Exhibit 20: TECHNICAL NARRATIVE – REGION

EXHIBIT 20: TECHNICAL REQUIREMENTS NARRATIVE RESPONSE - Region

23.0.0: Describe the key success factors for the RNSP and how the RNSP will measure, monitor, and ensure timely implementation of NG 9-1-1 services. The description must include challenges and mitigation strategies that impact the project's critical path, and how the RNSP will comply with project plans and interfaces set by the PNSP.

CenturyLink will collaborate with the State to develop a comprehensive project schedule and conduct Process Integration Activity Workshops to integrate existing Cal OES processes with CenturyLink standard processes to standardize and optimize service delivery.

NextGen Platform Choice:

CenturyLink made a calculated choice to partner with Synergem to provide core services for our NG9-1-1 platform for California. While there were many factors in this decision, a key driver was the extraordinary level of monitoring, instrumentation, and alarming access that's provided through our partnership. Specifically, CenturyLink has access (in real time) to all the same raw monitoring, alarm, and instrumentation data that Synergem internally harvests about the core services and associated network infrastructure. Because of this, CenturyLink is able to leverage the core services platform without operational restrictions and visibility limitations that are often unavoidable in jointly provided solutions. Joint alarming and ticketing feed the detailed dashboard via APIs so that California can access and understand the health of its 9-1-1 network via the prime's required dashboard. APIs will connect the CenturyLink Regional Dashboard to the Synergem platform, as well as include the CenturyLink NG core platform, BRIX probes, and our SD WAN solution. The deployment model CenturyLink will implement for California includes deploying monitoring tools such as SolarWinds, BRIX probes and SD WAN. The combined tools provide extremely detailed reporting and visibility to network functionality across the PSAPs and the regional cores.

Dedicated NG9-1-1 NOC:

The CenturyLink NG9-1-1 Operations Center is tailored specifically to meet the requirements of the state of California RFP. CenturyLink will leverage a number of highly sophisticated monitoring tools to ensure the CenturyLink and Synergem system components and networks maintain the highest quality and availability. These tools include CenturyLink Remedy, SolarWinds, [redacted] Work Force Administration for monitoring all network elements, data communications, and remote facility environments. The Network Operations Center will provide continuous system support and monitoring 24 x 7 to the regional core processing center and database management system. The NOC monitors all PSAP connections into the ALI nodes at the application level. Staffing in the NOC is a US (24x7x365) and follows ITIL processes and frame work (Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement) to ensure the highest level of service. This team will have responsibility for reporting and notification for the state and custom development will include a dashboard for reporting. Notification responsibilities included with the solution ad hear to what CenturyLink has developed to meet FCC guidelines.

9-1-1 Circuit Tagging Methodology:

For CenturyLink 9-1-1 platforms that are supported via CTL network, we implement circuit tagging that flows through our systems and alerts anyone who is touching the circuit that it is carrying 9-1-1 service. The CTL NOC assigns an internal "TSP (telecommunications service priority)-like" code so we know that the circuit is tied to 9-1-1 services to ensure it is routed correctly and is flagged for optimal support. As a result, these circuits are tagged for priority in case of any emergency in terms monitoring, maintenance, and redundancy. CenturyLink will utilize this approach for all 9-1-1 network circuits that are required as part of this project.

Field Operations:

CenturyLink utilizes a multiple threaded sparing program which includes local, regional, and national sparing centers that allow CenturyLink to deploy spares within the SLA requirements in our customer contracts. Our network is designed , where possible, to be able to sustain a card failure without affecting customer services.

Our network operations centers work closely with our field teams on prevention and fiber cuts. The cooperation begins with building a robust plant, documenting network assets to ensure locates are done appropriately, and restoring quickly when a fiber cuts do occur. Similar to our sparing program our Field Techs are in market to accommodate such repairs and meet our SLA and contractual obligations. As a practice our field and operations center leadership review network outages caused by fiber cuts that are long duration for preventative and performance improvement items and put focus on areas that have a larger occurrence of cuts to prevent future.

Example of recent challenge and mitigation scenario for NG9-1-1 deployment:

CenturyLink encountered a challenge with the implementation of a NG 9-1-1 solution for another state. The challenge was this state only had one POP in the state that all MPLS traffic would have been homed to, this does not meet CenturyLink NG9-1-1 design standards due to lack of diversity for the ESInet. CenturyLink had to mitigate this issue by working with another transport carrier for the state leveraging our experience as an IXC and using relationships to provide the required diversity for the solution. Through our skilled PMO and Architecture teams CenturyLink has now provided the state a better solution providing additional diversity, reduced costs, and improved timeline. This is just one example of how CenturyLink uses it breadth of services to create a CenturyLink designed NG9-1-1 solution.

Program Milestones and Governance for Timely Implementation:

1. Key Milestones identified pre-contract signature:
    a. Identify Program Sponsors
    b. Establish Governance Comprehensive Governance Structure
        i. Develop Communication Plan
        ii. Implement Project and Monitor Project Progress
        iii. Identify Risk and Mitigation Strategy
        iv. Implement Program Lifecycle Governance
    c. Requirements Documentation
    d. Complete Network Design Documents
    e. Detail IP Addressing
    f. Define interfaces and connection locations to PNSP aggregation points
    g. Negotiate with LECs and Wireless providers
        i. Establish carrier connections
    h. Determine Routing protocol
    i. E-Bonding/API development
    j. Establish POI and Aggregation points
    k. SIP interconnection testing from SBC to SBC
    l. Installation/Deployment Plan
        i. Identify Points of Contact at each PSAP
        ii. Develop SDWAN WAN/LAN config
        iii. Site Surveys
        iv. Training
        v. Test/Turn-up Punch List
2. In depth knowledge transfer during the assessment phase of the program (stages initiation, discovery, analysis and design) from Cal OES and the Prime Service Provider service providers to CenturyLink prior to the first service migration in any given Regional Deployment to ensure operational readiness based on the agreed new process framework developed by the program

management team while taking into account previous lessons learned and ensure exchange of critical technical and operational details for lifecycle management.

3. Account for Regional OSP Providers, Cal OES, PSAPs, detail any differences based on requirements to be provided by Cal OES to achieve successful delivery & migration of network services existing environment to CenturyLink with no downtime without the use of legacy selective routers.
4. Achieve operational excellence for any migrated service from the existing provider to CenturyLink in alignment with all Service Level Requirements
5. Establish a framework for continuous improvement for continuous identification, development and implementation of proposed and approved changes to the program to deliver on the client benefits.

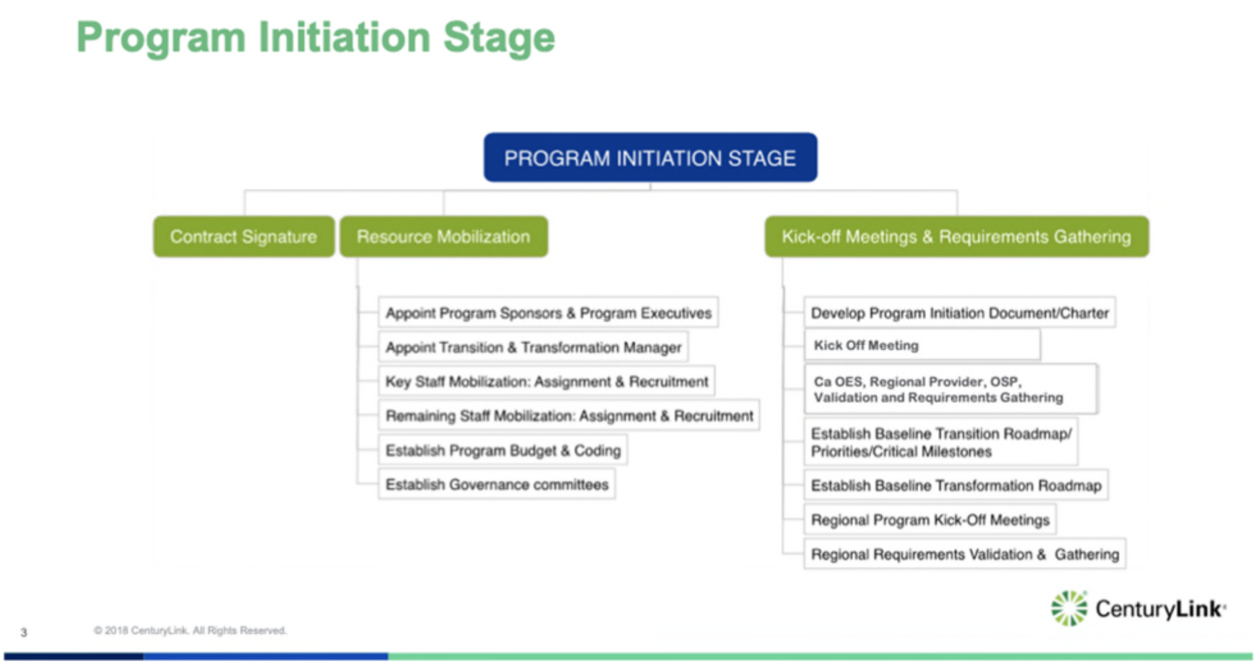
CenturyLink identified the following main work streams for the Scope of Work which will be directly mapped to Phases in the Program Schedule:

Program Initiation & Planning

The extreme large size of the overall program requires a dedicated program initiation stage and a program planning stage to ensure:

- All contract and statement of work requirements are properly translated into actionable program deliverables, to be reviewed and approved by Cal OES prior execution.
- Full review and gathering of technical requirements including gaps identified during due diligence and contract negotiation
- Sufficient time is planned for the mobilization and recruitment of the required dedicated core team and additional resources as per proposed staffing plan by CenturyLink as per RFP
- Sufficient time is planned for CAL OES to mobilize the critical "peer" resources as part of the proposed governance model in the RFP
- Critical communications structures can be established
- Critical governance processes can be put in place

The Program Initiation and Planning stage will comprise of the following key activities:



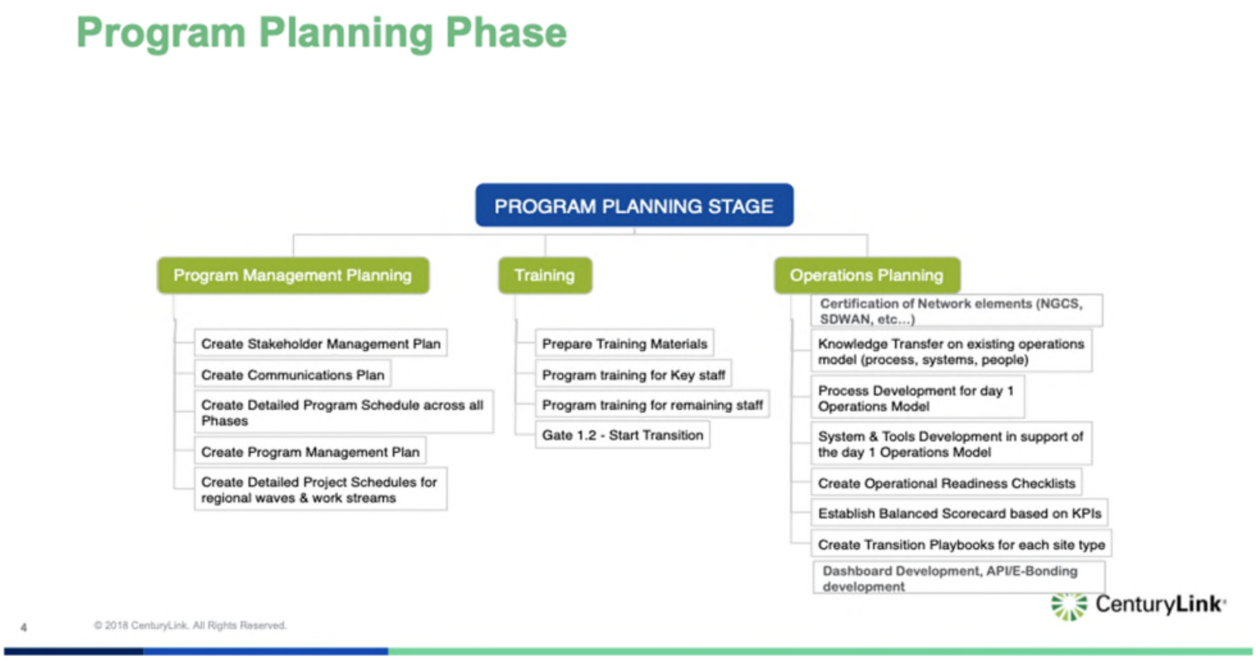
Program Initiation Stage

PROGRAM INITIATION STAGE

Contract Signature

Resource Mobilization
- Appoint Program Sponsors & Program Executives
- Appoint Transition & Transformation Manager
- Key Staff Mobilization: Assignment & Recruitment
- Remaining Staff Mobilization: Assignment & Recruitment
- Establish Program Budget & Coding
- Establish Governance committees

