# APPENDIX B.7B

# TRANSFORMATION APPROACH AND METHODOLOGY

**for**

**COUNTY**

## Contents

# 1.0 Overview

## 1.1 Objective

Transformation is where the Vendor moves the County from its legacy data and voice networks into a converged network utilizing Voice over Internet Protocol (VoIP).

- Complete all Transformation milestones by mutually agreed-on dates. This objective will be measured by the delivery of the defined artifacts in Amendment 1 milestone six (6) by submission & approval of Quality Review Form (QRF) for a given subset of completed sites in the Transformation Project.
- Minimize impact and risk to County of Orange business operations, IT departments and user community.
- Continue a solid relationship between County of Orange and Vendor account team. The TMO Client Satisfaction Survey will measure the success of this objective.
- Solidify the long-term strategic relationship; fostering a strong commitment toward the common goals

## 1.2 Approach and Methodology

Vendor will incorporate a disciplined project management approach and methodology utilizing Microsoft Project to create the necessary project artifacts. Vendor will utilize the results created during the Transition Project to drive transformation.

### 1.2.1 Data Network

Vendor will transform the County legacy data network infrastructure to a converged voice/data infrastructure utilizing Cisco network equipment, technology and network protocols required to support the deployment of Converged Network and VoIP services for County End Users. Transformation includes the installation of a new telecommunications network and hardware to support a converged set of services.

Vendor will deploy the data network in a phased approach. This begins with implementing the 10 core sites creating the backbone for the entire network. Once the initial phase is complete and the core backbone is established additional in-scope sites will be added in a phased approach.

**Project Lifecycle for Network Services Transformation**

Vendor employs a standard system development & implementation approach to each defined discipline within the Transformation. The following provides a general description of the approach applied to each area of this Transformation:

- Analysis and Design:
    - Develop and finalize network architecture design
    - Develop and finalize security architecture design
    - Develop and collaborate with County of Orange on transformation schedule
    - Develop and collaborate with County of Orange on transformation approach plan
    - Develop and collaborate with County of Orange on transformation acceptance criteria

    - Joint reviews of design document, approach plan and schedule for sign-off by County of Orange

- Construct:
    - Develop cutover implementation plans on a rolling phase approach
    - Initiate procurement for Network Core and Phase 0 site cutovers
    - Initiate procurement of security devices
    - Validate training requirements for support personnel
    - Develop communication plans
    - Develop test and quality assurance plans
- Implement:
    - Vendor installs network core infrastructure
    - Vendor rolls out test site(s)
    - Site migration to Cisco network systems
    - Site migration to Sourcefire IDS/IPS monitoring system
    - Site migrations to remaining security tools, as appropriate
    - Address process improvement and risk mitigation on an ongoing basis

  Vendor will implement industry best practice for implementation using Vendor and Customer agreed upon strategy for minimizing impact risk, outages and Security issues for the network rollout.

#### 1.2.1.1 Analysis and Design

- Discovery - Vendor will identify current environment information and obtain knowledge of existing processes for County of Orange services support. This will be accomplished through assignments of Transformation team members and knowledge transfer sessions.
- Obtain system/workflow Inputs-Vendor will obtain input from County of Orange business workflow, policy and procedures, incident management, and change management and reporting.
- Identify in-scope systems
- Identify in-scope security systems and agencies to be monitored
- Identify ticket escalation procedures
- Identify security incident escalation procedures
- Verify maintenance contracts exist for supported systems
- Identify list of systems to be monitored
- Identify list of systems to be monitored by security products
- Review County of Orange reporting requirements
- Identify inventory for each site

#### 1.2.1.2 Construct

- Establish and document main points of contact for County of Orange
- Development - Vendor will build and implement the necessary hardware, software and business workflow processes necessary to support the defined requirements
- Procurement – Initiate procurement of hardware, software, or services required to complete the deliverable

- Testing and Quality Assurance - This includes development of test plans, configuration test, user acceptance test, and Go/No Go decision
- Document all network devices at each County location
- Define and document each vendor's ticketing procedures
- Define and document security incident handling procedures
- Document hours of operation for each supported site
- Completed letter of agency for County of Orange telecom vendors
- Define who will provide reports, how they will be provided, when they will be provided
- Provide data engineering with IP addresses to be monitored
- Obtain devices to be monitored by security tools
- Confirm back-up schedules
- Develop plan for necessary core infrastructure to be installed in the Orange County Data Center (OCDC) and Building 12
- Develop plan for migration of sites to new core infrastructure
- Develop plan for migration of sites to new security tools
- Develop roll-back plans
- Review data with County of Orange in support of establishing budget cost allocations
- Generate and maintain knowledge documents and make these available to the County of Orange upon request for the duration of the Transformation project.
- Create comprehensive vendor list
- Document in-flight projects, deliverables, and associated due dates
- Develop communication plan with the County

#### 1.2.1.3 Implement

- Following a "Go" decision based on successful testing and approval, and with the concurrence of County IT, the implemented solution is put into production.
- During post implementation, a defined burn-in period will extend for an agreed upon duration where all activities associated with the implemented solution are closely monitored and issues or incidents are addressed by the Transformation team. Once this burn-in period is over, VoIP migrations are cleared to occur.
- Verify Vendor network engineers can access the County of Orange network systems
- Verify Vendor Security Operations Center (SOC) engineers can access security tools
- Order network hardware
- Build required network components in OCDC and Building 12
- Execute training program
- Migrate sites to new infrastructure
- Migrate sites to IDS/IPS and security tools, as appropriate
- Migrate legacy security tools to new environment
- Install new security tools in new environment
- Execute site test plan to verify migration
- Execute security test plan to verify migrations
- Verify Network Tools are monitoring all future state equipment
- Verify Security Tools are monitoring future state equipment, as appropriate
- Validate required Design, As-built(s) and Training documentation is complete and documented in the QRF for the site
- Validate vendor specific in-scope back-ups are working

#### 1.2.1.4 Close

- Obtain customer concurrence that deliverables have been met
- Execute the site decommissioning procedure, including the de-install and decommission of legacy phone equipment and the inventory of legacy phone equipment
- Obtain Agency and County I.T. approval to close project
- Complete administrative project close activities
- Obtain Account Team Sign-Off
- Obtain Client Sign-Off

### 1.2.2 Voice Network

Vendor will deploy three instances of the HCS environment in the Vendor's Dallas and Pittsburgh data centers. These platforms will provide both physical and geographic redundancy.

Vendor will perform VoIP site deployments using a wave approach that follows the data network connectivity and network equipment transformation. During each wave, Vendor will be configuring the Hosted Cisco HCS platforms to support the IP-based voice services. Vendor will also be remotely staging and configuring new voice equipment and providing onsite installation and configuration of new IP-phones for all users.

Implementation will consist of building the new clusters, data collection of the Nortel systems, building these remote locations and phones in the new clusters, and migrating the remote site to the new cluster. Implementation will also consist of creating a new Voice Service queue, testing on-call procedures, verifying remote connectivity to the supported hardware, defining escalation procedures, and Change/Problem Management administration.

**Project Lifecycle for Voice Services Transformation**

Vendor employs a standard system development & implementation approach to each defined discipline within the Transformation. The following provides a general description of the approach applied to each area of this Transformation:

- Analysis and Design:
    - Develop and finalize the VoIP architecture design
    - Develop and collaborate with County of Orange on transformation schedule
    - Develop and collaborate with County of Orange on transformation approach plan
    - Develop and collaborate with County of Orange on transformation acceptance criteria
    - Joint reviews of design document, approach plan and schedule for sign-off by County of Orange
- Construct:
    - Develop cutover implementation plans on a rolling wave approach
    - Initiate procurement for VoIP Core and Wave 0 site cutovers
    - Validate end user training requirements and develop training material and processes
    - Validate training requirements for support personnel
    - Develop communication plans
    - Develop test and quality assurance plans
    - Develop roll-back plans

- Implement:
    - Vendor will observe industry best practice for implementation using Vendor and Customer agreed upon strategy for minimizing impact risk and outages for the VoIP rollout.
    - Vendor installs VoIP core infrastructure
    - Vendor rolls out test site(s), tailors process for County of Orange culture
    - PBX and end user migration to Cisco VoIP systems
    - Address process improvement and risk mitigation on an ongoing basis
    - •Vendor will make available on-site end user training and training documentation (including training slideware on SharePoint and “leave behind material”) as well as specialized training for executives, executive assistants and ACD agents.

