NIC PARTNERS
Employee Built. Employee Owned.

CITY OF
CHULA VISTA

Statement of Work
City of Chula Vista
Technology Refresh

December 06, 2017

This Statement of Work (SOW) is made and entered into between Network Integration Company Partners, Inc. hereinafter referred to as "NIC Partners", with offices at 11981 Jack Benny Dr., Rancho Cucamonga, CA 91739 and City of Chula Vista, hereinafter referred to as "CUSTOMER" This SOW defines the services and deliverables that NIC Partners shall provide to the Customer under the terms of the Agreement ("Services"). The terms of this SOW are limited to the Scope of this SOW and shall not be applicable to any other Scopes of Work, which may be executed and attached to this Agreement. Acceptance of this proposal is subject to the standard NIC Partners Terms and Conditions attached herewith.

The information contained in this SOW is ***confidential*** and ***privileged***. It is intended to be reviewed only by the Organization named above. If you are not an authorized employee of the organization, you are hereby notified that any review, dissemination or copying of this SOW is prohibited.

Prepared For:	**Prepared By:**	**Account Manager:**
Gary Halbert City of Chula Vista 276 Fourth Ave Chula Vista, CA 91910 Phone: 619-691-5031 ghalbert@chulavistaca.gov	Steven Vargas NIC Partners, Inc. 11981 Jack Benny Drive, Suite 103 Rancho Cucamonga, CA 91739 Phone: 909- 919-2703 svargas@NicPartnersInc.com	Matt Robbart NIC Partners 11981 Jack Benny Drive, Suite 103 Rancho Cucamonga, CA 91739 Phone: 909-257-2733 mrobbart@NicPartnersInc.com

City of Chula Vista - Technology Refresh

Project overview:
NIC Partners has been in discussions with the City of Chula Vista regarding network equipment and services required to provide the base infrastructure which will be needed for successful Smart City projects. The City has requested a solution that prioritizes security and automation for ease of maintenance, and would cover the City's needs for base infrastructure, and network security.
The project will consist of the following components:

- Cisco Catalyst 9000 series switches and ISR 4000 series routers for the base network infrastructure
- Cisco DNA Center for intent-based network configuration and automation
- Cisco ISE for identity management and TrustSec
- Cisco ASR routers for BGP multi-homing the Internet connection across dual ISPs
- Cisco security products, including Firepower 4000 series next-gen firewalls, AMP for Endpoints, Umbrella for filtering of DNS requests, and StealthWatch for anomaly detection
- Cisco wireless access points and controllers

Customer Locations:

- City Hall
- Police Department
- Public Works
- Fire Stations (9)
- Living Coast Discovery Center
- Animal Care Facility
- Recreation Centers (9)

Services to be performed by NIC Partners:

During the low-level design phase of the project, the following information will be collected and defined:

- Active Directory information
- Categorize common user groups and the systems they are permitted to access
- Applications to permit or deny access to network-wide
- Desired virtual networks (VNs), such as VNs for Guest, HVAC, SCADA, IP Camera, Quarantine, etc. VNs will be used inside of the SD-Access fabric(s), and VRFs may be used outside of the fabric(s) if necessary.
- Acceptable authentication methods for wired and wireless devices
- Wireless radio resource management features and options
- QoS policies and traffic classification
- E911 requirements and PSAP information
- Existing paging systems and paging group requirements
- OVA sizing for Cisco Collaboration applications

- VLANs
- Routing / Protocols
- Multicast
- IP addresses and ranges
- DHCP configuration – which device or server?
- Hypervisor configuration details
- Application requirements
- Standard operating systems & patch levels to deploy
- Login/password information and requirements
- SNMP strings and telnet/SSH requirements for remote login
- Copper/fiber patch cable requirements and availability
- Power and rack space requirements for equipment in IDFs/MDF
- Requirements for post-installation testing and customer sign-off documents
- Project implementation dates and project close-out procedure
- Centralized infrastructure monitoring applications & report scheduling
- Wireless access point installation locations & associated cabling
- Any design requirements that were not explicitly stated here, but are necessary for a successful implementation.

At each of the locations indicated in the Customer Locations section of this document, NIC Partners will perform the following Professional Services tasks:

- Perform discovery of the following network components:
  - Existing network equipment:
    - Routers
    - Switches
    - Firewalls
    - Wireless
    - Other critical network appliances and devices (content filters, etc)
  - Network closet conditions:
    - Power
    - Rack space, depth, and screw type
    - Patch cable types and length
    - Fiber backbone type (OM1,2,3,4,SM1,2) and fiber patch cable type
  - Document logical configuration on network equipment:
    - VLANs
    - IP addresses and routes
    - QoS policies
    - ACLs
    - Special configurations
  - Create port map indicating which VLAN or L3 interface is assigned to each port in the cable patch panel

- Replace existing switches with the new equipment specified in the bill of materials

  - Un-patch existing fiber & copper patch cables from switches
  - Remove old switches
  - Install new switches (pre-configured for the designated location)
  - Connect equipment to UPS (if provided) or to wall power
  - Re-patch fiber and copper patch cables according to the port map previously created in the discovery phase
    - New patch cables will be used if they are included in the bill of materials or provided by Customer
  - Dress the cables such that they presentable and not blocking other equipment from being installed in or removed from the rack
    - Existing cable management devices will be used if available
  - Verify configuration of new equipment and adjust if necessary
  - Verify functionality of critical end user devices connected to switch

- Replace existing routers with the new equipment specified in the bill of materials
  - Un-patch existing fiber & copper patch cables from routers
  - Remove old routers
  - Install new routers (pre-configured for the designated location)
  - Connect equipment to UPS (if provided) or to wall power
  - Re-patch fiber and copper patch cables according to the port map previously created in the discovery phase
    - New patch cables will be used if they are included in the bill of materials or provided by Customer
  - Dress the cables such that they presentable and not blocking other equipment from being installed in or removed from the rack
    - Existing cable management devices will be used if available
  - Verify configuration of new equipment and adjust if necessary
  - Verify route tables, routing protocols, redistribution, ACLs, QoS, etc.