Kick-off Meetings & Requirements Gathering
- Develop Program Initiation Document/Charter
- Kick Off Meeting
- Ca OES, Regional Provider, OSP, Validation and Requirements Gathering
- Establish Baseline Transition Roadmap/ Priorities/Critical Milestones
- Establish Baseline Transformation Roadmap
- Regional Program Kick-Off Meetings
- Regional Requirements Validation & Gathering



Program Planning Phase

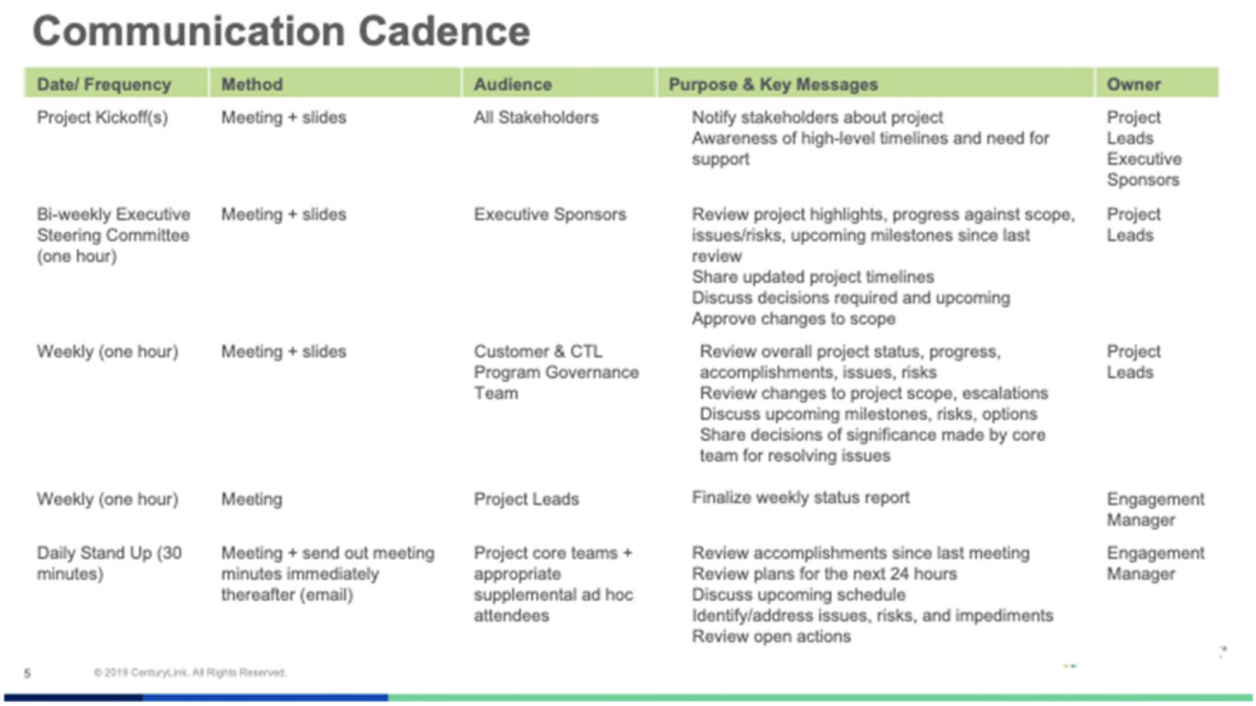
PROGRAM PLANNING STAGE

Program Management Planning
- Create Stakeholder Management Plan
- Create Communications Plan
- Create Detailed Program Schedule across all Phases
- Create Program Management Plan
- Create Detailed Project Schedules for regional waves & work streams

Training
- Prepare Training Materials
- Program training for Key staff
- Program training for remaining staff
- Gate 1.2 - Start Transition

Operations Planning
- Certification of Network elements (NGCS, SDWAN, etc…)
- Knowledge Transfer on existing operations model (process, systems, people)
- Process Development for day 1 Operations Model
- System & Tools Development in support of the day 1 Operations Model
- Create Operational Readiness Checklists
- Establish Balanced Scorecard based on KPIs
- Create Transition Playbooks for each site type
- Dashboard Development, API/E-Bonding development

Example of Communication Cadence:

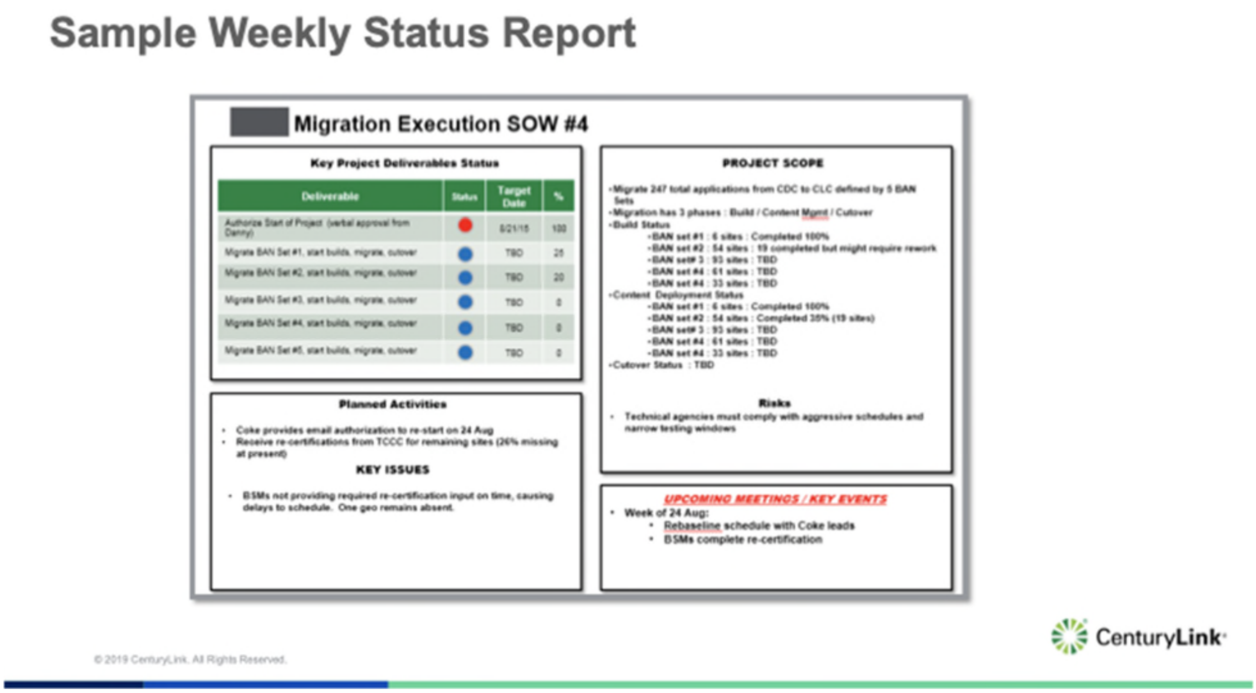


Communication Cadence

Date/ Frequency	Method	Audience	Purpose & Key Messages	Owner
Project Kickoff(s)	Meeting + slides	All Stakeholders	Notify stakeholders about project Awareness of high-level timelines and need for support	Project Leads Executive Sponsors
Bi-weekly Executive Steering Committee (one hour)	Meeting + slides	Executive Sponsors	Review project highlights, progress against scope, issues/risks, upcoming milestones since last review Share updated project timelines Discuss decisions required and upcoming Approve changes to scope	Project Leads
Weekly (one hour)	Meeting + slides	Customer & CTL Program Governance Team	Review overall project status, progress, accomplishments, issues, risks Review changes to project scope, escalations Discuss upcoming milestones, risks, options Share decisions of significance made by core team for resolving issues	Project Leads
Weekly (one hour)	Meeting	Project Leads	Finalize weekly status report	Engagement Manager
Daily Stand Up (30 minutes)	Meeting + send out meeting minutes immediately thereafter (email)	Project core teams + appropriate supplemental ad hoc attendees	Review accomplishments since last meeting Review plans for the next 24 hours Discuss upcoming schedule Identify/address issues, risks, and impediments Review open actions	Engagement Manager

5

Example of Weekly Status Report:



Sample Weekly Status Report

Migration Execution SOW #4

Key Project Deliverables Status

Deliverable	Status	Target Date	%
Authorize Start of Project (verbal approval from Danny)	🔴	8/21/15	100
Migrate BAN Set #1, start builds, migrate, cutover	🔵	TBD	25
Migrate BAN Set #2, start builds, migrate, cutover	🔵	TBD	20
Migrate BAN Set #3, start builds, migrate, cutover	🔵	TBD	0
Migrate BAN Set #4, start builds, migrate, cutover	🔵	TBD	0
Migrate BAN Set #5, start builds, migrate, cutover	🔵	TBD	0

Planned Activities

- Coke provides email authorization to re-start on 24 Aug
- Receive re-certifications from TCCC for remaining sites (26% missing at present)

KEY ISSUES

- BSMs not providing required re-certification input on time, causing delays to schedule. One geo remains absent.

PROJECT SCOPE

- Migrate 247 total applications from CDC to CLC defined by 5 BAN Sets
- Migration has 3 phases : Build / Content Mgmt / Cutover
- Build Status
  - BAN set #1 : 6 sites : Completed 100%
  - BAN set #2 : 54 sites : 19 completed but might require rework
  - BAN set# 3 : 93 sites : TBD
  - BAN set #4 : 61 sites : TBD
  - BAN set #4 : 33 sites : TBD
- Content Deployment Status
  - BAN set #1 : 6 sites : Completed 100%
  - BAN set #2 : 54 sites : Completed 35% (19 sites)
  - BAN set# 3 : 93 sites : TBD
  - BAN set #4 : 61 sites : TBD
  - BAN set #4 : 33 sites : TBD
- Cutover Status : TBD

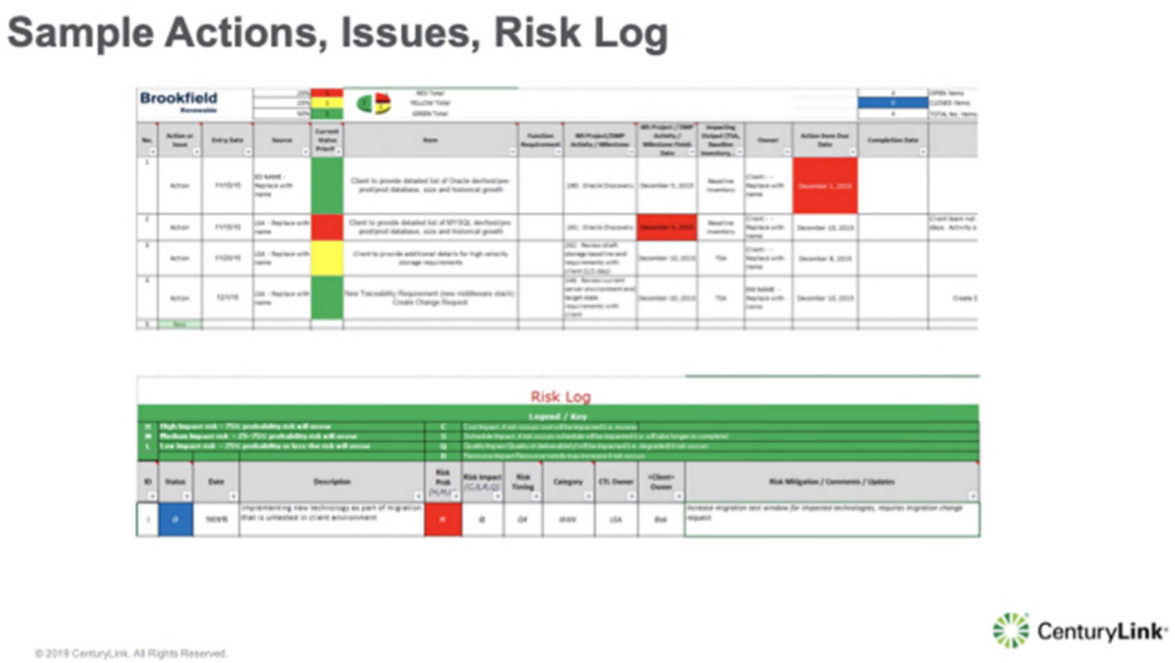
Risks

- Technical agencies must comply with aggressive schedules and narrow testing windows

