- The other party attempts to assign, terminate or cancel the Master Contract or this Statement of Work contrary to the terms hereof; or
- The other party ceases to do business as a going concern, makes an assignment for the benefit of creditors, admits in writing its inability to pay debts as they become due, files a petition in bankruptcy or has an involuntary bankruptcy petition filed against it (except in connection with a reorganization under which the business of such party is continued and performance of all its obligations under the Master Contract and this Statement of Work shall continue), or if a receiver, trustee or liquidator is appointed for it or any substantial part of other party's assets or properties.

Any notice of default shall identify this Section of this Statement of Work and shall state the party's intent to terminate this Statement of Work if the default is not cured within the specified period.

Notwithstanding anything contained herein to the contrary, upon termination of the Master Contract or this Statement of Work by either party for default, the Company shall continue to perform the Services required by this Statement of Work for the lesser of: (i) six (6) months after the date the terminating party delivers a written termination notice; or (ii) the date on which the Lead Public Agency completes its transition to a new Service Provider.

b. ADDITIONAL GROUNDS FOR DEFAULT TERMINATION BY THE LEAD PUBLIC AGENCY.

By giving written notice to the Company, the Lead Public Agency may also terminate this Statement of Work with no penalty or buyout upon the occurrence of one or more of the following events (which shall each constitute grounds for termination without a cure period and without the occurrence of any of the other events of default previously listed):

- Failure of the Company to complete a particular task by the completion date set forth in this Statement of Work;
- The Company makes or allows to be made any material written misrepresentation or provides any materially misleading written information in connection with this Statement of Work, or any covenant, agreement, obligation, term or condition contained in this Statement of Work; or
- The Company takes or fails to take any action which constitutes grounds for immediate termination under the terms of the Master Contract or this Statement of Work, including but not limited to failure to obtain or maintain the insurance policies and endorsements as required by the Master Contract, or failure to provide the proof of insurance as required by the Master Contract.

The foregoing termination provisions shall not affect either party's right to terminate the Master Contract according to the terms of the Master Contract.

8. DATA SECURITY AND PRIVACY

- a. **Contract Data.** The parties acknowledge that the Lead Public Agency has exclusive ownership of all data generated, provided to or made available to the Company in connection with this Statement of Work, and all report structures in which such data are reported (the "Contract

- Data”). The Company will treat the Contract Data as Confidential Information under the Confidentiality Agreement in the Master Contract. The Company will not reproduce, copy, duplicate, disclose, or use the Contract Data in any manner except as necessary to perform this Statement of Work.
- b. **General Requirements.** With respect to Contract Data, the Company shall:
- Establish and maintain safeguards against the destruction, loss, unauthorized alteration of, or unauthorized access to the Contract Data;
 - Comply with all laws and regulations that may apply to the Contract Data, including without limitation all laws relating to identity theft;
 - Store all personal identifying information about individuals that the Lead Public Agency is prohibited from disclosing by law, including credit card numbers, in accordance with Peripheral Component Interconnect (or successor) standards then in effect (“PCI Standards”);
 - Encrypt all personally identifiable information and/or credit card data that is transmitted to or from the Company’s systems in connection with this Contract;
 - Ensure that Contract Data storage complies with all relevant laws, regulations and standards, including but not limited to states laws, and applicable regulatory and professional standards; and
 - Ensure that transmission of Contract Data to and from the Company’s system is secure.
- c. **Authentication.** The Company will require an authentication process approved by the Lead Public Agency as a condition to releasing Contract Data to Lead Public Agency employees. At a minimum, such process will require a Lead Public Agency user ID and password. It may also require validation challenge questions if specified by the Lead Public Agency in writing from time to time.
- d. **Preventing Unauthorized Access.** The Company shall take appropriate measures to protect against the misuse of and/or unauthorized access to the Contract Data, including the use of passwords and validated user identification for Company employees and take appropriate measures to address any such misuse or unauthorized access.
- e. **If Unauthorized Access Is Suspected.** The Company shall promptly investigate any suspicion or allegation of misuse or unauthorized access to Contract Data. If the Company learns or has reason to believe that Contract Data has been disclosed or accessed by an unauthorized party, the Company shall notify the Lead Public Agency immediately and shall take at the Company’s expense all remedial action required by law or as reasonably requested by the Lead Public Agency to remedy such disclosure or unauthorized access.
- f. **Lead Public Agency’s Right To Obtain Contract Data.** The Company shall provide the Lead Public Agency with prompt access to Contract Data when requested (subject to the authentication requirements referenced herein), which such access shall in any event be within five business days after the request. The Company shall retain all Contract Data through the duration of this Statement of Work. When requested by the Lead Public Agency from time to time, the Company shall provide the Lead Public Agency with a copy of all Contract Data accumulated to date (or such smaller subset as may be requested by the Lead Public Agency) in a format in which the Lead Public Agency can use, search, copy and access the Contract Data. Within thirty (30) days after expiration or termination of this Statement of Work for any reason, the Company shall: (a) return all Contract Data to the Lead Public Agency in a format in which the Lead Public Agency can use, search, copy and access the Contract Data; and (b) following such return destroy all copies of the Contract Data in the Company’s possession, except to the extent the Company is required to maintain copies of such Contract Data by state or federal law or regulation. If requested by the Lead Public Agency, the Company shall allow the Lead Public Agency access to the Company’s systems if reasonably needed to use, search, and copy or access the Contract Data. The Company shall comply with its obligations under this Section at no cost to the Lead Public Agency.

- g. **Transition Services.** Upon expiration or termination of this Statement of Work for any reason, the Company shall at no cost to the Lead Public Agency provide such services as are reasonably requested by the Lead Public Agency to transition the Contract Data to the Lead Public Agency or to another service provider, including without limitation providing information regarding data fields and data format and responding to questions.

PROJECT FINANCIALS

Company anticipates that the Hosted Communications Solution and Contact Center Enterprise system (the "Hosted Services") will go live on April 1, 2012. As a result, Company anticipates that it will begin invoicing for the Hosted Services on April 1, 2012; provided, however, that the Lead Public Agency will not be required to pay Company for the Hosted Services if the Hosted Services are not functioning in accordance with this Statement of Work. Invoicing will be on a quarterly basis with payments of \$119,136.00 (\$39,712.00 per month). As this Statement of Work is a part of the Master Contract, Company will pay the Lead Public Agency a 1% Administrative Fee in the amount of \$1,119.36 per quarterly billing.

5-Year Pricing – 3-Year Contract with Two 1-Year Renewal Options

300 Standard User Subscriptions (Monthly Fee)	\$6,600.00
Hosted Connectivity and Facility Charge (Monthly Fee)	\$8,800.00
Hosted Applications – Standard UCM Cluster (Monthly Fee)	\$1,000.00
Hosted Applications – 200 user Contact Center Enterprise (Monthly Fee)	\$23,312.00
Enablement Fee (One Time) waived	\$0.00
Total Monthly Investment	\$39,712.00

Company will provide the Lead Public Agency the above pricing based on an initial term of approximately thirty-nine (39) months with two (2) one (1) year renewal options. The initial term of this Statement of Work shall commence on the Amendment Effective Date, as that term is defined in the First Amendment to the Contract to Provide Cisco Products and Services, and end on March 31, 2015. It is anticipated that Hosted Services shall commence on April 1, 2012. If the first renewal period is exercised, that period will begin on April 1, 2015 and end on March 31, 2016. If the second renewal period is exercised, that period will begin on April 1, 2016 and end on March 31, 2017

If the Lead Public Agency chooses not to exercise the 1st renewal option, the Lead Public Agency shall provide Company a ninety (90) day notice of such intent and shall pay Company a one-time fee of \$312,500.00. If the Lead Public Agency chooses not to exercise the 2nd renewal option, the Lead Public Agency shall provide Company a ninety (90) day notice of such intent and shall pay Company a one-time fee of \$156,250.00. Above pricing includes a \$20,000.00 credit for the trade-in of the Avaya system, which Company will pick up from the Lead Public Agency's facility and properly dispose of once the Hosted Services are up and fully functioning.

(Per the CCPA Contract, Company will pay the Lead Public Agency \$397.12 each month for the required Administrative Fee).

If the first renewal period is exercised, Company will provide an upgrade to the HCS Solution to insure the highest quality of service to the Lead Public Agency.

Company's rates for adding additional users are indicated in this chart.