- Replace existing firewalls with the new equipment specified in the bill of materials
  - Un-patch existing fiber & copper patch cables from firewalls
  - Remove old firewalls
  - Install new firewalls (pre-configured for the designated location)
  - Install new Firepower Management Console appliance (if applicable)
  - Connect equipment to UPS (if provided) or to wall power
  - Re-patch fiber and copper patch cables according to the port map previously created in the discovery phase
    - New patch cables will be used if they are included in the bill of materials or provided by Customer
  - Dress the cables such that they presentable and not blocking other equipment from being installed in or removed from the rack
    - Existing cable management devices will be used if available
  - Verify configuration of new equipment and adjust if necessary

  - Verify route tables, routing protocols, NAT/PAT, ACLs, QoS, IPS & AMP, etc.

Internet Connectivity
The intent of this project component is to provide the Customer with equipment that will connect to two or more ISPs at speeds of 10 Gbps or less using a multi-homed BGP configuration for resiliency and load-sharing.

- Assist Customer with arranging dual ISPs for BGP
  - Confirm that Customer has filed paperwork for their own IP address range with ARIN
  - Confirm that Customer has filed paperwork for their own AS number with ARIN
  - Confirm that Customer has two or more Internet circuits installed and functional
  - Confirm that Customer has filed paperwork with all directly-connected ISPs allowing Customer to use BGP to advertise its own public IP address range and ASN through those ISPs
    - Identify whether the ISPs are providing the full routing table, partial routing table, or default route only, and modify configurations as needed.

- Set up connection to ISPs using new equipment
  - This procedure is assuming that the Customer has two or more ISPs available, and is assuming that IPv4 is used exclusively with those ISPs.
    - If the Customer has only a single ISP available, or does not plan to migrate to a multi-homed Internet connection before the end of this project, then the BGP aspect of the configuration may be skipped.
  - Configure the ASR1001X routers to connect to the upstream ISPs
    - If there are two upstream ISPs, then each ASR router should only connect to one ISP. If there are more than two ISPs, then they should be split evenly across the two ASR routers.
  - Configure the ASR1001X routers to advertise the Customer’s own public IP address range to the ISPs using BGP and the Customer’s own ASN.
    - Route filtering should be used so that only the Customer’s local address range is advertised to other ISPs.
    - Inbound and outbound metrics should be adjusted so the utilization of both connections is roughly proportional.
  - The ASR routers should be connected to a pair of stacked Catalyst 9500 switches, to be considered the ‘Outside’ switches.
    - Multichassis EtherChannel should be used to allow the ASR routers to connect to both switches over a single logical connection (per router) for high-availability.
    - If a DMZ is desired, the ports on the Catalyst 9500 switches should be separated into two VRFs: Outside and DMZ. The ‘Outside’ VRF connects the Outside interface(s) on the firewall to the ASR routers, and the ‘DMZ’ VRF connects the DMZ interface(s) on the firewall to DMZ servers and equipment.

- Set up new Internet firewalls
    - Load the latest stable Firepower Threat Defense 6.x software platform onto the firewall appliances.
    - Configure the new firewalls for the following features, assuming IPv4 only:
        - NAT traffic from the Inside to the Outside using the Customer's own public IP address range
        - Permit traffic from the Inside to the DMZ without NAT
        - Configure static NAT translations from the Outside to requisite services on the DMZ and/or inside networks where necessary.
        - Configure IPS services in monitor mode (no blocking).
            - After running in monitor mode for one week, export reports to Customer so they may identify critical services which are unintentionally being marked as 'bad'.
                - Tune the IPS rules according to Customer's input, and turn on blocking mode.
        - Enable AnyConnect VPN connectivity for remote users
    - The firewall Inside interfaces should be connected to the City Hall core Catalyst 9500 switches using Multichassis EtherChannel where possible for high-availability. The Outside interface(s) will be connected to the Outside switch/VRF and the DMZ interface(s) will be connected to the DMZ switch/VRF.

- Set up Firepower Management Center
    - The Firepower Management Center appliance should be connected to the network at 1 Gbps via RJ45 copper cables
    - The FMC should be configured to manage all firewalls in this project, including the City Hall firewalls and Police Department firewalls.
        - Enable multitenancy support by creating the following domains within FMC and associating them with their corresponding firewall(s):
            - City Hall
            - Police Department
        - Each domain will have its own user accounts to enable the different divisions within the City to manage their own equipment.