UPCOMING MEETINGS / KEY EVENTS

- Week of 24 Aug:
  - Rebaseline schedule with Coke leads
  - BSMs complete re-certification

Example of Actions, Issues, and Risk Log:



Sample Actions, Issues, Risk Log

Brookfield
Renewable

25%	1	RED Total
25%	1	YELLOW Total
50%	2	GREEN Total

4	OPEN Items
0	CLOSED Items
4	TOTAL No. Items

No.	Action or Issue	Entry Date	Source	Current Status Priority	Item	Function Requirement	MS Project/DMP Activity / Milestone	MS Project / DMP Activity / Milestone Finish Date	Impacting Output (TSA, Baseline Inventory,...	Owner	Action Item Due Date	Completion Date	
1	Action	11/15/15	ED NAME - Replace with name	🟩	Client to provide detailed list of Oracle dev/test/pre-prod/prod database, size and historical growth		190: Oracle Discovery	December 5, 2015	Baseline Inventory	Client - - Replace with name	December 1, 2015		
2	Action	11/15/15	LSA - Replace with name	🟥	Client to provide detailed list of MYSQL dev/test/pre-prod/prod database, size and historical growth		191: Oracle Discovery	December 5, 2015	Baseline Inventory	Client - - Replace with name	December 10, 2015		Client team not days. Activity
3	Action	11/20/15	LSA - Replace with name	🟨	Client to provide additional details for high velocity storage requirements		242: Review draft storage baseline and requirements with client (1/2 day)	December 10, 2015	TSA	Client - - Replace with name	December 8, 2015		
4	Action	12/1/15	LSA - Replace with name	🟩	New Traceability Requirement (new middleware stack) - Create Change Request		246: Review current server environment and target state requirements with client	December 20, 2015	TSA	EM NAME - Replace with name	December 10, 2015		Create E
5	New												

Risk Log

Legend / Key

H	High Impact risk - 75% probability risk will occur	C	Cost Impact: if risk occurs cost will be impacted (i.e. increase)
M	Medium Impact risk - 25-75% probability risk will occur	S	Schedule Impact: if risk occurs schedule will be impacted (i.e. will take longer to complete)
L	Low Impact risk - 25% probability or less the risk will occur	Q	Quality Impact: Quality of deliverable(s) will be impacted (i.e. degraded) if risk occurs
		R	Resource Impact: Resource needs may increase if risk occurs

ID	Status	Date	Description	Risk Prob (H,M,L)	Risk Impact (C,S,R,Q)	Risk Timing	Category	CTL Owner	<Client> Owner	Risk Mitigation / Comments / Updates
1	O	11/6/15	Implementing new technology as part of migration that is untested in client environment	H	Q	Q4	WAN	LSA	Bob	Increase migration test window for impacted technologies, requires migration change request.

23.0.1: Describe the process using a non-proprietary NENA i3 compliant solution to route any 9-1-1 traffic to the correct PSAP within California for the awarded Regional NG Core Services, or when the Prime routes a call to the awarded region:

CenturyLink NGCS provides NG9-1-1 core services (NGCS) operated within the CenturyLink suite of hosted network solutions. CenturyLink NGCS Core(s) are a fully redundant network designed to offer services in compliance with the NENA NG9-1-1 standards defined in NENA-STA-010.2-2016 and future updates. CenturyLink NGCS Core(s) provide the essential routing functions of NG9-1-1, including the ESRP/PRF and ECRF/LVF, and in the case of this project will integrate with the PNSP to provide geolocation data for any awarded Region.

CenturyLink utilizes the prototypical architecture as specified in NENA STA-010 for routing calls from OSP end office trunks eliminating the legacy selective router. Specifically, arriving calls–either from the RNSP POIs, or transferred from the PNSP–are evaluated to determine whether they have location information in the arriving SIP headers; if they do not, a HELD request to the LDB allows location to be inserted. The location associated with the call is then used to make a LoST query to the ECRF, which yields a destination URI (i.e. the correct PSAP). Policy routing rules are applied, and the call is directed to the destination based on the information received and policies applied. The ESInet PSAP endpoint would be determined by the Call Handling Equipment(CHE) capabilities, which will be detailed during a site survey process. This would include SIP and location data delivery or options for a Legacy PSAP Gateway(LPG) if required.

23.0.2: Describe the process to route any 9-1-1 traffic to the Prime when the awarded region is unable to deliver the call to the correct PSAP. Description should include how this function will be supported when there is a complete loss of awarded region NG 9-1-1 services, and when the correct PSAP is not directly connected to the awarded region, and when the correct PSAP is connected to the awarded region, but is unreachable due to network or transport outage:

~~For calls destined to any PSAP that is not directly connected to the RNSP network, recursion of the LoST query to the PNSP ECRF will result in the PSNP ESRP being returned as the next hop for delivery of that call. The PNSP will then have responsibility for delivering the call.~~

Regional core services are deployed [redacted] This logic can be configured in the inbound SBCs such that if all instances of the RNSP core services are unavailable then the call will be directed to the PNSP. In the unlikely event that regional datacenters were completely unavailable, calls originating from all wireless carriers, AT&T wireline, Consolidated Communications wireline, and Frontier wireline should have the upstream elements (OSP SBCs or TDM gateways) configured to deliver calls to a PNSP aggregation point.

For calls correctly pointed to PSAPs that are connected to the region but are unavailable, the PRF will determine any potential alternate PSAPs that may accept the call. If all alternates are exhausted then the call will be directed to the default routing instructions, which presumably would be the PNSP. However, this will be determined at the time of system configuration.

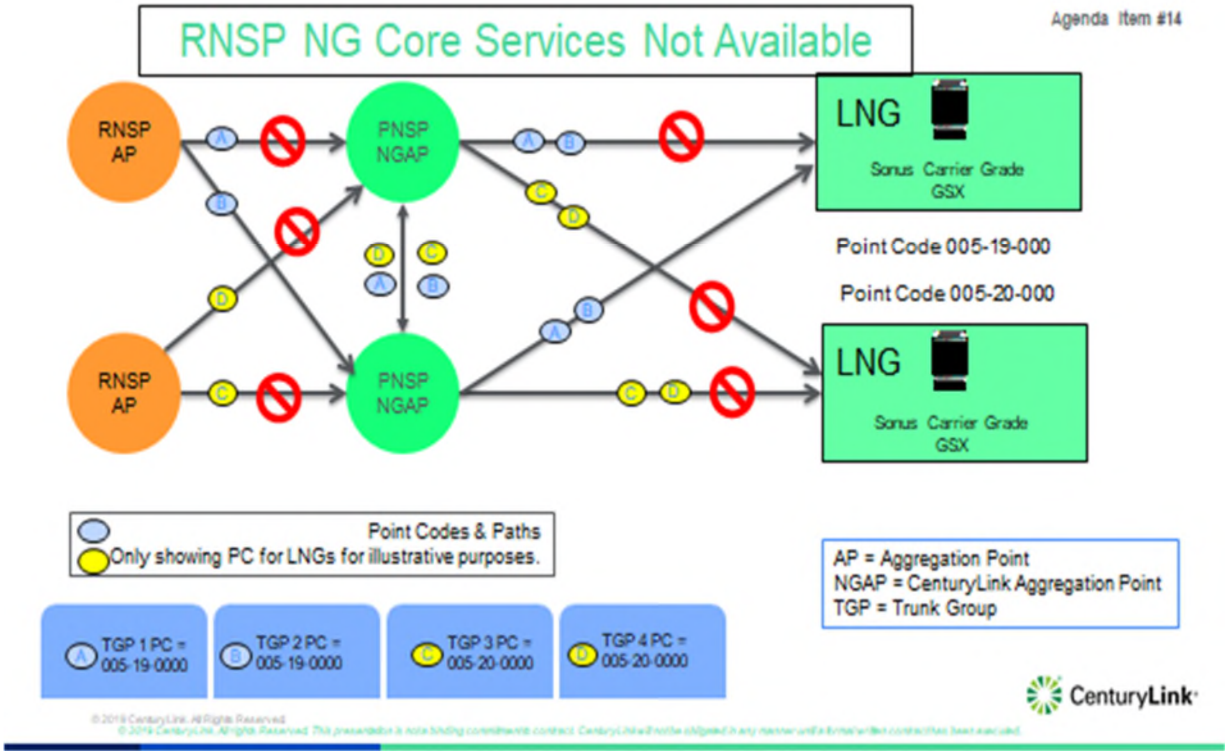
~~In the case of catastrophic loss of routing capabilities for the Region, the system as it has been envisioned by the State will route the call to the PNSP for handling within the rules defined by that system. This assumes the PNSP has maintained connections to the call-originating OSP as a backup.\~~

A PSAP that is not directly connected to the RNSP network, recursion of the LoST query to the PNSP ECRF will result in the PSNP ESRP being returned as the next hop for delivery of that call. The PNSP will then have responsibility for delivering the call.

For calls correctly pointed to PSAPs that are connected to the region but are unavailable due to a network or transport outage, the PRF will determine any potential alternate PSAPs that may accept the call. If all alternates are exhausted, the call will be directed to the default routing instructions, which presumably would be the PNSP. However, this will be determined at the time of system configuration.

Additionally, if regional core services were to become unavailable, trunking scenarios would trigger failures that would direct calls to the PNSP Aggregation point using SS7 point codes on different links that are established in this design. Based on the capabilities of the OSP our aggregation could contain MF or CAS trunking that will also have addition routing configured for failover as well that will include redundant path to the PNSP Aggregation location. This would include the calls originating from all wireless carriers, AT&T wireline, Consolidated Communications wireline, and Frontier wireline that have the upstream elements configured to deliver calls to a PNSP aggregation point.

Ideally this layer of contingency will be configured on the inbound regional LNG to relay this messaging back to the OSP switch that the NGCS SS7/MF/CAS paths are down to ensure that the calls are not delivered from the OSP to the LNG to choose the alternate path for this TDM delivery method.