#### 1.2.2.1 Analysis and Design

- Discovery - Vendor will identify current environment information and obtain knowledge of existing processes for County of Orange services support. This will be accomplished through assignments of Transformation team members and knowledge transfer sessions.
- Obtain system/workflow Inputs-Vendor will obtain input from County of Orange business workflow, policy and procedures, incident management, and change management, reporting and IMAC.
- Identify in-scope voice services and voice systems connected to the legacy PBX, including voice-mail, call recording, ACDs, IVRs, PA systems, security alarms and any other voice equipment
- Identify ticket escalation procedures
- Verify maintenance contracts exist for supported systems
- Identify list of systems to be monitored
- Review County of Orange voice reporting requirements
- Identify inventory for each site

#### 1.2.2.2 Construct

- Establish and document main points of contact for County of Orange
- Development - Vendor will build and implement the necessary hardware, software and business workflow processes necessary to support the defined requirements
- Procurement – Initiate procurement of hardware, software, or services required to complete the deliverable
- Training – Determine training requirements based on the existing knowledge base and the solution to be implemented
- Develop training program and material
- Testing and Quality Assurance - This includes development of test plans, configuration test, user acceptance test, and Go/No Go decision
- Document phone model, user, phone number per site for every phone
- Document voicemail boxes and users per site
- Document Auto Attendant applications and scripts
- Document voice gateway dial-peers, voice resources, and SRST for each voice gateway
- Document analog gateway model, user, phone number per site for every phone

- Define and document each vendor's ticketing procedures
- Document hours of operation for each supported site
- Completed letter of agency for County of Orange telecom vendors
- Define who will provide reports, how they will be provided, when they will be provided
- Provide data engineering with IP addresses to be monitored
- Confirm back-up schedules
- Develop plan for installing clusters into Dallas and Pittsburgh data centers
- Develop plan for necessary core infrastructure to be installed in the Orange County Data Center (OCDC) and Building 12
- Develop plan for migration of sites to new clusters
- Review data with County of Orange in support of establishing budget cost allocations
- Generate and maintain knowledge documents and make these available to the County of Orange upon request for the duration of the Transformation project. (VOIP rack diagrams, user training guides and Call Center guides)
- Review data with County in support of establishing budget cost allocations
- Create comprehensive vendor list
- Document in-flight projects, deliverables, and associated due dates
- Gather NORTEL ACD requirements for UCCX
- Develop Day 2 Roles and Responsibilities with L&JA
- Develop communication plan and post-hyper care support with SAIC

#### 1.2.2.3 Implement

- Following a "Go" decision based on successful testing and approval, and with the consensus of the Agency and County I.T., the implemented solution is put into production.
- Verify Vendor voice engineers can access the County of Orange voice systems
- Order voice hardware
- Build new clusters in Pittsburgh and Dallas data centers
- Build required telephony components in OCDC and Building 12
- Baseline and build the sites in CUCM
- Import the phones, gateways, and users into CUCM
- Import the users into Unity Connection
- Build ACDs on new UCCX cluster
- Execute training program
- Migrate sites to new clusters
- Execute site test plan to verify migration
- During post implementation, a defined "Critical Care or Hypercare" period will extend for an agreed upon duration where all activities associated with the implemented solution are closely monitored and issues or incidents are addressed by the Transformation team. Once this "critical care" period is over, incident management will be addressed by the defined operational support organization.
- Verify Network Tools are monitoring all future state equipment
- Validate required Design, As-built(s) and Training documentation is complete
- Validate back-ups are working

#### 1.2.2.4 Close

- Obtain Agency and County I.T. concurrence that deliverables have been met
- Obtain Agency and County I.T. approval to close project

- Complete administrative project close activities, including completion of QRF documentation
- Follow the procedure for decommissioning and inventory of legacy equipment
- Obtain Account Team Sign-Off
- Obtain Client Sign-Off

### 1.2.3 Law and Justice Environments

Vendor will deploy hardware and software to meet the physical separation requirements for the Law and Justice agencies.

#### 1.2.3.1 Public Defender

For Public Defender sites, Vendor will physically separate their networks from other County voice and data traffic. Public Defenders Unity (voice mail) will be built in the Orange County Data Center (OCDC)/Public Defender HQ. Public Defender has chosen to utilize the voice encryption capability for all of its locations.

### 1.3 Schedule

**Transformation Deliverables and Milestones**
**Please refer to the following two artefacts to obtain this information:**

1. **Appendix B 1A - Transition Plan**
2. **Appendix B-8B to Attachment B - Transformation Deliverables and Milestone Lists**

### Program Dependencies, Assumptions, Constraints and Risks

Dependencies

- County of Orange facility floor plans
- AD Read Permissions for Single Sign On
- VIP and Administrative Assistant programming
- In Scope Ancillary Information – e.g. Call Recording, Call Center, External Paging
- County of Orange Facility readiness including Power, Space and Cooling (changed to County)
- In Scope ACD – Call Center
- Access to existing to PBX information
- Porting DID from ATT to Subcontractor
- Site contacts and access to all County of Orange facilities to be transformed
- Vendor equipment procurement
- New circuit provisioning
- New circuit provisioning into facility (Subcontractor)
- County of Orange Facility readiness including Power, Space and Cooling
- **County Dependencies**
  - Perform DID Assignments if necessary
  - County resources for requirements determination/validation
  - County resources for building access and escort duties
  - County resources available for timely approvals of:
    - site scope sign-offs
    - legal agreements

  - formal approvals-to-proceed
- Define process governing how we process out-of-cycle/scope requests from County
- Ensure County of Orange Facility readiness including Power, Space and Cooling
- Provide Site contacts and access to all County of Orange facilities to be transformed
- Provide County of Orange facility floor plans
- Provide AD Read Permissions for Single Sign On
- Provide VIP and Administrative Assistant programming details

Assumptions

- Vendor will be able to rely on County of Orange employees to provide access/coordination on floor plans, hours, operations and contacts
- A 3rd party vendor who has been vetted and approved by OC I.T. will be used to provide hands-on support where we can't use local Vendor staff
- SMS will be used for all change/problem management
- Vendor will also use the County designated Service Desk (SAIC)
- Vendor will have access to County of Orange facilities where Transformation Project work is being conducted

Constraints

- The data network must be in place before monitoring tools can be installed and tested
- The data network must be in place in the data site before the VoIP clusters can be built
- The data network must be in place for remote management
- County and Agency engagement and communications constraints will be clearly defined by the County

Risks

- Lack of County resources for building access and escort duties could cause delays
- Lack of properly vetted and background-checked Atos resources could cause delays
- Lack of County resources available for timely approvals of sign offs and to provide floor plans could cause delays
- Lack of County of Orange Facility readiness including Power, Space and Cooling could cause delays
- Issues with AT&T and Subcontractor DID Porting numbers
- Issues with access to existing PBX data

# 2.0 People

### 2.1 Transformation Team

Vendor will establish a Transformation Team consisting of both dedicated and leveraged resources to implement the converged network.

| Vendor Role | Responsibilities |
|---|---|
| Program Executive<br><br>**Greg Mitchell** | Provides executive support for transformation goals and objectives; |

| | |
|---|---|
| | Resolves escalated issues<br><br>Manages executive relationships with the County. |
| Transformation Manager<br><br>**John Crockett** | Responsible for Network Transition and Transformation of outsourcing services including all transition and transformation deliverables, project plan execution, status reporting and progress; communication with the County stakeholders. |
| SUL - Network<br><br>**James Duley** | Responsible for delivery execution for the Data Network Management Services and Converged Network Management Services as Service Areas defined in Schedule 2A. This individual shall be a management interface and escalation point of contact for all matters relating to these Service Areas or sub-service areas. |
| SUL – Voice<br><br>**Keith Snyder** | Responsible for delivery execution for the Voice Communications Services and Converged Voice Management Services as Service Areas defined in Schedule 2A. This individual shall be a management interface and escalation point of contact for all matters relating to these Service Areas or sub-service areas |
| SUL - Security<br><br>**Wes Kanamori** | Responsible for delivery execution for the Security Services, as Service Areas defined in Schedule 2A. This individual shall be a management interface and escalation point of contact for all matters relating to this Service Area. |
| Service Delivery Manager<br><br>**Ukesh Chand** | Oversees delivery of day-to-day operational.<br><br>Manages development and implementation of the problem/incident, change, request, asset, and procurement management interface processes; defines and implements performance management procedures, including definition, development, and implementation of operational and SLR reporting<br><br>Manages development and delivery of content for the management portion of the policies and procedures manual; provides QA function for all sections of the manual; coordinates the County's review and sign-off on the manual;<br><br>Manages the definition, development, and implementation of in-flight projects. |
| 1. VoIP Transformation Manager | Responsible for implementing the Voice over IP Network. |

| | |
|---|---|
| **Michael Durk** | |
| Network Transformation Manager<br><br>**Garth Lowther** | Responsible for implementing the Data Network. |

### 2.2 Transformation Governance Model

Vendor will train all Transformation staff on the governance structure for decision making defined during Transition. Vendor will assign select Transformation staff to the appropriate governance committees including roles and responsibilities specific to governance.

### 2.3 Develop Communications Plan

Vendor will implement the Transformation specific elements of the communication plan. The details of the plans will be documented under Appendix B.5 Communication Plan.

### 2.4 Staffing Plan

Vendor has identified key candidates for positions and will complete the fulfillment of Transformation staff, including the Subcontractors listed under Attachment I Subcontractors. Our on-boarding model requires background investigations for certain key positions and conform to County requirements. Vendor has included time in the project to complete the following required screenings:

- Background check
- Drug testing
- Criminal background screening

In addition to these screenings, Vendor will carefully screen each candidate for competency and cultural fit within our organization and County environment.