General Routing & Switching

The intent of this project component is to provide the Customer with a policy-driven system for managing and operating their routing & switching infrastructure. Cisco's DNA Center will serve as the single-pane-of-glass management interface for translating intent into action across switches, routers, wireless access points, and (in the future) firewalls. The components that make this work include DNA Center, ISE, Campus Fabric, and the various controllers for each technology (Catalyst 9000 switches, ISR4XXX routers, 5520/3504 wireless controllers). The equipment, user groups, and policies can all be defined in the DNA Center

- Design the route/switch underlay network upon which the fabric overlay will ride
    - Use the Network Plug & Play function in DNA Center (wherever possible) to automate the deployment of network gear. If network configuration must be done manually, the following guidelines should be followed:
        - Increase default MTU to 9100 bytes
        - Use layer 3 links from the network core to the edge
        - Use point-to-point links
        - Use a dedicated IGP process for the fabric
        - Use /32 addresses for loopbacks on each network device and propagate them via IGP using route tags

- Install Cisco ISE
    - Load (4) ISE 2.3 virtual machines into the existing VMware environment
    - Perform basic setup of ISE virtual machines including administration account(s), IP address, DNS server address, NTP server address, etc.
    - Configure two of the ISE VMs as Policy Administration Nodes (PANs) in high-availability mode.
    - Configure two of the ISE VMs as Policy Service Nodes (PSNs).
    - Integrate ISE with Customer's Active Directory
    - Enable ERS (external RESTful services) to allow DNA Center to communicate with ISE.
        - Enable ERS read/write
        - Create ERS admin account in ISE
        - Enable SXP service, passive identify service, and PxGrid

- Set up DNA Center
    - Load or update DNA Center 1.x (APIC-EM 2.x) software on the (3) DNA Center appliances
    - Set up CIMC for remote administration
    - Complete basic setup for the appliance. If asked for a CCO account, use the Customer's account. Ensure that the Customer's account is associated with the Smartnet contracts.
    - Configure integration with ISE
    - Define ISE PSNs as AAA servers
    - Import switches, routers, and WLCs, and their corresponding device credentials
    - Import maps and floorplans
    - Define IP address pools
    - Define wireless profiles: SSIDs, authentication methods, security type, etc
    - Define security policies: virtual networks (VNs), user groups and access rights (contracts) as determined in the low-level design process.
    - Add Netflow Collector and SNMP Trap services as necessary for Stealthwatch.
    - Associate hardware to sites and policies, and provision according to the timeline & schedule determined in the low-level design meeting.

The table below illustrates which sites will participate in software-defined access (SD-Access) based on the size of the location and the equipment that will be available.

Locations	Main Fabric	Individual Fabric	Not on Fabric
City Hall LAN	x		
City Hall Core	x		
City Hall Datacenter			x
City Hall Internet			x
Police Department		x	
Public Works		x	
Animal Care Facility			x
Living Coast Discovery			x
Recreation Centers			x

- Install and configure Cisco Nexus 9K switches in the datacenter.
  - The Nexus 9K switches will operate in NX-OS mode.
  - The Nexus 9K switches should be connected to each other and to the network core at 40 Gbps provided that single-mode fiber infrastructure is in place. If single-mode fiber is not available between the network core and the datacenter, then NIC Partners will connect the equipment at the highest speed supported by existing infrastructure.
  - Connectivity to the network core will be via point-to-point layer 3 connections.
  - The pair of Nexus 9K switches will function in virtual port-channel mode so both network core switches and servers can have ‘teamed’ connections to them.

Security

The intent of this project component is to provide the Customer with network security software which will provide multiple layers of protection against threats such as exploits, ransomware, and other malware.

Umbrella will be used to filter and report on DNS queries from within the network and for clients who are roaming outside of the network.

AMP for Endpoints will be used to proactively identify threats which are run on Windows and Mac OS-X machines, and retrospectively identify threats that result from changed disposition on files.

StealthWatch will leverage Netflow from the switches to identify anomalies within the network traffic on the LAN. This will allow the IT staff to quickly identify security problems like breaches, rogue servers, traffic from suspect countries, protocols which do not belong on the LAN, and other issues.

- Set up Umbrella
  - Redeem Umbrella licensing and associate to Customer’s SMART account
  - Create administrative user account in Umbrella for Customer (allow Customer to change password)
  - Configure Customer’s public IP address range(s) and associate with the default policy
  - Configure Customer’s internal networks and associate them with the default policy
    - Summarize address ranges where possible

  - Deploy Active Directory connector to Customer's AD domain controller
  - Deploy (3) Umbrella virtual appliances to Customer's existing VMWare environment
    - Each instance of Umbrella virtual appliance should be on a separate host
  - Configure Umbrella internal domains
  - Connect Umbrella's external logging system to Customer's Amazon S3 bucket
    - If Customer does not have an Amazon S3 bucket available, then this task can be ignored
  - Tune policies as defined in the low-level design process
  - Test deployment of Umbrella by changing the DNS server of (2) test machines to use the Umbrella virtual appliances for DNS
    - Verify that requests for internal sites are being forwarded to internal DNS servers by the Umbrella virtual appliances
    - Verify that requests for 'good' web sites are proceeding as expected
    - A request for a 'bad' site can be simulated by visiting http://www.internetbadguys.com
    - Verify that the correct data is showing up in the Umbrella reports
  - Demonstrate to customer how Umbrella agent software can be deployed on mobile Windows and Mac OS-X devices to protect roaming clients.
    - Optionally, the Umbrella plug-in for AnyConnect may be used instead of the agent software if desired.