RNSP NG Core Services Not Available

Agenda Item #14

Point Code 005-19-000

Point Code 005-20-000

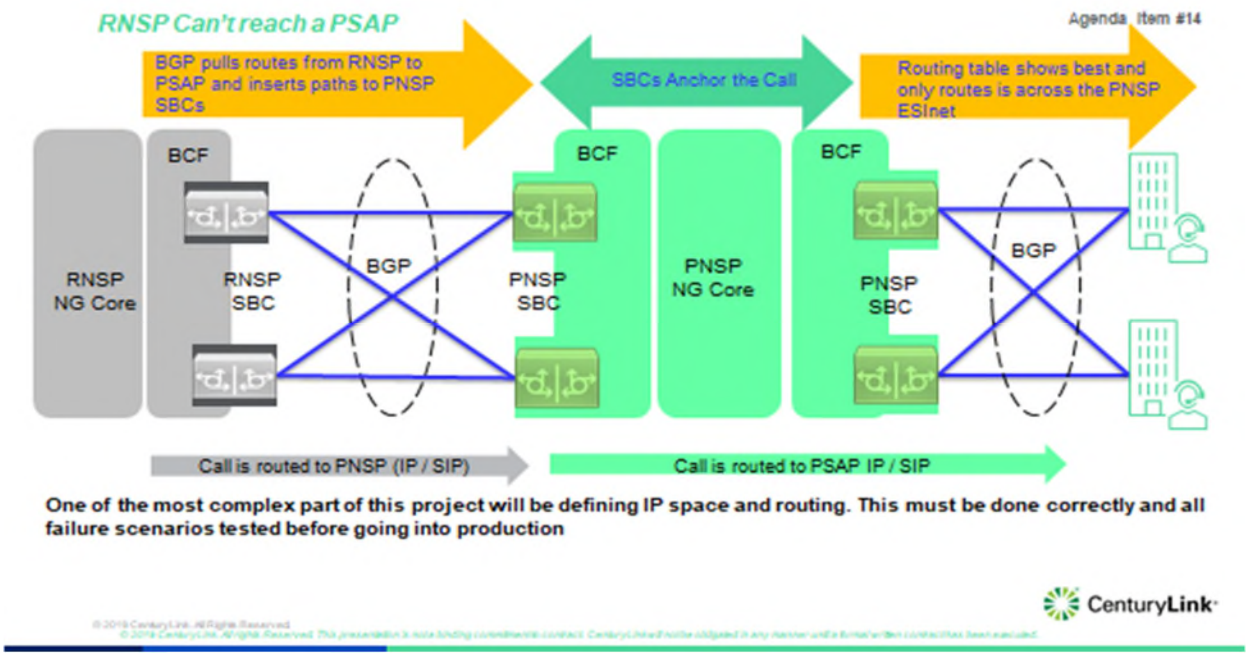
Point Codes & Paths
Only showing PC for LNGs for illustrative purposes.

A TGP 1 PC = 005-19-0000	B TGP 2 PC = 005-19-0000	C TGP 3 PC = 005-20-0000	D TGP 4 PC = 005-20-0000

AP = Aggregation Point
NGAP = CenturyLink Aggregation Point
TGP = Trunk Group

In the event of an RNSP ESInet outage to the PSAP, RNSP SBC can utilize connectivity to the PNSP to route traffic. This will utilize IP routing protocols to converge the traffic to the PSAP, most likely this will be BGP and mutual discussions with all RNSP and PNSP vendors will need to design, configure and document these networks part of the Planning and design phases.

- BGP is the external routing protocol and proper configuration of BGP with BFD is essential for fast convergence times
- When the RNSP network to a PSAP is down, RNSP will send updated BGP neighbors, removing the two PSAP RNSP network connections from the neighbor and routing tables. RNSP BGP will send the changes to PNSP BGP and PNSP tables will be updated.
- RNSP will route traffic to PNSP who will route the traffic to the PSAP over the PNSP network.
- Integration with RNSP ESRP/PRF and ECRF/LVF will allow CenturyLink to route on that data.
- By default, these routes from the RNSP can be prepended or set to have a local preference set so they as not preferred routes.



RNSP Can't reach a PSAP

Agenda Item #14

BGP pulls routes from RNSP to PSAP and inserts paths to PNSP SBCs

SBCs Anchor the Call

Routing table shows best and only routes is across the PNSP ESInet

Call is routed to PNSP (IP / SIP)

Call is routed to PSAP IP / SIP

One of the most complex part of this project will be defining IP space and routing. This must be done correctly and all failure scenarios tested before going into production

23.0.03: Describe the program management, collaboration and communication needed for the RNSP to comply with the best practices and interfaces developed for POI, aggregation, Region to Prime interface and Region/Prime interface to PSAP by the PNSP in coordination with the CA 9-1-1 Branch that demonstrates a commitment to transparency.

It is anticipated there will be migration to NENA i3 NG protocols as a region that are brought online during the initial term of this agreement. All stakeholders must be involved, and the process must be totally transparent if their complete cooperation is to be assured. Our PM plan incorporates the following steps to achieve this goal:

1. Fully involving all stakeholders in the planning process. This requires thoughtful briefings characterized by interactive communications and clear consideration of everyone's input.
2. Publication of a migration plan well in advance of its initiation date.
3. Proactive solicitation of stakeholder comments.
4. Collaboration with the PNSP to come to common interface for delivery of calls at the PSAP allowing monitoring and potentially terminating to a common SBC for a single SIP ingress to the Call Handling Equipment.
5. Building to the set specification and e-bonding interface with the PNSP for sharing ticketing information as well as an overall monitoring feed to the PNSP interface that is defined.
6. Designation of roles and responsibilities in the operation of parallel systems and specific training to help them cope efficiently.
7. Preparation of a detailed project management plan with sufficient task levels to ensure that all legacy and third-party interfaces are accounted for, all actions are identified and scheduled,

responsible management is assigned, proper resources are allocated, and operational impacts are articulated.

8. Simulating each migration step in a lab environment that employs actual end-users when possible.
9. Detailed acceptance testing against criteria described in a comprehensive test plan.

NG9-1-1 interconnection between OSPs and CenturyLink's is straightforward. It involves three phases – design phase, provisioning and cutover.
Design phase: (1) OSP inventories 9-1-1 connectivity and capacity requirements and reviews end-to-end signaling design with our team and; (2) A LOA/CFA (Letter of Authority/ Customer Facility Assignment) is created defining POI location, cross-connect information, and circuit activation and test requirements.

Provisioning Phase: (1) OSP submits SS7 ISUP orders and; (2) Once interconnectivity is established, end to end test calls to RNSP POI are coordinated with the OSP. Both parties ensure proper routing is in place on the voice and signaling switches to deliver calls to the POI.

Cutover: (1) The test strategy contained in the acceptance test plan is confirmed; (2) Offline testing is completed; (3) The POI test plan is executed; (3) A final maintenance operations protocol (MOP) review is conducted with each OSP; (4) Ability of POI to accept live calls is confirmed and; (5) Cutover is executed.

These phases are governed by our migration protocol that includes:

1. Ensure all state legal requirements are satisfied and coordinate contract requirements with OSPs;
2. Host kick-off meeting for all stakeholders;
3. Publish detailed migration matrix for local review that identifies risk situations and mitigation plans;
4. Develop tentative schedule on PSAP by PSAP basis;
5. Coordinate OSP involvement, scheduling and their need for routing products and services provided by STI;
6. Coordinate with call-handling vendor and incorporate that company in the migration process.
7. Integrate that vendor's plan with the STI master plan;
8. Meet with individual PSAP officials to ID local needs that may differ from the standard approach and to confirm that expected space and infrastructure are as expected and is ready for migration;
9. Deploy legacy gateways as necessary and required CPE;
10. Coordinate changes to Agency SOPs in accordance with recommendations made in step 3 above;
11. Train personnel in use of ESInet;
12. Confirm OSP readiness;
13. Activate cutover command center;
14. With fallback procedure in place, cutover CPE and call-for-service channels to ESInet;
15. Conduct preliminary acceptance test; Conduct 30-day observation period;
16. Report on lessons-learned that need to be acknowledged in follow-on installs;
17. Carry out remainder of schedule.

The POI test plan is a key component is this process. It involves:

1. SBC Security Testing
    a. Topology Hiding – The SBC will be configured to protect the identity of phones, computers and IP devices under test. (optional)
    b. Rogue RTP Protection – RTP stands for Real-Time Protocol which is responsible for delivering real-time media. The SBC will be configured to include provisions to detect and block Rogue RTP media streams. (optional)
2. SBC/SIP Call Routing/Policy Management tests (signaling and Media). Signaling and media will be generated by the CSP.
3. SIP Trunking Interoperability between i3-Interconnect™ and NGCS Production Environment
4. TDM to SIP messaging conversion/Translation
5. SIP Message manipulation/Mediation – ESRN/ESQK and ESRN SIP Header Insertion
6. Media Transcoding – Testing Different Codecs, G.711, G.726 optional, G.729 optional and ensuring the Media Codecs are supported.
7. DTMF/Fax Interworking – Dual-tone multi-frequency and IP based T.38 Fax Transmission functionality
8. Abandoned and Silent Calls
9. DTMF tone testing
10. TDD/TT/TTY call testing
11. Basic T1 BERT Testing – ESF (Extended Super Frame), AMI (Alternative mark Inversion) or B8ZS (Bipolar 8 zero substitution) encoding methods, CRC error testing.
12. Redundant Components Failover Testing
13. Circuit Failover Testing
14. Site Failover Testing
15. End to end Validation testing - CSP to PSAP
16. Load Balancing – Distributing Traffic Load testing. SIP call load balancing vs failover functionality testing.
17. Simulation of Peak Traffic Load.
18. Reporting/Monitoring Testing (Peak Load)
19. Alerting/Alarm Validation Testing (Peak Load)
20. SLA Compliance Testing (Peak Load)
    a. Packet Latency – (20ms)
    b. Packet Loss – (0.5%)
    c. Jitter – (20ms)
21. 21. MF trunk (CAS signaling) testing (if required)
    a. Trunk seizure and wink back
    b. Feature group D testing
    c. Wireless emergency call routed via MSC over MF trunk (ANI and ESRD out-pulse)
    d. Wireless emergency call routed via MSC and uses wireline compatibility mode
    e. On-hook indication to SIP BYE
22. 22. SS7 interface
    a. SS7 ISUP call end-to- end testing
    b. Supervisory message testing (blocking/unblocking/ acknowledgement)
23. Call Transfer/Conference functionality testing

23.0.04: Describe how the solution will support Location Based Routing using location data provided by either an Originating Service Provider, a device operating system, or a location clearing house, as directed by the CA 9-1-1 Branch:

CenturyLink's solution utilizes the best location available at the time the call is routed. This can be from location that is sourced from the LDB provided by an inbound carrier natively, or alternate location providers derived from third-party sources such as a location clearing house. The system has the flexibility to query the appropriate database for location information if location is not included with the call.

For scenarios where location is natively provided by the OSP, our core services recognize that a location (either location by value or location by reference) is available and therefore will not perform a look-up to the LDB, and instead use the natively provided location to determine routing for the call.

For handset OS-derived location it is expected that this data may be available via location clearing houses in the near- to mid-term, and that such location data will eventually be the source of the data natively provided by the OSP to the core services.

For location clearing house data, we have existing relationships with some of these entities, and are prepared to utilize the data provided by them when the State moves forward with one or more of these services. In cases where this results in multiple locations for a call, the core services make an automated determination as to which of the available locations to use for the call.

23.0.5: Describe the methodology that will be employed after contract award to ensure NG9-1-1 services provided are consistent with tariff filings:

The tariff provides technical details for each element of the service that can be purchased, along with pricing. The service order process will become the definitive contractual obligation for what services are to be provisioned. CenturyLink will work closely with Cal OES and other stake holders to fulfill the order obligation using comprehensive cutover and acceptance plans at every level to ensure the services are as defined in the tariff. CenturyLink will have reporting and analytics once the service is implemented to ensure that the services maintain compliance with the order (therefore the tariff), which includes verification of available capacity, performance metrics, pricing, etc. CenturyLink has dedicated regulatory personnel that work closely with the Cal PUC to file the services that comply with the RFP design and state statutory obligations. Tariff filing will be updated to mirror what the State has provided in the Exhibit 22 Cost Workbook tab #13 for Regional Cost Elements.

23.0.5.1: Of the four regions, what is you preferred region and why your company would have an advantage in that region? Why is this region assignment in the best interest of The State? The State makes no guarantee preferences will be accommodated and region assignment is determined solely by the State to achieve the best NG 9-1-1 solution.

CenturyLink is capable and confident that it can perform for the regional duties in any region of the state, if we are fortunately chosen for RNSP we would prefer to operate in the Los Angeles region of the state. This is based on the establish infrastructure that is in place which include Data Center space that our NGCS is already established in, as well as existing POPs for MPLS and access to the established POIs in the LATA or LATAs depending on the actual detailed boundary.

23.0.6: Describe how the RNSP shall utilize the statewide GIS database that is maintained and updated by the NG 9-1-1 Prime vendor for routing all 9-1-1 traffic:

Upon receipt of an updated GIS dataset from the Prime, it will be loaded into the ECRF/LVF by way of the SI. It will provide quality control checks on the data prior to loading into the production routing dataset and any discrepancies will be reported back to the Prime vendor. Once the GIS data has successfully passed the quality control checks, changes to the data are published to the ECRF and can be used for call routing. CenturyLink will work with the PNSP to define a process for adjudicating instances where there is a conflict in validity determination between CenturyLink the PNSP. CenturyLink's recommended approach for this resolution, at a high level, will be to determine the type of discrepancy, assess the source of the conflict, apply automated and if necessary human intelligence to resolve, and then to implement the resolution.