NWN Hosted Collaboration Pricing Model

*Does not include infrastructure or devices

Required Components	Description	Price Per Month 1 - 1,000 Users	Price Per Month 1001 - 3,000 Users	Price Per Month 3001 - 6,000 Users	Price Per Month 6001- 12,000 Users
Licensing per User or Device	<ul style="list-style-type: none"> ▪ Essential Devices ▪ Foundation ▪ Foundation + UM ▪ Standard ▪ Premium ▪ Contact Center UCCE 	<ul style="list-style-type: none"> ▪ \$ 4 ▪ \$14 ▪ \$19 ▪ \$22 ▪ \$26 ▪ \$89 	<ul style="list-style-type: none"> ▪ \$ 4 ▪ \$13 ▪ \$18 ▪ \$21 ▪ \$25 ▪ \$84 	<ul style="list-style-type: none"> ▪ \$ 4 ▪ \$13 ▪ \$17 ▪ \$20 ▪ \$25 ▪ \$79 	<ul style="list-style-type: none"> ▪ \$ 4 ▪ \$13 ▪ \$17 ▪ \$19 ▪ \$24 ▪ \$74
Applications per Customer Environment	<ul style="list-style-type: none"> ▪ Call Control HA ▪ Voicemail/UM HA ▪ Presence Server HA ▪ Paging ▪ Recording 	<ul style="list-style-type: none"> ▪ Included ▪ \$990 ▪ \$990 ▪ TBD ▪ TBD 	<ul style="list-style-type: none"> ▪ Included ▪ \$990 ▪ \$990 ▪ TBD ▪ TBD 	<ul style="list-style-type: none"> ▪ Included ▪ \$990 ▪ \$990 ▪ TBD ▪ TBD 	<ul style="list-style-type: none"> ▪ \$400 ▪ \$1800 ▪ \$1800 ▪ TBD ▪ TBD

NWN

Features included at each HCS licensing level are indicated in this chart

Hosted Collaboration Licensing Model

Hosted Collaboration Applications Bundles

Functionality	Collaboration Apps	Foundation	Foundation Plus Messaging	Standard	Premium
IP Telephony	Unified Communication Manager	●	●	●	●
Number of Devices		1	1	2	10
Mobility	Cisco Unified Mobility	●	●	●	●
Native Video	Video Endpoint(s)	●	●	●	●
Unified Messaging and Voice Mail	Unity Connection	○	●	●	●
Presence/IM/Chat	Cisco Unified Presence	○	○	●	●
Soft Client License	CUPC/CIPC/CUCI/CUVA	○	○	●	●
Smart Phone Integration	Cisco Mobile Clients	○	○	○	●
Video Conferencing	TelePresence	○	○	○	○
Web Conferencing	Cisco WebEx	○	○	○	○
Contact Center	Unified Contact Center	○	○	○	○

● Included ○ Optional Add-ons

N/A

APPENDICES

Appendix 1 – Project Delivery Methodology

This Appendix 1 is hereby incorporated into Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work, Exhibit F of the Contract to Provide Cisco Products and Services dated April 11, 2011 (the "Statement of Work").

Phases	Actions	Processes
Initiate	Identify / Define / Launch	
Plan & Design	Work Breakdown Structure Technical Designs Approach / Assess	
Execute	Staging / Lab/ Test/ Pilot Proof of Concept Migration/ Production	
Closure	Orientation / Care Plan Transition to Operations Wrap up & close out	

A Company Project Manager ("PM") will be assigned to this project, utilizing the NWN project methodology, to ensure the successful delivery of this initiative as defined in this scope. The PM will provide timely communications, status updates, project timelines and tasks, team activity coordination and issues management and escalation to the project sponsor. Based on the scope of work for the project the NWN PM will use the appropriate tools necessary to complete the project successfully.

In the event of changes that occur during the project the PM will process a Project Change Request ("PCR") to identify the needed change and effects it will have on the project along with funding that may be needed to complete the change. This PCR will be reviewed and agreed to by Company and Lead Public Agency prior to the change being implemented.

As phases are completed the Project Deliverables Acceptance document will be revised and discussed during status meetings. Percent complete will be documented and initialed by the Lead Public Agency so that recognition for progress can be acknowledged throughout the project. At the end of the project this document will be signed by the Lead Public Agency's project sponsor indicating that the project is complete.

Appendix 2 – UCCE Implementation

This Appendix 2 is hereby incorporated into Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work, Exhibit F of the Contract to Provide Cisco Products and Services dated April 11, 2011 (the "Statement of Work").

Proposed Environment

The Lead Public Agency is implementing Hosted Cisco's Unified Contact Center Enterprise (UCCE) for its 311 contact center and other Call Center environments. The 311 contact center is using GetAbby for self and assisted service. Cisco provides a Peripheral Gateway (PG) that establishes the integration of GetAbby with UCCE. In addition, The Lead Public Agency uses Verint for Workforce Optimization and an upgraded version of Verint will be integrated with the UCCE platform.

Solution Overview

The overall solution will entail design, installation/configuration, test (unit testing through User Acceptance Testing), production cutover and knowledge transfer for:

- 200 concurrent UCCE licenses
- ICM scripting in support of call routing when calls are transferred from GetAbby to UCCE
- Out of the box standard Intelligence Center 8
- Historical Data Server and Administrative Workstation
- Roggers Side A and Side B
- PGs (Side A and Side B) for supporting 10 ports of GetAbby
- 200 IPIVR Queuing Ports (100 Side A, 100 Side B)
- Integration of Verint to UCC Enterprise for Call Recording, Screen Capture and Workforce Optimizer:
 - Install and configure two Verint PGs (Side A and Side B)
 - Configure and connect Verint PGs with Verint Impact360 applications
 - Test the Call Recording and Screen Capture
 - Configure and connect Verint Workforce applications with UCCE CTI server
 - Test the Workforce applications
- System regression testing and Cutover

Specifically excluded from the scope of SimpliCTI's services in this Statement of Work includes (but is not limited to):

- "Screenpop" or any other integration of GetAbby collected information with UCCE
- Interactive Voice Response application development. IPIVR is being used for queuing only.
- Verint Impact 360 implementation or Verint services other than the integration of Impact 360 with UCCE.
- Desktop implementation or customization. CAD (Cisco Agent Desktop) will be running in the background.

Assumptions

This Statement of Work and SimpliCTI's ability to perform the work described in this document are based on the assumptions listed in this section. Invalidation of any of these assumptions at any time by

Company, the Lead Public Agency or SimpliCTI may have an impact on the work, schedule, fees, terms and/or conditions set forth in the Statement of Work. As the project progresses, some of the assumptions may change or become invalid. The parties agree that the failure of any of the described assumptions below will constitute an unanticipated event resulting in a possible delay of the project and increased costs.

- Two hundred (200) IPIVR Ports were estimated for queuing in the absence of call volume/Average Handling Time data. This number may go up or down depending on the actual call volumes/Average Handling Times.
- There is no IPIVR application development
- ICM scripting will be only for call routing once the call is handed-off from GetAbby to UCCE.
- The ten (10) GetAbby ports in the Bill of Materials were estimated based on the number of PRIs going into GetAbby; this number should be verified.
- SimpliCTI will generally perform all services and travel during normal business hours: 9:00 a.m. - 5:00 p.m. (United States Time Zones), Monday through Friday. Work performed outside of normal business hours must be negotiated through the Change Management process and additional fees will apply. Ten (10) hours of after-hours cutover support has been included in the price.
- SimpliCTI will perform some of the development and testing remotely from SimpliCTI work locations. High speed network access, such as through a VPN, must be provided by the Lead Public Agency to the SimpliCTI development team.
- Company will install, configure, test and cutover any required Unity Voice Mail boxes utilized by the call center.
- Any required customization of GetAbby or the 311 desktop applications is the responsibility of the Lead Public Agency.
- There is no CAD (Cisco Agent Desktop) in the 311 User Interface. Cisco Agent Desktop (CAD) provides contact center agents the call control through their desktop. However, the GUI portion of CAD is highly customizable and can be removed entirely when running CAD in the background.
- If the Lead Public Agency suspends, cancels or terminates this Statement of Work for any other reason than scoped within this project, the Lead Public Agency shall pay all reasonable amounts incurred for all analysis and work performed prior to such suspension, cancellation, or termination and a penalty fee of 15% of total fees.
- SimpliCTI will be ordering and provisioning the required UCCE and IPIVR software components only for this solution. All Cisco hardware and non-UCCE/IPIVR software will be provided by Company / Lead Public Agency. This includes general-purpose workstations for access to CUIS, and UCCE AW/HDS.
- The "out of the box" Standard CUIS reports will be utilized.
- The Cisco Unified Communications Manager (UCM) platform required servers, required voice gateways and network will be installed and operational prior to SimpliCTI starting implementation of the project.
- Tools built by SimpliCTI and utilized for this implementation are considered intellectual property of SimpliCTI Software Solutions.
- Some tasks in the Statement of Work will be performed in parallel with others and others are performed in a serial fashion.
- SimpliCTI will provide a 3-days UCC Enterprise Admin hands-on training. This will include understanding the process to add or remove an agent, create new reports, etc. For additional

training the Lead Public Agency is advised to participate in a certified Cisco class for UCE Administrators.

- If applicable, SimpliCTI will require Lead Public Agency to provide access to Lead Public Agency facilities and suitable workspace for all project team members when working at the Lead Public Agency facilities. Suitable workspace includes, but is not limited to, desks, telephones, analog line for dial-up access, and meeting rooms.
- A more specific list of project assumptions, requirements, roles and responsibilities will be developed jointly by Company / Lead Public Agency and SimpliCTI during the first week of this project.

Deliverables

SimpliCTI will provide Consulting Services (Services) and Deliverables (Deliverables) listed in this Statement of Work (SOW) to Lead Public Agency during the project.

All Services and Deliverables included in the SOW are described below. Any Services and Deliverables not described below which Lead Public Agency may request will be processed in accordance with the Change Management Process. The investigation and implementation of changes may result in modifications to the Estimated Schedule, Fees, and/or other terms of the Statement of Work, and shall be subject to approval by Company and Lead Public Agency and SimpliCTI. Any subsequent phases of the project will be estimated and priced separately.