- Set up AMP for Endpoints
  - Redeem AMP for Endpoints licensing and associate to Customer's SMART account
  - Create administrative user account in AMP portal for Customer
    - Allow Customer to change password if desired
  - Customize endpoint groups, policies, and exclusions as defined in the low-level design process
    - Identify which clients should have ETHOS & SPERO enabled
  - Demonstrate AMP for Endpoints portal administrative tasks to Customer IT team
  - Test deployment of AMP for Endpoints client to (3) separate customer-owned endpoints
    - Customer will be responsible for deploying AMP for Endpoints software to clients in the production network

- Set up StealthWatch
  - Install each StealthWatch component
    - Note: StealthWatch components can be deployed through DNA Center
  - Configure the firewall(s) to allow communications with the StealthWatch products
  - Change System admin & root passwords
  - Use the Appliance Setup Tool to configure the following settings for each appliance:
    - Host and domain information
    - DNS settings
    - NTP settings
  - After setting up the SMC, use the System Setup Tool to configure the following:

        - IP address ranges
        - Add FlowCollectors to system
        - Add FlowSensors
        - Configure SMTP Service
        - Configure SNMP polling
        - Set Internet Access and proxy server (if applicable)
        - Active license
    - Launch the Appliance Admin interface for each product and configure these general settings:
        - Configure the system time
        - Change the Admin password
        - Configure the FlowSensor application ID and payload
        - Configure flow replicator rules
    - Launch the SMC client software from the web app interface and configure the following:
        - Verify that the SMC is seeing traffic
        - Create an Admin user account
        - Add an identify device
        - Add SLIC Threat Feed feature
        - Place all default IP space for the network into the 'Catch All' host group
    - Configure network equipment to forward Netflow data to the StealthWatch FlowCollectors.

Wireless

The intent of this project component is to provision high-quality wireless service across the City's buildings (exact AP locations will be determined at the low-level design meeting). The wireless controllers will be located at the City Hall, Public Works, and Police Department. These APs will function in fabric mode (if supported at time of installation) with their configuration being defined in the DNA Center. Other APs may operate in FlexConnect mode and register with the controllers at City Hall.

- Configure new Cisco wireless controllers for network connectivity and administration credentials
    - The 5520 controllers will be located at the City Hall in an HA SSO pair, and will participate in the SD-Access fabric (if software feature set permits at time of installation).
    - The 3504 controllers will be located at the Police Department, and Public Works buildings. They will participate in the SD-Access fabric (if software feature set permits at time of installation).
- For APs which will become part of the SD-Access fabric:
    - Within DNA Center, perform the following tasks:
        - Place the location of all installed access points on the maps/floorplans.
        - Create global SSIDs
        - Create wireless interfaces for the SSIDs to use
        - Associate end user groups with sites and policies
        - Provision fabric APs and WLCs
- For APs which will not become part of the SD-Access fabric:
    - Configure non-fabric APs to be in FlexConnect mode

    - The APs will function as bridges, and will be configured with the VLANs that are used with the wireless network.
    - Map APs to global SSIDs and associated authentication methods
- For all APs, review wireless RRM features and options with the Customer and configure accordingly.
- Review wireless QoS settings with the Customer and provision accordingly.

General Deployment Methodology

1. The project kick-off, low-level design, and site survey will take place.
2. If there is sufficient rack space, fiber backbone, and power available, the New City Hall core and LAN equipment will be installed in a 'parallel' network alongside the existing equipment.
    a. The routers functioning as border nodes will be required to de-encapsulate the VXLAN traffic destined for remote sites, the Internet, and the datacenter.
3. DNA Center, ISE, Stealthwatch, and other network services will be brought online and configured.
4. Once the SD-Access fabric is up and running, end user devices at the City Hall will be migrated to the new LAN switches, and the old switches can be removed from the network.
    a. The new wireless LAN controllers shall be installed, and City Hall wireless access points replaced with new 802.11AC wave 2 fabric-enabled APs.
    b. Repeat this process at the Police Station, and Public Works facilities; each of these locations will have its own fabric. The remaining locations will not participate in the SD-Access fabric.
5. Replace equipment at the Animal Care Facility, Living Coast Discovery Center, (9) recreation centers, and (9) fire stations as the schedule permits.
    a. At these locations, new wireless access points can be deployed at the same time as the LAN switches and routers.

Project Constraints

- NICP will discuss CCV IT Team with the implementation details in order to avoid service impact.

Assumptions and Exclusions

- Services not specifically documented in this agreement are considered out of scope and will be addressed with a separate Work Authorization, SOW or Change Order.
- Customer is responsible for all multicast configuration on their network to support InformaCast Paging System.
- Spark users can register for free, depending on the service there will be a fee. This is something that NIC Partners and CCV will need to discuss at low level meeting.
- The pricing is for the implementation services only and does not include pricing for travel and living expenses. NIC Partners will bill travel and living expenses on an as-incurred, cost-only basis, if required.