Once the on-boarding process for the employee is complete, Vendor will engage in the following major transition activities:

- Completion of knowledge transfer- The knowledge transfer process will provide a transition of knowledge required to support the transformation environments. Detailed knowledge transfer plan is provided under Appendix B.6 Knowledge Transfer plan.
- Training staff on Vendor tools and processes

### 2.5 Stakeholders

#### 2.5.1 County of Orange

| Name | Role |
|---|---|
| Charlie Eckstrom | Interim CIO |
| Rob Newton | Transformation Program Director |

| Name | Role |
|---|---|
| KC Roestenberg | Operations Director |
| George Marcos | Transformation Program Manager |

### 2.5.2 Vendor

| Name | Role |
|---|---|
| Brad Rich | Executive Sponsor |
| Greg Mitchell | Account Executive |
| James Duley | Network Service Unit Leader |
| Keith Snyder | Voice Service Unit Leader |
| Wes Kanamori | Security Service Unit Leader |

# 3.0 Process

3.1 Overview

Vendor will adhere to all processes and procedures developed during Transition and develop additional processes and procedures where required during Transformation. The Transformation process is broken into phases and waves; Phases are data implementations and Waves are voice implementations. All Phases and Waves integrate with ITIL processes developed during Transition. The data phase is a predecessor to the associated voice wave. Vendor selected sites for each phase based on their relationship to the core backbone. Sites in each wave are based on their relationship to the associated data phase.

### 3.2 Phases

The data network transformation for in-scope sites will occur in four phases:

1. Phase 0 – core sites (backbone)
2. Phase 1 – large sites and satellite sites
3. Phase 2 – medium sites and satellite sites
4. Phase 3 – remaining Class 3 sites

Vendor selected sites for each phase based on their relationship to the core backbone.

### 3.3 Waves

The voice network transformation for in-scope sites will occur in four waves:

1. Wave 0 – core sites
2. Wave 1 – large sites and satellite sites
3. Wave 2 – medium sites and satellite sites
4. Wave 3 – remaining Class 3 sites

Sites in each wave are based on their relationship to the associated data phase.

### 3.4 Site Surveys

Vendor will perform Site Surveys 45 business days (or 74 calendar days) before site migrations occur. Site surveys include onsite visits, cabling build-outs if required, physical rack space assessments, and power requirement evaluations. Site survey results and requirements will be shared with the County within 3 days after the site survey allowing sufficient time for building preparation work to be performed. Other preparation tasks to be performed during site surveys include site user lists (DID's, Names, phone models), call routing patterns, phone and analog counts.

### 3.5 Transformation and Post Transformation Support for L & J Agencies

Upon completion of Transition, Vendor will provide monitoring and network management for County Enterprise WAN segments up to the L&J legacy network point of demark.

Vendor will procure, configure, provision the circuits and install the in-scope WAN and Voice equipment. Vendor will manage the transformed County Enterprise WAN up to where it interfaces with L&J Agency networks.

For the LAN equipment within each L&J Agency, Vendor will install, configure, test and turnover the converged network to L&J IT staff. The IT organizations within each L&J-designated Agency will be responsible for supporting their LAN and Voice steady-state infrastructures after transformation. Vendor will maintain and support County Enterprise off-premise voice components for L&J Agencies (excluding existing VoIP systems of the Public Defender). L&J will coordinate with Vendor NOC for the resolution of any incidents or outages that involve the County's converged network infrastructure.

Vendor will provide network engineering support for the L&J Agencies on a time-and-materials basis after Transformation is completed.

### 3.6 Operational Readiness

Vendor will perform Operational Readiness to ensure operations staff is prepared to accept the converged network.

### 3.7 Supplemental Management Plans

Following is a summary description of supplemental management plans that will be utilized, created and delivered by the Transformation management team to manage program deliverables.

#### 3.7.1 Communications Management Plan

The Communications Management Plan defines the following areas:

- Program structure including program governance, organization and roles and responsibilities
- Program communications schedule
- Program contacts
- Issue and action management process
- Escalation management process

#### 3.7.2 Risk Management Plan

The Risk Management Plan defines the following areas:

- Risk definition
- Risk tracking tool

- Risk management process
- Risk escalation process

### 3.7.3 Change Management Plan

The Change Management Plan defines the following areas:

- Program change management process
- Roles and responsibilities
- Change Control Board (CCB)
- Change request tracking and reporting

## 4.0 Tools

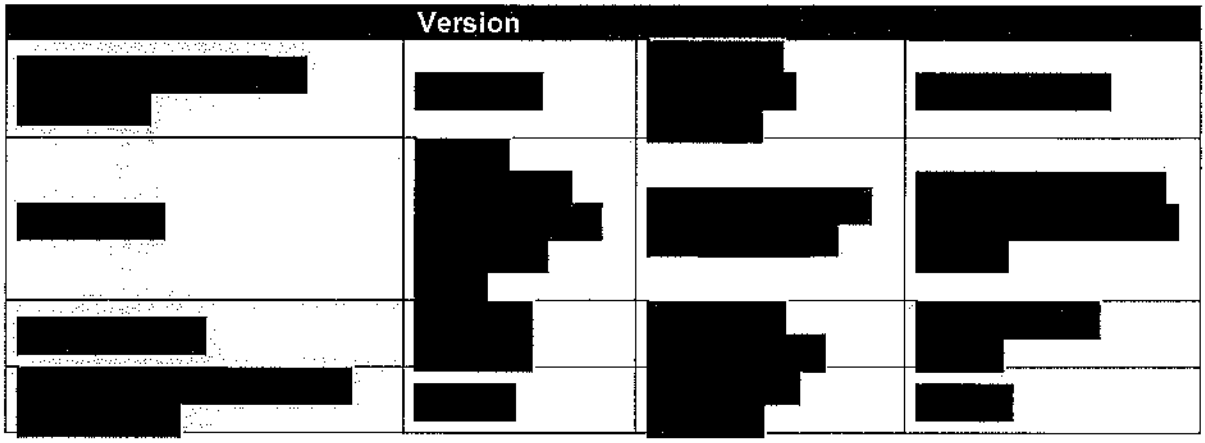
Vendor will utilize the following tools to monitor, measure, and perform service level reporting:

| Data Network Management Processes | Product Name & Version | Functions & Features | County Service Area – Components |
|---|---|---|---|
| SNMP Monitoring of Network Devices | SevOne | Real-time SNMP monitoring and Management | Routers, Switches, Firewalls, Wireless Devices |
| WAN Circuit Monitoring | SevOne | WAN Availability and Performance Management | Data & Voice Circuits |
| LAN Port Monitoring | SevOne | LAN Port Availability, LAN Utilization, Device Utilization | LAN POE Switches, Layer 3 Core Switches |
| [redacted] | [redacted] | [redacted] | [redacted] |
| VPN Monitoring | SevOne | Manages VPN circuits and appliances for UP/DOWN Connectivity | Remote Access Circuits, Firewalls |
| Remote Access Monitoring | SevOne | Manages Remote Access Users | Remote Access Circuits, Firewalls |
| Network Environment Monitoring (e.g., Circuits, Devices and Traffic) | AppNeta | Availability and performance management, traffic management and shaping. Application utilization and prioritization | All active devices, circuits – WAN/LAN traffic – Application traffic and device utilization |
| Network Utilization Monitoring | AppNeta, Cisco IPSLA | LAN/WAN Utilization, Device Utilization, Proactive | Routers, switches, firewalls |

| | | | |
|---|---|---|---|
| | | interaction with NetCool | |
| [redacted] | [redacted] | [redacted] | [redacted] |
| Consolidated MOMs | NetCool | Manager of manager consolidates alerts and information from all management tools | Vendors / County Network Management Tools and Apps |
| Network Availability | SevOne, Atos-ServiceNow, AppNeta, | End-to-End Network Availability | All In-Scope Network Devices, WAN Circuits |
| Network Performance | SevOne, | End-to-End Performance management and measurement | All In-Scope Network Devices |
| Network Administration | SevOne | Administration Management tools | All In-Scope Network Devices |
| Configuration Change Management | NetMRI | Equipment configuration management, backup and administration | All network equipment, firewalls |
| SNMP Monitoring of Network Devices | SevOne | Real-time SNMP monitoring and Management | Routers, Switches, Firewalls, Wireless Devices |
| WAN Circuit Monitoring | SevOne | WAN Availability and Performance Management | Data & Voice Circuits |
| LAN Port Monitoring | SevOne | LAN Port Availability, LAN Utilization, Device Utilization | LAN POE Switches, Layer 3 Core Switches |

Vendor will utilize the following tools installed during *Transformation* to monitor, measure, and perform service level reporting:

| Data Network Management Processes | Product Name & | Functions & Features | County Service Area – Components |
|---|---|---|---|




### 4.1 Program Portal

The program portal provides a consolidated view of the status of the various management plans and project schedule activities. The Vendor Transformation Manager is responsible for monitoring the definition, implementation and execution of the program portal process.

The program portal tracks project actions, issues, decisions and risks; the weekly calendar of meetings, project contacts, and detailed Transformation schedules, the quality management plan, and the change management plan. The tool is published daily to program stakeholders.

The following subsections briefly describe the supplemental plans contained in the program portal that are used for program governance and control.

A repository for electronic information exchange between Vendor and County of Orange will be created

## 5.0 Technology

### 5.1 Data Network Transformation

#### 5.1.1 Overview

Vendor will transform the County's legacy network into a converged voice/data environment with network equipment using Cisco technology and protocols supporting the deployment of converged data and voice services for County End Users. Transformation includes the installation of a new telecommunications network and hardware to support a converged set of services.