23.0.7: Describe the Emergency Call Routing Function (ECRF) and Location Validation Functions (LVF) that comply with GIS standards that include but not be limited to NENA STA-010.2-2016 Detailed Functional and Interface Standards for the NENA i3 Solution. Description shall include how the ECRF will updated based on GIS changes published by the PNSP:

~~ECRF and LVF functions are designed to meet NENA specifications as noted. We have provided functional descriptions within this document that show how each element is used in the system architecture. For the sake of brevity, we will refer the reader to the NENA specification if more detailed technical information is desired.~~

~~Regarding updating of the ECRF between the PNSP and RNSP, there is no interface defined in the NENA standard for this, but as an RNSP we will work jointly with the PNSP and other RNSPs to design and develop the appropriate solution.~~

CenturyLink will employ an ECRF/LVF with a fully featured LoST server, implementing all aspects of the protocol and behaviors specified in RFC 5222, and designed as a combined implementation to fulfill the NENA i3 requirements for both call routing and location validation. It can answer all described query types, supports queries in both the civic and geodetic-2d baseline profiles, performs location validation when requested, and is interoperable in a tree structure with other authoritative LoST servers using recursion or redirection (iteration). All service URNs in RFC 5031 are supported by default and additional service URNs may be added via configuration. The ECRF/LVF also supports discovery of additional data associated with a location and logging to an i3-compatible event logging service.

Because the ECRF/LVF is a critical functional element used both within the ESInet and by calls originating external to the ESInet, separate internal and external ECRF/LVF replicas will be deployed for each logical node. Internal replicas will only receive queries originating internally or from other trusted ESInets. External replicas will handle queries from untrusted networks and the public Internet. If external ECRF/LVF replicas are attacked or compromised, the internal replicas will still be available to service internal calls and those from trusted networks.

Validation of GIS updates is performed by the SI. When changes are submitted to it, a quality control process immediately begins checking the data for errors, which are rated for severity and flagged for follow-up. This solution includes configurable QC thresholds that can be used to block publishing to the ECRF/LVF. These thresholds can be set based on the total number or the total rate of errors above a chosen severity level, and multiple thresholds can be established. When publishing is blocked due to detected errors greater than a configured threshold, e-mail notification is sent to interested parties. In the CenturyLink NGCS regional instance for California, the updates will be via the PNSP. Thus, there is a potential for the variances in the QA algorithms in use at the PNSP and those employed by our NGCS at the RNSP to expose edge-case variances in the underlying datasets. CenturyLink will collaborate with the

PNSP to define a process for communicating such cases when they arise and for resolving the underlying discrepancy in order to resolve each such case.

23.0.7.1: List all subcontractors that will be used for ECRF/LVF. There is potential for some subcontractors to be used by multiple RNSP's or the PNSP. In that scenario, describe the bidder's strategy to prevent or mitigate one subcontractor's outage from causing an outage in multiple regions. Bidder shall describe how their solution provides an autonomous solution for ECRF/LVF.

CenturyLink's NGCS solution employs Synergem as a subcontractor for NGCS for the ECRF/LVF functional elements of its core services, Synergem obtains these elements via product purchase from third parties. Synergem has significant flexibility to deploy one or more of several providers [redacted] according to the needs of the project, including such considerations as which of those platforms are used by the PNSP and other regions.

23.0.8: Describe how the dashboard will display and report the health of the Regional network from ingress to egress. Description should include how the Dashboard shall monitor all 9-1-1 traffic in the assigned region and all NG9-1-1 trunks to ensure that SLAs are being met. Description shall also include how CA 9-1-1 Branch will access the Dashboard Monitoring, this shall include statistical data, printable reports, and outage notifications with duration:

The monitoring system detailed in this proposal supports our Next Generation 9-1-1 platform. CenturyLink has proposed our CenturyLink NG9-1-1 Operations Center, tailored specifically to meet the requirements of the state of California. A 24/7/365 NOC that monitors network and systems end to end. This monitoring includes component level monitoring, diagnosis and reporting. These reporting metrics and reports will be available for branch access via a secure URL and customized regional dashboard. The reporting metrics and reports will be available via the PRIME (PNSP) dashboard when appropriate E-Bonding has been established.

Joint alarming and ticketing feed the detailed dashboard via APIs so that California can access and understand the health of its 9-1-1 network via the prime's required dashboard.

The monitoring tools and system outlined below allow for error reporting and includes data collection and reporting capabilities. The following response will address components monitored and reported by the combined CenturyLink and Synergem solution. APIs connecting the CenturyLink Regional Dashboard will have visibility into the Synergem platform as well as include our CenturyLink next generation core services platform (NGCS), BRIX Probes and our SDWAN solution. CenturyLink will develop the API interfaces with Synergem for singular alarm and ticketing visibility.

1. All ingress and egress traffic will be routed through diverse regional core POPs – and continuously monitored. CenturyLink will deploy a Brix verifier solution for End-to-End MOS scoring from Ingress to PSAP edge.

2. As a Regional – CenturyLink will assign a developer to work with the appropriate PRIME (PNSP) contacts to ensure that the CenturyLink reporting and metric fields align with the PRIME(PNSP) from an Ingress perspective and script alignment. As well as coordinate the appropriate Egress metrics and fields delivered from the PNSP

3. Resiliency is designed and built into the solution with 99.999% availability. CenturyLink will deploy multiple virtual servers with load balancing between them.

4. Via SolarWinds CenturyLink will monitor all network elements and E-Bonding to the Dashboard to provide "Near" Real-Time data for alarming, notification, SLA reporting, etc...

- CenturyLink will consume and display the data for SLA compliance. CenturyLink cannot ensure SLAs for Prime Service Provider (PNSP).

- The dashboard is customizable and provides a multi-tenant view available via a web GUI.

    - API Integration into the State Ticketing system available upon request.
    - Two factor authentications.
    - Analytics, statistical data and reports will be developed based on requirements and agreed upon thresholds.

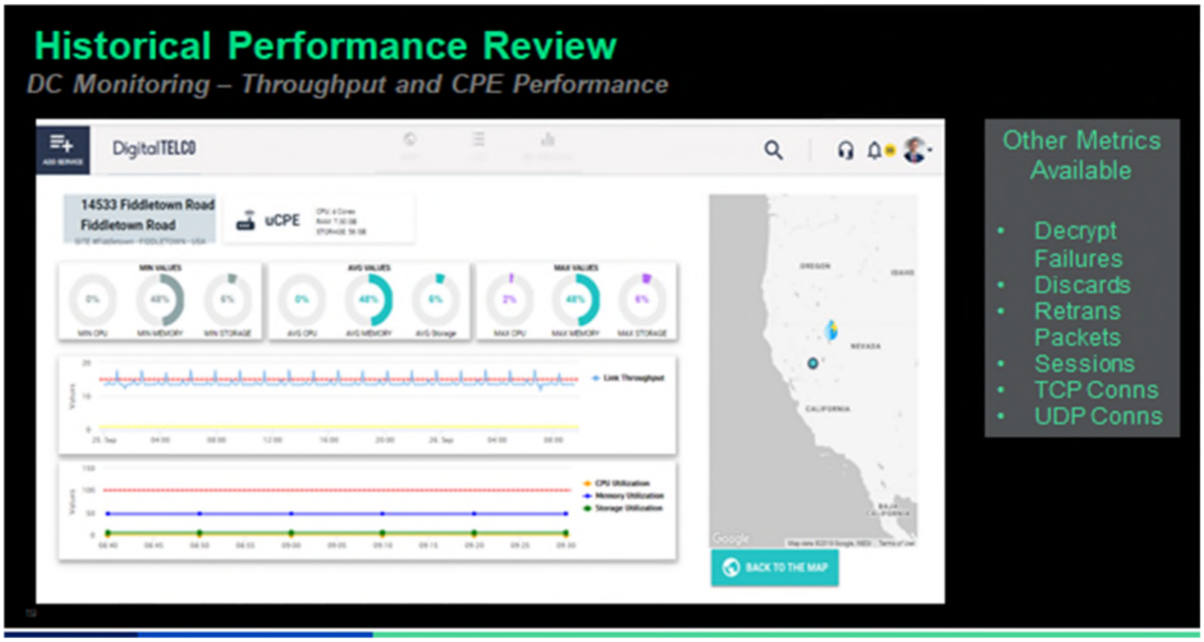
Auto ticket and alarming thresholds are to be customized based on negotiated SLAs and triggers.

5. Brix verifier solution for End-to-End MOS scoring from Ingress to PSAP edge. Brix is the probe system we utilize to generate, test and measure the results to the probes located at the PSAP. Probes will generate alarms/tickets on the impacted service If specific criteria are met. The NMA system will work with our PSAP notification tool to send automated notifications to the PSAP of impacted 9-1-1 services in awarded region.

    a. Brix Probes – will test end to end call quality metrics (MOS Scoring) this system will also do automatic call testing to insure network availability and functionality.

6. CDR Streaming for call by call reporting.

7.



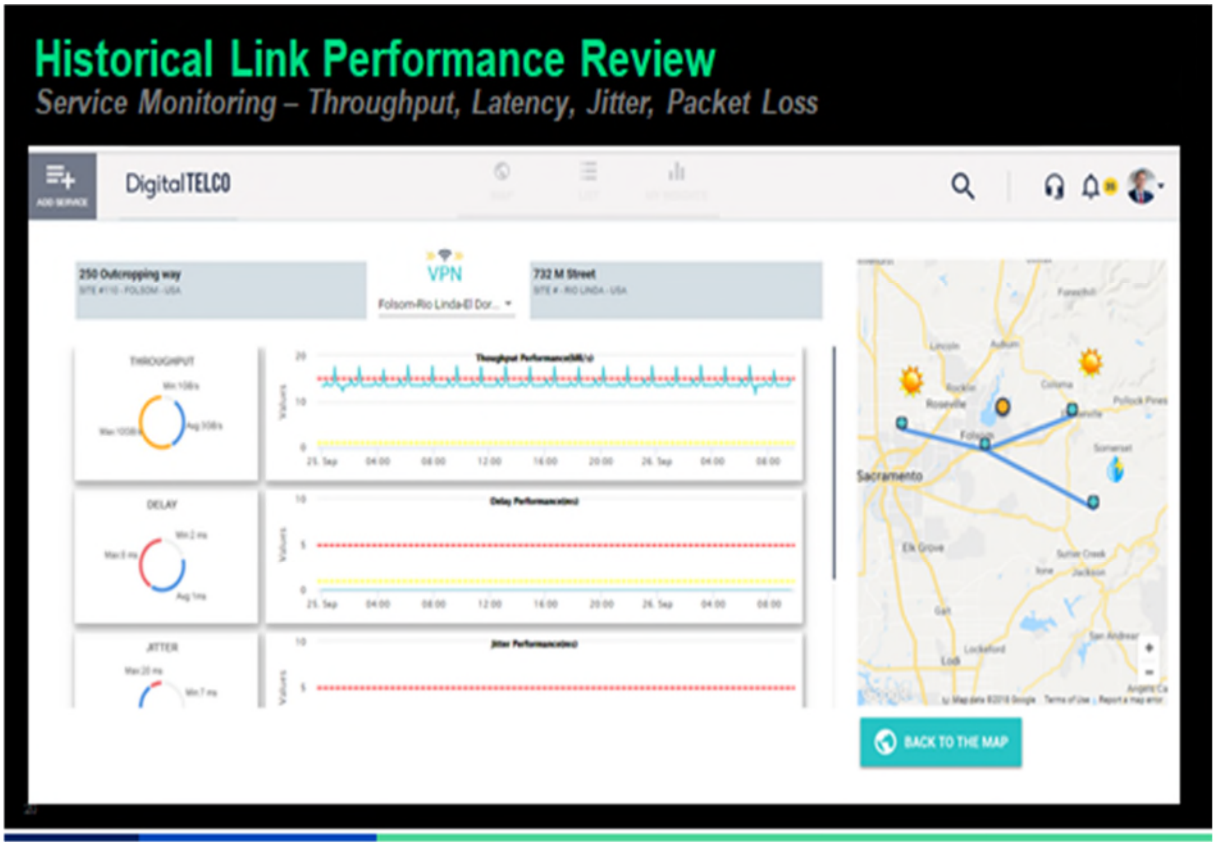
Historical Performance Review

DC Monitoring – Throughput and CPE Performance

Other Metrics Available

- Decrypt Failures
- Discards
- Retrans Packets
- Sessions
- TCP Conns
- UDP Conns

