CenturyLink

Response to Request for Proposal

State of Nebraska

Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS)

RFP No.: 6264 Z1

Technical Proposal 1

June 3, 2020

CenturyLink

LEGAL STATEMENT:

Informational Purposes Only
CenturyLink has endeavored to provide responses as requested by the RFP, but our response is not intended to create a binding contractual commitment between the parties without further discussions between the parties and execution of a mutually acceptable agreement. Specifically, our responses and our offer are dependent upon the final solution and information exchanged during discussions between the parties. Therefore, regardless of any condition contained within the RFP, including but not limited to CenturyLink's signature to its submission, the responses are informational only and are provided for your evaluation.

Contract Structure
As requested by the RFP, CenturyLink is proposing to provide its Services pursuant to the Terms and Conditions contained in *Section II. Terms and Conditions* of the RFP ("RFP Terms and Conditions"), as modified by CenturyLink's exceptions, clarifications, and additions in this response and subject to further discussion and negotiation by the parties to arrive at mutually agreeable terms. CenturyLink has made every effort to provide limited exceptions to the RFP Terms and Conditions, and requests changes consistent with terms the parties have agreed to in the past as much as possible. Many requested language changes are similar to the provisions agreed to in Contract 70987 O4 for network services, signed by the parties in 2016. However, some proposed terms necessarily differ from what the parties have agreed to in past contracts due to the unique and high-risk nature of 911 services. Accordingly, CenturyLink has proposed some additional and different terms that are necessary for CenturyLink to maintain an appropriate risk profile for the provision of 911 services and allows us to offer our 911-related services at competitive rates. In preparing this response, CenturyLink has made every effort to streamline its response and to comply with the terms of the RFP to the maximum extent possible.

As permitted by the introductory paragraphs of *Section II. Terms and Conditions* of the RFP, CenturyLink has included with our proposal the service exhibits, service level agreements (SLAs), and technical documents that apply to the services proposed (collectively, the "CenturyLink Attachments"). CenturyLink's proposal to provide its Services pursuant to the RFP Terms and Conditions specifically contemplates that the RFP Terms and Conditions will be modified and supplemented by the CenturyLink Attachments, and that the RFP Terms and Conditions will be negotiated and modified in accordance with CenturyLink's exceptions and clarifications contained in this response. Our response is dependent upon incorporating the CenturyLink Attachments into the final agreement between the parties. If there is any conflict between the RFP Terms and Conditions, the responses provided, and the CenturyLink Attachments, the CenturyLink Attachments control and contain the complete CenturyLink offer. In the context of an intent to award, CenturyLink anticipates that the parties will discuss and review the exceptions and clarifications provided in this response and the CenturyLink Attachments and that these documents and terms will be incorporated into a final definitive contract in the manner mutually agreed to by the parties.

Affiliated Companies
CenturyLink services are provided through affiliated companies. The CenturyLink Contract and/or the applicable Service Exhibits attached thereto will identify the legal CenturyLink affiliate providing the services.

Critical 9-1-1 Circuits
To the extent services are provided in the United States, the Federal Communications Commission's 9-1-1 reliability rules mandate the identification and tagging of certain circuits or equivalent data paths that transport 9-1-1 calls and information ("9-1-1 Data") to public safety answering points defined as Critical 911 Circuits in 47 C.F.R. Section 9.4(a)(5). CenturyLink policies require tagging of any circuits or equivalent data paths used to transport 9-1-1 Data. We require that customers agree to cooperate with CenturyLink regarding compliance with these rules and policies and to notify CenturyLink of all Services customers purchase under the Agreement utilized as Critical 911 Circuits or for 9-1-1 Data.

Insurance
CenturyLink purchases sufficient insurance limits to protect the company from risks and liabilities associated with providing its commercial services and products. CenturyLink's standard coverage is in accordance with generally accepted industry standards for the type services and/or work proposed. CenturyLink's Memorandum of Insurance is available at www.centurylink.com/moi.

TABLE OF CONTENTS

COVER LETTER

June 3, 2020

Annette Walton / Nancy Storant, Procurement Contacts
State of Nebraska State Purchasing Bureau
1526 K St. Suite 130
Lincoln, NE 68508

Dear Mss. Walton and Storant,

CenturyLink is pleased to present this response to your Request for Proposal for Contractual Services related to RFP 6264 Z1 to provide a Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS).

CenturyLink has made every effort to respond with accurate and relevant information. Occasionally, it was necessary for CenturyLink to make assumptions to formulate a timely response. Therefore, CenturyLink reserves the right to correct any errors and to modify any responses based on the final solution or information received during further discussions. Notwithstanding anything in this response to the contrary, including CenturyLink's signature on its response, CenturyLink will not be legally bound until execution of a mutually agreed-upon definitive agreement.

Best regards,

Jon Osborne

Central Region Account Director Public Safety
Public Sector
118 South 19th Street Omaha, NE, 68102
Tel: (402) 998-7392 Cell: (402) 216-1009 Fax: (402) 422-3545
jon.osborne1@CenturyLink.com

EXECUTIVE SUMMARY

CenturyLink is proud to respond to the *Next Gen 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS)* RFP with a history of successfully supporting 9-1-1 services throughout the United States for more than 60 years. CenturyLink is fully committed to supporting the State of Nebraska Public Service Commission (PSC) and all 68 PSAPS in the implementation and support of an Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) solution.

CenturyLink understands there are several reasons to engage in the journey of NG9-1-1. NENA states, "anyone should be able to connect to 9-1-1 on any device, from anywhere, at any time" with the goal of saving more lives. NG9-1-1's new technology will deliver faster call set up, more accurate caller location, sophisticated policy-based routing, and waves of new data. The journey of NG9-1-1 is complicated, but with the right partner it can be done successfully. All the right players need to be at the table, the best designed technology must be deployed, and all the work needs to be organized.

The complexity of NG9-1-1 requires effective collaboration. CenturyLink is proud to have been a part of the state's transition process and to have met with Mission Critical Partners in January 2017 to provide input to the "*Nebraska Public Service Commission 9-1-1 Service Plan*". Since then, CenturyLink has remained focused on assisting the PSC and the PSAPs execute their plan. CenturyLink is ready to deliver the PSC's plan functional areas of 911 System Design, integration of Geographic Information System data, Continuity of Operations & Disaster Recovery, and coordination with FirstNet.

The complexity of NG9-1-1 also requires a single point of management for all elements of the NG9-1-1 solution. CenturyLink's ESInet will be the fabric that connects all elements of the state's NG9-1-1 solution. Nebraska's PSAPs and the PSC will benefit from full visibility and management of the entire solution and the ability to have a single point of contact with the state's trusted partner: CenturyLink.

Why CenturyLink does collaboration better

In order to deliver the best, feature-rich, i3 compliant, and public safety grade NG9-1-1 solution for the State of Nebraska, effective collaboration between all players in the ecosystem is essential.
A CenturyLink-led journey of NG9-1-1 is designed with **all the elements** required to produce effective collaboration - the right team, effective conversations to explore all the options, and flexible thinking. The goal of CenturyLink's methodology is to develop an implementation plan that will deliver all designed functionality on time and within budget.

CenturyLink's commitment to the State of Nebraska

CenturyLink's resume of data transformation experience is expansive. CenturyLink is recognized as a worldwide leading provider of networking solutions, security solutions, cloud-based strategies, and products through a Unified Communications suite. Because our solution portfolio is comprehensive, our public safety customers have the unique advantage of making choices to create a NG9-1-1 solution that best meets their needs.

CenturyLink is proud of its long history of partnering with the State of Nebraska to deliver communications technology that has made a positive impact on government institutions, businesses, and citizens. Specifically, CenturyLink has decades of experience working with Nebraska public safety professionals to deliver public safety solutions that save lives, protect property, and ensure the safety of first responders.

CenturyLink's commitment to the State of Nebraska shines bright in the lives of our dedicated team of 9-1-1 service technicians. For example, Craig Blocher, a Nebraska native with 15 years servicing 9-1-1 PSAPs believes he is, "making a real difference and is contributing to saving lives in Nebraska." Craig's dedication to his customers is demonstrated by his detailed technical training and expertise, his ongoing communication, and his willingness to quickly respond in a time of need. Craig was a part of the team that installed the first Intrado VIPER system in Douglas County in 2005. He is also the first technician to install the first multi-node hosted solution in Buffalo and Dawson County for the South Central Region. According to Craig, he is, "driven by his tremendous sense of pride in his job, the friendships he's made, and supporting Nebraska's 9-1-1 services."

CenturyLink's 9-1-1 experience

CenturyLink's extensive 9-1-1 experience demonstrates our ability to take on the challenges of implementing NG9-1-1 in Nebraska. We know the challenges because we have not only been presented with them, but we have helped resolve them.