- Public CA signed Certificates will be the responsible of CCV for applications that needed a CA signed cert.
- DNS/AD/DHCP configuration will be the responsible of CCV.
- It is assumed that CCV is using exchange server as a mail server to integrate with Unity Connection for Unified messaging.
- NIC Partners assumed customer network VoIP QoS is to best practice.
- The pricing and deliverables descriptions contained within this agreement represent our current understanding of the overall voice mail and IVR/processes needed at this time. Should additional discussion reveal additional complexity or effort, they will be handled via the Change Order (CR) process.
- This quote is valid for 60 days from date of quotation.
- All parties involved understand that some projects call for short timeframes to implementation. However, Implementation timelines and schedules will be verified and negotiated following the project kick-off.
- NIC Partners will generally perform all implementation services and travel during normal business hours: 9:00 a.m. - 5:00 p.m., Monday through Friday. Work performed outside of normal business hours. Anything beyond that must be negotiated through a Change Management process and additional fees will apply, unless otherwise specifically identified in this SOW.

<u>Specific tasks outside this SOW include, but are not limited to:</u>

- Efforts required to provide support for or diagnose issues related to unsupported platform elements are specifically not included within the scope of this agreement.

<u>Revision Notes</u>

First draft 11/20/17 – SV

City of Chula Vista – Technology Refresh

Stakeholders, Roles & Responsibilities

City of Chula Vista – Technology Refresh				
Project Team Contacts				
Name	**Company**	**Role**	**Phone**	**Email**
Gary Halbert	City of Chula Vista	City Manager	619-691-5031	ghalbert@chulavistaca.gov
Steven Vargas	NIC Partners	Sales Engineer	909-919-2703	svargas@nicpartnersinc.com
Matt Robbart	NIC Partners	Account Manager	909-257-2733	mrobbart@NicPartnersInc.com

City of Chula Vista – Technology Refresh

Customer Responsibilities

If the project is to be successful, Customer must commit to the following general obligations unless specifically specified otherwise in this SOW:

1. Provide approved purchase orders in a timely manner, to ensure that hardware and software (if required) will be obtained before the commencement of any phase where needed.
2. Appoint a lead technical resource that will be the point of contact for all technical questions.
3. Meet with NIC Partners Engineer to provide adequate input into the design requirements.
4. Ensure that adequate physical access to project locations (rooms, equipment, and wall jacks) be afforded to NIC Partners personnel such that they can complete the integration and design work in a timely manner.
5. Provide security clearance and access to facilities, as required. This includes badges, passwords, access cards, parking privileges. This includes access to PCs and desktop systems.
6. Ensure customer provided wiring is in place and functioning per manufacturer specifications.
7. Customer is responsible for all cabling and cross connecting of wires needed to complete any of the project tasks for PCs and servers.
8. Provide patch cords for all newly installed equipment, if applicable (if not purchased with the new equipment). IP Phones come with a single patch cord out of the box.
9. Configuration outside of the requirements for the product being installed will not be performed. NIC Partners and the customer must agree jointly on a configuration change and document that change as a Change Order to the project.
10. Provide the necessary power and access to power sources for all equipment being installed.
11. If customer-provided racks/enclosures are used, sufficient space must be afforded to fit new equipment. If the new equipment will not fit in existing racks/enclosures, a change order will be issued by NIC Partners, which may potentially result in additional labor and/or cost.
12. Provide adequate cooling for newly installed equipment (not included in statement of work).
13. Perform any configuration necessary on all end-users' personal computers. NIC Partners is not responsible for software conflicts caused by standard installation of customer software.
14. Ensure accuracy of data/information supplied to NIC Partners.
15. Provide NIC Partners Engineers with appropriate extensions, specific codes and zone information for voice projects.
16. Provide a complete list of any required usernames and logon IDs, where needed.
17. Assist in testing on any required integrated systems.
18. Customer is responsible for all system backups upon project completion.
19. Customer will provide adequate training facilities, if applicable.
20. Customer understands that training on any NIC Partners-installed hardware or software is not provided unless specifically written in Project Specifications section of this SOW.
21. Customer understands that change orders issued after project commencement will be evaluated for impact to the project, and may result in the need for additional time and cost.

City of Chula Vista – Technology Refresh

Acceptance Criteria

NIC Partners will determine, in conjunction with the customer at the customer kickoff meeting, what the acceptance criteria will be for this project to enable a successful completion to the satisfaction of both NIC Partners and Customer. These criteria are used to demonstrate the successful installation and operation of the required services for Customer and this project within the scope of this Statement of Work.

During this project, NIC Partners may request that you initial and date each criterion to signify acceptance. Upon successful completion of all tests, NIC Partners will provide Customer with a Project Completion Form. Customer agrees to promptly sign the Project Completion Form to confirm the completion of the project described in this Statement of Work. Please see **Appendix C - Completion Certificate** at the end of this document.

If additional work other than that listed in this SOW Project Specifications is required, NIC Partners reserves the right to document and incorporate a Change Order to this Statement of Work. Please see **Appendix B - Change Order Request Form**, at the end of this document.

Project Pricing

Please refer to the following NICP Quotes:

- **28523 - FF - Chula Vista, City of-Comprehensive Tech Refresh - City Hall/Security/Spares/Cables/Learning Credits/GoldMile - NASPO**
- **28524 - FF - Chula Vista, City of-Comprehensive Tech Refresh - Police/PublicWorks/LCDC/Animal Facility/RecCenters/Fire/Wireless – NASPO**
- **28522 - Chula Vista, City of-Comprehensive Tech Refresh - Professional Services - NASPO**

Payment Schedule

NIC Partners will bill 100% of equipment and materials upon receipt and 25% of labor upon execution of contract. Additional labor invoices shall be submitted once a month for labor performed during that month.