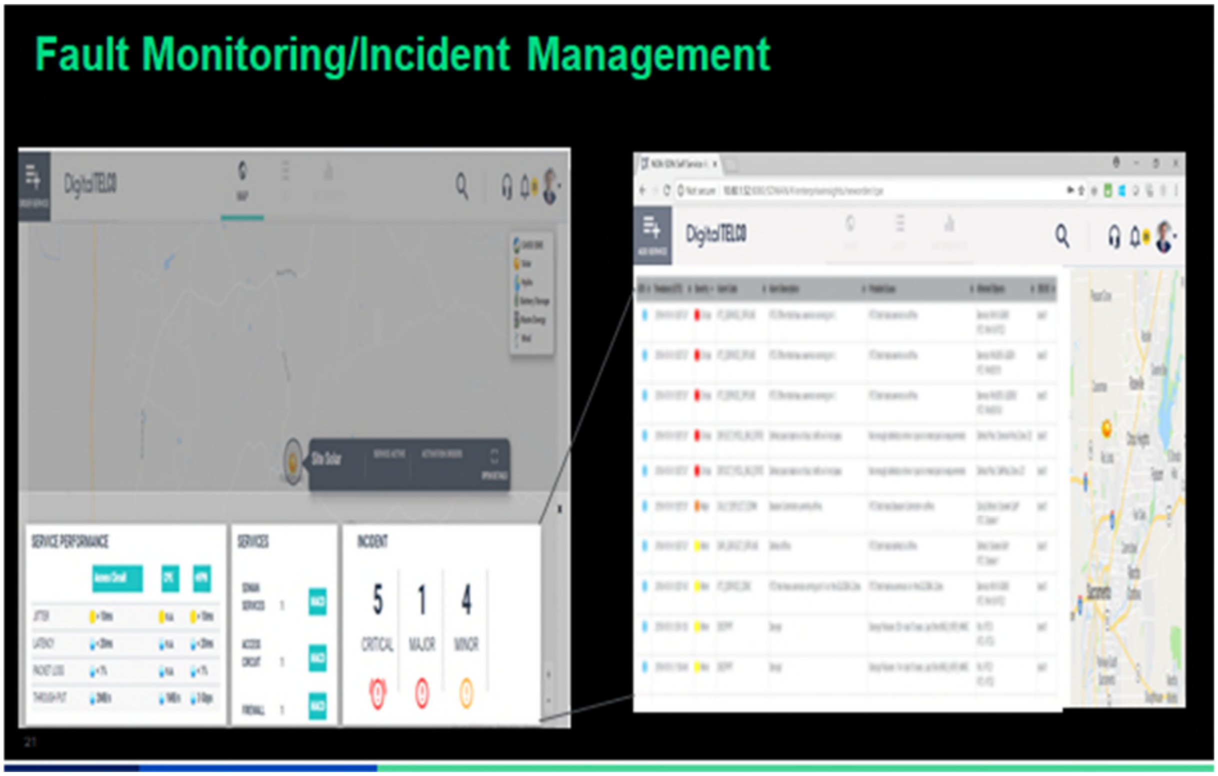
8.



Historical Link Performance Review

Service Monitoring – Throughput, Latency, Jitter, Packet Loss

9.



Fault Monitoring/Incident Management

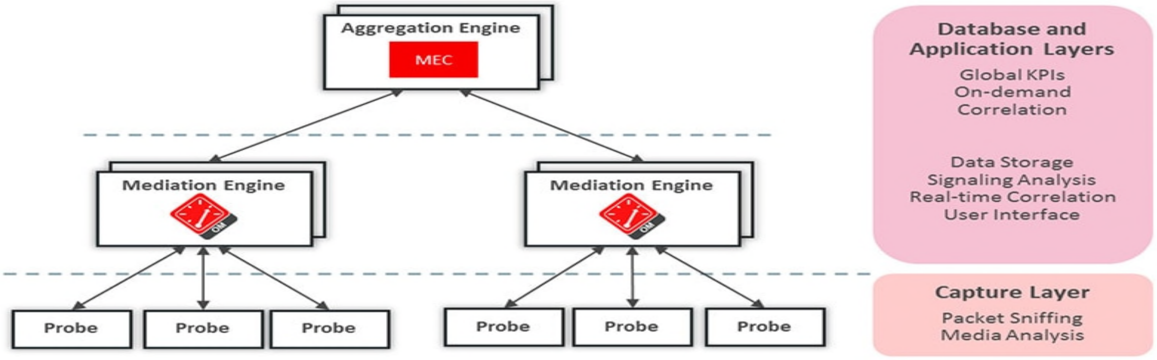
All Dashboard features and functionality are custom developed to incorporate all CenturyLink services. Dashboard will provide a single pane of glass for monitoring and management for regional visibility and performance tracking.

Via APIs, CenturyLink will consume and report Synergem alarms and ticketing into the Regional dashboard that will E-Bond to the PNSP.

Management Information Systems (MIS) will be provided [redacted]. This product captures all messages transiting the network using network probes linked to a correlation engine. Results and the dashboard are viewable through a web-architected GUI that will be integrated with CenturyLink dashboard and available to the State 3 to 6 months from Regional award.

The EOM is tightly integrated with [redacted] session border controller (SBC) service delivery platforms. Reporting efforts are 100% passive, nonintrusive and vendor agnostic. The [redacted] supports any next-generation network architecture and offers full, end-to-end correlation of all calls in real time. It enables network-wide views of calls and registrations as well as global KPIs and statistics, network equipment statistics and information, and user group and trunk information. It offers drill-down into the network, providing diagrammatic call flow analyses with full protocol details, raw capturing, and registrations end to end.

The below diagram illustrates the operating components of the EOM and describes some of the reports that it generates:



- **Network Tracing**

[redacted] provides real-time and historical call and transaction tracing facilities, with drill-down to sequence diagrams showing signaling transactions and media sessions (with the Media Quality extension) for each call across the entire network. Each step of the call can be viewed and analyzed to assess issues.

- **Network Alerts**

- Network issues and alerts for numerous issues, such as poor voice quality or slow responses, can be established with configurable network and service KPI alarm thresholds, and the alerts can be viewed instantly through a configurable dashboard. Dashboard graphs can include transit and response times, the number of registered users, the number of error calls, and so on. Alerts can be exported to network management systems with SNMP traps.

- **Call Logs** [redacted]
- [redacted] provides a list of all active and finished calls for the full network as well as a filter capability to identify problematic calls for further analysis.

- **Service Dashboards**

Color-coded dashboards enable problems to be recognized at a glance. Statistics on recent calls can include:

- Successes versus failures
- Voice quality information (requires the Media Quality extension)
- Call history with detail information

- **Statistics Dashboards**

The statistics and KPIs provided for a single subscriber include

- Distribution of calls by destination
- Call success rate
- Average call length
- Average number of calls per day
- Ratio of incoming versus outgoing calls
- Average mean opinion score (MOS) value

23.0.9: Describe the integration of system monitoring with data delivered / provided from each Regional network to include the e-bonded trouble ticket process.

The CenturyLink NG9-1-1 Operations Center is tailored specifically to meet the requirements of the state of California RFP. CenturyLink will leverage a number of highly sophisticated monitoring tools to ensure the CenturyLink and Synergem system components and networks maintain the highest quality and availability. These tools include CenturyLink Remedy, [redacted] Work Force Administration for monitoring all network elements, data communications, and remote facility environments. The Network Operations Center will provide continuous system support and monitoring 24 x 7 to the regional core processing center and database management system. The NOC monitors all PSAP connections into the ALI nodes at the application level. Staffing in the NOC is a US (24x7x365) and follows ITIL processes and framework (Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement) to ensure the highest level of service. This team will have responsibility for reporting and notification for the state and custom development will include a dashboard for reporting.

The CenturyLink NG-9-1-1 NOC will provide continuous system support and monitoring 24x7 to the regional core processing center and database management system.

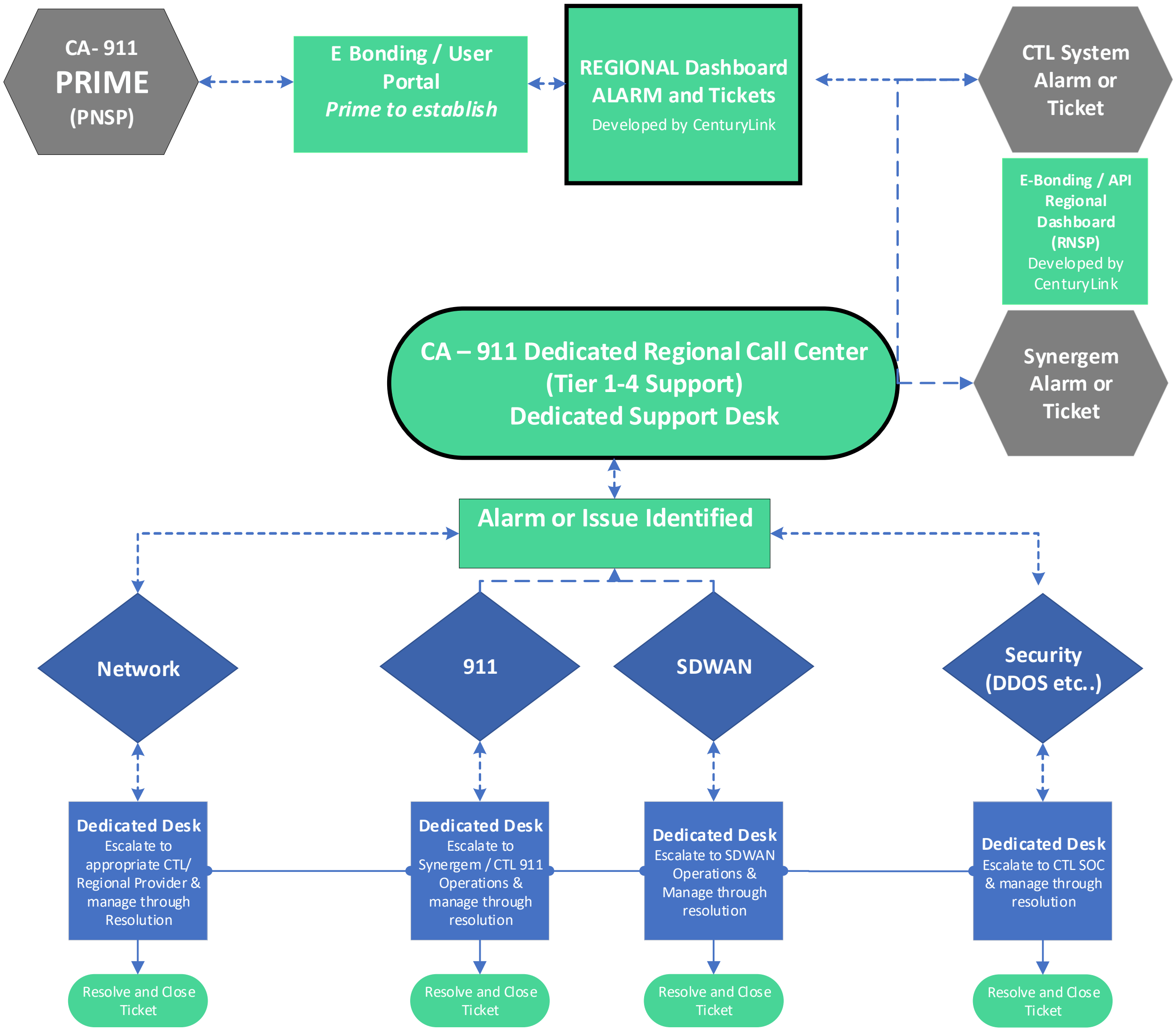
As a Regional – CenturyLink will assign a developer to work with the appropriate PRIME (PNSP) contacts to ensure that the CenturyLink reporting and metric fields align with the PRIME(PNSP) from an Ingress perspective and script alignment. As well as coordinate the appropriate Egress metrics and fields delivered from the PNSP.