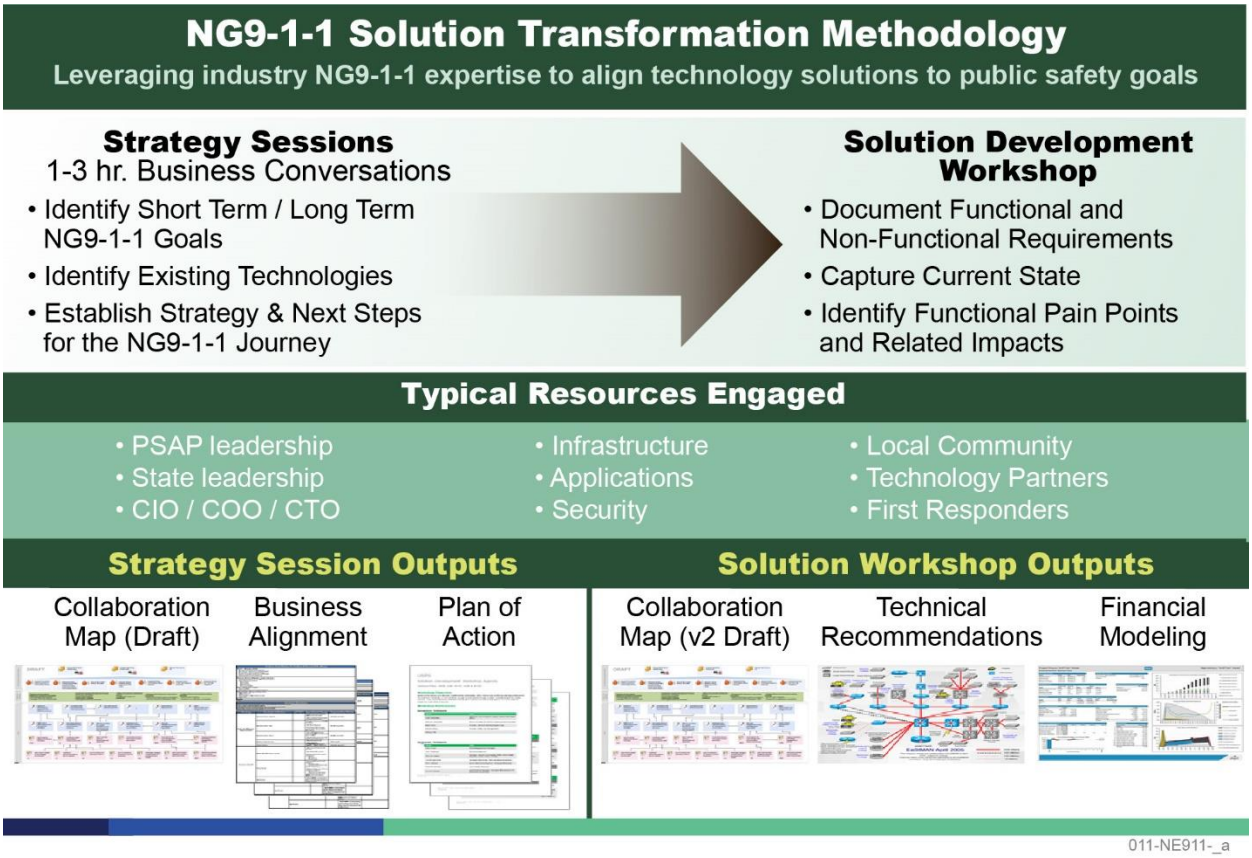
CenturyLink provides 9-1-1 solutions to 1572 PSAPs across 35 states and has implemented and managed NG9-1-1 solutions (ESInets and NGCS) in nine states. Our experience with 9-1-1 dates to the first 9-1-1 call made in 1968. As NG9-1-1 has evolved, CenturyLink has worked with our customers to understand all the technology options available and helped them make the technology choices that best fit their situation. CenturyLink recognizes there is no "one size fits all" to NG9-1-1 and has assembled a broad portfolio of technology options available to our customers.

CenturyLink's NG9-1-1 solution is built on the foundation of our world class reliable, resilient, fault tolerant, secure, and i3 compliant ESInet. Current and future next generation core services (e.g., GIS-based call routing) will be integrated into our ESInet to provide the State of Nebraska with a full range of NG9-1-1 functionality designed to better connect citizens to PSAPs. Armed with more accurate location information, new data sources, and enhanced call routing management, Nebraska PSAPs will be able to improve the situational awareness of first responders.

CenturyLink's Public Safety Network Operations Center (NOC) stands ready to manage Nebraska's CenturyLink ESInet and NGCS solution to ensure superior performance and timely notification of any service impacting event. Our 24/7/365 Public Safety NOC is constantly assessing the health of the network and quickly responding with appropriate notifications and actions. Additionally, CenturyLink's industry leading security solutions and practices will be deployed to scan the ESInet and identify and resolve any vulnerabilities. By adopting CenturyLink's approach to NG9-1-1 solutions, Public Safety professionals across the state can be confident that their PSAP will be ready to answer calls for help and save lives.

CenturyLink's NG9-1-1 Strategic Design Approach

A CenturyLink-led NG9-1-1 journey begins with a comprehensive NG9-1-1 Solution Development Workshop (SDW). During the SDW, CenturyLink will lead collaborative discussions on design options, security strategies, program/project plans, and roles and responsibilities. At the conclusion of the SDW, the right plan will be identified to ensure the project delivers all functionality on time and within budget. An SDW is part of our overall NG9-1-1 solution transformation methodology (shown below).



Our NG9-1-1 design principles drive our approach to creating and managing NG9-1-1 solutions that save lives and property protect first responders. Our design principles Influence all we do and include the following.

1. Solutions based on ***i3 standards***.
2. Highly reliable, resilient, and redundant ***Public Safety Grade*** design
3. NG9-1-1 building blocks that ***Future Proof*** your solution
4. ***Flexible design process*** that explores all the available options
5. Collaboration on a Program Development Plan document that details the installation process and timelines

CenturyLink Next Generation Core Services Design Options

In this procurement, CenturyLink is offering two NGCS technology options – 1) CenturyLink NGCS (Synergem Technologies) and 2) CenturyLink NGCS (Intrado). Both NGCS options have been proven in customer implementations in several states. Additionally, both NGCS options are delivered over CenturyLink's industry leading, Public Safety grade ESInet is hardened by CenturyLink cybersecurity technology and managed by CenturyLink's 24x7x365 NOC.

Both NGCS platforms provide the full suite of next generation core services required to complete a NG9-1-1 emergency call. In both options, the functionality delivered is consistent with i3 standards. CenturyLink is confident either option will meet and exceed the requirements defined in the "*Nebraska Public Service Commission 9-1-1 Service Plan".*

CenturyLink commits to a series of collaborative discussions within our NG9-1-1 Solutions Transformation Methodology to determine which option fits best with the state's strategic vision for the future.

State of Nebraska State Purchasing Bureau
REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES

RETURN TO:
Name: State Purchasing Bureau
Address: 1526 K St. Suite 130
City/State/Zip: Lincoln, NE 68508
Phone: 402-471-6500

SOLICITATION NUMBER	RELEASE DATE
RFP 6264 Z1	March 17, 2020
OPENING DATE AND TIME	**PROCUREMENT CONTACT**
June 3, 2020, 2:00 P.M. Central Time	Annette Walton / Nancy Storant

PLEASE READ CAREFULLY!

SCOPE OF SERVICE

The State of Nebraska (State), Department of Administrative Services (DAS), Materiel Division, State Purchasing Bureau (SPB), is issuing this Request for Proposal (RFP) Number 6264 Z1 for the purpose of selecting a qualified bidder to provide a Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS). A more detailed description can be found in Section V. The resulting contract may not be an exclusive contract as the State reserves the right to contract for the same or similar services from other sources now or in the future.

The term of the contract will be five (5) years commencing upon notice to proceed. The Contract includes the option to renew for five (5) additional one (1) year periods upon mutual agreement of the Parties. The State reserves the right to extend the period of this contract beyond the termination date when mutually agreeable to the Parties.

ALL INFORMATION PERTINENT TO THIS REQUEST FOR PROPOSAL CAN BE FOUND ON THE INTERNET AT: **http://das.nebraska.gov/materiel/purchasing.html**.

An optional Pre-Proposal Conference will be held on April 1, 2020 from 10:00 AM – 12:00 PM at 1526 K St. Lincoln, NE 68508.

IMPORTANT NOTICE: Pursuant to Neb. Rev. Stat. § 84-602.04, State contracts in effect as of January 1, 2014, and contracts entered into thereafter, must be posted to a public website. The resulting contract, the solicitation, and the awarded bidder's proposal or response will be posted to a public website managed by DAS, which can be found at http://statecontracts.nebraska.gov.

In addition, and in furtherance of the State's public records Statute (Neb. Rev. Stat. § 84-712 et seq.), all proposals or responses received regarding this solicitation will be posted to the State Purchasing Bureau public website.

These postings will include the entire proposal or response. Bidders must request that proprietary information be excluded from the posting. The bidder must identify the proprietary information, mark the proprietary information according to state law, and submit the proprietary information in a separate container or envelope marked conspicuously using an indelible method with the words "PROPRIETARY INFORMATION" or as a separate electronic file. The bidder must submit a detailed written document showing that the release of the proprietary information would give a business advantage to named business competitor(s) and explain how the named business competitor(s) will gain an actual business advantage by disclosure of information. The mere assertion that information is proprietary or that a speculative business advantage might be gained is not sufficient. (See Attorney General Opinion No. 92068, April 27, 1992) THE BIDDER MAY NOT ASSERT THAT THE ENTIRE PROPOSAL IS PROPRIETARY. COST PROPOSALS WILL NOT BE CONSIDERED PROPRIETARY AND ARE A PUBLIC RECORD IN THE STATE OF NEBRASKA. The State will determine, in its sole discretion, if the disclosure of the information designated by the Bidder as proprietary would 1) give advantage to business competitors and 2) serve no public purpose. The Bidder will be notified of the State's decision. Absent a determination by the State that the information may be withheld pursuant to Neb. Rev. Stat. § 84-712.05, the State will consider all information a public record subject to disclosure.

If the agency determines it is required to release proprietary information, the bidder will be informed. It will be the bidder's responsibility to defend the bidder's asserted interest in non-disclosure.

To facilitate such public postings, with the exception of proprietary information, the State of Nebraska reserves a royalty-free, nonexclusive, and irrevocable right to copy, reproduce, publish, post to a website, or otherwise use any contract, proposal, or response to this solicitation for any purpose, and to authorize others to use the documents. Any individual or entity awarded a contract, or who submits a proposal or response to this solicitation, specifically waives any copyright or other protection the contract, proposal, or response to the solicitation may have; and, acknowledges that they have the ability and authority to enter into such waiver.

This reservation and waiver are a prerequisite for submitting a proposal or response to this solicitation, and award of a contract. Failure to agree to the reservation and waiver will result in the proposal or response to the solicitation being found non-responsive and rejected.

Any entity awarded a contract or submitting a proposal or response to the solicitation agrees not to sue, file a claim, or make a demand of any kind, and will indemnify and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials from and against any and all claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses, sustained or asserted against the State, arising out of, resulting from, or attributable to the posting of the contract or the proposals and responses to the solicitation, awards, and other documents.