Implementation Activities

These activities include all activities that will be performed regardless of the desired solution functionality. Activities are considered standard and are required for every UCCE Solution Implementation. Activities are as follows:

SimpliCTI will participate with the project team on a conference call to be held approximately one week prior to the commencement of the UCCE solution implementation to review the readiness of Lead Public Agency and the Lead Public Agency environment for the commencement of installation/configuration/test/cutover. The purpose of the call includes, but is not limited to:

- Ascertaining the readiness of the Lead Public Agency environment
- Addressing questions Lead Public Agency may have regarding the project

Lead Public Agency / Company shall ensure that the following resources are on the conference call. They should be prepared to validate that all platform pre-requisites have been met. These resources shall include:

- UCM System Administrator
- GetAbby and Verint System Administrators
- AVST Administrator
- Network Administrator

Requirements Analysis - SimpliCTI will lead and facilitate an interactive working solution requirements session to synthesize and validate Lead Public Agency specifications. During the interactive session the SimpliCTI consultant will walk through each Lead Public Agency in-scope requirement that is to be addressed by the UCCE solution. The solution requirements session will address the following.

- Lead Public Agency Architecture, both Server and Workstation
- Business rules and Workflows
- Functional Requirements

Project Initiation and Kickoff - the SimpliCTI Project Manager ("PM") will initiate the project as follows:

- Coordinate project logistics with Company and Lead Public Agency including estimated project start and end dates
- Confirm SimpliCTI associates are assigned to the project team
- Validate Company / Lead Public Agency resource support as defined in the Statement of Work
- Review project objectives with Company / Lead Public Agency and project team
- Establish project timelines and activity assignments
- Communicate the project schedule to Lead Public Agency and project team

The SimpliCTI PM will present a resource schedule to the Company PM for sign-off prior to the project start date. The SimpliCTI PM and Company PM will jointly develop a preliminary project schedule, prior to conducting the Project Kickoff meeting.

The SimpliCTI PM and Company PM will be responsible for planning the Project Kick-off meeting. The SimpliCTI PM will be responsible for leading the UCCE Project Kickoff meeting. The Company project manager will be responsible for acquiring adequate meeting space and equipment at the project location for the entire Project Team, and verifying attendance by Lead Public Agency personnel. The Project Kickoff meeting will include, but not be limited to, the following agenda items:

- Introduce the team members
- Review the preliminary project plan
- Present the approach, processes and procedures associated with the project
- Review Project Team member roles and responsibilities
- Review project deliverables
- Review product capabilities and architecture
- Review proposed solution
- Review knowledge transfer process

Solution Design - SimpliCTI will lead and facilitate an interactive working solution design session to validate Lead Public Agency design specifications where required. During the interactive session the SimpliCTI consultant will walk through each component of the UCCE Solution ("Solution") that is to be implemented and that requires Lead Public Agency specific design consideration. The Solution Design session will address the following:

- Solution Architecture
- Queues, Skills and Routing Rules
- Testing procedures

Solution Implementation – SimpliCTI will install/configure/customize the hosted UCCE components per the Solution Design.

Solution Testing - SimpliCTI will perform a unit test of each developed component and an integrated system test of the Solution in Lead Public Agency 's environment.

Solution Demonstration - SimpliCTI will demonstrate the developed Solution to Lead Public Agency 's technical and business staff.

Knowledge Transfer - SimpliCTI will provide project specific informal knowledge transfer throughout the life of the project to include System Administration.

Project Completion and Review - SimpliCTI will review all work completed with the Company PM and Lead Public Agency sponsor in order to:

- Determine if unresolved issues exist and jointly develop an action plan to resolve such issues if appropriate;
- Review ongoing solution support provisions; and
- Gain project phase(s) sign-off.

Deliverables

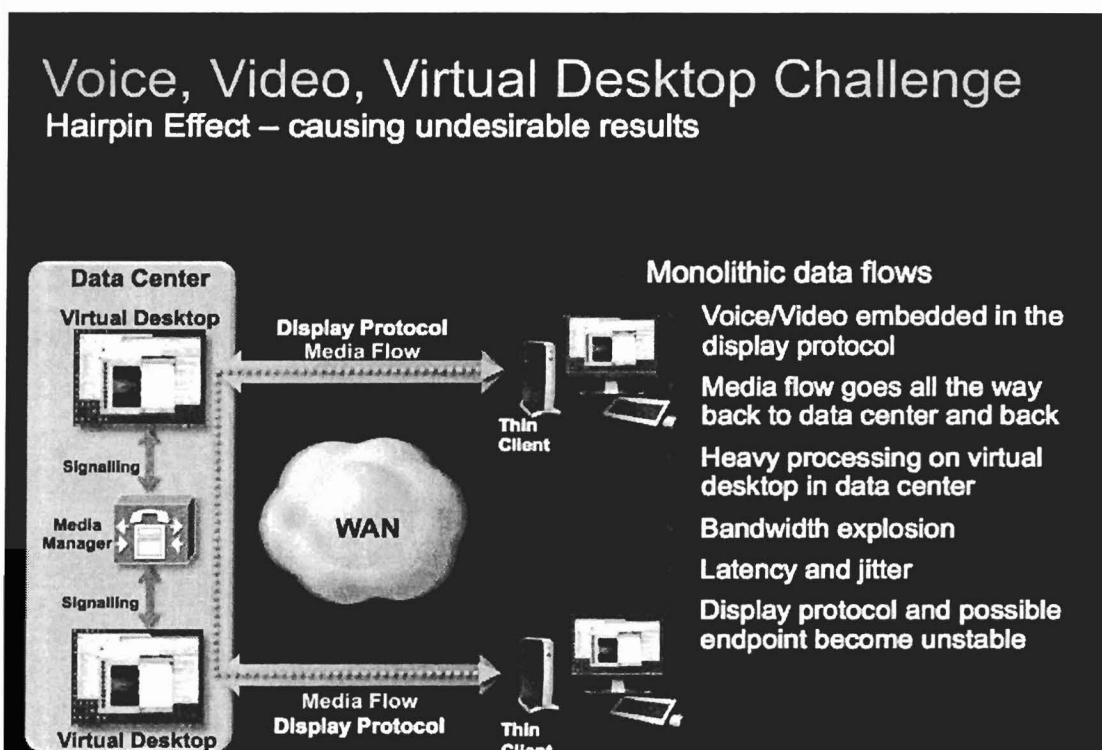
THE OVERALL DELIVERABLE IS THE UCCE SOLUTION PER THE SOLUTION DESIGN. THIS INCLUDES:

- Solution Design and Test Plan Document
- UCCE software installation/configuration
- UCCE to Verint Impact 360 integration
- UCCE to GetAbby Integration
- UCCE to AVST Integration
- UCCE scripting
- Unit Testing, System Testing and User Acceptance Testing Implementation
- Production Cutover

Appendix 3 – Concerns Regarding Implementation of Softphones on Virtual Desktops

This Appendix 3 is hereby incorporated into Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work, Exhibit F of the Contract to Provide Cisco Products and Services dated April 11, 2011 (the "Statement of Work").

When implementing softphones on desktops in a Virtual Environment, such as with Citrix or VMware the typical desktop data flow is through the servers located in the data center as illustrated below. This data flow combines all traffic, whether Video or Voice, in what is referred to as a "hairpin effect" and does not allow for segmentation, which is required in the Voice environment in order for QOS to be implemented which ensures the highest quality of voice communication.



The solution for this Hairpin Effect is the implementation of Cisco's VXi infrastructure and VXC clients, such as the Cisco VXC6215. The Cisco VXC6215 is embedded with firmware that allows the client to terminate the voice and video traffic directly on the client rather than via the display protocol. This capability is not currently supported on any other thin client device in the industry. Another option is the Cisco VXC4000 Software Appliance, which can be installed on a desktop or laptop. Both of these options are shown in the illustrations that follow:

Convergence of VDI + Video + Voice with VXC Thin Client and Software Appliance

NEW

Avoiding the Hairpinning Problem

Cisco VXC

User interacts with "soft client" on virtual desktop in data center

VDI communicator provides local client-to-client streaming of video / voice

Benefits

- Bandwidth reduction
- Reduced processing in data center, increase in VM blade density
- High quality voice and video
- Network handling real-time data (QoS, CAC)
- Eliminates hairpinning of media through data center

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 4

The results of implementing Cisco VXi and VXC in the Virtual Environment are shown below.

Cisco Innovation Solving VDI + Video + Voice

Avoiding the Hairpinning Problem

Future Solution

- User interacts with "soft client" on virtual desktop in data center
- VDI communicator provides local client-to-client streaming of video / voice

Benefits

- Bandwidth reduction
- Reduced processing in data center, increase in VM blade density
- High quality voice and video
- Network handling real-time data (QoS, CAC)
- Eliminates hairpinning of media through data center

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 15

Appendix 4 - nCare Managed Services for HCS and Contact Center Enterprise for the City of Charlotte

This Appendix 4 is hereby incorporated into Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work, Exhibit F of the Contract to Provide Cisco Products and Services dated April 11, 2011 (the "Statement of Work").

CONTACT INFORMATION

NAME	TITLE	OFFICE	MOBILE	EMAIL
CLIENT NAME				
Bellverie E. Ross	Sr. Program Manager	704-432-5627		bross@ci.charlotte.nc.us
NWN CORP				
Rodger Bakken	Account Manager	704-496-6917		rbakken@nwnit.com
Greg Syer	Practice Leader	919-653-4477	919-610-4858	gsyer@nwnit.com

EXECUTIVE SUMMARY

SUMMARY OF SERVICES

Investment Summary

- Annual Managed Services: \$111,000 (included in Hosted Solution)
- Enablement: (Waived)

nCare Service Level

- Custom

Scope of Service

- 24x7x365 Enterprise Phone Support
- 24x7x365 Device Monitoring and Management
- 24x7x365 Application Monitoring and Management
- End User Help Desk
- nCare Managed Service Portal Access
- Patch Management
- Assigned System Engineers (Primary and Backup Engineers)
- Dedicated Customer Delivery Manager
- Regularly scheduled status/support meetings
- Quarterly Onsite Engineering Visits
- Contact Center Add/Moves/Changes
- Monthly reporting and analysis

Value Proposition

- 24x7 Enterprise Phone Support
- Assigned Engineer becomes an extension of Lead Public Agency's team
- Assurance that health of Lead Public Agency's network infrastructure is maintained
- Highly trained resources for escalation and quick resolution

SERVICES SELECTED

The table below presents a summary of the items included in each level of service.