• As a Regional provider CenturyLink will provide API feeds from monitoring tools such as SolarWinds, Synergem, Brix Probes and integrate SDWAN network monitoring and reporting tools.

• Regional ticketing information via e-bonding will be presented to the PNSP for overall reporting.

• Bandwidth, Inventory, ticketing, configuration data, are provided and accounted for in the CenturyLink response.

• The Operations and Program Management team follow ITIL standards and governance practice Order, Change, and Service Management.


CA- 911
PRIME
(PNSP)
E Bonding / User Portal
Prime to establish
REGIONAL Dashboard ALARM and Tickets
Developed by CenturyLink
CTL System Alarm or Ticket
E-Bonding / API Regional Dashboard (RNSP)
Developed by CenturyLink
CA – 911 Dedicated Regional Call Center (Tier 1-4 Support)
Dedicated Support Desk
Synergem Alarm or Ticket
Alarm or Issue Identified
Network
911
SDWAN
Security (DDOS etc..)
Dedicated Desk
Escalate to appropriate CTL/ Regional Provider & manage through Resolution
Dedicated Desk
Escalate to Synergem / CTL 911 Operations & manage through resolution
Dedicated Desk
Escalate to SDWAN Operations & Manage through resolution
Dedicated Desk
Escalate to CTL SOC & manage through resolution
Resolve and Close Ticket
Resolve and Close Ticket
Resolve and Close Ticket
Resolve and Close Ticket

23.0.10: Describe realistic timeline for Dashboard development that includes at a minimum Real Time Network Outage Monitoring and Reporting to support the description given for 23.0.8.

The Regional (RNSP) dashboard development and E-Bonding interfaces require a 3-6-month development cycle and will begin upon contract signature.

Real Time Monitoring

The proposed Next Generation Core Services (NGCS) platform is monitored in "near" real time for the satisfactory operation and security of all significant components and required performance parameters.

The State or its designated representative will be able to ascertain the status of major IP network elements and PSAP endpoints by viewing a status map or display with a Web browser or URL which will connect to the dashboard.

- CenturyLink's solution includes "Near" Real Time Network Outage Monitoring and Reporting for Regions to support failover interoperability and 9-1-1 traffic, show network uptime and downtime duration in the dashboard

Network Outage Monitoring and Reporting

CenturyLink's solution will meet the contracted SLA criterion to meet all monitoring and reporting for notification from the Next Generation Core Services (NGCS) platform. By employing e-bonding with systems to an integrated monitoring approach that provides end to end monitoring and notification. Logging of these events are captured and used for near real-time and historical reporting. System alarming for the NGCS solutions is being provided on each element from the NGCS to the SDWAN appliance at the PSAP which will alert the NOC for appropriate triage of the issue

CenturyLink will develop API functions as a RNSP to provide monitored data to the Prime

- CenturyLink will monitor and display the network and performance data for SLA compliance. CenturyLink cannot ensure SLAs for Prime Provider.
- Via APIs the Dashboard will have visibility into various platforms included in the CenturyLink solutions such as SDWAN, NGCS and CenturyLink and Synergem combined ticketing platform.
- Analytics, statistical data and reports will be developed based on requirements and agreed upon thresholds, displayed via dashboard and passed thru to PRIME (PNSP).
- The system monitoring program and MIS effort described in response (23.0.8) will recognize the Prime and the State as an authorized customer. Information will be pushed to them in the same way as other users. An E-Bonding capability will be developed when the PNSP vendor is known.

23.0.11: Describe the OSP traffic aggregation service for all wireless, AT&T wireline, Consolidated Communications wireline, and Frontier wireline OSPs in the awarded region in the State of California. Describe how the POI locations will be determined to support the ingress of OSP traffic, and how they will work with the OSP, CA 9-1-1 Branch and the CPUC throughout this process:

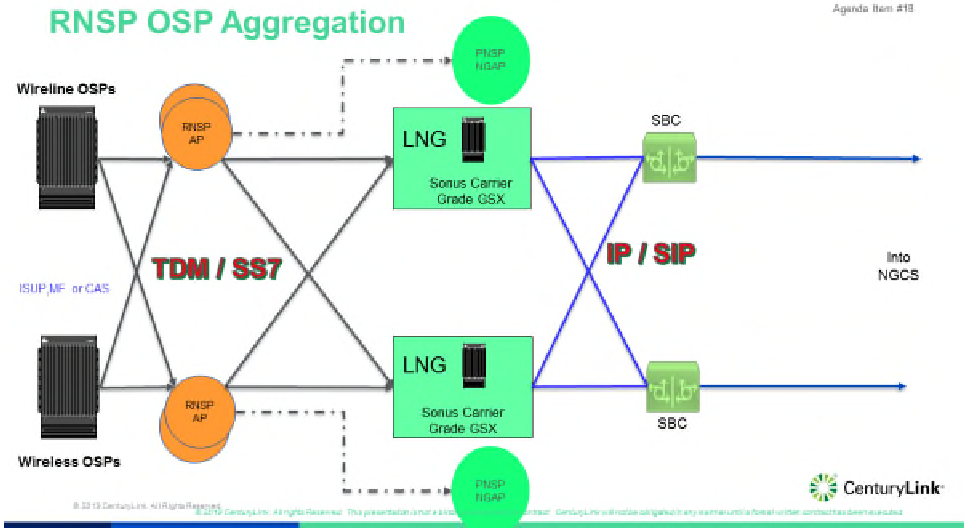
OSP traffic will be aggregated using CenturyLink's POIs for the region, CenturyLink design standards dictates at least two POIs per region as well as aggregation points. In most cases these POIs and Aggregations points are in the same locations but depending on the region and LATAs within that region could dictate more POIs than aggregation points. POI location will be determined based on an analysis of existing carrier traffic, as well as identification of locations (e.g. Tier III data centers) that have suitable network connectivity and processing capacity.

Inbound traffic can be delivered in either TDM(ISUP, MF, or CAS) format or in SIP format. CenturyLink's network enables the OSPs to:

- Directly connect to the CenturyLink network environment via supported POIs with a detailed order form;
- Pass and receive signaling information and call path Information through the platform to appropriately route traffic using the CenturyLink NGCS Core(s);
- Enable protocol conversion between signaling and encoding standards as needed to migrate from legacy to NG9-1-1 formats.

Depending on LATA and rules for intra-LATA trunking CenturyLink can meet the needs of engineering POI's in each region by either using existing CenturyLink infrastructure or establishing new POI's by adding DACS, MUX or Channel Bank hardware within the LATA or region. Additional POIs will be deployed on a "as needed" bases per the intra/inter OSP LATA requirements. Where required CenturyLink will provide long haul intra-LATA trunking to connect to the OSP via diverse facilities to the regional POI, this is not the preferred method but is an option on how to overcome LATA restrictions if building a POI in the LATA is not viable. If existing POI is available in a LATA or there is a viable build for a POI CenturyLink prefers to establish in a 2 POI per LATA format for diversity rules with the contingency that the OSP cannot feasibly deliver trunks outside of its LATA footprint.

- CenturyLink project team will work with each stakeholder for the deployment of the POI's that will require close coordination with each service provider including OSPs, CA 9-1-1 Branches and the CPUC. All service providers will receive all necessary information and details to obtain connectivity to the CenturyLink systems. CenturyLink project team will ensure that service provider's connectivity to the POIs is engineered and ordered correctly. This is an essential part to the plan for the NG9-1-1 services transition. The CenturyLink project team will provide designs customized provisioning plans (including incoming trunk route plans, bridge lists, and dialing plans). Additionally, our CenturyLink project team and engineers will provide customized drawings, details and process documents for the each of the service providers, if needed, to meet the needs of CA NG9-1-1 deployment.

- [redacted]
- 

23.0.12: Describe how the bidders proposed aggregation plan complies with the SOW and Exhibit 23. Description shall include the solutions ability to transfer between regions, or if PSAP is not reachable then shall send to Prime for delivery to PSAP:

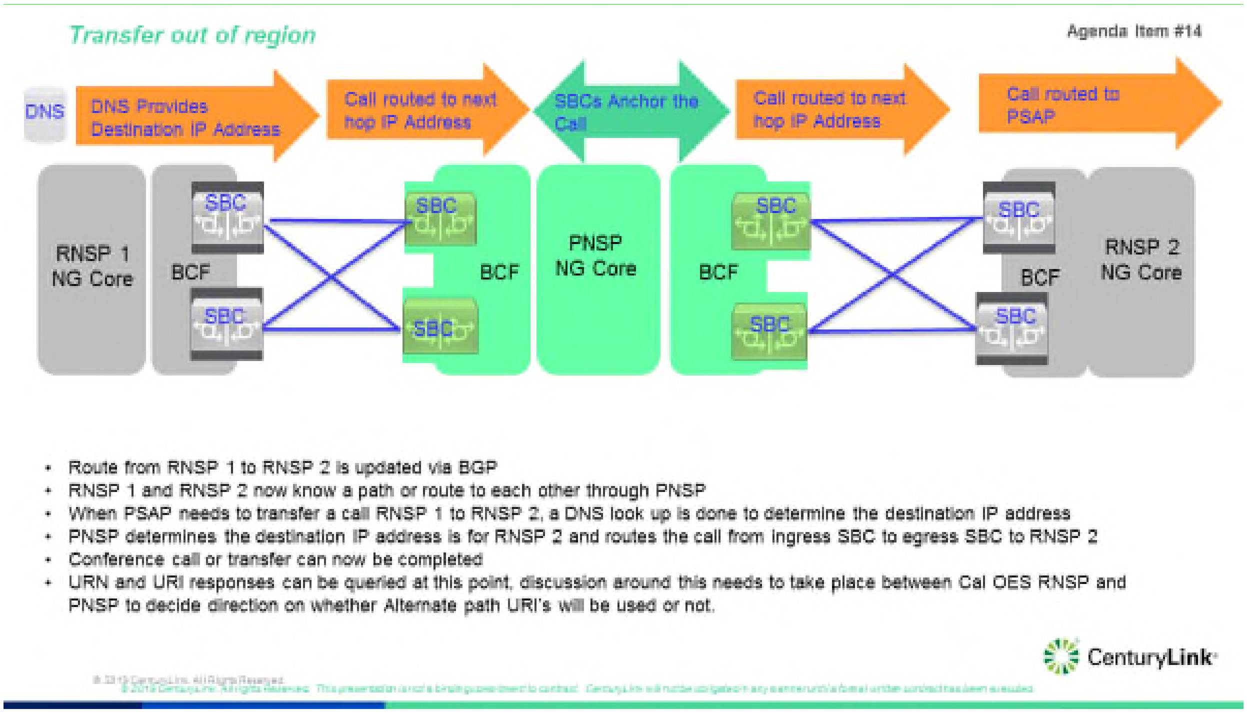
CenturyLink meets aggregation compliance requirements with (1) Two aggregation locations and two POIs in the region; (2) Our CenturyLink NGCS Core(s) service linking all OSPs to our ESInet and; (3) An aggregation configuration that holds all calls until it can be assured the proper PSAP can process messages. CenturyLink's NGCS Core(s) also allows the seamless movement of calls across and out of a region or among regional ESInets, as described below in the response of this section of the document.

ESInet routing is accomplished through use of dynamic routing protocol such as OSPF, as defined in RFC 2328 and RFC 5340. If the regional NCGS were unable to reach a PSAP, default policy would take effect and the system would employ the NGCS provided by the prime. External network routing is accomplished through the use of the Border Gateway Protocol("BGP") as defined in IETF RFC 4271.These routing protocols will include authentication between neighboring routers and include BFD for faster convergence. Should this authentication fail, the Prime NCGS would assume the routing role. From a NGCS perspective the RNSP core in return will be provisioned to pass this URI to the PNSP for look up and route determination to another region for connectivity and route determination.