Vendor will perform Site Surveys 45 business days (or 74 calendar days) before site migrations occur. Site surveys include onsite visits, cabling build-outs if required, physical rack space assessments, and power requirement evaluations. Site survey results and requirements will be shared with the County within 3 days allowing sufficient time for building preparation work to be performed. Other preparation tasks to be performed during site surveys include site user lists (DID's, Names, phone models), call routing patterns, phone and analog counts.

Vendor will install the required patch panels, racks and associated wiring equipment to support the installation of 19000 CAT6 cables to meet County requirements and County cabling standard. Vendor will meet County's survivability standards and install new UPS devices if

required at each site within the required IDF and MDF wiring closets. All cables will be tested and certified to meet specifications and labeled according to County standards.

As part of Transformation, Vendor will perform all hardware procurement and onsite installations, fiber build-outs for diverse access into County facilities, network equipment staging and configuration, installation of new network cables and associated wiring equipment, circuit provisioning and installation, and will perform network engineering and production testing at the OCDC.

**Dependencies, Assumptions, Constraints and Risks**

Dependencies

- Delivery of equipment per schedule
- Accurate inventory of all supported systems
- Accurate information detailing the current County network (E2)
- Physical access to network infrastructure in order to complete the site surveys
- Security tools are dependent on core network functioning and have internet connectivity
- The data network must be in place and an agency migrated to the new network before monitoring can be tested
- County agencies and SAIC provide testers during migration into new network
- County approval of security services architecture in new network on a timely manner
- Horizontal cabling installation

Assumptions

- New Core Network up and available per schedule
- Delivery of vendor hardware is available and delivered on time
- County Agencies and SAIC are available to migrate Security services to new network
- County will approve security services architecture in a time manner
- Vendor personnel and their sub-contractors will have access to all County facilities

Constraints

- New IDS/IPS and other heuristic baselines will have to be determined each time a new agency is brought onto the Vendor network
- County Freeze calendar restricting timeframes to migrate security services to new network
- Limited County resources to perform site surveys with Vendor
- Variable levels of detail and accuracy provided by County agencies

Risks

- Monitoring tools will not be available if the data network is not established by the required due date if hardware not delivered on time
- The Vendor data network is not ready in the proposed timeframe and/or internet connectivity cannot be established
- Cabling/infrastructure is not ready in the proposed timeframe, which delays migration of legacy tools and installation of new tools
- Vendor hardware not delivered per schedule
- County Agencies and SAIC are not available to migrate security services to new network
- Incomplete documentation
- County does not approve Security Services architecture in new network
- Time needed to transform cabling infrastructure exceeds approved schedule
- Additional power requirements and the time to install new power
- Limited space for equipment configuration/burn-in prior to installation
- Inadequate environmental controls in IDF/MDF locations

- Access to building for build-outs to support Subcontractor infrastructure

### 5.2 Network Infrastructure Overview

Vendor will provide a complete refresh to transform the County's in-scope WAN/LAN infrastructure.

The solution is built on Cisco routing and switching equipment. All new equipment will be covered under maintenance contracts and onsite service will be provided to ensure SLRs are met. Additionally, Vendor will provide a pool of on-site spares within the County.

Vendor will connect sites with Subcontractor Metro Ethernet circuits where available. Sites that are not connected thru Metro Ethernet access and are off-net will either be connected with County fiber or Subcontractor fiber access back to the data center. These sites will be configured with dual Cisco ASR1002routers that have redundant 1 GB interface modules to support the County requirements. For sites that have County fiber segments, Vendor will provision a single circuit into the site and leverage the county fiber for the redundant connection required to meet SLA requirements.

**Dependencies, Assumptions, Constraints and Risks**

Dependencies

- Proper circuit provisioning with Subcontractor
- Warehouse location to store on-site equipment

Assumptions

- TW Telecom Circuits will be delivered per schedule
- Availability of County Fiber

Constraints

- Limited ability for County Fiber to work as redundant network connectivity
- No County Fiber from the OCDC to the Civic Center area to provide adequate redundancy

Risks

- Bandwidth provisioned through Subcontractor Metro Ethernet may be over or under subscribed
- Off-net sites circuit installation could be delayed

#### 5.2.1 Network Devices and Security

Vendor will configure additional firewall and security capabilities into the new Cisco routers and switches that will be installed at each of the Class 1, 2 and 3 facilities. This equipment will allow firewall functionality and functions, such as VLANs, data/voice traffic segmentation, VRFs and VPN tunneling to be available at remote facilities and eliminate the need for a physical device to be located at the OCDC for each agency. This will reduce the need for extensive firewall administration and large numbers of Access Control Lists (ACLs), and reduce labor and support requirements.

The Vendor implementation team will work closely with the Scope 1 vendor and County to ensure all security needs are considered and mitigated during Transformation. As each location is transformed to its future state, Vendor will ensure all Vendor Scope 2 managed devices and monitoring are integrated into the SEIM. Additionally, all processes and procedures defined in Transition will be applied.

The Vendor will provide controls and measures to control access, protect against intrusion, malware, vulnerabilities, and data loss, blocking and filtering, encryption, and policy compliance. These network and security tools will be installed locally within the data center and provide the support for the legacy and transformed infrastructures.

Additionally, all processes and procedures defined in Transition will be applied.

### 5.2.2 Firewall Transformation

Vendor will replace the current in-scope firewall appliances with new Cisco ASA 5585 firewalls. These firewalls allow the creation of virtual firewalls in each appliance that can be configured for individual County agency segmentation and security requirements. The virtual firewall environment addresses spoofing, denial of service (DoS) attacks, SNMP queries, ICMP attacks, and malicious traffic associated with NIMDA-type viruses and illegal IP address spaces.

Vendor will install two sets of Cisco 5585s within the Orange County Data Center (OCDC). These firewalls will be configured with dual redundant access and failover as part of the data center LAN infrastructure and will monitor all data traffic coming into or leaving the data center from the County and Agencies.

The firewall replacement approach consists of nine steps (for added details- please see MS Project Plan for Transformation):

1. Requirements analysis
2. Detailed design
3. Define critical practices
4. Establish network monitoring
5. Configuration and build
6. Test
7. Migrate
8. Provide operation readiness and documentation
9. Turn-over to operations

### 5.2.3 Datacenter LAN Infrastructure

The Vendor solution utilizes a three-tier architecture for the Orange County Data Center LAN infrastructure to provide all routing/switching and security requirements for the County. Vendor will transform the current OCDC Brocade switching/routing infrastructure and the existing internet/extranet infrastructures to support the future data/voice, IP telephony, network Metro-Ethernet and MPLS connectivity and convergence requirements. Vendor will replace the legacy Brocade routing /switching equipment at the data center and remote firewall appliances within the agencies with a three-tiered Cisco LAN infrastructure at the OCDC. This infrastructure comprises a Core Network Layer that provides switching/routing functionality and switched native LAN Metro Ethernet connectivity for Class 1 and Class 2 sites on the Time Warner carrier network. Class 3 sites will be connected thru MPLS circuits and access into the Subcontractor carrier network. The Distribution support Layer-2 agency 1GB fiber connectivity to the OCDC, internet/extranet segmentation, Layer 3 routing / switching, data/voice traffic tagging and routing, and LAN Switch connectivity. The boundary

layer will support network connectivity for 1GB high-end servers, data center users, IP phones, Internet/extranet appliances and network management and monitoring tools.

Two ASR 1002 Routers will be installed as Internet access routers. These routers will run BGP protocol and handle load balancing of internet traffic. The core backbone of the network will consist of ASR1004 routers with 8GB diverse connectivity to the Time Warner Telecom carrier network. These routers will handle the core routing/switching requirements on the Subcontractor carrier network between the Metro Ethernet and MPLS networks. A pair of Cisco Nexus 7010 Layer 3 switches will handle the core routing/switching requirements within the data center and the segmentation of the LAN infrastructure thru VDCs which provide redundant instances and interfaces. Cisco 5596 Switches will support all Layer-2 connectivity for County and Agency locations that utilize County fiber access:

- Four interfaces in each chassis will be connected to Subcontractor Metro Ethernet backbone network (two for MPLS site connectivity and two for Core Ring connectivity)
- Eight interfaces will be configured between the two Nexus 7010s to support load balancing and redundancy
- Four interfaces are configured to support the ASA5585 Firewalls
- Eight interfaces to support the 5596 Distribution Switches (Side A)
- Eight interfaces to support the 5596 Distribution Switches (Side B)

The remaining six 10 GB interfaces will be used to support connectivity of the Boundary Cisco 3850 switches that provide the user connectivity and access into the data center

The distribution layer of the data center LAN infrastructure will consist of two redundant Cisco Nexus 5596 Layer 2 switches. The 1GB interfaces on the Cisco 5596 switches will be used to support Layer-2 and county fiber connectivity for agency sites into the data center.

In addition, these switches will provide connectivity for 22 Nexus 2248s internal switches and four Cisco ASA 5585s firewall appliances within the data center LAN Infrastructure. This configuration of the Nexus 2248s will provide for 1056 1GB switch ports for LAN switch connectivity into the core LAN Infrastructure.