Response:

CenturyLink understands the requirements regarding labeling and submission of proprietary information and has followed those requirements in its submission of this proposal. If the State evaluates the material CenturyLink has submitted as proprietary information and determines that it does not meet the State requirements for non-disclosure, CenturyLink respectfully requests that, prior to disclosing such information, the State provides CenturyLink with notice and a reasonable opportunity to respond to and remedy such reasons for non-compliance prior to the disclosure so as to prevent and/or limit the disclosure. In such scenario, CenturyLink respectfully reserves the right to amend its response to revise or withdraw the material that was submitted as proprietary in order to protect the proprietary status of such information. CenturyLink's primary concerns are to ensure that certain information related to 911 configuration or security must remain proprietary in order to protect 911-related services from potential security threats or vulnerabilities, and to maintain the proprietary nature of CenturyLink's 911 service offers from being disclosed to competitors.

A. PROPOSAL SUBMISSION

1. CORPORATE OVERVIEW

The Corporate Overview section of the Technical Proposal should consist of the following subdivisions:

a. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

Response:

CenturyLink Communications, LLC d/b/a "CenturyLink"
931 14th Street, # 900
Denver, CO. 80202

CenturyLink Communications, LLC is a single member limited liability company and its sole member is CenturyLink, Inc.

CenturyLink's Headquarters is located at 100 CenturyLink Drive, Monroe, LA. 71203

CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC was "Organized" in Delaware June 10, 1966; the charter number in Delaware is: 0642301.

The attachment named "1_a_CC__LLC_Certificate_of_Name_Change__Incorporation" shows the Name Change Certificate of Amendment that became effective on April 1, 2014.

b. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that proposal evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

The State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

Response:

Complete financial information, including CenturyLink Inc.'s annual Form 10-K and quarterly reports on Form 10-Q are available for review on our Investor Relations web site at: https://ir.centurylink.com/financials/sec-filings/default.aspx
Each of the last three annual Form 10-K report are in excess of 200 pages. If printed copies of the financial statements are desired, CenturyLink will provide them upon request.

Contact information for CenturyLink's banking references is as follows:

Courtney R Broderick
Assistant Vice President
Treasury Management Sales Consultant
U.S. Bank
425 Walnut Street Cincinnati, OH 45202
(414) 765-6118
courtney.broderick@usbank.com

Pablo Pinedo
Executive Director, Corporate & Investment Bank Treasury Services
J.P. Morgan
4 New York Plaza, 13th Floor
New York, NY 10004
(212) 623-8786
pablo.m.pinedo@jpmorgan.com

Due to size of CenturyLink, various suits, proceedings, and claims typical for an enterprise business can be pending against CenturyLink at any one time. While it is not possible to determine the ultimate disposition and resolution of any suits, proceedings or claims, and whether they are consistent with CenturyLink's position, CenturyLink expects the outcome of such proceedings, individually or in aggregate, will not have a materially adverse effect on the financial condition or results of CenturyLink operations or its business segments; nor negatively affect its ability to provide the services proposed.

As a public corporation, CenturyLink is required to fully disclose material data and relevant information that may influence investment decisions to all investors at the same time. CenturyLink does not provide detailed information on litigation except through its securities filings. Please refer to CenturyLink's Annual Report on Form 10-K, available on http://www.centurylink.com/ for a description of certain litigation or claims.

CenturyLink has read and understands that the State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

c. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the proposal due date, the bidder should describe the circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded bidder(s) will require notification to the State.

Response:

No change of ownership within CenturyLink is anticipated during the 12 months following the proposal due date. As a public company subject to securities laws disclosure and filing requirements, CenturyLink would provide any such notice of change of ownership to the extent permitted by applicable securities laws.

d. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

Response:

CenturyLink
118 S 19th St.
Omaha, NE 68105

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous five (5 years. If the organization, its predecessor, or any Party named in the bidder's proposal response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

Response:

CenturyLink understands and complies. CenturyLink, formerly Qwest, has a long history of servicing the State of Nebraska Government agencies, specifically in Public Safety.

In the last five years, CenturyLink has extensively participated in the development and support of the of the Nebraska Public Service Commission "*9-1-1 Service System Plan"* in preparation for the implementation of NG9-1-1. The CenturyLink local support team has acted in one capacity or another as the consultant, design engineers, support technicians, and project managers with the South Central, North Central, East Central, Northeast, Metro, and Metro West 911 regions. The team has also consulted with individual PSAPS not associated with an assigned region. We helped upgrade multiple regions' call handling and networks in preparation NG9-1-1. Currently, a member of our Nebraska Public safety local support team was appointed to the Public Service Commission 911 Service System Advisory Committee. As a member of this committee, CenturyLink has not only been able to support at the PSAP level, but also support the Public Service Commission 911 initiatives.

We currently have 93 active Public Safety specific contracts with 29 PSAPs. These contracts support network, call handling equipment, and call routing. CenturyLink is the predominate Local Exchange Carrier (LEC) in the state and provides an extensive network of voice and data circuits. CenturyLink owns four of the five 911 selective routers which transmit 911 calls via our network to the respective PSAPS.

CenturyLink has multiple voice and data circuits and 911 trunks that are contracted via the State of Nebraska Tariff; implemented on 9/29/2000 *"Qwest Corporation Exchange and Network Services Catalog"*. Additionally, within the last five years, CenturyLink has accumulated a total of 68 voice and data master contracts/amendments. These are contracted through the State of Nebraska OCIO. Every government entity: state, county,

and local municipality are able to purchase off of these existing contracts. There are 93 counties and 531 cities and villages in the State that may have individual voice or data contracts with CenturyLink. We have provided all public safety CPE, maintenance, and network contracts and the 68 master contracts/amendments. The State of Nebraska Tariff; *"Qwest Corporation Exchange and Network Services Catalog"* can be accessed via the two links below.

https://www.centurylink.com/aboutus/legal/tariff-library.html

http://www.centurylink.com/tariffs/ne_qc_ens_c.pdf

NE%20Active%20Contracts%20Public%2

Please see the PROPRIETARY INFORMATION in file 4 of 4
File named: A.1.e NE Active Contracts Public Saftey & SoNE PROPRIETARY

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's proposal response is or was an employee of the State within the past five (5) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

If any employee of any agency of the State of Nebraska is employed by the bidder or is a subcontractor to the bidder, as of the due date for proposal submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this proposal. If no such relationship exists, so declare.

Response:

No CenturyLink employee was an employee of the State within the last five months. CenturyLink is not aware of any employee relationships with the State that would be considered a conflict of interest.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past five (5) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past five (5)) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's proposal accordingly. If no such termination for default has been experienced by the bidder in the past five (5) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

Response:

Please see our response to Item 1.B Financial Statements above. Additionally, this question is extremely broad and would require disclosure of information that is confidential and beyond the scope of this proposal. Despite CenturyLink's reasonable efforts to avoid disputes, the sheer volume of contracts entered into by CenturyLink dictates that CenturyLink is occasionally involved in contract disputes. CenturyLink is not aware of any disputes or relevant defaults at the time of this response that will have a material negative impact on our ability to provide the services proposed.

h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the previous projects similar to this solicitation in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the proposal.

The bidder should address the following:

i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this solicitation. Provide the number of ESInet and NGCS solutions implemented by the bidder that are in production today and lessons learned throughout the project that will be applied to the deployment of the Nebraska ESInet and NGCS solution. These descriptions should include:

a) The time period of the project.
b) The scheduled and actual completion dates.
c) The bidder's responsibilities.
d) For reference purposes, contracting entity name, contact name, contact title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.); and
e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

Response:

CenturyLink has read, understands, and complies. Three references are provided below.

Reference # 1

a) The time period of the project;	ESInet installed in 2013 to 2016
b) The scheduled and actual completion dates;	Matched requested timeframe
c) The bidder's responsibilities;	Provide NGCS through the state-wide ESInet
d) For reference purposes, contracting entity name, contact name, contact	State of North Dakota Jason Horning, EMP

title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.); and	Jason.horning@ndaco.org 701-328-7334 In an effort to respect our customers' confidential and proprietary information and accommodate schedules of all parties involved to yield the most productive discussions possible, we respectfully request that communication with CenturyLink's references be coordinated through Jon Osborne, your Central Region Account Director (402) 998-7392; jon.osborne1@centurylink.com or Bjorn Johnson, your CenturyLink Senior Account Manager, at Bjorn.Johnson@CenturyLink.com or at (605) 977-2820.
e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.	CenturyLink was Prime Contractor for the North Dakota State-wide implementation of NGCS. CenturyLink was the Prime Contractor for the North Dakota State-wide ESInet project incorporating all PSAPS within the State of North Dakota. Phase one completion finished 2017 within budget and timeline. Phase two is ongoing and will include GIS integration.

Reference # 2

a) The time period of the project;	2019 – February of 2020
b) The scheduled and actual completion dates;	December of 2019
c) The bidder's responsibilities;	Managed Emergency Call Handling including State-wide NG Core Services and Hosted Call Handling System.
d) For reference purposes, contracting entity name, contact name, contact title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.); and	State of South Dakota Maria King – State 911 Coordinator maria.king@state.sd.us (605) 773-3264 In an effort to respect our customers' confidential and proprietary information, and accommodate schedules of all parties involved to yield the most productive discussions possible, we respectfully request that communication with CenturyLink's references be

	coordinated through Jon Osborne, your Central Region Account Director (402) 998-7392; jon.osborne1@centurylink.com or Bjorn Johnson, your CenturyLink Senior Account Manager, at Bjorn.Johnson@CenturyLink.com or at (605) 977-2820.
e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.	CenturyLink was Prime Contractor in implementing a State-wide ESInet with hosted call handling. The solution is a completely managed system including 911 Ingress, Core Services, Egress and Call Handling Services. All monitoring and maintenance are provided for the term of the agreement. The State of South Dakota had an incredibly aggressive 6-month implementation timeline. CenturyLink was the Prime Contractor on the NG911 project, and the project completed within budget. The projects only delay was due to additional Core Network Improvements that was undetermined at the start of the project. Through a collaboration and design enhancements the completion was delayed by only 2 months and still fell within acceptable parameters set by the state.