General Customer Information				SK-V6
Category	Quantity	Category	Quantity	
Number of Users	300	Number of Locations	1	
Renewal	No	Number of Locations with >20 Monitored or Managed Devices	0	
Device Monitoring and Management				
Device Services			Application Services	
	Monitor	Monitor & Manage	Monitor	Monitor & Manage
Application Server (Physical or Virtual)				
Windows				
Linux				
Cisco Appliance		14		
Server (Physical or Virtual)				
Datacenter				
Virtual Host or VCenter		7		
SAN				
Switch				
Blade Systems (BladeCenter or UCS)				
Switch				
Core				
Distribution (Closet Switch)				
Access (Stackable)				
Gateway (Includes SRST)		3		
Router				
CallManager Express or Unity Express				
Wireless Controller				
Firewall				
Firewall (High Availability Pair)				
IDS / IPS				
Websites				
			Email	
			Exchange	
			BES	
			Cisco Collaboration	
			Cummunications Manager	3
			Cisco Contact Center	
			CUIC (Webview Replacement)	1
			IPIVR PG/GetAbby PG	2
			UCCE AW/HDS	2
			IPIVR	2
			UCCE Rogger	2
			Agent PG/Verint PG	2
			Mail / Web Filtering	
			Back-up Server	
			SharePoint	
			Database (SQL)	
			Total Application*	0
			Total Application Servers*	14
			* Number of Application Services should be greater than or equal to the number of Application Servers .	
			** Citrix server farms with more than 5 servers may require follow up pricing. Configurator pricing should be treated as an estimate only.	
Additional Support Services and Options				
Service			Comments	
Enterprise Phone Support		Yes	Enterprise phone support is included with Device Monitoring and Management.	
Bundled Service Block (Dollars)				
Additional Support Services				
Scheduled Visits (Days)		4		
Add/Move/Changes per Month		10		
ICM Changes - Yearly Total		80 Hours		
Patch Management Services		Count		
Server Patch Management		21		
Help Desk Services		Count		
Estimated calls per month				
			3 UCM Servers, 11 Contact Center Servers, 7 Virtual Hosts	

NCARE SERVICES

The following outlines the nCare services that NWN Corporation ("NWN" or "Company") will perform for the City of Charlotte ("Lead Public Agency" or "City") under this Appendix 4.

DEVICE AND APPLICATION PROACTIVE MONITORING SERVICE

7x24 Monitoring and Multi-Tier Notification

With 7x24 device and application monitoring, Company will monitor the Lead Public Agency's Cisco Unified Communications Manager and Contact Center Enterprise environments through the use of specially configured applications and tools installed at the 7x24 monitoring facilities at Company's Datacenter in Waltham, MA. Company is able to monitor the status of the devices and be alerted to problems and potential problems. Thresholds will be set to trigger alarms for immediate, remedial response.

There are hundreds of attributes which are tracked and captured across the different devices Company monitors. Examples of the types of attributes Company captures include:

- Disk, memory, and CPU usage
- Event log errors
- Communication Manager and Contact Center Service availability
- Reboot detection
- Server and application patch status
- Voice Gateway performance statistics

Incident Assessment and Escalation

System monitoring provides a significant amount of information which must be evaluated to determine if a true incident has occurred. As part of the incident assessment activity, alerts which the monitoring tools have created are evaluated for validity. Company's team of qualified engineers are reviewing these alerts 7x24 and determining if they are true incidents.

In addition to incidents which are identified through the monitoring tools, the initial incident assessment is applicable for incidents which are raised via a phone call, email, fax, etc. These incidents are also assessed to determine their root cause. Through this activity they will either be resolved quickly or escalated appropriately depending on the service requirements.

7x24 Case Management Tool

Incidents identified and escalated are documented in an online case management system. Company will provide customer access to this online system upon request.

7x24 Online Monitoring Portal

As part of the monitoring solutions, the Lead Public Agency has access to all the relevant monitoring information through an online portal. This information is provided both in a summary fashion as well as a drill down into the status and activities of a particular device.

Management of the monitoring tool

As part of the proactive monitoring, Company will perform the initial enablement of the monitoring tool as well as the ongoing maintenance of the tool. This includes activities such as reviewing the current threshold levels, making updates based on best practices and customer specific requirements and keeping the tool current to the latest revision.

Monthly analysis reports

On a monthly basis, the Lead Public Agency will receive an analysis report of the critical information captured with regards to the client's environment along with a technical summary about the key statistics.

These reports can be utilized to identify preventative maintenance activities as well as future planning on the technical direction for the network environment.

DEVICE AND APPLICATION PROACTIVE MONITORING AND MANAGEMENT

Note: Device and Application Proactive Monitoring and Management include and are in addition to all services listed above in the Device and Application Monitoring section.

7x24x365 Onsite Engineering Support

Company provides 7x24x365 onsite support services as a foundation for Company's managed services contract. An Assigned Solutions Engineer respond to incidents 7x24x365 in order to best support the Lead Public Agency's networking environment. Company's Command Center will log, track, and prioritize incidents providing onsite engineering support depending on the level of onsite support chosen by the Lead Public Agency.

Incident Support

Company focuses on supporting Company's customers IT Infrastructure. The scope of incidents which we will help Company's customer resolve includes:

Task	Supported
Incidence	
Contact Center Applications and Services	✓
IP Communication Applications and Services	✓
Voice Gateway Services	✓
Hardware	✓
Operating System	✓
Configuration	✓
Performance	✓
Circuit	✓
Security	✓
Back-ups	✓
Device Management	✓

Examples of the types of issues Company will help resolve include:

- Contact Center Server ran out of memory and shut down
- Contact Center Services are failing to start
- Users are reporting dropped calls or voice quality degradation
- Call Manager ran out of memory and shut down
- PRI connected to the voice gateway is down
- Router stops working
- Tunnel disconnected

Incidents are escalated based on criticality. Criticality is defined as follows:

Criticality Level	Description
Priority 1 (Critical)	"Critical" (also known as Priority Level 1, P1): The system is inoperative and the Lead Public Agency's inability to use the product has a critical effect on the Lead Public Agency's operations. This condition is generally characterized by complete system failure and requires immediate correction. In addition, any condition that may critically impact human safety is considered a Priority Level 1 Critical problem.

Priority 2 (Major)	"Major" (also known as Priority Level 2, P2): The system is partially inoperative but still usable by the Lead Public Agency. The inoperative portion of the system significantly restricts the Lead Public Agency's operations, but has a less critical effect than a Priority Level 1 condition.
Priority 3 (Minor)	"Minor" (also known as Priority Level 3, P3): The system is usable by the Lead Public Agency, with little or limited impact to the function of the system. This condition is not critical and does not severely restrict overall Lead Public Agency operations.

Should a level 1 issue be identified, Company will focus an engineer or team of engineers to fix the problem.

Vendor escalation will many times be immediate. Vendor involvement is agreed upon by both the Lead Public Agency and Company staff based time on constraints and the criticality of the situation.

For Level 2 and Level 3 situations, the Lead Public Agency and Company will agree upon an action and escalation plan based upon criticality and resource availability.

The Lead Public Agency will designate a list of authorized callers that Company will validate for security purposes upon opening a new case. It is the Lead Public Agency's responsibility to notify Company should this contact list change. Notifications should be emailed and all urgent changes should be followed up via a phone call to the command center.

Company maintains support escalation contracts with Cisco, Microsoft, HP, Novell, Citrix, and Symantec. These contracts stipulate that Company will act as 1st and 2nd level support. For all Level 2 and Level 3 issues, Company staff will attempt remediation of issues. Should the issue not be solved within a reasonable amount of time, Company will escalate calls to these vendors using its contracts. Clients may request that all Level 1 calls be immediately escalated to these vendors.

Company will work with other Lead Public Agency vendors directly and will coordinate troubleshooting efforts over the phone. It is the Lead Public Agency's responsibility to maintain all other vendor escalation contracts with their individual respective vendors. Many vendors require directly purchased support in order to provide 2nd and 3rd level support and code updates.

Scheduled Maintenance

Scheduled maintenance is defined as activities which are planned in advance to keep a network healthy. This type of support may be performed either remotely or on-site depending on the circumstances of the activity. Examples of potential schedule maintenance tasks depending on the device may include:

- Patch management
- Scheduled Reboot Call Manager Server
- Verify Backups of Servers
- Scheduled backup of router configurations
- Review of Contact Center or Communication Server error and or console logs
- Remediation of issues documented in customer issue list

Functional Change request

A functional change request is defined as a request to change the operation of a device that is being managed in production. These requests typically come in the form configuration changes to the device. Functional Change requests are submitted by the client through the on-line customer portal or emailed. They are reviewed, assessed, approved, scheduled and executed as part of the standard processes. All functional change requests are tracked within Company's ticketing system. The levels at which Company will perform functional changes include:

Company has included ten (10) call center add/move/changes per month and up to 80 hours of ICM scripting changes per rolling twelve (12) month period.