The ASA 5585s firewalls have been configured as two redundant pair of devices with diverse paths within the data center. The two redundant pairs of Cisco ASA5585s will support Internal and External firewall requirements and rules. These appliances allow for access control between Agencies and access control to the servers themselves on an agency-independent basis. The ASA5585s have the ability of contexts, which are multiple firewall policies on a single device. This allows firewall policies to meet individual Agency requirements without affecting other policies. This configuration supports the requirements requested for agency segmentation and separation of traffic.

The boundary layer of the LAN infrastructure will be configured with 12 Cisco Catalyst 3850X switches and six Cisco Catalyst 3850X-10GB switches. These switches will support user and device connectivity within the data center and can be configured to support VLAN segmentation for individual data center LANs or IP phones. Vendor network engineers will work with the County to configure the logical and physical segmentation for each agency. The Law and Justice agencies will have physical network separation of all data and voice traffic as required.

Vendor will configure a separate LAN segment within the OCDC to handle the connectivity requirements of the network management, security and monitoring tools. These network and security tools will be installed locally within the data center and provide the support for the legacy and transformed infrastructures.

### 5.2.4 Core Sites Infrastructure – Class 1 On-Net

For Class 1 Sites, On-Net is defined as locations where Subcontractor has or will provide their fiber directly into facilities. Current boundary routers at the remote County and Agency Headquarters locations will be refreshed with two different equipment configurations depending on the WAN access the site requires into the core network. Sites that are network connected on-net directly to the Subcontractor Metro Ethernet network thru fiber access will be configured with dual Cisco ASR1004 routers with redundant 10GB interface modules.

All network processing and switching functions will be handled within the Core of the network. The distribution layer will handle the server connectivity and processing functions, as well as supporting fiber access and remote sites connectivity in addition to supporting the security requirements for segmentation between agencies and access control. The boundary layer will be configured to support all user accesses (such as well as Internet, intranet, extranet, VPN and IP telephony).

### 5.2.5 Class 1 Sites - Off-Net

For Class 1 Sites Off-Net is defined as locations where Subcontractor utilizes a 3rd party local exchange carriers (AT&T) for entrance facilities (last mile access into facilities). Vendor will provide new Cisco networking equipment for all Class 1 sites.

The sites will be configured with dual Cisco ASR1002 routers to support WAN connectivity back to the OCDC.

The existing LAN edge switches that support user connectivity will be replaced with new Cisco switches with the designated IOS and interfaces capable of supporting Power over Ethernet (PoE) technology in addition to MPLS and the required network protocols for data tagging, encryption, VLANs and voice/data traffic segmentation. Vendor will also be responsible for the installation of Cisco 4507 LAN switches and Cisco 3850 switches with 1GB interface cards.

### 5.2.6 Class 2 Sites - Off-Net and County Fiber Sites

For Class 2 Sites Off-Net is defined as locations where Subcontractor use utilize a 3rd party local exchange carriers (AT&T) for entrance facilities (last mile access into facilities). These locations will be configured and transformed with a single Cisco ASR1002 router. Each router will have dual network circuits either through existing County fiber connectivity or Subcontractor MPLS circuits. The existing LAN switches at Class 2 sites will be replaced with new Cisco 4507 and Cisco 3850 LAN switches that will support network requirements for network segmentation and VLANs, and provide 1 GB ports for new IP phones at each facility.

### 5.2.7 Class 3 Sites

The Phase 3 transformation will include the replacement of WAN routers and LAN edge switches at each site. Sites will be connected to the Subcontractor network through MPLS cloud-based technology and have been configured with the required equipment and protocols to support connectivity, encryption, segmentation and data/voice traffic prioritization and remote management. For the WAN connectivity, Vendor will install Cisco 2951 voice-enabled routers. Each router is designed to support IP-VPN MPLS access from 1.45mbps-10mbps.

All current LAN Edge switches at the Class 3 sites will be replaced with new Cisco switches capable of supporting PoE, VLAN segmentation and MPLS protocols. Vendor will replace the existing LAN switches with Cisco 3850 switches at the larger Class 3 sites and Cisco 2960s LAN switches at the smaller sites.

### 5.2.8 Wide Area Network Circuits

### 5.2.8.1 Vendor Network Topology Overview

The network topology is architected to support data/voice convergence. This service delivery infrastructure is based on Cisco routing, switching and IP-based unified communications technology, which enables migration from legacy-based voice communications. The two circuit types delivered by Subcontractor are Metro-Ethernet and MPLS within a single carrier network. Vendor will leverage existing County fiber and fiber switching equipment where available to support converged network connectivity requirements at large County and Agency locations.

Additionally, network firewalls and security functionality have been included to provide the necessary physical and logical segmentation of traffic and access for Law & Justice agencies and operations.

Vendor will have responsibility for all new Subcontractor Metro Ethernet, Voice and MPLS Circuits, Fiber Switches and fiber build-out costs for new entrance facilities to support the diversity/redundancy requirements and service level metrics.

As sites are migrated onto the new data network from Subcontractor, Vendor will work with the County to establish a decommissioning process for the existing AT&T circuits in place. AT&T circuits will not be pulled or damaged without County approval.

### 5.2.8.2 Class 1 Sites - On-Net and OCDC LAN/Security WAN

The core Class 1 facilities will be connected through diverse 10 GB circuits to the Time Warner Metro Ethernet backbone. Vendor will install dual-ring connectivity and diverse path access for the connections into the data center and other core Class 1 facilities. This configuration will provide redundancy and failover in case of a fiber cut or circuit outage. Vendor will build out fiber circuits and local access into Class 1 On-Net facilities designated to be provisioned with Subcontractor 10GB circuits.

### 5.2.8.3 Class 1 Sites - Off-Net WAN

Vendor will replace the current carrier circuits at these sites with Time Warner Metro Ethernet circuits at equivalent bandwidth to support availability and redundancy. For these sites Subcontractor does not have entrance facilities built into the building. These locations will require the use of a Subcontractor 3rd party carrier for the local exchange access (AT&T).

### 5.2.8.4 Class 2 Sites - Off-Net and County Fiber

Vendor will leverage the County fiber connectivity where available at these sites for one of the required network circuits into each facility. Vendor will replace the current carrier circuits at these sites with Time Warner Metro Ethernet circuits at equivalent bandwidth to support availability and redundancy. These circuits will provide a diverse path option, either connectivity through the Metro Ethernet network or through the MPLS network in case of a circuit outage or fiber cut.

### 5.2.8.5 Class 3 Sites

Class 3 sites will be re-engineered with a new Time Warner MPLS IP-VPN circuit that provides connectivity into the Subcontractor MPLS network. Vendor will configure sites with T1 or NxT1 Metro Ethernet circuits, depending on the size of the site and the number of users at each location. Vendor will implement SRST as part of managed voice services to provide phone access through the PSTN in the case of a WAN circuit outage.

### 5.2.9 LAN Cabling

#### 5.2.9.1 Upgrade all non-standard cabling

Vendor will upgrade all non-standard cabling to the County CAT6 standard, including patch cables that run between the LAN wall-jack and phone. Existing cables will be removed to provide necessary access for new cabling into raceways and conduits within designated facilities. In raceways and/or conduits where previously existing cables are encountered, Vendor will remove at least one previously existing cable from that same raceway or conduit for each new cable Vendor installs. Vendor will certify, dress and label all cabling, patch panels and jacks to meet established County standards within MDF and IDF locations, including termination of preexisting cabling found to be not yet terminated. Vendor has included 19,000 LAN cables for replacement and upgrade to the County CAT6 standard. Fewer LAN cables may be required once information obtained during site surveys is reviewed and Vendor will follow the agreed upon change control process to reduce any segments below the 19,000 cables proposed. On a prospective basis, beginning June 1, 2016, the Vendor agrees to provide, "as-built floor plans, under the same operational procedures in place prior to June 1, 2016, but with the Vendor's addition of the representation of those cables that are certified by the Vendor under the terms of PCR #14.

#### 5.2.9.2 Existing LAN Cabling Certification

County has requested that, in certain circumstances, Vendor certify and support existing cable environments instead of upgrading to or installing new CAT6 per the Transformation Design Specification. CAT5e and existing CAT6 cable are satisfactory to support the Gigabit Ethernet and Power over Ethernet standards that will be utilized at the County with the current Scope 2 converged network offerings provided by Vendor, however, Vendor agrees to provide only CAT6 cable in providing Services to the County's LAN environments. Further, certain circumstances or conditions may make it impractical to re-cable a building, e.g., the County may have a short term lease and it would be too costly to re-cable for such a short duration, or it may not be practical to run new CAT6 cable in an environment because of asbestos or other hazardous or limiting factors. The use of existing cabling is in compliance with the County Standards.

##### 5.2.9.2.1 Scope of work:

- Re-certify of a maximum amount of 7,000 existing cables so they can be attached to the Vendor converged data network during the Transformation Project. A new Change Order will be required if this number is exceeded.
- Approval from the County will be provided using the Cabling Statement of Work (i.e. the cabling statement that accompanies all transformations) prior to the work being performed.
- Certify that cables will pass the 1 GB certification tests (performance) required to be supported on the Converged network. This certification process includes an end-to-end test with output that can be provided upon request. See Appendix A for the detailed specification tested when using the testing equipment.