Cancellation of Contract

A 30-day notice must be given in writing for all cancellation or change in personnel requests. If the customer requests a new project lead/consultant, NIC Partners will work to fill that role as soon as possible within that 30-day period.

If the customer cancels the contract after work has been performed, customer is liable for services completed to date. Customer agrees to pay for the amount of services rendered.

City of Chula Vista – Technology Refresh

Proposal Acceptance / Change Management Procedures

After both parties sign this Statement of Work document, no change to the statement of work shall be entertained by either party unless both parties agree to and sign a completed Change Order Request (Appendix B).

Engineering support not specified in this Statement of Work is billable at published hourly rates. Any delays caused by the customer's equipment, facility, personnel, or network provider shall be billed on a time and materials basis in one-hour minimums. Services provided do not include troubleshooting problems related to existing network infrastructures. NIC Partners is not liable for configurations or integration work not performed by NIC Partners.

AGREEMENT PROVISIONS: This agreement includes the attached terms and conditions and any amendments which have been signed by both parties.

Network Integration Company Partners, Inc.

By: ______________________________

Name: ____________________________

Title: _____________________________

Date: _____________________________

City of Chula Vista

By: ___________________________

Name: _________________________

Title: __________________________

Date: __________________________

Standard Terms and Conditions

PAYMENT TERMS: NIC Partners will bill 100% of equipment and materials upon receipt and 25% of labor upon execution of contract. Additional labor invoices shall be submitted once a month for labor performed during that month. A late payment charge of 1 ½ % per month (18% annually) may be applied to amounts outstanding ten days (10) days after the date of the statement.

EQUIPMENT PAYMENT TERMS: Established accounts, Educational Institutions and Government Agencies are net 30 days. All others are payment in full prior to shipping. Customer agrees to pay finance charge on all over due balances.

INTEREST: If payment is not received by NIC PARTNERS within 30 calendar days of the invoice date, the Customer shall pay as interest an additional charge of 1 ½% (or the maximum allowable by law, whichever is lower) of the PAST DUE amount per month. Payment thereafter shall first be applied to accrued interest and then to the unpaid principal.

TAXES: Prices shown may not include all sales or other taxes imposed on the sale of goods and services. Taxes now or here after imposed upon sales or shipments shall be added to the purchase price. Buyer agrees to reimburse Seller for any such tax or provide Seller with acceptable tax exemption.

COLLECTION COSTS: In the event legal action is necessary to enforce the payment provisions of this Agreement, NIC PARTNERS shall be entitled to collect from the Customer any judgment or settlement sums due, reasonable attorneys' fees, court costs and expenses incurred by NIC PARTNERS in connection therewith and, in addition, the reasonable value of NIC PARTNERS time and expenses spent in connection with such collection action, computed at NIC PARTNERS prevailing fee schedule and expense policies.

SUSPENSION OF SERVICES: If the Customer fails to make payments when due or otherwise is in breach of this Agreement, NIC PARTNERS may suspend performance of services upon five (5) calendar days' notice to the Customer. NIC PARTNERS shall have no liability whatsoever to the Customer for any costs or damages as a result of such suspension caused by any breach of this Agreement by the Customer.

TERMINATION OF SERVICES: If the Customer fails to make payment to NIC PARTNERS in accordance with the payment terms herein, this shall constitute a material breach of this Agreement and shall be cause for termination by NIC PARTNERS.

SET-OFFS, BACKCHARGES, DISCOUNTS: Payment of invoices is in no case subject to unilateral discounting or set-offs by the Customer, and payment is due regardless of suspension or termination of this Agreement by either party.

INDEMNITY AND INSURANCE: Each party shall be responsible for and hold the other party harmless from any loss sustained by such party relating to death, bodily injury, or damage to tangible physical property which is caused by the negligent acts or omissions of the party's agents or employees. NIC PARTNERS shall obtain and keep in force at all times liability insurance coverage for bodily injury, death, and property damage in an amount not less than One Million Dollars ($1,000,000.00)

BOND: Costs of Performance and Payment bond is not included. If required, NIC PARTNERS shall furnish Customer, in a form satisfactory to Customer, full and duly executed Performance and Payment Bonds, underwritten by a surety or sureties satisfactory to the Customer, in the full amount of this Agreement. Cost of such bonds to be paid directly by Customer.

ARBITRATION: All claims, disputes, and other matters in question arising out of, or relating to, this Contract or the breach thereof, shall be decided by arbitration in accordance with the Construction Industry Arbitration Rules of the American Arbitration Association then obtaining unless the parties mutually agree otherwise. This agreement to arbitrate shall be specifically enforceable under the prevailing arbitration law. The award rendered by the arbitrators shall be final, and judgment may be entered upon it in accordance with applicable law in any court having jurisdiction thereof. Notice of the demand for arbitration shall be filed in writing with the other party and with the American Arbitration Association. The demand for arbitration shall be made within a reasonable time after the claim, dispute, or other matter in question has arisen, but in no event shall it be made after substantial completion of the project for which this Contract is awarded.

LIABILITY: NIC PARTNERS shall not, in any event be liable to customer for incidental or consequential damages, including without limitation, lost business, profit or unavailability of all or part of the system. The pricing granted elsewhere in this agreement is based upon and is in partial consideration for this limitation on remedies.