Reference # 3

a) The time period of the project;	March 2017 – April 2019
b) The scheduled and actual completion dates;	Matched requested timeframe
c) The bidder's responsibilities;	Managed Emergency Call Handling including State-wide NG Core Services and Hosted Call Handling System.
d) For reference purposes, contracting entity name, contact name, contact title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.);	Pima County, Arizona Sheila Blevins, Pima County 911 Administrator, sblevins@marana.com, 520-382-2038

and	In an effort to respect our customers' confidential and proprietary information, and accommodate schedules of all parties involved to yield the most productive discussions possible, we respectfully request that communication with CenturyLink's references be coordinated through Jon Osborne, your Central Region Account Director (402) 998-7392; jon.osborne1@centurylink.com or Bjorn Johnson, your CenturyLink Senior Account Manager, at Bjorn.Johnson@CenturyLink.com or at (605) 977-2820
e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.	CenturyLink was Prime Contractor. PIMA County has a population of 1M+ - that include 10 PSAPs. CenturyLink Implemented, NG911 Core services Network and Hosted CenturyLink MECH product (Managed Emergency Call Handing) and TXT 2 9-1-1. Description of services provided: i3 compliant NG911 Core services, hosted VESTA Call handling equipment, integrated Text to 911, mapping, 24x7x365 monitoring and security of entire network and CPE. 24x7x365 maintenance and software support. Full implementation which includes training pre and post deployment, project management and a suite of additional services.

ii. Contractor and subcontractor(s) experience should be listed separately. Narrative descriptions submitted for subcontractors should be specifically identified as subcontractor projects.

Response:

CenturyLink has read, understands, complies. CenturyLink's vendors are listed as subcontractors and are listed as such in the description below.

iii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the Contractors above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

Response:

CenturyLink has read, understands, complies, and offers aforementioned description of subcontractor(s) most recent experience, including the narrative description that identifies the same information as requested for the Contractors above. Project responsibilities and time period is listed. Contract costs are not included and are considered to be customer specific proprietary information. Therefore, contract cost is not listed.

Synergem's NGCS serves 29.2 million people and 653 PSAPs. Synergem is subcontracted to support statewide or regional NG9-1-1 projects in Washington, Massachusetts, Alabama, Wisconsin, Michigan, California and Missouri. The following are some of the recent major projects.

Commonwealth of Massachusetts,
9-1-1 Commission via RFP: Next-Generation 9-1-1 System and Services RFP2013 – 08 – DB;

Scope of Work: Beginning in August 2014, Synergem has served as a principal subcontractor providing functional network elements and professional services to the Commonwealth of Massachusetts. Synergem's scope involves provisioning the ESRP, PRF, LNG, LSRG, and LPG, as well as, providing subject matter expertise on the overall solution design and provisioning. Synergem's functional elements are currently supporting every 9-1-1 call for the Commonwealth's 259 PSAPs and a population of over 6.9M. Synergem has met all its milestones in this project. **Contact:** Norm Fournier, Deputy Executive Director Massachusetts County 911 Department 151 Campanelli Drive, Suite A, Middleborough MA 02346,
508-821-7209

California Governor's Office of Emergency Services,
ESInet equipped with NGCS

Scope of Work: Beginning in 2018, Synergem has served as the prime contractor in a turnkey project that is migrating 36 PSAPs in 13 northeast California counties to an ESInet equipped with NGCS. The new Synergem network is replacing the "NG9-1-1" service provided by West Corp (formerly Intrado). This project has now been expanded to include all 167 PSAPs in the northern region of California. Additionally, through our partnership with CenturyLink, Synergem is providing NGCS for all 95 PSAPs in the southern region of California. Synergem will be serving a population of 20M. **Contact :** Ryan Sunahara Ryan.Sunahara@CalOES.ca.gov 916.657.9100 10370 Peter A. McCuen Blvd.
Mather CA 95655

TDS Telecom:
NG9-1-1 interconnect services

Scope of Work: STI has been contracted by TDS for several projects. Synergem provides TDS with NG9-1-1 interconnect services in Michigan, Wisconsin, Washington, and Alabama. In Wisconsin, Synergem is replacing TDS's legacy 9-1-1 network with NGCS. **Contact:** Jamie Jones Jamie.jones@tdstelcom.com
608.664.4477 525 Junction Road Madison WI, 53701

i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this solicitation. The names and titles of the team proposed for assignment to the State project should be identified in full, with a description of the team leadership, interface and support functions, and reporting relationships. The primary work assigned to each person should also be identified. Project managers assigned to the project shall be certified Project Management Professionals (PMP) and are highly encouraged to possess the Emergency Number Professional (ENP) certification.

The bidder should provide resumes for all personnel proposed to work on the project. The State will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the solicitation in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the State.

Response:

CenturyLink describes our two-team approach for program/project management and account management below. In the initial meeting with the State, after the contract is awarded, both teams will be represented to explain our management approach.

CenturyLink's Program Management team will be involved in the planning and installation of services and products until the service implementation is accepted and the project is complete. CenturyLink's account management team is assigned during the bid process and will provide dedicated services to the State throughout the term of the contract. Each team is described below.

CenturyLink Standard Program/Project Management Approach

CenturyLink Program/Project Management (CPrgM & CPM) adheres to Best Practices Methodology as prescribed by the Project Management Institute standards and ITILv3. The CPrgM/CPM charter underscores CenturyLink's commitment to facilitate a seamless transition for our customer's communications services to CenturyLink's network, ensures compliance with the terms of the contract, and maintains customer satisfaction throughout the project life cycle. We believe that by following these proven project management practices, the project milestones can be successfully achieved. The PMO's goal and commitment is to professionally manage and deliver projects on time and with satisfaction. CenturyLink is committed to the successful implementation of our customer's projects through the skills of Project Management by providing:

- Experienced, professional CPMs (many with PMP certifications)
- Recognized Authority to Manage and Direct Team Members and Resources
- Extensive Telecommunications Background

- Overall Project Management Background
- Project Management as a Functional Role within CenturyLink

A CPrgM will engage after the contract negotiations have been finalized. Throughout the program lifecycle, Maggie Cook, PMP, CISSP, CCSK and ITIL certified, will work with the CenturyLink Account team to provide customer support across the organizations of CenturyLink. Ms. Cook will serve as the CenturyLink Single Point of Contact during the implementation and transition phase to identify critical project success factors and mutually negotiate modifications and time frames for inclusion in the customized Project Plan. Maggie will:

- Provide high-quality services through efficient, resourceful, and responsive Program/Project Management
- Confirm compliance with terms of contract
- Maintain customer satisfaction
- Ensure project meets scheduling and technical requirements
- Manage external suppliers, vendors, and third-party contributors to the project
- Facilitate rapid response to changing technologies and environments through change/configuration management

Program and Project Management Representatives

Please note that the final Program/Project Plan, including the development of components such as the communications plan, test plan, cutover plan, and actual timeline (with expected task duration and detailed task assignments) will be developed after contract award and will be tailored to the unique needs, requirements, and scope of the customer's contract. This document will be developed after a thorough review of the contract, SOW, and discussion with the CenturyLink Account Team, the CenturyLink Operations & Network teams, and the customer's representatives. A sample of what the Program Development Plan will look like is in the appendix named "**4.2.C_CenturyLink Sample Program Development Plan for Nebraska**".

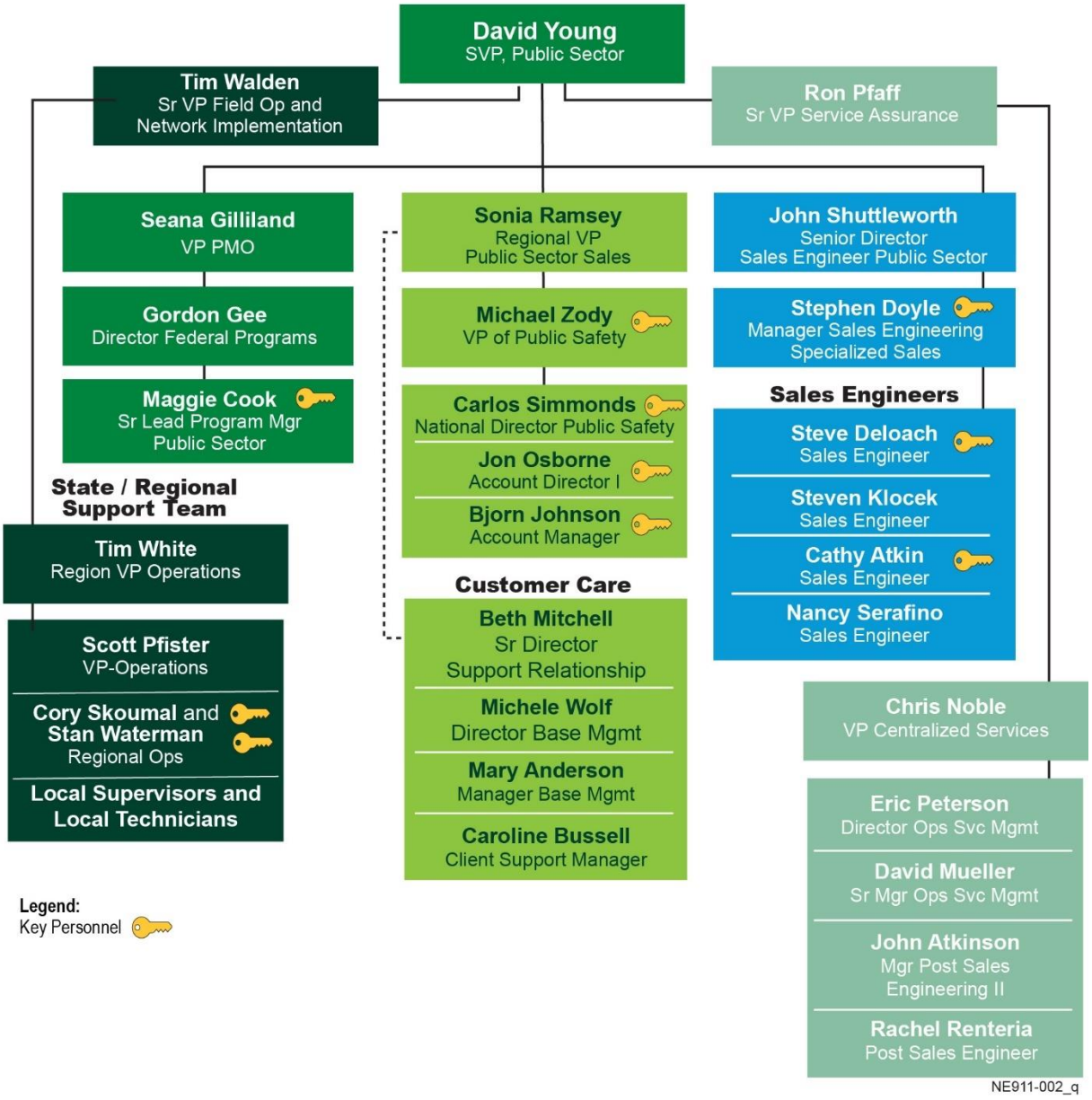
Account Team Introduction

Our Account and Service Teams are structured around a clear, focused, and disciplined market strategy designed to drive near and long-term value to our customers who we serve by delivering solutions and value that our competitors cannot easily duplicate.