Note: If the cable does not pass this re-certification it will be required to be replaced with a new cable as part of the 19,000 until which time all the 19,000 cables have been deployed. Once depleted, the new cable will be charged using 3.1 Fee Sheet, Network

ADD Services Rate, Additional LAN Cable Installation & Additional LAN Cable Installation (Material) Unit Rates.

**5.2.9.2.2 Conditions:**

1. Existing cables certified by Vendor will not count towards the 19,000 cable resource units included in the Transformation Project.

2. Network Availability and Network Performance Service Level Requirements have no applicability to the re-certified LAN cables.

3. Incident Resolution and Response Service Level Requirements, as articulated in the standard problem resolution responsibilities defined in the Master Service Agreement, remain in effect.

4. Existing Cat6 cables can only be used from the user panel in closet to the office, cubical and common area.

5. Repair or replacement of cable, patch panels, jacks or inserts is not included in the initial scope of work required to re-certify the cable.

6. Includes a patch cable at the time the end-point is transformed to the converged network.

**5.2.9.2.3 Ongoing Support (Post Transformation):**

1. Cable failure of re-certified cables determined by due diligence to be caused by non-interrupted use within the facility will be Repaired/Replaced by Vendor at no additional cost.

2. Cable failure determined to be caused by mis-use or natural causes (furniture moves, pest damage, fire) will not be covered after re-certification occurs. If required, a separate work order will be opened and price will be negotiated with the County prior to the work being performed.

3. Cable failure determined to be caused by Vendor or one of its subcontractors will be Vendor's responsibility to repair/replace at no additional cost.

4. Normal and customary replacement of cable components such as biskets, face plates and cable connectors not determined to be caused by misuse or natural causes (furniture moves, pest damage, fire) will be repaired/replaced by Vendor at no additional cost.

5. Ongoing Support outlined above is applicable from the date of certification to the end of the term of the Agreement (March 16, 2019). This excludes the extension of the Term for up to two (2) additional successive periods of not more than one (1) year each.

**5.2.9.2.4 Certification Tests**

Vendor will perform the following tests using the testing instrument. Each re-certified station cable will be tested for the following pursuant to the field test specifications defined in ANSI/TIA-568-C.2 "Commercial Balanced Twisted-Pair Telecommunications Cabling and Components Standard":

a. Wire Map

b. Length

c. Insertion Loss

d. NEXT Loss

e. PS NEXT Loss

f. ACR-F Loss

g. PS ACR-F Loss

h. Return Loss

i. Propagation Delay

j. Delay Skew

The County is fully responsible for funding the cable hardware and installation of LAN cabling needed by the County in excess of the 19,000 cables referenced above. Vendor's charges to the County for this additional cabling over and above the 19,000 cable threshold shall be provided and charged to the County under Pass-Through Fees as described in Section 3.1.4 (Pass-Through Fees) of Schedule 3 (Fees).

### 5.2.10 County Provided Fiber Optic Cabling

Vendor will test the County's fiber. Fiber must meet or exceed the minimum transmission specifications as defined in ANSIITIAIEIA-568-C.3.Vendor will notify the County if any existing County fiber does not pass certification and will present the County with an option to resolve the issue.

#### 5.2.10.1 Once certified, the County's fiber will be:

1. supported by Vendor as is other Vendor supported fiber in the environment,

2. subject to Service Level Requirements, measurements and Fee Reductions.

#### 5.2.10.2 Ongoing Support (Post Transformation):

1. failure of certified fiber, determined by due diligence to be caused by non-interrupted use within the facility, will be repaired/replaced by Vender.

2. Fiber failure determined to be caused by misuse or natural causes (furniture moves, pest damage, fire) will not be covered after certification occurs. If required, a separate work order will be opened and price will be negotiated with the County prior to the work being performed.

3. Fiber failure determined to be caused by Vendor or one of its Subcontractors will be Vendor's responsibility to repair/replace.

4. Failure of fiber determined to be caused by something outside of Vendor's control is County's responsibility to repair/replace.

5. Ongoing Support outlined above is applicable from the date of certification to the end of the term of the contract (March 17, 2019). This excludes the extension of the Term for up to two (2) additional successive periods of not more than one (1) year each.

6. Atos agrees to pay for Fiber that is useable but the wrong type (Mode) of fiber for the solution.

7. County agrees to pay for any fiber that is not useable. This includes the repair and certification of the fiber.

### 5.2.11 Furniture Moves

#### 5.2.11.1 Out of Scope for Vendor - The following are examples of items that are out of scope for furniture moves:

1) Any move or condition that presents a human health hazard, such as standing water, exposed or unsafe power lines, the presence of asbestos or other materials that are known to cause harm, and the presence of hazardous materials (such as bio-toxins, sharps, and medical waste ).

2) Any furniture that requires disassembly, tools, or special equipment.

3) HIPPA cabinets/storage or objects where special handling is required

4) Furniture weighing more than 100 pounds.

5) Attached fixtures or furniture such as cabinets, desks with earthquake bracing brackets, modular furniture requiring a technician to disassemble or re-assemble.

6) Fragile items of a highly delicate nature i.e. MDF furniture, laboratory equipment

7) Items of high value, such as works of art, sculptures, etc..

8) Precision equipment that requires an installer to place the equipment or level the equipment.

9) Bookshelves, stacks of boxes, and other storage containers.

10) Furniture or items that are difficult to access or blocked by obstacles, such as pillars, permanent fixtures, or refrigerators.

#### 5.2.11.2 The following tasks are provided by Vendor, considered ancillary, inherent or necessary components of certain Services, including cabling installations and/or removals. Movement of:

1) Furniture under 100 pounds that can be easily moved.

2) One-piece desks not secured to walls or the floor.

3) Small electronic devices, such as workstations, monitors, and workgroup printers.

4) Office waste baskets not containing hazardous materials.

5) Small filing cabinets that are not excessively heavy.

#### 5.2.11.3 Vendor Responsibilities:

- Vendor will provide recommendations for furniture moves during each site survey, cabling survey, and power walkthrough (as applicable).

- Vendor will request for all cabling vendors to use care when moving furniture at all County Agency facilities and caution will be taken to not damage any furniture or other items at sites. In many cases, furniture moves may not be necessary when the work area can be accessed without moving the furniture in question (such as crawling under a desk or working around a printer). Upon completion of work in an area, Vendor is instructing cabling vendors to make best effort to return the area to the original state prior to moving the furniture (excluding the work that was being performed, such as removal of a rack or replacement of a faceplate).

County/Agency Responsibilities:

- The County and Agencies will alert Vendors of any furniture or items that should not be touched/moved (sensitive equipment, high-dollar items, HIPAA documents) as well as any known or possible hazards or dangers.
- Prior to known plans that may include furniture moves by the Vendor, the County will communicate to Agencies and their users to clear furniture surfaces of personal effects.
- Provide reasonable consideration in granting appropriate performance relief when Vendor encounters circumstances (described herein as "Out of Scope" for furniture moves) that delay Vendor's efforts.
- County will hire movers as necessary to comply with the parameters

## 5.3 Voice Network Transformation

### 5.3.1 Overview

Voice Transformation will occur in waves as described about in section 3.3.

Vendor will deploy three instances of the HCS environment in the Vendor's Dallas and Pittsburgh data centers. These platforms will be geo-redundant. Vendor will deploy three pair of Cisco Cubes within the OCDC to terminate the SIP Trunking to the County. The Cubes will be configured in a redundant configuration to support the 2,500 concurrent calls throughout the county.

Vendor will perform VoIP site deployments in a phased approach that follows the data network connectivity and network equipment transformation. During each Phase, Vendor will be configuring the Hosted Cisco HCS platforms to support the IP-based voice services. Vendor will also be remotely staging and configuring new voice equipment and providing onsite installation and configuration of new IP-phones for all users.

Vendor will provide enhance support during post-site migration periods (varies by site size – period ranges from 4 to 48 hours).

SIP trunking will be used to support all Inbound/outbound dialing to the County network and local circuits. PRIs and 1MBs at remote sites will support survivability and E911 functions in the case of a network failure.

All class 1, 2 and 3 sites will deploy Survivable Remote Site Telephony (SRST).

Vendor will export data from the current PBX where technically feasible and provide this data to the County Site POC. The County Site POC will coordinate with the Site organizations to validate the data's accuracy before site specific converged configurations are created.

Vendor will deploy a seven-digit dial plan across the county.