WARRANTY (Limited): NIC PARTNERS warrants the products installed under this agreement against defects in material and workmanship from a period of one year from project completion. NIC PARTNERS shall repair or replace defective product during the warranty period with new or like new parts. Returned product becomes the property of NIC PARTNERS when replaced. This warranty is void if installed product is abused, misused or altered. This warranty is exclusive and is Customer's only remedy. Without limiting the generality of the foregoing limitations and disclaimers, while the system is not designed, sold, or intended to be used to detect, intercept, transmit or record oral or other communications of any kind, NIC PARTNERS cannot control how the system and its components are used and, accordingly, NIC PARTNERS does not warrant or represent, expressly or implicitly, that use of the software, licensed materials derived there from will comply and conform to the requirements of Federal, State and or Local statutes, ordinances and laws, or that the use of the system will not violate the privacy rights of the third parties. You shall be solely responsible for using the system you the system in full compliance with applicable law and the rights of third persons. Further, regardless of any prior statements, representations, or course of dealings by any NIC PARTNERS representatives, NIC PARTNERS does not warrant or represent, expressly or implicitly, that the software, licensed materials, or use of any of the same will: result in the prevention of crime or hostile enemy action, apprehension or conviction of any perpetrator of any crime, military prosecution of any enemy force, or detection or neutralization of any criminal, combatant or threat; prevent any loss, death, injury, or damage to property due to the discharge of a firearm or other weapon; in all cases detect and plot the location of all firearm discharges within the designated coverage area; the supplied network will remain in operation at all times or under all conditions. Any and all warranties, express or implied, of fitness for high risk purposes requiring fail-safe performance are hereby expressly disclaimed. You and NIC PARTNERS each acknowledge and agree that the software, license materials, and the system are not consumer goods, and are not intended for sale to or use by or for personal, family or household use.

OWNERSHIP: NIC Partners shall retain ownership of all materials supplied until the customer takes possession of the materials at their facilities. Upon receipt the customer assumes the risks and ownership of all materials. NIC Partners has the right to restore ownership of the materials to NIC Partners if the customer fails to pay for the materials under the terms of the contract. Once ownership has been restored to NIC Partners due to non-payment, NIC Partners may retrieve from the Customer's premises any material supplied where payment has not been tendered. The Uniform Commercial Code of California shall govern this sale and this order shall not be assignable, but shall bind the representative and successors of the parties and their benefits.

LIENS: Seller may file a lien within 90 days after furnishing labor, materials, or services to a project as long as preliminary lien notice is sent to Buyer under the provisions of the Construction Lien Law of the state where services are rendered. The lien notice is no way intended to reflect the financial stability of the Buyer, but simply advises the Buyer of Seller's rights to file the lien if required.

RETURNS: Credit may be allowed for goods returned with prior approval. A deduction may be made from credits issued to cover the cost of handling and restocking charges.

DELAYS: Seller is not responsible for delays in delivery or installation occasioned by acts of God or other circumstances over which the Seller has no control.

MISCELLANEOUS: This Agreement constitutes the entire understanding of the parties with respect to the subject matter of this Agreement and merges all prior communications, representations, and agreements. This Agreement may be modified only by a written agreement signed by the parties. If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be construed under the laws of the state where services are rendered, excluding rules regarding conflicts of law.

City of Chula Vista – Technology Refresh

Appendix A – Project Approach

NIC Partners will provide the following services in a phased or milestone approach to ensure the most accurate and successful deployment of product and services for the project. There are three distinct phases that make this project, which are outlined below. NIC Partners will provide project coordination on behalf of the customer to help ensure a successful deployment.

The NIC Partners approach includes a dedicated Project Manager who will work with the Customer in prioritizing and developing a project plan with agreed timelines, payment milestones, and completion criteria. The Project Manager will work with the Customer to develop a communications plan which outlines the communications process expected by the Customer throughout the project lifecycle. The Project Manager will conduct weekly status meetings (or as required) with the customer to address progress of the project and to resolve any outstanding issues before moving on to new tasks or phases. Our experienced Project Manager will become the single point of contact for the project in all its phases and will provide a consistent communication link with identified Customer employees. All work will be scaled to be within the scope as stated herein.

Phase 1: Project Planning and Design
Phase 2: Project Implementation, Cutovers and Testing
Phase 3: Project Documentation and Closeout

Phase 1: Project Planning and Design

Objectives & Scope

1) NIC Partners Project Management will work with the customer to plan and design the required management type components to successfully implement the proposed solution(s). NIC Partners will include the following (where applicable):
   a) High-level project schedule
   b) Develop the project phase and or milestone sign-off forms
   c) Develop the payment schedule (tie to Project phases, equipment list and/or WBS)
   d) Develop the project equipment transmittal form requirements

2) NIC Partners Project Management will work with the customer to plan and design for the physical component requirements to successfully implement the proposed solution(s). NIC Partners will include the following (where applicable):
   a) Customer site and or location staging requirements
   b) Review the physical locations and options for power and network connectivity
   c) Identify and determine of method of access for project teams and staff to project sites