The company's open management model drives fast decision-making and promotes discipline, enabling CenturyLink to be closer to its customers and to more responsively deliver services to the market and reply to individual customer requests. CenturyLink's global sales and support model matches its network footprint and delivers a consistent and superior customer experience worldwide.

CenturyLink's vision "is to be the recognized leader in connecting business, people and information around the world".

Below is the organizational chart for the CenturyLink Account Team that will be dedicated to the Nebraska account.



Below is an account team profile. It provides the title, responsibilities, contact information, years of experience, and certifications, if applicable, for each member of the account team that has worked on the 911 NGCS system design and/or will work on the project. Please note that Maggie Cook is PMP, CISSP, CCSK and ITIL certified and Nancy Serafino is ENP certified.

The CenturyLink Account Team Profiles for Nebraska

Account Team Experience and Expertise

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Sr. Account Manager - SLED	Proposes customer solutions based on customer requirements and needs resulting in decisions for CenturyLink. Provides consultative oriented solutions sales leveraging the CenturyLink Corporate portfolio. Collaborates with technical and other support services, and with other CenturyLink sales resources to maximize sales focus. Leads account strategy planning and build key customer relationships.	Bjorn Johnson Bjorn.Johnson@centurylink.com Office: 605 977 2820 Cell: 605 321 6188	25 Years of Industry experience managing large complex enterprise accounts 2+ years' experience in the Public Safety, State & County Government, and Education markets.
Account Director I - SLED	Strategically engages with state and local leadership through establishing C-Level and Director level relationships within multiple market verticals. Specifically, State Government and 911 Public Safety. Supports State 911 Agencies and acts as center point of contact to resolve issues quickly	Jon Osborne Jon.Osborne1@centurylink.com Office: 402 998 7392 Cell: 402 216 1009	17+ years in telecommunications and leadership roles. 6+ years in Public Safety and Government support roles. Member of APCO and NENA. Active in 911 Local Advisory boards and Government Community support roles
National Director 9-1-1 Public Safety	Oversees national public safety sales team. Responsible for the success of the business unit and customer projects. Aligns ecosystem partners to ensure successful delivery of revenue commitments.	Carlos Simmonds Carlos.Simmonds@centurylink.com Office: 602 512 2535 Cell: 602 319 4758	19+ years in telecommunications. 13 years in Public Safety, State, Local Government and education market leadership. Active member of NENA and APCO as well as various local community organizations.

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
VP of Public Safety	Oversees administrative sales staff that identifies markets and outline strategies. Coordinates a team that helps government, education and public safety sector organizations implement proven IT solutions to address public infrastructure continuity, ensure safety and security, facilitate economic growth, build stronger educational systems and augment technology needs.	Michael Zody michael.zody@centurylink.com Office: 610 785 1486 Cell: 717 443 9535	30+ years in telecommunications and IT leadership roles. 20+ years in Public Sector enterprise roles. Corporate Alliance member of NASCIO and NASTD. Active in Local Government and Community roles
Senior Sales Engineer	Responsible for reviewing technical requirements of solicitation to design and architect world-class networking solutions.	Steve Deloach Steve.Deloach@CenturyLink.com Office: 407 252-6333 Mobile: 407 252-6333	Over 20 Years Public Safety Experience. Over 30 years Combined Service with CenturyLink. Served on NC 911 Wireless Board in 2013.
Senior Sales Engineer	Responsible for reviewing technical requirements of solicitation to design and architect world-class networking solutions.	Steven Klocek Steven.Klocek@CenturyLink.com Office: 763 400 5492 Cell: 952 857 9609	Over 36 years of experience in the Telecommunications Industry. 21+ years' experience in the Public Safety, State & County Government, and Education markets. Strong performance in Next Gen 911,
Senior Sales Engineer	Responsible for reviewing technical requirements of solicitation to design and architect world-class networking solutions.	Cathy Atkin Cathy.Atkin@CenturyLink.com Office: 520 526 1877 Cell: 520 331 3021	45 years with CenturyLink in support of both Global Enterprise Customers and Government and Education Services. MISM - University of Phoenix, Cisco-CCNA/CCDA, Avaya, Juniper,Mitel, Vesta, Viper, VMWare Certified

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Senior Sales Engineer	Responsible for reviewing technical requirements of solicitation to design and architect world-class networking solutions.	Nancy Serafino Nancy.C.Serafino@centurylink.com Office: 419 755 7366 Mobile: 419 610 6645	32+ years' experience with CenturyLink. 25 years serving 911 customers throughout the US. **ENP Professional**. State 911 Technical Advisory Committee 5 years
Manager Sales Engineering Specialized Sales	Manages Sales Engineers who are focused on the technical aspects of the solution. Serves as first point of escalation for any design-related issues.	Stephen Doyle Stephen.Doyle@CenturyLink.com Office: 520 292 5618 Mobile: 520 904 5699	41 years with CenturyLink in support of both Global Enterprise Customers and Government and Education Services. MISM - University of Phoenix, Cisco, Adtran, Avaya, Mitel, Vesta, Viper Certified
Senior Director Sales Engineer Public Sector	Responsible for all aspects of the pre-sales engineering/solution architecture functions for the CTL Public Sector.	John Shuttleworth john.shuttleworth@centurylink.com Office: 571 730 6522 Cell: 703 407 6177	39 years Telecom Engineering and Solution Architecture with CenturyLink. Additional prior experience in wireline and wireless technologies.
Client Support Manager (CSM)	The CSM is your on-going personal contacts for support. Your CSM will be the main support contacts for order review, input and tracking through install, and reviewing your service to ensure that it is up to date. Additional responsibilities include maintaining the account for inventory accuracy, assisting with implementation and review and handling of billing and credits.	Caroline Bussell caroline.bussell@centurylink.com Cell: 317 697 4499	2+ years of Industry experience, Government, Education and Public Safety in both sales and sales support roles. BA- Indiana University Telecommunications & Sociology

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Manager Base Management	Responsible for the all CSMs that support Strategic Accounts within CenturyLink's territory. The manager is a point of escalation and is the point of ultimate responsibility for overall customer satisfaction. Responds to billing inquiries and resolves billing disputes. Proactively monitors service provider-billing accuracy. Works with order processing group to minimize billing errors on the front end.	Mary Anderson Mary.Anderson1@centurylink.com Office: 402 998 7386 Mobile: 402 215 2282	17 years telecom experience, 13 years as Customer Service Manager 5 years at CenturyLink
Director, Base Management	Manages the Account Consultants and Service Managers. Dedicated to working with our Government & Education Services (GES) clients in either a sales or sales support role.	Michele Wolf Michele.Wolf@CenturyLink.com Office: 952 885 3940 Mobile: 651 492 3361	19 years' experience with CenturyLink MBA from Augsburg College and BS – Economics and Business Management Lean Six Sigma Green Belt
Post Sales Engineer & Service Manager	The Service Assurance Manager is the post-sales technical support and repair escalation. Your Service Assurance Manager will assist in trouble ticket management, escalation, and provide RFO (reason for outage) upon request. Additional responsibilities include coordination of change management and client business review and recommendations. The Service Assurance Manager reports directly to the Regional Support Manager.	Rachel Renteria Rachel.Renteria@centurylink.com Office: 214 989 3577	26 years telecom experience with 7 at CenturyLink. CCNA, with 20 years of Service Management experience and 10 years NOC management.

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Manager Post Sales Engineering II	Manager Post Sales Engineering responsible for overall operational performance for regional clients within the Public Sector.	John Atkinson John.Atkinson@CenturyLink.com Office: 602 563 3292 Cell: 480 888 5104	33 years of service at CenturyLink including 13 years in service management and over 15 in a NOC environment
Sr Mgr Operations Service Management	Sr. Manager Operations Service Management responsible for overall operational performance for all clients supported by Operations Service Managers and Post Sales Engineers within the Public Sector.	David Mueller dave.mueller@centurylink.com Office: 720 888 2634 Cell: 303 905 7432	18 years in the telecommunications industry with 16 at CenturyLink and legacy companies. Lean Six Sigma Green Belt, Bachelors in Political Science, MBA
Dir Operations Service Management	Director of Operations Service Management responsible for overall operational performance for all clients supported by Operations Service Managers and Post Sales Engineers within CenturyLink.	Eric Peterson eric.peterson@centurylink.com Office: 918 547 7754 Cell: 918 809 1994	22 years with CenturyLink, Bachelors in Finance, MBA.
Manager Regional Operations II	Responsible for overall field operations including installation and maintenance of fiber and copper transport networks and installation and maintenance of all 911 equipment and CPE. Oversees all CenturyLink Technician activities	Stan Waterman Stan.Waterman@centurylink.com Office: 531 301 3080 Cell: 308 631 2653	39 Yrs. Telecommunication experience including Installation, maintenance and construction of CenturyLink network and residential and enterprise customers. Manage teams doing this work
Manager Regional Operations II	Responsible for overall field operations including installation and maintenance of fiber and copper transport networks and installation and maintenance of all 911 equipment and CPE. Oversees all CenturyLink Technician activities	Cory Skoumal Cory.Skoumal@CenturyLink.com Office: 402 998 6012 Cell: 402 320 6261	20 Yrs. Telecommunication experience including, managing teams of engineers, installation and maintenance teams for residential and enterprise customers
VP Operations	Located in Houston, TX. Responsible for field provisioning, maintenance, and repair of physical plant in TX, NM, KS, NE, OK	Scott Pfister scott.pfister@centurylink.com Office: 281 618 3972 Cell: 214 755 4239	25 years with CenturyLink, Bachelors in Finance.