**Dependencies, Assumptions, Constraints and Risks**

Dependencies

- Delivery of the data network
- Vendor delivery of Hardware
- Roles and responsibilities will be established between Vendor and all third party vendors
- Vendor must have an accurate inventory of all supported systems.
- Dependent on AT&T to pull PBX data
- AT&T and Subcontractor DID Porting
- Dependent on County for access to all county locations for Vendor and Vendor's vendors
- Dependent on County for off-hours access to all county locations for Vendor's and Vendor vendors
- Dependent on County for all DID assignments during Site Requirements Determination
- Access to existing to PBX information
- VIP and Administrative Assistant programming
- In Scope ancillary Information – e.g. Call Recording, Call Center, External Paging
- In Scope ACD – Call Center

Assumptions

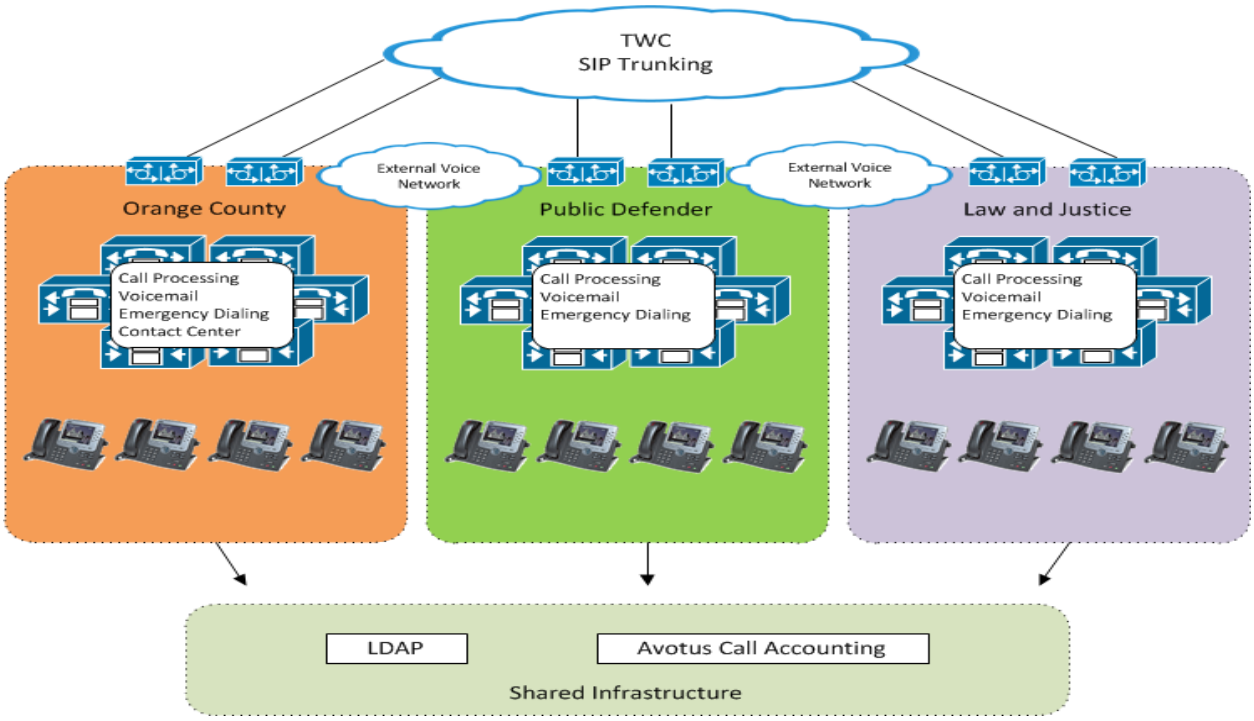
- Vendor will be able to rely on local County of Orange employees to provide access/coordination support
- Vendor personnel and their sub-contractors who have been properly vetted and where required have had successful background checks will have access to ~~all~~ the County facilities where they are performing work
- Vendor will have access to the PBX's to pull data
- A 3rd party vendor vetted and approved by OC IT will be used to provide hands-on support where we can't use local Vendor staff

Constraints

- The data network must be in place before monitoring tools can be installed and tested
- The data network must be able to support VoIP
- The local County of Orange spaces must be ready from a facilities perspective Power, Space, Cooling
- The data network must be in place for remote management

Risks

- Monitoring tools will not be available if the data network is not established by the required due date
- Incomplete inventory of in scope telephone systems
- Incomplete documentation
- Hardware not delivered on time
- Network not ready to support POE/VoIP
- Cabling/infrastructure not ready to support VoIP
- Issues with AT&T and Subcontractor DID Porting numbers
- Issues with access to existing PBX data




### 5.3.2 Hosted VOIP environment – Hardware/Hosting environment

Vendor will provide a combination of shared and dedicated components to deliver the solution to the County. Vendor will use a Shared Cloud Server infrastructure to deliver the core server components for the solution. The County's PBX applications will reside on dedicated blades within the Cloud Infrastructure to meet the requirements.

**Shared Components**

- Shared Cloud Server infrastructure to deliver the core server components for the solution
- All ITSM Tools and PBX monitoring tools

**Dedicated Components**

- Server Blades that contain the applications for the PBX
- Contact Center Express Premium Servers that support the ACD and IVR
- Emergency Responder Servers that support the E911 Solution
- Three separate pairs of Session Border Controllers (Cubes) that reside in California
- Dedicated Network connecting the Dallas and Pittsburgh Data Centers to the County MPLS Network
- CPE devices such as Phones, Analog devices, Voice Gateways

Vendor will implement geographically redundant Call Manager servers in Dallas, TX and Pittsburgh, PA. Vendor will implement a dedicated SIP trunking solution that is designed with redundant SIP Cubes in two locations in two separate County facilities within California.

Vendor will implement a Call Processing and Voicemail solution that can scale to 20,000 users on the County system and 5,000 users on the L&J solution without additional hardware. Vendor will implement a separate redundant Voicemail solution that resides in Orange County for the Public Defender environment.

Vendor will provide the following end-user voice equipment (see full list in Appendix 2C.1) (the "Basic+ Devices"):

- Cisco 6901 IP Phone
- Cisco 7841 IP Phone
- Cisco 7965 IP Phone
- Cisco 7916 IP Phone Expansion Module
- Cisco 8831 IP Conference Phone
- Cisco 8800 Keyboard Expansion Module
- Cisco 8851 IP Phone
- Soft Phones only with headsets for 10% of the user population

### 5.3.3 Hosted VOIP environment - VOIP Modules/Software

Vendor will provide the Cisco HCS foundation plus bundle using v8.6 or later. Foundation plus edition includes call control, voice messaging, instant messaging and presence

Additionally, the following modules are included in the solution:

- Cisco Call Manager for Call Processing
- Cisco Unity Connect for Voicemail
- Cisco Contact Center Express for ACD, IVR
- Cisco Emergency Responder for E911
- Normal Call Manager functions for tracking 411 calls and can route calls to the counties 411 provider

Detailed Voice Software list is provided under Appendix 2C.2.

The table below defines the service bundles:

| Bundle | Functionality | Devices Supported |
|---|---|---|
| Essential | Voice dial tone / Call Control for analog devices<br>1 Device | Fax<br>Analog |
| Foundation+ | Voice dial tone / Call Control<br>Single Number Reach mobility<br>Unified Messaging<br>Instant Messaging and Presence<br>Video calling<br>Desktop client license<br>Mobile client license<br>1 Device | All Basic+ devices, plus<br>78xx, 79xx, 88xx,89xx, 99xx<br>694x, 696x<br>Jabber desktop & mobile<br>Third party SIP<br>EX60, EX90<br>IMS Integration |

### 5.3.4 Softphone Deployment

Softphone deployments require coordination and communications with the Scope 1 Vendor or local Agency support since the desktop solution area is required for implementation. Meetings will be conducted with the Scope 1 Vendor as part of the initial pre-work before site migrations. Schedules will be confirmed with the Scope 1 Vendor. The Vendor will develop and provide the Scope 1 Vendor with service desk and desktop instruction scripts for softphone installations.

### 5.3.5 911 Calling

Vendor will document the 911 plan. This plan will include a design step to understand the 7 digit dialing plan along with the 911 staff location map. The resulting design requirements will determine configuration and operational documentation. Specific phone, messaging, and user templates will be developed. Vendor will use this data to configure the 911 data base. Site validation test plans will be performed which will included both inbound and outbound PSTN and 911 calls.

Prior to transformation, E911 and 411 will be handled using current processes, and Vendor will manage the current vendors for E911 and 411.

The Vendor will support E911 capability and functionality at all in-scope County locations. The Cisco Emergency Responder, in conjunction with the CUC Manager, sends emergency calls to the appropriate Public Safety Answering Point (PSAP). The calling party number is passed on as a DID number (called the Emergency Location Identification Number (ELIN)) which is tied to the specific location 911 call. If the call is dropped for any reason, the PSAP operator can dial the ELIN number to reach the 911 caller. Additionally, the system allows for notification of the 911 information to a front desk or security station if desired.

The 911 plan involves a design step where the Vendor meets with the County to understand the 7 digit dialing plan along with the 911 staff location map. The resulting design requirements are then used to determine configuration and documentation. Phone, messaging, and user templates are developed. The 911 data base configuration and synchronization is implemented. Site validation test plans are performed including inbound and outbound PSTN and 911 calls.

### 5.3.6 Seven Digit Dialing

Vendor will conduct a design meeting with the County stakeholders to define the requirements during the System design process. Vendor will implement this design for each site as it is transformed over to the VoIP environment. Sites managed by County staff will be cut over based on current design restrictions, platform versions and data network build-out.