City of Chula Vista – Technology Refresh

3) NIC Partners Project Management will work with the customer to plan and design for the logical component requirements to successfully implement the proposed solution(s). NIC Partners will plan for the following (where applicable):
   a) Equipment Information Sheet requirements (EIS)
      i) Asset tag requirements
      ii) Special labeling requirements
   b) Design requirements
   c) IP and Naming convention requirements
   d) Security access plans (usernames, passwords, ACS integration, etc.)
   e) Quality of Service requirements (QoS)
   f) Backup systems and or policies

4) NIC Partners Project Management will work with the customer to plan and design for the testing component requirements to successfully implement the proposed solution(s). NIC Partners will include the following for NIC Partners provided equipment (where applicable):
   a) Physical and logical testing plan
   b) Testing and site completion plan documents
   c) Customer specific application testing, if specified in this SOW Project Specifications

Deliverables (if applicable to the project)

Items outlined in the “Objectives & Scope” section above

a) Project Management documents
   i) Project Schedules
   ii) Payment schedules
b) Physical Planning and Design documents
   i) Sample site survey reports
   ii) Badges and or key requirements
c) Logical Planning and Design documents
   i) EIS sample document
   ii) Visio planned designs (one high-level page for new network designs)
   iii) IP and Naming convention sample document
   iv) Dial Plans sample document (required for Voice projects only)
   v) Obtain any required asset tags
   vi) Sample labels if needed
d) Testing Plans
   i) Testing plan and site completion sign form

City of Chula Vista – Technology Refresh

Phase 2: Project Implementation, Testing and Cutovers

Objectives & Scope

1) This section should include project and or site specific information to deploy the equipment to and in the customer's site and network along with testing and sign-off documents (where applicable).
    a) Oversight of NIC Partners Engineering Deployment Procedures
    b) Customer-specific requirements as outlined in the Planning and Design phase above
    c) Time and location for delivery of equipment, along with customer-required signatures and approvals
    d) Install and test all equipment per NIC Partners testing plan and project or site specific testing plan as developed in the Planning and Design phase
2) Project and/or site specific cut-over requirements as outlined from the Planning and Design phase (where applicable)

Assumptions and Exclusions

1) See Customer Responsibilities section above.

Deliverables (if applicable to the project)

1) Signed equipment transmittal(s)
2) Signed site-specific, or project testing and sign off form, if required
3) Signed customer retired equipment form, if required
4) Signed Notification of Completion

Phase 3: Project Documentation and Closeout

Deliverables (if applicable to the project)

1) Completed Equipment Information Sheets (EIS)
    a) Make, model, IP address, MAC address, access (ID, password), and required information
    b) Physical design documentation; NIC Partners will update customer-provided electronic 2D drawings for cabling projects, where required. NIC Partners will document one page per location that will show location of NIC Partners-provided main components (Surveillance, Access Control, Cable Runs)
    c) NIC Partners can create a new CAD drawing, at additional costs to the project
2) NIC Partners will provide the customer with only basic configurations in printed and electronic format, where possible. Note that installation instructions, how-to user guides, training guides and the like are not provided unless specifically included in this SOW Project Specifications. NIC Partners will assist in providing access to applicable vendor-provided online documentation
3) Provide all required maintenance and warranty information

City of Chula Vista – Technology Refresh

Appendix B - Change Order Request

In reference to the section titled Change Management Procedures of the above referenced Statement of Work between Network Integration Company Partners, Inc. (NIC Partners) and City of Chula Vista, both parties hereby certify, by the signature of an authorized representative, that this Change Order shall amend and be fully incorporated into the existing Statement of Work (SOW).

Change Order Number:

1. **Reason for Change Request:**

2. **Changes to SOW:**

3. **Impact (cost, schedule):**

4. **Purchase Order Issuance (If applicable):**

IN WITNESS WHEREOF, the duly authorized representatives of the parties hereto have caused this Change Order Request to be fully executed.

Submitted by:	**Acknowledged and Agreed:**
Network Integration Company Partners, Inc.	City of Chula Vista
By: ______________________________	By: ______________________________
Name: ______________________________	Name:______________________________
Title: ______________________________	Title: ______________________________
Date: ______________________________	Date: ______________________________

City of Chula Vista – Technology Refresh

Appendix C - Completion Certificate (Sample)

NOTICE OF COMPLETION

Network Integration Company Partners, Inc. (NIC Partners) does hereby notify City of Chula Vista that all work performed under the statement of work specified under the below listed purchase order has been completed in accordance with standards and regulations governing such work. This work is ready for your review and as such NIC Partners does hereby request authorization to invoice the full amount as stated in the PO listed below to include any applicable retention percentages, for all work performed.

Customer:	City of Chula Vista
Project Name:	Technology Refresh
Job Number:	
Customer PO:	

As an authorized representative of the above listed customer, I do hereby affirm all work has been inspected for thoroughness and compliance and has been completed.

1. Customer agrees that the project can be billed complete.

Inspected By:

Name: ____________________________________ Title: ______________________

Customer Authorized Representative

Signature: _________________________________ Date: ______________________

Customer Authorized Representative

As an authorized representative of the above listed customer, I do hereby authorize Network Integration Company Partners, Inc., (NIC Partners) to invoice 100% of the above listed PO for the work performed at the above listed facility. By signing I do hereby acknowledge this project as accepted as delivered in accordance with the statement of work applicable to this project.

Authorized By:

Name: ____________________________________ Title: ______________________

Customer Authorized Representative

Signature: _________________________________ Date: ______________________

Customer Authorized Representative