Additionally, for PSAP unreachable conditions a Policy will be created in the RNSP Core for each PSAP that will route to the PNSP that can use the secondary network path from the PNSP to deliver the call to the PSAP URI set for PNSP route options.

For a PSAP to transfer a call out of the RNSP it will need to route the call through the PNSP. This is accomplished via the following:

- Route from RNSP 1 to RNSP 2 is updated via IP routing.
- RNSP 1 through 4 will know a path or route to each other through PNSP sharing its routing tables to the attached RNSP networks.
- When PSAP needs to transfer a call from RNSP 1 to RNSP 2, a DNS look up is done to determine the destination IP address.
- PNSP determines the destination IP address is for RNSP 2 and routes the call from ingress SBC to egress SBC to RNSP 2.
- Conference call or transfer can now be completed.
- URN and URI responses can be queried at this point, discussion around this needs to take place between Cal OES RNSP and PNSP to decide direction on whether Alternate path URI's will be used or not.
- Additional work will need to be done at the PSAP level to add specific autodial context for its respective CHE.



Transfer out of region

Agenda Item #14

- Route from RNSP 1 to RNSP 2 is updated via BGP
- RNSP 1 and RNSP 2 now know a path or route to each other through PNSP
- When PSAP needs to transfer a call RNSP 1 to RNSP 2, a DNS look up is done to determine the destination IP address
- PNSP determines the destination IP address is for RNSP 2 and routes the call from ingress SBC to egress SBC to RNSP 2
- Conference call or transfer can now be completed
- URN and URI responses can be queried at this point, discussion around this needs to take place between Cal OES RNSP and PNSP to decide direction on whether Alternate path URI's will be used or not.

CenturyLink

[redacted]

23.0.12.1: List all subcontractors that will be used for aggregation. There is potential for some subcontractors to be used by multiple RNSP’s or the PNSP. In that scenario, describe the bidder’s strategy to prevent or mitigate one subcontractor’s outage from causing an outage in multiple regions. Bidder shall describe how their solution provides an autonomous solution for aggregation.

CenturyLink’s solution provides its own aggregation services and does not use subcontractors for this service.

23.0.13: Describe how the bidder will receive, maintain, and push the centralized policy routing instructions for the region.

CenturyLink in conjunction with its partner Synergem will collaborate with the State, other RNSPs, and the PNSP to determine the optimal methodology for policy routing rule maintenance. While there are several possible approaches to this problem, we believe that under normal circumstances normal maintenance will be best performed at the PNSP PRF. This will significantly reduce the likelihood of conflicting rules being provisioned and will eliminate the issue of rule edit silo’s wherein a rule being edited at a RNSP is valid in the context of that RNSP’s ruleset, but not valid in the context of the ruleset at the PNSP or another RNSP once propagated. If this model is adopted, CenturyLink’s provided PRF would receive rule updates subsequent to maintenance activity performed at the PNSP PRF. In cases where a PRF optimization is identified at the RNSP, these changes would not be pushed directly to the PNSP PRF, but instead would be communicated to the PNSP via an agreed process for validation and subsequent provisioning at the PNSP PRF to be propagated to all regions in a controlled, predictable fashion.

Of course, if another approach is adopted CenturyLink stands ready to contribute to and participate in that development to meet the need of the PSAP as well.

23.0.14: Describe the security and firewalls needed to protect NG9-1-1 Services in accordance with NENA NG-SEC 75-001. The solution must be able to detect, mitigate and report TDOS, DDOS and any other Cyber attacks.

In designing its products and services, CenturyLink employs guidance contained in NENA Technical Information Document 03-501, Network Quality Assurance; NENA 75- 001, Security for Next-Generation 9-1-1 Standard (NG-SEC) and NENA 75-502, NG-SEC Audit Checklist. The [redacted] is the foundation of the CenturyLink security solution.

Threats are detected by monitoring the NENA-defined Security Posture and creation of log events which may include (1) Normal operation; or the presence of suspicious activity that does not impact normal operations; (2) The presence of fraudulent calls and events that are stressing a facility's ability to continue most operations; and (3) System under active attack and overwhelmed. Cascading impacts are minimized so as not to affect timing or invoke DoS for throughput of legitimate emergency calls. This solution meets all applicable NENA and federal security standards.

The ESInet and NGCS are provided with an array of firewalls. The firewall component of the BCF inspects all traffic transiting the network edge. It provides both application and network layer protection and scanning. The network firewall also mitigates lower layer protocol attacks. SDWAN in an HA configuration, overlaid on the MPLS delivery adds secure flows, IDS and IPS to ensure segmentation of traffic for 9-1-1 call delivery to the PSAP endpoints.

The BCF provides Denial of Service (DoS) and Distributed Denial of Service (DDoS) detection and protection. Our network supports the use of firewall rules, access control lists ("ACLs"), virtual local area networks ("VLANs"), virtual private networks ("VPNs"), and Secure Sockets Layer ("SSL") protocols to control network traffic and access.

These protective measures are supplemented with aggressive physical security for our data centers, the CenturyLink NG9-1-1 monitors and will provide notification if any failure is detected.

23.0.15: Provide a diagram(s) that shows 9-1-1 traffic flow architecture from ingress to egress using a non-proprietary NENA i3 compliant solution with dedicated NG Core Services for California.

Note: The LSRG is included in the diagram to illustrate an optional capability of CenturyLink understand it is not part of the RFP scope of work" and should be stricken from the existence for any deployment related to California NG9-1-1 deployment.

CenturyLink's solution is capable of supporting the LSRG as a transitional element but understands that it will not be used for anything in California. CenturyLink's solution delivers a i3 call stream from OSP end offices that will perform the appropriate lookup for NGCS routing using ECRF\LVF and LIS functional elements.

[redacted]

[redacted]

The elements in this system meet the following standards:

- NENA-STA-010.2-2016, Detailed Functional and Interface Specification for the NENA i3 Solution, and its successors.
- NENA 75-001, Security for Next Generation 9-1-1 Standard ("NG-SEC") and its successors
- NENA-INF-016.7-2018 Emergency Services IP Network Design for NG9-1-1 Information Document, Version 1, and its successors
- NENA-STA-003.1.1-2014, NENA Standard for NG9-1-1 Policy Routing Rules and its successors
- NENA-REQ-002.1-2016, NENA Next Generation 9-1-1 Data Management Requirements and its successors
- NENA-STA-004.1.1-2014, NENA Next Generation 9-1-1 United States Civic Location Data Exchange Format ("CLDXF") and its successors
- NENA-INF-027.1-2018, NENA Information Document for Location Validation Function Consistency
- APCO NENA 2.105.1-2017, NENA/APCO Emergency Incident Data Document ("EIDD"), to be replaced by its eventual ANSI document
- NENA-STA-006.1-201x, NENA GIS Data Model for NG9-1-1
- IETF Base IP Protocols
- IETF IP Routing Protocols such as Border Gateway Protocol ("BGP") and Open Shortest Path First ("OSPF")

- IETF Session and Media Protocols such as Session Initiation Protocol ("SIP"), Session Description Protocol ("SDP"), Message Session Relay Protocol ("MSRP"), and Real-Time Transport Protocol ("RTP")
- IETF Protocols such as Location-to-Service Translation ("LoST"), HTTP-Enabled Location Delivery ("HELD"), and Presence Information Data Format Location Object ("PIDF-LO")

23.0.16: Describe how NGCS shall use a non-proprietary NENA i3 compliant multi-layered redundancy of systems, software, and facilities with no single point of failure that supports the ability to update all system components including but not limited to routers, router tables, servers, NG Core Services, and all NG9-1-1 functions without any loss of service 24x7x365.

Our non-proprietary NGCS operate within a highly survivable network architecture. [redacted]

[redacted]

Our geographically diverse data centers monitor all critical systems automatically 24x7x365. Electronic logs are created and maintained in the system dashboard controlled through centralized management tools for operating each core instance. This includes an historical record of availability and outage. These facilities meet Tier II-III standards stipulated in the two main data center tier classifications developed by the Telecommunications Industry Association (TIA) and the Uptime Institute (UI).

23.0.17 Describe how the bidders solution will support a minimum of two geographically diverse cores or a cloud based equivalent, dedicated to California and located in the CONUS, with the capability to maintain 99.999% avaliability.

As described in our reply directly above, our solution employs two geographically diverse datacenters that are each equipped with [redacted]. Each datacenter will be provisioned with NGCS dedicated for the exclusive support of California agencies and CALOES.

Within each center, data is backed up and recovered based upon global standards and best practices. All functional elements of the network architecture are N+1.

All applications are deployed on virtual servers and all applications and data are shared among and within each datacenter. The applications will be leveraging all HA functionality within the hypervisor, DRS and HA features are utilized to ensure an "always on" architecture

An outage would require failure of both sets of services in both datacenters. Calculating the possibility of such an occurrence is extremely difficult given that we have never experienced a failure of even one set in one datacenter diverse from the solution provided by our subcontractor Synergem's direct bid to ensure that diversity is met for the State of California.

To ensure circuit 99.999% reliability will require at least two diverse circuits going to different POPs and utilizing different carriers where possible and at a minimum media diversity.

CenturyLink NG9-1-1 standards are based off of experience in the marketplace being a provider in the space for over 8 years we have homed in on what works and where the gaps for a true NG9-1-1 solution exist. For our design standard that starts at Ingress developing at minimum two POIs per region/LATA each providing diverse paths to CenturyLink provided LNGs. Each LNG which have a set geographic distance requirement then have diverse paths to the geo-diverse HA CenturyLink SBCs that provides a secure connection to our NGCS. [redacted] Leaving the NGCS via SBCs the solution utilizes diverse MPLS paths with HA SDWAN overlay. This SDWAN solution provides secure traffic flows to the PSAP and enable features such as packet duplication to allow for SIP call presentation with a low impact of the voice caller to the call handling equipment. [redacted] are employed for additional BCF\security where required in the solution to delivery IPS and stateful packet inspection. These are all provided as part of the service designed with monitoring and NG9-1-1 NOC professional services to ensure that CenturyLink is meeting customer expectations and mutually agreed upon terms.

23.0.18: Describe the maximum call volume the solution will support and how the proposed solution is scalable and the role licensing agreements with subcontractors have in scalability if applicable.

The CenturyLink NGCS platform is scalable software-as-a-service(SaaS) platform.

There are two instances in separate data centers, each capable of…

- Flexibility to Scale with bandwidth that can grow from 1Gbps-10Gbps easily and support multiple 10Gbps links.
- Currently designed with the intent to support over [redacted] concurrent SIP sessions per instance on diverse 1Gbps links to each Session Border Controller.

The CenturyLink solution, as presented, can support today a max of [redacted] SIP-TLS concurrent sessions per instance that can be expanded to meet additional scale with additional hardware.

This allows CenturyLink to size the capacity of circuits in accordance with expected call volume and call handling capacity of the connected sites. Data Center links will be provisioned and sized to handle the expected call volume. It is difficult to envision a capacity issue that would be beyond this system. This solution differs from our NGCS partner by having a different plan for Ingress aggregation and is not collocated in the same datacenters as the partners provided solution.

23.0.19: List all subcontractors that will be used for NGCS. There is potential for some subcontractors to be used by multiple RNSP's or the PNSP. In that scenario, describe the bidder's strategy to prevent or mitigate one subcontractor's outage from causing an outage in multiple regions. Bidder shall describe how their solution provides an autonomous solution for NGCS.

CenturyLink subcontractor used for the NGCS portions of this solution is Synergem. Synergem and the CenturyLink NGCS solution differ on several key factors such as these NGCS data centers are in different locations with CenturyLink having its own dedicated NGCS for CenturyLink PSAP customers. CenturyLink and Synergem have differing ingress methodology as well being that CenturyLink provides its own LNGs to deliver SIP into the NGCS. CenturyLink also has it own verification and testing program regardless of vendor our company works with testing requirements before being deployed are followed with an additional amount of focus from CenturyLink core engineering. This same method applies for and patching and upgrades, code validation is a must that has to pass validation before being introduced to the production environment.