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Sr. Lead Program Manager (PM)	Oversees overall implementation including project planning development, project execution, quality, change control, meeting coordination, and documentation. Main customer point of contact and integrator, ensuring compliance with contract terms and objectives are incorporated consistently throughout the project implementation.	Maggie Cook margaret.cook@centurylink.com Office: 571 730 3096 Cell: 703 867 2095	26+ years in the telecommunication industry, with 15+ years focused on mission critical Department of Defense networks. B.S in Information Systems, **Certified Project Management Professional (PMP) since 2005. Certified Information Systems Security Professional (CISSP), Cloud Computing Security Knowledge (CCSK) and Information Technology Infrastructure Library (ITIL) certified**
Director Public Sector Program Management	Responsible for all aspects of the Project Management process for the lifecycle of a project's implementation. Directly responsible for PMO managers and, by extension, individual contributors. Point of escalation both internally and customer-facing to ensure appropriate project support and alignment with project goals.	Gordon Gee gordon.gee@centurylink.com Office: 571 730 6591 Cell: 703 593 0080	30 years in the telecommunications industry and 8 years with CenturyLink. B.Sc. Electrical Engineering and MBA – Carey Business School, Johns Hopkins University
Customer Data Technician	Responsible for all aspects of installation and maintenance of 911 systems. Including Network elements and CPE	Craig Blocher Craig.Blocher@centurylink.com Office: 308 324 3302 Cell: 308 325 5234	30 yrs. Telecommunication experience 15 yrs. Specific 911 experience Intrado Viper Certified Enterprise Design Services installation and maintenance of fiber and copper networks

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Customer Data Technician	Responsible for all aspects of installation and maintenance of 911 systems. Including Network elements and CPE	Jim Stacy James.Stacy@centurylink.com Office: 308 530 4011 Cell: 308 530 4011	12 yrs. Telecommunications experience 1 yr. specific 911 experience Intrado Viper Certified Enterprise Design Services installation and maintenance of fiber and copper networks
Customer Data Technician	Responsible for all aspects of installation and maintenance of 911 systems. Including Network elements and CPE	Don Cramer Donald.Cramer@CenturyLink.com Office: 402 708 3261 Cell: 402 708 3261	25 yrs. Telecommunications experience 14 yrs. Specific 911 experience Intrado Viper training Enterprise Design Services installation and maintenance of fiber and copper networks
Customer Data Technician	Responsible for all aspects of installation and maintenance of 911 systems, including Network elements and CPE	Ryan Scott Ryan.Scott@centurylink.com Office: 402 592 6016 Cell: 402 312 4880	22 yrs. Telecommunications experience 13 yrs. specific 911 experience Intrado Viper training Lifeline training Enterprise Design Services installation and maintenance of fiber and copper networks
Customer Data Technician	Responsible for all aspects of installation and maintenance of 911 systems, including Network elements and CPE	Tom Hodge Thomas.v.hodge@centurylink.com Office: 402 727 4974 Cell: 402 720 2883	29 yrs. telecommunication experience 16 yrs. specific 911 experience Intrado Viper Certified Lifeline Certified Enterprise Design Services installation and maintenance of fiber and copper networks

Title	Responsibility	CenturyLink Personnel and Contact Information	Experience
Central Office Technician	Responsible for the installation and maintenance of fiber and copper transport networks in NE	Christopher Kautz Christopher.Kautz@centurylink.com Office: 402 644 3530 Cell: 402 290 8317	27 yrs. Telecommunications experience installation and maintenance of fiber and copper transport networks
Central Office Technician	Responsible for the installation and maintenance of fiber and copper transport networks in NE	Grant True Grant.True@centurylink.com Office: 402-433-5182 Cell: 402 433 5182	25 yrs. Telecommunications experience installation and maintenance of fiber and copper transport networks
Central Office Technician	Responsible for the installation and maintenance of fiber and copper transport networks in NE	Brenda Kobobel-Troy Brenda.Kobobel-Troy@centurylink.com Office: 402 336 1144 Cell: 402 340 4616	30 yrs. Telecommunications experience installation and maintenance of fiber and copper transport networks

CenturyLink reserves the right to make changes to its organization. CenturyLink understands the importance of consistency in personnel and will attempt to limit changes. CenturyLink agrees that the State may request personnel changes and CenturyLink will work with the State to address any concerns, but we must ultimately retain responsibility for how our employees are assigned to projects.

CenturyLink has detailed the project plan and timeline in the Program Management Plan (PMP). CenturyLink presents the resumes for the people who will work on the State's project and focus on providing an excellent customer experience in the attachment named "I.A.1.i Key Employee Resumes".

j. SUBCONTRACTORS

If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

i. name, address, and telephone number of the subcontractor(s);

Response:

Synergem technologies
Jeffery J. Schlueter, COO
371 Windrush Lane,
Mt. Airy NC 27030

ii. specific tasks for each subcontractor(s);

Response: Synergem Technologies Inc. (STI) will be providing the NGCS. CenturyLink proposes to install SynergemNET™, a nationwide, fully redundant service designed in compliance with the NG9-1-1 standards defined in NENA-STA-010.2-2016 as updated.

SynergemNET™ is provided as a “Software as a Solution”. The ability to grow and integrate new capabilities is a built-in network characteristic. It can be enhanced centrally with performance bounded only by the size and scope of local infrastructure. As it is proposed, however, this network is highly scalable

- Up to 4 million routes
- Up to 500,000 SIP-TLS sessions

iii. percentage of performance hours intended for each subcontract; and

Response: STI will have approximately 10% of the contract hours

iv. total percentage of subcontractor(s) performance hours.

Response: STI will have approximately 10% of the contract hours

II. TERMS AND CONDITIONS

Bidders should complete Sections II through VI as part of their proposal. Bidders should read the Terms and Conditions and should initial either accept, reject, or reject and provide alternative language for each clause. The bidder should also provide an explanation of why the bidder rejected the clause or rejected the clause and provided alternate language. By signing the solicitation, bidder is agreeing to be legally bound by all the accepted terms and conditions, and any proposed alternative terms and conditions submitted with the proposal. The State reserves the right to negotiate rejected or proposed alternative language. If the State and bidder fail to agree on the final Terms and Conditions, the State reserves the right to reject the proposal. The State of Nebraska is soliciting proposals in response to this solicitation. The State of Nebraska reserves the right to reject proposals that attempt to substitute the bidder's commercial contracts and/or documents for this solicitation.

Bidders should submit with their proposal any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The State will not consider incorporation of any document not submitted with the bidder's proposal as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated as addendums if agreed to by the Parties.

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:1. If only one Party has a particular clause then that clause shall control;

2. If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;
3. If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink requests a revision to the order or precedence consistent with what the parties have agreed to in prior contracts and as shown below. This change ensures clarity about any modifications to the RFP specifications provided in CenturyLink's response and ensures the final definitive contract between the parties reflecting the specific solution selected by the State takes first priority: 1) Amendment to the executed Contract with the most recent dated amendment having the highest priority, 2) executed Contract and any attached Addenda or Service Attachments, 3) the bidder's submitted Proposal, 4) Amendments to solicitation and any Questions and Answers, 5) the original solicitation document and any Addenda

The contract resulting from this solicitation shall incorporate the following documents:

1. Request for Proposal and Addenda;
2. Amendments to the solicitation;
3. Questions and Answers;

4. Bidder's proposal (Solicitation and properly submitted documents);
5. The executed Contract and Addendum One to Contract, if applicable; and,
6. Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

Unless otherwise specifically stated in a future contract amendment, in case of any conflict between the incorporated documents, the documents shall govern in the following order of preference with number one (1) receiving preference over all other documents and with each lower numbered document having preference over any higher numbered document: 1) Amendment to the executed Contract with the most recent dated amendment having the highest priority, 2) executed Contract and any attached Addenda, 3) Amendments to solicitation and any Questions and Answers, 4) the original solicitation document and any Addenda, and 5) the bidder's submitted Proposal.

Any ambiguity or conflict in the contract discovered after its execution, not otherwise addressed herein, shall be resolved in accordance with the rules of contract interpretation as established in the State of Nebraska.

B. NOTIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			Regarding Item D, Governing Law, CenturyLink understands that the State of Nebraska must comply with applicable law, statutes, and regulations. However, rather than include a blanket statement that the contract may be overridden for a broad list of reasons, CenturyLink proposes that the parties should closely review the contract during the finalization process and ensure that that terms in the contract comply with applicable laws. The parties will benefit from the certainty of having definitive contract terms that can only be changed via a mutually agreed upon amendment to the contract.

Contractor and State shall identify the contract manager who shall serve as the point of contact for the executed contract.

Communications regarding the executed contract shall be in writing and shall be deemed to have been given if delivered personally or mailed, by U.S. Mail, postage prepaid, return receipt requested, to the parties at their respective addresses set forth below, or at such other addresses as may be specified in writing by either of the parties. All notices, requests, or communications shall be deemed effective upon personal delivery or five (5) calendar days following deposit in the mail.

Either party may change its address for notification purposes by giving notice of the change, and setting forth the new address and an effective date.

C. BUYER'S REPRESENTATIVE

The State reserves the right to appoint a Buyer's Representative to manage (or assist the Buyer in managing) the contract on behalf of the State. The Buyer's Representative will be appointed in writing, and the appointment document will specify the extent of the Buyer's Representative authority and responsibilities. If a Buyer's Representative is appointed, the Contractor will be provided a copy of the appointment document, and is required to cooperate accordingly with the

Buyer's Representative. The Buyer's Representative has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

D. GOVERNING LAW (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must be brought in the State of Nebraska per state law. (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity, limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

The Parties must comply with all applicable local, state and federal laws, ordinances, rules, orders, and regulations.

E. BEGINNING OF WORK

The bidder shall not commence any billable work until a valid contract has been fully executed by the State and the awarded bidder. The awarded bidder will be notified in writing when work may begin.

F. AMENDMENT

This Contract may be amended in writing, within scope, upon the agreement of both parties.