Task	Supported
Functional Change Requests	
Configuration	✓
Operating System	✓

Monthly Management Reporting

Tracking and reporting are key components of the support services. On a monthly basis, Company will provide a summary report of the work performed on the Lead Public Agency's behalf. This will include:

- Incidents
- Scheduled Maintenance
- Functional Change Requests

Monthly Incident reporting

Incidents are captured in the ticketing system. On a monthly basis a snapshot is taken of what incidents have been completed over the course of the month as well as what incidents are currently outstanding. This information is included as part of the monthly summary report.

Monthly Scheduled Maintenance reporting

Scheduled Maintenance activities are captured in the ticketing system. On a monthly basis a snapshot is taken of what scheduled maintenance has been completed over the course of the month as well as what schedule maintenance is currently outstanding. This information is included as part of the monthly summary report.

Monthly Change request reporting

Functional Change requests are captured in the ticketing system. On a monthly basis a snapshot is taken of what functional change requests have been completed over the course of the month as well as what functional change requests are currently outstanding. This information is included as part of the monthly summary report.

7x24 Online Ticket Creation and Status

7x24 online access to the Company ticketing system enables customers to both create new tickets and find out the status of an existing ticket. When tickets are created, they are immediately routed to Company's command center engineers who are available 7x24. These tickets will be reviewed and addressed appropriately depending on the priority and level of service required.

In addition, any time day or night the Lead Public Agency can check the status of an existing ticket. Find out where it is in the work cycle, who it has been assigned to and what work has been accomplished to date.

Tickets may also be created via email.

24X7 ENTERPRISE PHONE SUPPORT

Company provides 7x24x365 phone support services as a foundation for Company's managed services contract. This support entitles the client to an unlimited number of incident calls as well as the ability to schedule support visits. Company provides a fully-staffed command center that answers calls within fifteen (15) minutes on a 24x7x365 basis. All calls are logged, tracked, and prioritized via Company's support model and ticketing system.

Company's phone support services are intended to help the client resolve both emergency and routine production issues and questions. This service is intended to help the client troubleshoot, escalate, and resolve issues as well as to provide ad-hoc advice on best-practices for system preventative maintenance.

GENERAL SERVICES INCLUDED

Solution Engineer Assigned to Account

A solution engineer is a level 2 engineer with a broad set of experiences. For all levels of support, a solution engineer is assigned to the Lead Public Agency's environment to facilitate a deeper understanding of the Lead Public Agency's environment to assist in troubleshooting issues and providing valuable analysis reports of the Lead Public Agency's network infrastructure. Also, they represent an additional point of contact into the managed services organization and a single point of escalation.

Customer Delivery Manager Assigned to Account

Company will assign a Customer Delivery Manager (CDM) to take ownership for all activities associated with the Lead Public Agency's account. The key metric of their success is the customer satisfaction ratings provided by the Lead Public Agency as part of the annual operations assessment. Their role will be to manage the functional change request process, customer communications and being the Lead Public Agency's advocate.

Annual Operational Assessment

Company works to go beyond the tactical day-to-day support services, and include an annual operational assessment.

During the course of ongoing monitoring, support, and maintenance, work is performed and problems are solved on a tactical level. The annual assessment process is designed to ensure tactical IT Operations are in sync with strategic business goals and objectives.

Key components of the Annual Operations Assessment include:

- Match business challenges to potential Technology Solutions
- Review and adjust existing levels of support. Create action plans for improving level of support and value.
- Provide feedback on new and emerging technologies and trends
- Discuss effectiveness and satisfaction with Company's services
- Improve Company's understanding of the Lead Public Agency's Business and internal Processes
- Understand the Risks and Impact to the Organization related to technology options
- Understand the Financial Metrics / ROI of technology choices

SERVICE LEVEL AGREEMENTS

Service Priority Agreements ("SLAs") are intended to ensure a common set of expectations between the Lead Public Agency and Company. Below is the full set of SLAs with the percentage compliance. Only those associated with the Statement of Work apply.

Area	Service Priority Agreement
Support	
<ul style="list-style-type: none"> Availability 	<ul style="list-style-type: none"> Phone and Email support will be available 7 days a week, 24 hours a day, 365 days of the year
<ul style="list-style-type: none"> Response Time 	<ul style="list-style-type: none"> Phone calls answered or returned within 15 minutes (100%)
HCS Cloud	
<ul style="list-style-type: none"> Service Availability 	<ul style="list-style-type: none"> HCS services will be available from Company's facility 99.9% each month, excluding scheduled maintenance.
Incident Response SLA	
<ul style="list-style-type: none"> Incident Notification 	<ul style="list-style-type: none"> Incidents will be identified* within the following parameters (90%) <ul style="list-style-type: none"> Priority 1 – 30 minutes Priority 2 – 60 minutes Priority 3 – 24 hours
<ul style="list-style-type: none"> Incident Resolution 	<ul style="list-style-type: none"> Incidents within Company's control will be closed within the following timeframes (80%) <ul style="list-style-type: none"> Priority 1 – 4 hours Priority 2 – 8 hours Priority 3 – 24 hours
Changes	
<ul style="list-style-type: none"> Functional change request 	<ul style="list-style-type: none"> Functional change requests completed within the following timeframes (80%) <ul style="list-style-type: none"> Priority 1 – 3 business days Priority 3 – 2 weeks
<ul style="list-style-type: none"> User Moves, Adds & Changes (MAC) 	<ul style="list-style-type: none"> MAC requests completed within the following timeframes (80%) <ul style="list-style-type: none"> Priority 1 – 4 hours Priority 2 – 3 days (volume <= 50) Priority 3 – 2 weeks
Maintenance	
<ul style="list-style-type: none"> Maintenance Windows 	<ul style="list-style-type: none"> Company will perform HCS system maintenance between 1am and 5am ET on the second or fourth Saturday of every month.
<ul style="list-style-type: none"> Notification 	<ul style="list-style-type: none"> Maintenance requiring or possibly causing unavailability of the HCS service will be advertised with a minimum of 1 week notice.

* Identification is defined as time from incident occurrence to ticket creation. Identification is a team effort between Company and the Lead Public Agency. Company's experience is that for certain types of issues, users will discover the problem before Company's remote monitoring tools can highlight the problem to Company.

P1 (Critical Alarm)	Within 15 Minutes	P1 issues will be escalated by the NOC to the next level within 30 minutes	Within 4 Hours*
P2 (High Alarm)	Within 30 Minutes	P2 issues will be escalated by the NOC to the next level within 60 minutes	Within 8 Hours*
P3 (Medium Alarm)	Within 60 Minutes	P3 issues will be escalated by the NOC to the next level within 4 hours	Within 24 Hours*
Field Corrective Maintenance	4 hours		

*Incidents within Company's control will be closed within the applicable time frames stated above

ENABLEMENT PROCESS

The typical enablement process for a platinum implementation or custom implementation that includes monitoring or management is four to six weeks depending on the complexity of the environment. Below is a summary Gantt chart which outlines the major activities included as part of the enablement process on a five week schedule.

ID	Task Name	Duration	Week 1	Week 2	Week 3	Week 4	Week 5
1	Internal Kick-Off	8 days	█				
12							
13	Customer Kick-Off	7 days	█				
21							
22	Complete Enablement Documentation	5 days			█		
33							
34	VPN Enablement	11 days	█				
39							
40	Monitoring Enablement	7 days				█	
47							
48	Go Live Activities	2.5 days					█
56							
60	Go Live	0 days					█

Internal kick-off: This activity includes the assignment of the solution engineer and customer delivery manager as well as preparing for the customer kick-off and scheduling the follow-on activities

Customer Kick-off: This activity includes the scheduling of the kick-off as well as holding the actual kick-off meeting. The kick-off meeting will typically occur on the Lead Public Agency's premises and will include the assigned solution engineer, the Lead Public Agency's delivery manager and account executive. It will be a full day meeting where Company will obtain the initial information to support the documentation process and the VPN and Monitoring Enablement.

VPN Enablement: This activity is to establish the VPN tunnel between Company and the Lead Public Agency's site. It includes configuration of the associated devices as well as the actual tunnel build.

Monitoring Enablement: This activity is to load all of the devices to be monitored into the Company monitoring tools. The execution of this task is dependent on the successful completion of the documentation activity as well as the VPN enablement activity. At the completion of this task all devices would be loaded and initial monitoring parameters would be set.

Go Live activities: This is the final preparation to make sure Company is set to support the Lead Public Agency's environment. At the completion of this activity is the official customer "go-live" where Company is live with supporting the Lead Public Agency's environment.

Please refer to Attachment B for the Pre-Enablement Customer Check List.

NCARE ASSUMPTIONS AND TERMS

- The term for the nCare Managed Services described in this Appendix 4 is concurrent with the term for the Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work. All pricing is based on a total five year term.
- Billing:
 - Enablement fees have been waived for the nCare Managed Services.
 - nCare Managed Services fees are included in the Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work..
- Incremental additions, changes and deletions to device counts can be executed via a written change order to this Appendix 4 and billing changes will be affected at the next billing cycle.
- The contract includes up to ten (10) Contact Center add/move/changes per month. Additional add/move/changes will be billed at \$100/add/move/change. Unused add/moves/changes can be carried over from month to month but cannot be carried over to the next contract year.
- The contract includes up to eighty (80) hours of ICM scripting changes per rolling twelve (12) month period. These eighty (80) hours are support hours to be expended for services such as ICM scripting, fixing user-error issues, etc.
- For On-Premise Monitoring Support: The Lead Public Agency will provide space, power, network and internet connectivity for each monitoring server needed for the scope of the Statement of Work. Company will provide the hardware and software for the monitoring server, if applicable.
- The scope of services as outlined in this Appendix 4 applies to maintaining a healthy production environment. Upgrades to the environment or the implementation of new technology would be considered outside the scope of this arrangement and would be treated as a project which would be contracted separately.