Implementation details are as follows to implement 7 digit dialing:

- Unified Computing Infrastructure
- ''Meet with County on ""7 Digit"" Dial Plan & ""911"" Staff location map"
- Call Processing Infrastructure
- Messaging Infrastructure
- Presence Infrastructure
- Configuration & Settings Documentation
- “Create” “7 digit” “dial plan”
- Phone, Messaging, and User Templates
- Site Configuration Data Collection and Templates
- Create Templates for Site Assessments
- Develop Orange County Specific Training material
- Additional Details on 7 Digit Dialing
- Rack & Stack Voice Gateway & Analog Gateways
- Connect any new PSTN circuits to Router/Gateway
- Connect VG310 (Analog Gateway) w/ Analog Amphenol Cable from Patch Panels / 66 Block
- Bulk Import Users
- Configure Hunt Groups
- Configuration Auto Attendant

- "Create Site Restrictions and Dial Plans including" "7 digit" "dial plan"
- Configure Admins (Shared Lines w/ Managers)
- Configure Operators (If Required)
- Bulk Import Analog Devices

### 5.3.7 Voicemail

The voicemail platform will be deployed and integrated with the core infrastructure. Prior to migration, End Users will be notified of the migration with instructions that they will have a defined period of time (14 days, or as agreed with the County) before their accounts will be deactivated which will allow remove capture information on saved messages. As End Users are migrated to the new system, they will be set up on the new voicemail system. They will continue to have access to the old voicemail via PSTN access numbers until their account is deactivated.

### 5.3.8 Voice Conferencing

Vendor will work with the County to review the current Voice Conferencing users that reside on the existing platform. Once an audit is complete and the user list is verified including cost center information, email addresses and other information are used to correctly allocate costs. A mass creation of accounts will be set up on the voice conferencing platform.

Vendor will provide County with communication and training collateral for the End Users. The Vendor will provide to the Scope 1 Vendor service desk processes and procedures for creating, modifying and removing accounts, as well as instructions for escalating issues to the appropriate support teams.

Voice Conferencing will be transitioned to a new voice conferencing service.

### 5.3.9 Computer Telephony Integration

CTI requirements will be documented and reviewed with the County during the site information collection and site survey step preceding site cutovers. User lists, call routing, auto attendant, and ACD requirements are also determined. Design steps include the configuration of hunt groups, auto attendant, admins, voice and analog gates. Vendor will collaborate with Scope 1 Vendor as required for planning and testing prior to implementation.

### 5.3.10 Recording Devices

Vendor will determine Recording Device requirements during the site information collection and site survey steps that precede site cutovers. Approach includes collecting and developing a call flow design. County recordings definitions (WAV) would be defined. Voice recording is not included for L&J Agencies.

### 5.3.11 Conferencing Phones

Vendor will determine requirements for conference phones during the initial site information collection steps and site survey. Conference phone room requirements will be reviewed with the County. Conference phone implementation will be coordinated with the County and Scope 1 Vendor.

### 5.3.12 Current VOIP System Integration

Vendor will design and maintain the dial plan. The Vendor will provide required information to allow the out-of-scope Agencies to complete integration their integration configurations. Vendor will use direct SIP trunks and possible SIP trunks through the Cisco Cubes to complete the

integration. Vendor requires the OCPW and OCCR directory information be provided in comma delimited or some other standard readable electronic format and include it in the overall County directory.

## 5.4 L & JA Converged Network

### 5.4.1 Overview

L&J Agencies that are located in shared facilities with other Agencies will have a DMZ and stand-alone switch infrastructure installed to keep the agency traffic physically segmented from other agencies. This switch equipment has been included in the bill of materials for the solution.

Vendor will design, engineer and install the required WAN/LAN infrastructure and replace the network routing and switching equipment necessary to meet the requirements to support VoIP network connectivity to the county enterprise network. Vendor installed LAN switching, firewall and routing equipment will segment L&J Agency voice and data traffic both physical and logical from the County LAN and WAN.

Vendor will engineer the converged network equipment with the necessary VLANs and ACLs to allow voice and data traffic to be transported separately and securely across the LAN. VPLS tagging will be used to secure L&J Agency traffic across the WAN backbone network. Where required, Vendor will install separate LAN Switches in L&J sites that are shared between multiple Agencies to provide a physical segmentation of the L&J network and voice infrastructure. The IT organizations within those agencies will be responsible for all monitoring, management, tools and ongoing support for the LAN infrastructure within their facility.

### 5.4.2 Sites

#### 5.4.2.1 Class 1 Sites

Vendor will replace the current WAN access routers and switches at the L&J Headquarters Class 1 sites with Cisco ASR1004 routers that are configured with the required network interfaces to support redundant 10GB Metro Ethernet circuits into the County Enterprise network.

#### 5.4.2.2 Class 2 Sites

For Law and Justice Class 2 sites, Vendor will leverage the existing 1GB County fiber circuits at each site where possible and replace the existing carrier circuits with equivalent Subcontractor fiber circuits. To support redundancy requirements, where County fiber is unavailable, Vendor will provide a redundant Subcontractor circuit into each Class 2 location, which will give the ability to access the County Enterprise network in case of a circuit failure.

#### 5.4.2.3 Class 3 Sites

The L&J Class 3 sites will be reconfigured with new Cisco 2951voice-enabled routers. Each site will be provisioned with a Metro-Ethernet IP-VPN circuit with the ability to support bandwidth from T1 to 10mbps as needed based on the size of the site and the number of users supported. All new network equipment will support encryption capabilities and the ability for the L&J Agencies to segment voice/data traffic through multiple VLANs and VRF protocols.

The current LAN switches at each L&J location will be replaced with Cisco 4507e and Cisco 3850 PoE switches to support the IP phones and voice users. These switches can be used in either a centralized or distributed configuration within an Agency facility and can be segmented in locations where multiple Agencies share a County facility. This segmentation will enable L&J

Agencies to keep data and voice traffic separated from other agency traffic and can transport the traffic either over a single or multiple VRFs through the County network based on business requirements.

### 5.4.3 Public Defender

#### 5.4.3.1 Overview

For the Public Defender dedicated and shared sites, Vendor will engineer a DMZ with a Cisco 3925 router behind the County WAN access router to physically segment and separate the Public Defender networks from other County voice and data traffic. This router will be managed by the Public Defender IT staff and will limit accessibility of the network to only authorized personnel within the Agency.

#### 5.4.3.2 Public Defender Voicemail Solution

Vendor will implement a separate voicemail platform that resides on the County premise for the Public Defender. The solution will be a redundant platform. The County will be responsible for power, UPS and environmental requirements of the platform and will utilize switch ports within the facility that it resides. The platform does not have geographically redundancy.

### 5.4.4 Orange County Sheriff Department (OCSD)

#### 5.4.4.1 Overview

OCSD will have physically separate data networks including LAN and WAN for their data network at both dedicated and shared sites, therefor no DMZ is required at remote locations.

OCSD managed data network connections will terminate at identified OCSD sites to provide both primary and high availability network connectivity in alignment with the Class of Service definitions above. Vendor will provide a separate OCSD Data only Virtual Routing and Forwarding ("VRF") from Vendor managed network to route traffic back into the OCDC primary data network. Any traffic that OCSD would like to direct to other agencies will need to traverse that VRF and then through the Atos supported internal ASAs and IDS/IPS appliances as all other inter-agencies do for inspection. The OCSD Internet connection is provided by layer 2 point to point connection to the Atos supported external border routers at the OCDC where OCSD Internet traffic is un-altered and un-inspected.

The site-specific Transformation scope consists of the implementation of a data network with the specific intent to support of the utilization of the Atos Enterprise Cloud VoIP solution as a physically separate network from the primary data network used by OCSD to support agency-specific applications and business functions. Also, the Transformation Project will migrate the site-specific OCSD legacy telephone system(s) and handsets to the Atos Enterprise Cloud VoIP solution. The Transformation of the primary data network and on-going steady-state operation is not included in this scope. Any accelerated Transformation Implementation schedule, as requested by the County, will result in incremental expenses to perform the Architecture Design and incremental labor to accelerate the implementation (PM, Engineering & Tech time). The County will be responsible for these additional expenses.

### 5.4.5 Assessor

#### 5.4.5.1 Overview

Assessor has elected to manage their own data LANs and thus the hardware supporting local applications, PCs, Printers and servers will be physically separated from the voice network that Vendor provides and manages to support VoIP traffic. A common WAN infrastructure that Vendor manages will be the transport for both Assessors data and VoIP traffic. The demarcation point to Assessor managed data LAN will be at the layer 3 interface of the Vendor provided routers interface into the Assessor Data network.

# 6.0 Organizational Change

### 6.1 Implement Organizational Change Management Plan

Vendor will implement an Organizational Change Management Plan during Transformation to mitigate the impact on County staff as well as leverage the new functionality of the converged network. This includes identifying power users within Agencies to receive advanced training in order to help others understand the benefits of:

- Converged VoIP networks vs. separate voice and data networks
- Capabilities of the new environment and devices
- Leveraging new functionalities to improve productivity

Additionally Vendor will coordinate with Scope 1 Vendor include support scripts and workflow processes for initiating additional support from the Vendor so End Users have a seamless experience when seeking service support. Similarly, Vendor will coordinate with L&J IT staff to provide support scripts and workflow processes and mechanisms for initiating additional support from the Vendor.

# 7.0 Appendix

Please refer to Appendix 2A.2 for a list of sites