G. CHANGE ORDERS OR SUBSTITUTIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The State and the Contractor, upon the written agreement, may make changes to the contract within the general scope of the solicitation. Changes may involve specifications, the quantity of work, or such other items as the State may find necessary or desirable. Corrections of any deliverable, service, or work required pursuant to the contract shall not be deemed a change. The Contractor may not claim forfeiture of the contract by reasons of such changes.

The Contractor shall prepare a written description of the work required due to the change and an itemized cost sheet for the change. Changes in work and the amount of compensation to be paid to the Contractor shall be determined in accordance with applicable unit prices if any, a pro-rated value, or through negotiations. The State shall not incur a price increase for changes that should have been included in the Contractor's proposal, were foreseeable, or result from difficulties with or failure of the Contractor's proposal or performance.

No change shall be implemented by the Contractor until approved by the State, and the Contract is amended to reflect the change and associated costs, if any. If there is a dispute regarding the cost, but both parties agree that immediate implementation is necessary, the change may be implemented, and cost negotiations may continue with both Parties retaining all remedies under the contract and law.

In the event any product is discontinued or replaced upon mutual consent during the contract period or prior to delivery, the State reserves the right to amend the contract or purchase order to include the alternate product at the same price.

*****Contractor will not substitute any item that has been awarded without prior written approval of SPB*****

H. VENDOR PERFORMANCE REPORT(S)

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The State may document any instance(s) of products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or solicitation specifications. The State Purchasing Bureau may contact the Vendor regarding any such report. Vendor performance report(s) will become a part of the permanent record of the Vendor.

I. NOTICE OF POTENTIAL CONTRACTOR BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink will provide notice as soon as possible under the circumstances but does not agree that failure to provide immediate notice is grounds for denial of a request for waiver of a breach. The circumstances of what constitutes immediate notice are inherently subjective and difficult to quantify for an infinite number of potential scenarios.

If Contractor breaches the contract or anticipates breaching the contract, the Contractor shall immediately give written notice to the State. The notice shall explain the breach or potential breach, a proposed cure, and may include a request for a waiver of the breach if so desired. The State may, in its discretion, temporarily or permanently waive the breach. By granting a waiver, the State does not forfeit any rights or remedies to which the State is entitled by law or equity, or

pursuant to the provisions of the contract. ~~Failure to give immediate notice, however, may be grounds for denial of any request for a waiver of a breach.~~

J. BREACH; DAMAGES LIMITATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink proposes the changes shown below. Given the higher risk and cost associated with providing 911 services, CenturyLink cannot agree to a cost of cover provision. The State may seek services from a different provider if it chooses, but CenturyLink will not cover those costs. Additionally, CenturyLink requires limitations on its liability in order to provide the services at competitive rates and has provided additional language to address that concern below.

1. Breach. Either Party may terminate the contract, in whole or in part, if the other Party materially breaches its duty to perform its obligations under the contract in a timely and proper manner. Termination requires written notice of default and a thirty (30) calendar day (or longer at the non-breaching Party's discretion considering the gravity and nature of the default) cure period. Said notice shall be delivered by Certified Mail, Return Receipt Requested, or in person with proof of delivery. Allowing time to cure a failure or breach of contract does not waive the right to immediately terminate the contract for the same or different contract breach which may occur at a different time. ~~In case of default of the Contractor, the State may contract the service from other sources and hold the Contractor responsible for any excess cost occasioned thereby. OR In case of breach by the Contractor, the State may, without unreasonable delay, make a good faith effort to make a reasonable purchase or contract to purchase goods in substitution of those due from the contractor. The State may recover from the Contractor as damages the difference between the costs of covering the breach. Notwithstanding any clause to the contrary, the State may also recover the contract price together with any incidental or consequential damages defined in UCC Section 2-715, but less expenses saved in consequence of Contractor's breach.~~

   The State's failure to make payment shall not be a breach, and the Contractor shall retain all available statutory remedies and protections.

2. Damages Limitations. CenturyLink will not be liable for any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of data or cost of purchasing replacement services, or any indirect, incidental, special, consequential, exemplary or punitive damages arising out of the performance or failure to perform under this Agreement or any Service Attachment. UNLESS OTHERWISE SET FORTH IN A SERVICE ATTACHMENT, CUSTOMER'S EXCLUSIVE REMEDIES FOR CLAIMs WILL BE LIMITED TO THE TOTAL MRCs OR USAGE CHARGES PAID BY CUSTOMER TO CENTURYLINK FOR THE AFFECTED SERVICE IN THE ONE MONTH IMMEDIATELY PRECEDING THE OCCURRENCE OF THE EVENT GIVING RISE TO THE CLAIM. CENTURYLINK'S LIABILITY FOR ANY LOSS OR DAMAGE ARISING FROM ERRORS, INTERRUPTIONS, DEFECTS, FAILURES, OR MALFUNCTIONS OF ANY SERVICE OR ANY PART THEREOF CAUSED BY THE NEGLIGENCE OF CENTURYLINK WILL NOT EXCEED THE GREATER OF $50.00 OR AN AMOUNT EQUIVALENT TO THE PRO RATA CHARGES FOR THE SERVICE AFFECTED DURING THE TIME THE SERVICE WAS FULLY OR PARTIALLY INOPERATIVE. FURTHER CENTURYLINK, ITS AFFILIATES, AGENTS AND CONTRACTORS PROVIDING SERVICES ASSOCIATED WITH ACCESS TO 911

EMERGENCY SERVICE WILL NOT HAVE ANY LIABILITY WHATSOEVER FOR ANY PERSONAL INJURY TO OR DEATH OF ANY PERSON, FOR ANY LOSS, DAMAGE OR DESTRUCTION OF ANY PROPERTY RELATING TO THE USE, LACK OF ACCESS TO OR PROVISION OF, 911 EMERGENCY SERVICE. IN ADDITION, CENTURYLINK WILL NOT BE LIABLE FOR ANY DAMAGE THAT RESULTS FROM INFORMATION PROVIDED TO CUSTOMER BY ANY OTHER DATA PROVIDER(S).

3. Service Levels.

(a) Any "Service Level" commitments applicable to Services are contained in the Service Attachments applicable to each Service. If CenturyLink does not meet a Service Level, CenturyLink will issue to Customer a credit as stated in the applicable Service Attachment on Customer's request. CenturyLink's maintenance log and trouble ticketing systems are used to calculate Service Level events. Scheduled maintenance and force majeure events are considered excused outages.

(b) Unless otherwise set forth in a Service Attachment, to request a credit, Customer must contact Customer Service (contact information is located at http://www.level3.com) or deliver a written request with sufficient detail to identify the affected Service. The request for credit must be made within 60 days after the end of the month in which the event occurred. Total monthly credits will not exceed the charges for the affected Service for that month. Customer's sole remedies for any non-performance, outages, failures to deliver or defects in Service are contained in the Service Levels applicable to the affected Service.

K. NON-WAIVER OF BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The acceptance of late performance with or without objection or reservation by a Party shall not waive any rights of the Party nor constitute a waiver of the requirement of timely performance of any obligations remaining to be performed.

L. SEVERABILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

If any term or condition of the contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and conditions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the provision held to be invalid or illegal.

M. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	Regarding #1, CenturyLink cannot offer indemnification related to 911 services. SLAs and associated penalties will be defined in the contract and those will provide the sole and exclusive remedies for any claims related to service performance. Regarding #2, CenturyLink proposes changes that it reasonably believes will better clarify the scope of its IP obligations.

1. RESERVED. ~~The Contractor agrees to defend, indemnify, and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials ("the indemnified parties") from and against any and all third party claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses ("the claims"), sustained or asserted against the State for personal injury, death, or property loss or damage, arising out of, resulting from, or attributable to the willful misconduct, negligence, error, or omission of the Contractor, its employees, subcontractors, consultants, representatives, and agents, resulting from this contract, except to the extent such Contractor liability is attenuated by any action of the State which directly and proximately contributed to the claims.~~

2. INTELLECTUAL PROPERTY (Optional)

The Contractor agrees it will, at its sole cost and expense, defend, ~~indemnify, and hold harmless~~ the ~~indemnified parties~~ State from and against any and all third party claims filed against the State and alleging that a Service, as provided by Contractor, prospectively infringes, ~~to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of~~ any patent, copyright, trade secret, trademark, or other intellectual property right ("IP Right") ~~confidential information~~ of any third party by the Contractor or its employees, subcontractors, consultants, representatives, and agents; provided, however, the foregoing will not apply to any claim based on: (i) the combination of Service with other products, services or functionality, (ii) Contractor's design or modification of a Service in accordance with the State's specific written instructions, specifications or requirements; (iii) use or operation by or on behalf of the State of a Service other than in accordance with the Contract or other written documentation provided by Contractor; (iv) content, data, or other information provided by or on behalf of the State ("State Content"). Contractor's obligations under this section are contingent upon the State (i) ~~gave~~ giving the Contractor prompt notice in writing of the claim, (ii) providing Contractor with sole control and authority over the defense and/or settlement of such claim, and (iii) cooperating with Contractor (at Contractor's expense) in the defense and/or settlement of such claim upon Contractor's written request. The Contractor may not settle any infringement claim that will affect the State's use of the ~~Licensed Software~~ affected intellectual property without the State's prior written consent, which ~~consent may be withheld for any reason~~ may not be unreasonably withheld.

If a judgment or settlement is obtained or reasonably anticipated against the State's use of any intellectual property for which the Contractor has ~~indemnified the State~~ a defense or payment obligation, the Contractor ~~shall~~ may, at the Contractor's sole cost and expense, promptly modify the item or items which were determined to be infringing, ~~acquire a license or licenses on~~ obtain for the State the right to continue using the Service consistent with the Contract~~'s behalf to provide the necessary rights to the State to eliminate the infringement~~, or provide the State with a non-infringing substitute that provides the State ~~the same~~ with equivalent functionality. ~~At the State's election, the actual or anticipated judgment may be treated as a breach of warranty by the Contractor, and the State may receive the remedies provided under this RFP.~~

Notwithstanding the foregoing, any third-party service, system, CPE, equipment or software provided under this Agreement (each, a "Third Party Item") is provided without any obligation of Contractor to defend or indemnify the State against any claim of infringement of any IP Right arising in connection with any such Third Party Item, except that Contractor shall pass through to the State any contractual obligations of a third party provider of any such Third Party Item to defend or indemnify the State against such claims. The foregoing states Contractor's only obligations (and the State's sole and exclusive remedy) for any claims, actions, liabilities, damages or losses arising in connection with alleged or actual infringement, violation or misappropriation of an IP Right by the Services.