LEAD PUBLIC AGENCY'S REQUIREMENT/ DELIVERABLES

- Assigning a representative to the scheduled activities/ engineering work, who will coordinate the movement and activities of the Company staff member.
- A Lead Public Agency Point of Contact will be available as needed
- Provide access to all work locations.
- As needed, provide a work area for Company to use during on-site activities.
- Provide adequate parking or parking passes for the Company service team.
- Provide the best possible information (technical, policies, procedures, and prints, diagrams) to accomplish the assigned activities.
- Provide safety and security information related to the work area, building egress, etc. during the onsite work.
- Lead Public Agency will facilitate and provide any site work permits needed for requested services.

PROJECT FINANCIALS

Annual nCare Fee (included in Hosted Solution pricing)	\$111,000
One-time Enablement Fee	(Waived)
Total Investment per Year (included in Hosted Solution pricing)	\$111,000

TERMS & CONDITIONS

9. Payments for nCare Managed Services are included in Cisco Unified Workspace / Contact Center Hosted Implementation Statement of Work, which this is an Appendix to.

ATTACHMENTS

The following items are included as attachments to this Appendix 4:

1. Attachment A - Detailed list of City of Charlotte's equipment included in this contract
2. Attachment B - Sample Pre-enablement Check List
3. Attachment C - NWN Managed Services Value Proposition

ATTACHMENT A – DETAILED EQUIPMENT LIST

This Attachment A is hereby incorporated into Appendix 4 - nCare Managed Services for HCS and Contact Center Enterprise for the City of Charlotte. The following items are included in the scope of Appendix 4:

- Seven (7) Cisco UCS C-Series Servers
- Seven (7) Virtual Hosts
- Three (3) Unified Communications Manager Servers
- Eleven (11) Cisco Contact Center Enterprise Servers
 - 1 - CUIC (Webview Replacement)
 - 2 - IPIVR PG/GetAbby PG
 - 2 - UCCE AW/HDS
 - 2 - IPIVR
 - 2 - UCCE Rogger
 - 2 - Agent PG/Verint PG
- Three (3) Cisco Voice Gateways

Site A

UCS C210M2-VCD2 - 1							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
CUCM Publisher		Open					

UCS C210M2-VCD2 - 2							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
CUCM Subscriber A		Open					

UCS C210M2-VCD2 - 3							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
UCCE AW/HDS A							

UCS C210M2-VCD2 - 4							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
UCCE Rogger A							

Site B

UCS C210M2-VCD2 - 1							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
CUCM Subscriber B		Open					

UCS C210M2-VCD2 - 2							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
UCCE Rogger B				UCCE AW/HDS B			

UCS C210M2-VCD2 - 3							
CPU 1				CPU 2			
core	core	core	core	core	core	core	core
UCCE AW/HDS B				IPIVR PG/Verint PG B			

ATTACHMENT B – PRE-ENABLEMENT CHECK LIST

This Attachment B is hereby incorporated into Appendix 4 - nCare Managed Services for HCS and Contact Center Enterprise for the City of Charlotte.

In the weeks following contract execution, the Lead Public Agency's assigned nCare support team will work hard to ensure a smooth and timely nCare Managed Services enablement. To ensure that Company will be able to fully support the Lead Public Agency's environment, Company must complete the enablement before commencing support services. A new customer will typically be enabled 4 to 6 weeks after contract execution depending on complexity of the environment.

To keep the enablement on schedule, here is a list of documentation and technical requirements that Company will require to begin the enablement. Within 2 weeks of signing the contract, Company will hold a kick-off meeting at on-site location to review and finalize the Pre-Enablement Check List below.

1. Company will setup an account with the appropriate level of access required to manage all customer premise devices that are associated with Company's Hosted Collaboration Solution. These items include but are not limited to: voice gateways, Company's monitoring collector, MPLS routers and 3rd party application servers.
2. Static IP for the SilverStreak (monitoring device)
3. Static IP for the VPN appliance (remote connectivity device)
4. List of Managed Devices, with IP addresses as defined in the Design document
5. Hardware / Software Support Information, including
 - a. Serial Numbers
 - b. License Numbers
 - c. Contract Numbers (SmartNet, 3rd party Break/Fix Support)
6. Network Map
7. Network Documentation, including
 - a. Telco circuit IDs and contact information
 - b. Backup job schedule
 - c. Known issues or process documentation
8. Maintenance windows (for maintenance and changes requiring a planned outage)

Main Point of Contact

This contact should be able to assist Company in gaining access to and documenting the managed devices. The Company's primary point of contact at the Lead Public Agency for the enablement will be as follows:

Name	Office	Mobile	Email
Bellverie Ross	704-432-5627		bross@ci.charlotte.nc.us

VPN Connection Point of Contact

To remotely manage Lead Public Agency's network devices, Company will create a gateway to gateway, 'always on', VPN connection. The person responsible for approving and assisting with the VPN will be as follows:

Name	Office	Mobile	Email
Doris Glenn	704-336-4822		dglenn@ci.charlotte.nc.us

ATTACHMENT C – NWN MANAGED SERVICES VALUE PROPOSITION

This Attachment C is hereby incorporated into Appendix 4 - nCare Managed Services for HCS and Contact Center Enterprise for the City of Charlotte.

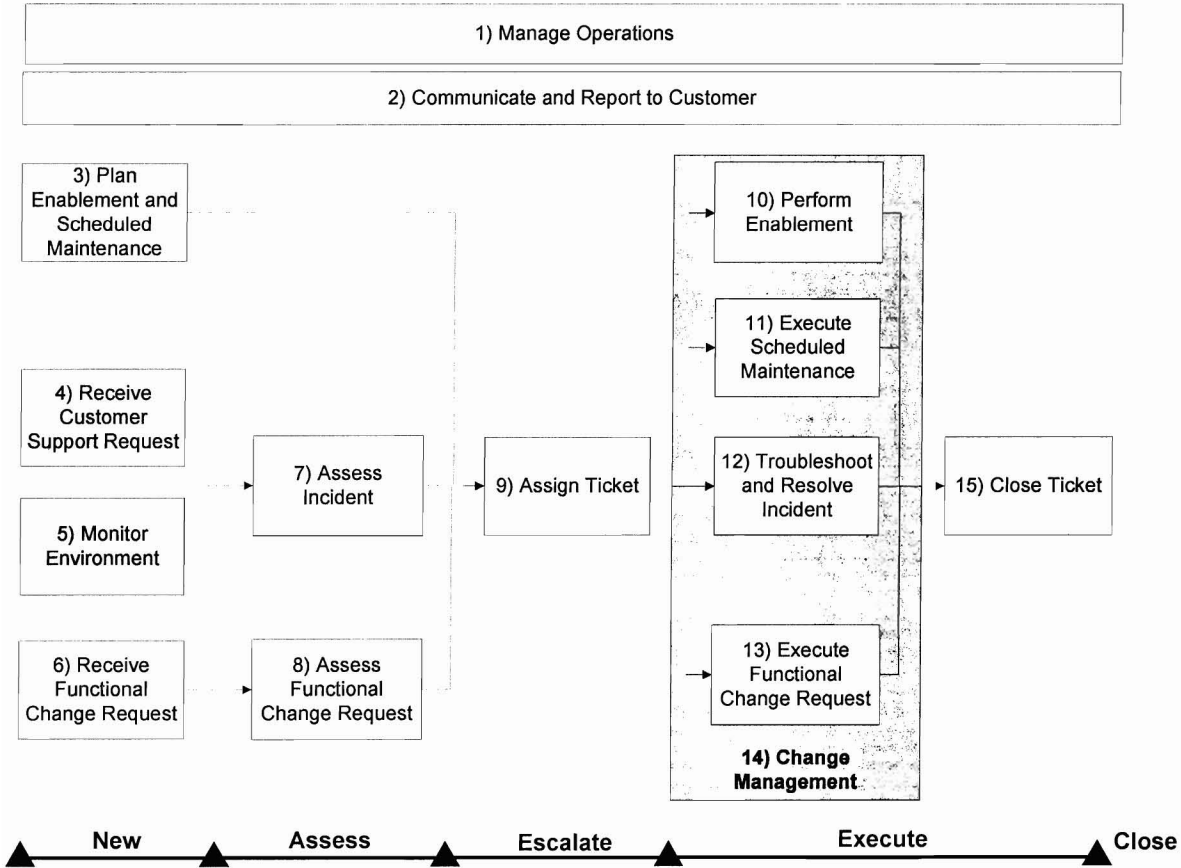
Company has been providing managed infrastructure services for over ten years to more than 250 customers with thousands of devices and has a long list of customer references. The Company believes the success of its managed services operations is based on following factors:

- Vision and strategy for success – Company's Managed Services Business Unit is the premier secure managed infrastructure services provider for the Mid-sized Business market offering a complete set of infrastructure services.
- Service delivery flexibility – Company's goal is to be a trusted partner who is willing to develop solutions that are a win – win for both the customer and Company. With a strong management team in place the Company has the capabilities to make quick decisions that enable it to develop services to meet its customers' needs.
- Focus on the Customer – The Company has structured its organization and motivated those within the organization to be customer centric. Formal customer satisfaction surveys are distributed annually with the feedback compiled and reviewed by management. Many of the Company's continuous improvement initiatives are a direct result of customer feedback.
- Commitment to continuous improvement – The Company is always focused on continuously improving its operations. The Company is committed to making strategic investments in new technologies and people to ensure the success of the operation. The Company is also always listening to its customers for suggestions on how to add additional value.
- Security and compliance focus – Security and regulatory compliance is a core service offering the Company provides to its customers. As part of the Company's commitment to security it has a formal security committee that meets every other week and an extensive security policy and infrastructure. The Company is **SAS/70 type II** certified.
- Proven processes and technology – With over ten years of managed services experience, working with thousands of devices at over 100 clients the Company has developed a set of processes and tools which enable the Company to deliver high quality services.
- Depth and quality of certified engineering team – The Company prides itself on its strong commitment to keeping the engineering team driven to stay current with the latest certifications and understanding of technologies.
- Partner for success – The Company believes in developing a core set of strategic partnerships and leverage the technologies and support of those partnerships to provide the technical capabilities of its solutions. Our strategic partnerships include
 - Microsoft Gold
 - Cisco Gold
 - HP Gold
 - EMC Velocity

The Company believes the value of its service to its customers is across four fundamental areas:

- People
 - Depth and Breadth of the Company's IT skills
 - Strength of the Company's vendor relationships
 - 7x24x365 manned coverage
 - Full coverage for holidays, vacations, sickness
- Process
 - Core Competency – Best practice approach
 - Predictable level of service – Service Level Agreement
 - Continuous investment in improvement
- Technology
 - Access to enterprise class tools
- Experience
 - Knowledge base from working with thousands of devices

The Company's master process framework enables it to successfully delivery its services with quality, reliability and predictability.



END OF DOCUMENT

**EXHIBIT G
CONFIDENTIALITY AGREEMENT**

This Confidentiality Agreement is made and entered into as of this ____ day of January, 2012, by and between the City of Charlotte, a North Carolina municipality ("the Lead Public Agency") and NWN Corporation, a corporation maintaining a place of business in Charlotte, North Carolina, (the "Company").

WHEREAS, the Lead Public Agency and Company are contemplating or have entered into certain business relationships and have exchanged and/or may need to exchange confidential information in connection with discussions of such relationships; and

WHEREAS, the Lead Public Agency and Company desire to stipulate and agree that any disclosure of confidential information in connection with such relationships has occurred or will occur under circumstances and conditions that will protect and preserve the confidentiality of the information.

NOW, THEREFORE, in consideration of the pursuit of current discussions, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and in further consideration of the covenants and representations contained herein, the parties agree as follows:

1. **CONFIDENTIAL INFORMATION.** "Confidential Information" means any information, in any medium (whether written, oral or electronic), obtained from the Lead Public Agency or the Company or any of their respective suppliers, contractors or licensors which falls within any of the following general categories:
 - 1.1. *Trade secrets.* For purposes of this Confidentiality Agreement, trade secrets consist of information of the Lead Public Agency or the Company or any of their respective suppliers, contractors or licensors: (a) that derives value from being secret; and (b) that the owner has taken reasonable steps to keep confidential. Examples of trade secrets include information relating to proprietary software, new technology, new products or services, flow charts or diagrams that show how things work, manuals that tell how things work and business processes and procedures. Notwithstanding the forgoing: (a) in order for written materials submitted by either party to be considered trade secrets, they must be clearly marked "CONFIDENTIAL" at the time of disclosure and (b) in order for any other type of materials or information submitted by either party to be considered trade secrets, the disclosing party must notify the receiving party in writing within fifteen (15) days after disclosure that such materials or information constitute a trade secret, and such notice must clearly identify the specific information that the disclosing party regards as trade secret in a manner that does not preclude the disclosure of non-trade secret materials of information.
 - 1.2. *Information relating to criminal investigations conducted by the Lead Public Agency, and records of criminal intelligence information compiled by the Lead Public Agency.*
 - 1.3. *Any attorney / client privileged information disclosed by either party.*
 - 1.4. *Information contained in the Lead Public Agency's personnel files, as defined by N.C. Gen. Stat. 160A-168.* This consists all information gathered by the Lead Public Agency about employees, except for that information which is a matter of public record under North Carolina law.
 - 1.5. *Personal identifying information about individuals* that the Lead Public Agency is prohibited from disclosing by law, including:
 - (a) Social security or employer taxpayer identification numbers.
 - (b) Drivers license (drivers license numbers are not included if the number appears on law enforcement records), State identification card, or passport numbers.
 - (c) Checking account numbers.
 - (d) Savings account numbers.
 - (e) Credit card numbers.

- (f) Debit card numbers.
- (g) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
- (h) Digital signatures.
- (i) Any other numbers or information that can be used to access a person's financial resources.
- (j) Biometric data.
- (k) Fingerprints.
- (l) Passwords.

- 1.6. *The security features of the Lead Public Agency's electronic data processing systems, information technology systems, telecommunications networks, and electronic security systems, including passwords, security standards, security logs, procedures, processes, configurations, software and codes.*
- 1.7. *Local tax records of the Lead Public Agency that contain information about a taxpayer's income or receipts.*
- 1.8. *Any data collected from a person applying for financial or other types of assistance, including but not limited to their income, bank accounts, savings accounts, etc.*
- 1.9. *Building plans of buildings or structures owned or leased by the Lead Public Agency, as well as specific details of public security plans.*
- 1.10. *Billing information of customers compiled and maintained in connection with the Lead Public Agency providing utility services.*
- 1.11. *Plans to prevent or respond to terrorist activity, including vulnerability and risk assessments, potential targets, specific tactics or specific security or emergency procedures, the disclosure of which would jeopardize the safety of government personnel or the general public or the security of any governmental facility, structure or information storage system(s).*
- 1.12. *Other information obtained from the Lead Public Agency that is exempt from disclosure under the North Carolina public records laws.*

The information described in Sections 1.5 through 1.12 is a subcategory of Confidential Information called "Highly Restricted Information." Highly Restricted Information is subject to all requirements applicable to Confidential Information, but is also subject to additional restrictions as set forth in this Confidentiality Agreement.

The parties acknowledge that Confidential Information includes information disclosed prior to execution of this Confidentiality Agreement as well as information disclosed after execution.

Notwithstanding the above, contracts between the Company and the Lead Public Agency are not Confidential Information and will be considered public records, except for attached exhibits that: (a) meet the legal requirements for trade secrets; and (b) are clearly identified as such.

- 2. **RESTRICTIONS AND REQUIREMENTS.** Each party shall comply with the following restrictions and requirements regarding Confidential Information:
 - 2.1. Neither party shall copy, modify, enhance, compile or assemble (or reverse compile or disassemble), or reverse engineer Confidential Information, except as authorized by written agreement of the parties or by the written consent of the other party.
 - 2.2. Neither party shall, directly or indirectly, disclose, divulge, reveal, report or transfer Confidential Information of the other to any third party, other than an agent, subcontractor or vendor of the Lead Public Agency or the Company who: (a) has a need to know such Confidential Information for purpose of performing work contemplated by written agreements between the Lead Public Agency and the Company, and (b) has executed a confidentiality agreement incorporating substantially the form of this

Confidentiality Agreement. Notwithstanding the Company shall not directly or indirectly, disclose, divulge, reveal, report or transfer Highly Restricted of the other to any third party without the Lead Public Agency's prior written consent.

- 2.3. Neither party shall use any Confidential Information of the other for its own benefit or for the benefit of a third party, except to the extent such use is authorized by this Confidentiality Agreement or other written agreements between the parties hereto, or is for the purpose for which such Confidential Information is being disclosed.
 - 2.4. Neither party shall remove any proprietary legends or notices, including copyright notices, appearing on or in the Confidential Information of the other.
 - 2.5. Each party shall use reasonable efforts to prohibit its employees, vendors, agents and subcontractors from using or disclosing the Confidential Information in a manner not permitted by this Confidentiality Agreement.
 - 2.6. In the event that any demand is made in litigation, arbitration or any other proceeding for disclosure of Confidential Information, the party upon which the demand is made shall notify the other party of the demand, and shall cooperate with and reasonably assist the other party in seeking a protective order or other appropriate relief to prevent or restrict and protect any disclosure of Confidential Information.
 - 2.7. All materials which constitute, reveal or derive from Confidential Information shall be kept confidential to the extent disclosure of such materials would reveal Confidential Information.
 - 2.8. Each party shall restrict employee access to the Confidential Information of the other party to those employees having a need to know for purposes of their jobs. For Company employees, "need to know" shall mean having a need to know in order to: (a) fulfill the Company's contractual obligations to the Lead Public Agency, or (b) resolve a dispute with the Lead Public Agency. For Lead Public Agency employees, "need to know" shall mean a need to know in order to: (a) use, test, evaluate or manage services or products provided by the Company, (b) to fulfill the Company's obligations to the Lead Public Agency, or (c) to resolve a dispute with the Company.
 - 2.9. The Company shall comply with the Lead Public Agency's Restricted Data Policy, a copy of which is posted on the Lead Public Agency's website, and with any instructions or procedures issued by Lead Public Agency key business units from time to time with respect to protecting specific types of Confidential Information.
 - 2.10. Each party shall take reasonable measures to prevent the use or disclosure of Confidential Information by its employees in a manner not permitted by this Confidentiality Agreement. The Company shall have each of its employees who will have access to the Confidential Information sign a confidentiality agreement which provides the Lead Public Agency and its vendors, licensors, subcontractors, employees and taxpayers the same level of protection as provided by this Confidentiality Agreement, including compliance with the Lead Public Agency's Restricted Data Policy.
 - 2.11. The Company shall further ensure that each person who obtains access to Confidential Information through the Company (including but not limited to Company's employees and subcontractors) has undergone training sufficient to understand his or her responsibilities with respect to this Confidentiality Agreement and the Lead Public Agency's Restricted Data Policy.
3. **EXCEPTIONS.** The disclosing party to this Confidentiality Agreement agrees that the receiving party ("Recipient") shall have no obligation with respect to any Confidential Information that the Recipient can establish:
- 3.1. was already known to Recipient prior to being disclosed by the disclosing party;
 - 3.2. was or becomes publicly known through no wrongful act of Recipient;

- 3.3. was rightfully obtained by Recipient from a third party without similar restriction and without breach hereof;
 - 3.4. was used or disclosed by Recipient with the prior written authorization of the other party;
 - 3.5. was disclosed pursuant to the requirement or request of a governmental agency, which disclosure cannot be made in confidence, provided that, in such instance, Recipient shall first give to the other party notice of such requirement or request;
 - 3.6. was independently developed without breach of this Agreement; or
 - 3.7. was disclosed pursuant to the order of a court of competent jurisdiction or a lawfully issued subpoena, provided that the Recipient shall take reasonable steps to obtain an agreement or protective order providing that this Confidentiality Agreement will be applicable to all disclosures under the court order or subpoena.
4. **DATA.** The Company will treat as Confidential Information all data provided by the Lead Public Agency or processed for the Lead Public Agency or for citizens under this Confidentiality Agreement (including metadata). Such data shall remain the exclusive property of the Lead Public Agency. The Company will not reproduce, copy, duplicate, disclose, or in any way treat the data supplied by the Lead Public Agency in any manner except that contemplated by this Contract.
 5. **PUBLIC RECORDS.** Notwithstanding anything contained herein to the contrary, the parties recognize and acknowledge that the Lead Public Agency is a subdivision of the State of North Carolina and is, therefore, subject to the North Carolina Public Records Act (the "Act") at N.C. Gen. Stat. 132-1 *et seq.* The parties further acknowledge that any Confidential Information that is a public record under North Carolina law may be released and disclosed by the Lead Public Agency pursuant to the Act, and that any such release or disclosure shall not in any way constitute a breach of this Confidentiality Agreement, nor shall the Lead Public Agency be liable to the Company for such release or disclosure.

In the event the Lead Public Agency receives a request for disclosure of Confidential Information which the Company has specifically marked "Confidential" or "Proprietary" the Lead Public Agency shall give the Company written notice of such request (the "Notice of Request for Disclosure"). In the event the Company has a reasonable basis for contending that the disclosure of such Confidential Information is not required by the Act, the Company shall within ten days after receipt of the Notice of Request for Disclosure notify the Lead Public Agency in writing of its objection to disclosure and the basis therefor. The Company shall indemnify, defend and hold harmless the Lead Public Agency from and against all losses, damages, liabilities, costs, obligations and expenses (including reasonable attorneys' fees) incurred by the Lead Public Agency in connection with any refusal by the Lead Public Agency to disclose Confidential Information after receiving an objection to disclosure from the Company. If the Lead Public Agency receives no written objection from the Company within ten days after the Company's receipt of a Notice of Request for Disclosure, the Lead Public Agency shall disclose the Confidential Information referenced in the Notice of Request for Disclosure.

Notwithstanding the forgoing, the parties agree that the computer database information that the Lead Public Agency is required to disclose under N.C. Gen. Stat. §132-6.1 shall not be deemed Confidential Information, and that the Lead Public Agency shall be entitled to disclose such information without notice to the Company.

6. **REMEDIES.** Each party acknowledges that the unauthorized disclosure of the Confidential Information of the other will diminish the value of the proprietary interests therein. Accordingly, it is agreed that if a party breaches its obligations hereunder, the other party shall be entitled to equitable relief to protect its interests, including but not limited to injunctive relief, as well as monetary damages.
7. **NOTICES.** Any notice, consent or other communication required or contemplated by this Confidentiality Agreement shall be in writing, and shall be delivered in person, by U.S. mail, by overnight courier, by electronic mail or by telefax to the intended recipient at the following address:

For the Company:
Rodger Bakken
NWN Corporation
2520 Whitehall Park Drive
Suite 250
Charlotte, NC 28273
PHONE: 704-496-6917
FAX: 704-496-6901
Email: rbakken@nwnit.com

For the Lead Public Agency:
Cindy White
Office of the City Attorney
15th Floor, CMCG
600 East Fourth Street
Charlotte, NC 28203-2841
PHONE: 704-336-3012
FAX: 704-336-6644
Email: cwhite@ci.charlotte.nc.us

Notice shall be effective upon the date of receipt by the intended recipient; provided that any notice of breach or default which is sent by telefax or electronic mail shall also be simultaneously sent by mail deposited with the U.S. Postal Service or by overnight courier. Each party may change its address for notification purposes by giving the other party written notice of the new address and the date upon which it shall become effective. Any notice of breach or default under this Confidentiality Agreement shall also be sent to:

For the Company:
Rodger Bakken
NWN Corporation
2520 Whitehall Park Drive
Suite 250
Charlotte, NC 28273
PHONE: 704-496-6917
FAX: 704-496-6901
Email: rbakken@nwnit.com

For the Lead Public Agency:
Cindy White
Office of the City Attorney
15th Floor, CMCG
600 East Fourth Street
Charlotte, NC 28203-2841
PHONE: 704-336-3012
FAX: 704-336-6644
Email: cwhite@ci.charlotte.nc.us

8. MISCELLANEOUS

- 8.1. *ENTIRE AGREEMENT.* This Confidentiality Agreement constitutes the entire agreement between the parties with respect to protection and disclosure of the Confidential Information. There are no other representations, understandings or agreements between the parties with respect to such subject matter. On the subject matter of this Confidentiality Agreement, it supersedes all prior agreements, negotiations, representations and proposals, written or oral.
- 8.2. *AMENDMENT.* No amendment or change to this Confidentiality Agreement shall be valid unless in writing and signed by both parties to this Confidentiality Agreement.
- 8.3. *GOVERNING LAW AND JURISDICTION.* North Carolina law shall govern interpretation of this Confidentiality Agreement and all other matters relating to this Confidentiality Agreement (all without regard North Carolina conflicts of laws principles). Any and all legal actions or proceedings relating to this Confidentiality Agreement shall be brought in a state or federal court sitting in Mecklenburg County, North Carolina. By execution of this Confidentiality Agreement, the parties submit to the jurisdiction of said courts and hereby irrevocably waive any and all objections which they may have with respect to venue in any court sitting in Mecklenburg County, North Carolina.
- 8.4. *BINDING NATURE AND ASSIGNMENT.* This Confidentiality Agreement shall bind the parties and their successors and permitted assigns. Neither party may assign any rights or obligations under this Confidentiality Agreement without the prior written consent of the other. Any assignment attempted without the written consent of the other party shall be void.
- 8.5. *SEVERABILITY.* The invalidity of one or more of the phrases, sentences, clauses or sections contained in this Confidentiality Agreement shall not affect the validity of the remaining portion of the Confidentiality Agreement so long as the material purposes of the Confidentiality Agreement can be determined and effectuated. If any provision of this Confidentiality Agreement is held to be unenforceable, then both parties shall be relieved of all obligations arising under such provision, but only to the extent that such

provision is unenforceable, and this Confidentiality Agreement shall be deemed amended by modifying such provision to the extent necessary to make it enforceable while preserving its intent.

- 8.6. *WAIVER*. No delay or omission by either party to exercise any right or power it has under this Confidentiality Agreement shall impair or be construed as a waiver of such right or power. A waiver by either party of any covenant or breach of this Confidentiality Agreement shall not constitute or operate as a waiver of any succeeding breach of that covenant or of any other covenant. No waiver of any provision of this Confidentiality Agreement shall be effective unless in writing and signed by the party waiving the rights.
- 8.7. *COUNTERPARTS*. This Confidentiality Agreement may be executed in any number of counterparts, all of which taken together shall constitute one single agreement between the parties.
- 8.8. *TITLES OF SECTIONS*. The section headings inserted herein are for convenience only and are not intended to be used as aids to interpretation and are not binding on the parties.

Nothing in this Confidentiality Agreement shall be deemed to eliminate or lessen any obligation either party may have at law with respect to protecting the confidentiality of Confidential Information, except as the provisions of this Confidentiality Agreement expressly authorize the release of Confidential Information.

IN WITNESS WHEREOF, and in acknowledgment that the parties hereto have read and understood each and every provision hereof, the parties have caused this Confidentiality Agreement to be executed on the date first written above.

NWN CORPORATION

CITY OF CHARLOTTE

BY: 

BY: 

TITLE: REGIONAL SALES DIRECTOR

TITLE: ASSISTANT CITY MANAGER

DATE: 1/6/12

DATE: 1/9/2013

dated by AMJ with direction

ATTEST: 

Deputy CITY CLERK