3. PERSONNEL

The Contractor shall, at its expense, indemnify and hold harmless the ~~indemnified parties~~ State from and against any claim with respect to withholding taxes, worker's compensation, employee benefits, or any other similar claim, demand, liability, damage, or loss ~~of any nature~~ relating to any of the personnel, including subcontractor's and their employees, provided by the Contractor to perform the services under this Agreement.

4. SELF-INSURANCE

The State of Nebraska is self-insured for any loss and purchases excess insurance coverage pursuant to Neb. Rev. Stat. § 81-8,239.01 (Reissue 2008). If there is a presumed loss under the provisions of this agreement, Contractor may file a claim with the Office of Risk Management pursuant to Neb. Rev. Stat. §§ 81-8,829 – 81-8,306 for review by the State Claims Board. The State retains all rights and immunities under the State Miscellaneous (§ 81-8,294), Tort (§ 81-8,209), and Contract Claim Acts (§ 81-8,302), as outlined in Neb. Rev. Stat. § 81-8,209 et seq. and under any other provisions of law and accepts liability under this agreement to the extent provided by law.

5. The Parties acknowledge that Attorney General for the State of Nebraska is required by statute to represent the legal interests of the State, and that any provision of this indemnity clause is subject to the statutory authority of the Attorney General.

N. ATTORNEY'S FEES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

In the event of any litigation, appeal, or other legal action to enforce any provision of the contract, the Parties agree to pay all expenses of such action, as permitted by law and if ordered by the court, including attorney's fees and costs, if the other Party prevails.

O. PERFORMANCE BOND

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			Please see the bond letter provided by our bonding company as "**Appendix III.O_Performance Bond**"

The Contractor maybe required to supply a bond executed by a corporation authorized to contract surety in the State of Nebraska, payable to the State of Nebraska, which shall be valid for the life of the contract to include any renewal and/or extension periods. The amount of the bond must be $500,000. The bond will guarantee that the Contractor will faithfully perform all requirements, terms and conditions of the contract. Failure to comply shall be grounds for forfeiture of bond as liquidated damages. Amount of forfeiture will be determined by the agency based on loss to the State. The bond will be returned when the contract has been satisfactorily completed as solely determined by the State, after termination or expiration of the contract.

P. ASSIGNMENT, SALE, OR MERGER; AFFILIATES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink proposes adding affiliates language to his section (or elsewhere in the contract as the parties may mutually agree upon during contract finalization) to clarify that CenturyLink is permitted to affiliates, subcontractors, and third parties, since those relationships would be part of the solution proposed in our response. However, regardless of CenturyLink's use of a third party, CenturyLink remains responsible to the State for the services under the contract.

Assignment, Sale, Or Merger. Either Party may assign the contract upon mutual written agreement of the other Party. Such agreement shall not be unreasonably withheld.

The Contractor retains the right to enter into a sale, merger, acquisition, internal reorganization, or similar transaction involving Contractor's business. Contractor agrees to cooperate with the State in executing amendments to the contract to allow for the transaction. If a third party or entity is involved in the transaction, the Contractor will remain responsible for performance of the

contract until such time as the person or entity involved in the transaction agrees in writing to be contractually bound by this contract and perform all obligations of the contract.

Affiliates. CenturyLink may use a CenturyLink affiliate, subcontractor or a third party to provide Service to Customer, but CenturyLink will remain responsible to Customer for Service delivery and performance.

Q. CONTRACTING WITH OTHER NEBRASKA POLITICAL SUB-DIVISIONS OF THE STATE OR ANOTHER STATE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor may, but shall not be required to, allow agencies, as defined in Neb. Rev. Stat. §81-145, to use this contract. The terms and conditions, including price, of the contract may not be amended. The State shall not be contractually obligated or liable for any contract entered into pursuant to this clause. A listing of Nebraska political subdivisions may be found at the website of the Nebraska Auditor of Public Accounts.

The Contractor may, but shall not be required to, allow other states, agencies or divisions of other states, or political subdivisions of other states to use this contract. The terms and conditions, including price, of this contract shall apply to any such contract, but may be amended upon mutual consent of the Parties. The State of Nebraska shall not be contractually or otherwise obligated or liable under any contract entered into pursuant to this clause. The State shall be notified if a contract is executed based upon this contract.

R. FORCE MAJEURE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Neither Party shall be liable for any costs or damages, or for default resulting from its inability to perform any of its obligations under the contract due to a natural or manmade event outside the control and not the fault of the affected Party ("Force Majeure Event"). The Party so affected shall immediately make a written request for relief to the other Party, and shall have the burden of proof to justify the request. The other Party may grant the relief requested; relief may not be unreasonably withheld. Labor disputes with the impacted Party's own employees will not be considered a Force Majeure Event.

S. CONFIDENTIALITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink proposes replacing the first paragraph with the new paragraph shown below. This language provides a more robust definition of confidentiality obligations and carves out common exceptions to confidentiality.

~~All materials and information provided by the Parties or acquired by a Party on behalf of the other Party shall be regarded as confidential information. All materials and information provided or acquired shall be handled in accordance with federal and state law, and ethical standards. Should said confidentiality be breached by a Party, the Party shall notify the other Party immediately of said breach and take immediate corrective action.~~

All Confidential Information provided by the Parties or acquired by a Party on behalf of the other Party shall be regarded as confidential information. Except to the extent required by an open records act or similar law, neither party will: (a) disclose any of the terms of the Contract; or (b) disclose or use (except as expressly permitted by, or required to achieve the purposes of, the Contract) the Confidential Information received from the other party. A party may disclose Confidential Information if required to do so by a governmental agency, by operation of law, or if necessary in any proceeding to establish rights or obligations under the Contract. All Confidential Information provided or acquired shall be handled in accordance with federal and state law, and each party will limit disclosure and access to Confidential Information to those of its employees, contractors, attorneys or other representatives who reasonably require such access to accomplish the Contract's purposes and who are subject to confidentiality obligations at least as restrictive as those contained herein. Should said confidentiality be breached by a Party, the Party shall notify the other Party immediately of said breach and take immediate corrective action. "Confidential Information" means any commercial or operational information disclosed by one party to the other in connection with the Contract and does not include any information that: (a) is in the public domain without a breach of confidentiality; (b) is obtained from a third party without violation of any obligation of confidentiality; or (c) is independently developed by a party without reference to the Confidential Information of the other party.

It is incumbent upon the Parties to inform their officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1), which is made applicable by 5 U.S.C. 552a (m)(1), provides that any officer or employee, who by virtue of his/her employment or official position has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

T. EARLY TERMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink suggests changes consistent with what the parties have agreed to in prior contracts and that reflect the unique nature of a contract for NG911 Services

The contract may be terminated as follows:

1. The State and the Contractor, by mutual written agreement, may terminate the contract at any time.

2. The State, in its sole discretion, may terminate the contract upon ~~thirty (30)~~ sixty (60) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination for cause or default, the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided. In the event of termination for convenience, the State shall remain liable for all costs incurred by CenturyLink up to the date of termination, including but not limited to 100% of the costs incurred for special construction and third-party expenses. These charges will be determined upon termination according to CenturyLink records

3. The Contractor in its sole discretion may terminate the contract for any reason upon sixty (60) days' prior written notice to the State. In addition, the Contractor may terminate the contract for Cause. If the Contractor terminates for Cause, non-payment excluded, prior to the conclusion of its Term, then the Contractor will be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided. Any changes to the scope of this Agreement or any Amendments thereof shall not be made without the Contractor's prior written approval. Any agreed to up-scopes shall include cancellation charges equal to Special Construction Charges.

4. The State may terminate the contract immediately for the following reasons:

- **a.** if directed to do so by statute;
- **b.** Contractor has made an assignment for the benefit of creditors, has admitted in writing its inability to pay debts as they mature, or has ceased operating in the normal course of business;
- **c.** a trustee or receiver of the Contractor or of any substantial part of the Contractor's assets has been appointed by a court;
- **d.** fraud, misappropriation, embezzlement, malfeasance, misfeasance, or illegal conduct pertaining to performance under the contract by its Contractor, its employees, officers, directors, or shareholders;
- **e.** an involuntary proceeding has been commenced by any Party against the Contractor under any one of the chapters of Title 11 of the United States Code and (i) the proceeding has been pending for at least sixty (60) calendar days; or (ii) the Contractor has consented, either expressly or by operation of law, to the entry of an order for relief; or (iii) the Contractor has been decreed or adjudged a debtor;

f. a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;

g. Contractor intentionally discloses Confidential Information ~~confidential information~~;

h. ~~Contractor has or announces it will discontinue support of the deliverable; and,~~

i. In the event funding is no longer available.

U. CLOSEOUT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Upon contract closeout for any reason the Contractor shall within 30 calendar days, unless stated otherwise herein:

1. Transfer all completed or partially completed deliverables to the State;
2. Transfer ownership and title to all completed or partially completed deliverables to the State;
3. Return to the State all information and data, unless the Contractor is permitted to keep the information or data by contract or rule of law. Contractor may retain one copy of any information or data as required to comply with applicable work product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures;
4. Cooperate with any successor Contactor, person or entity in the assumption of any or all of the obligations of this contract;
5. Cooperate with any successor Contactor, person or entity with the transfer of information or data related to this contract;
6. Return or vacate any state owned real or personal property; and,
7. Return all data in a mutually acceptable format and manner.

Nothing in this Section should be construed to require the Contractor to surrender intellectual property, real or personal property, or information or data owned by the Contractor for which the State has no legal claim.

Additional Terms and Conditions: CenturyLink proposes the following additional provisions to be added to the contract as important provisions that provide protections to both the customer and CenturyLink:

V. Critical 9-1-1 Circuits. The Federal Communications Commission's 9-1-1 reliability rules mandate the identification and tagging of certain circuits or equivalent data paths that transport 9-1-1 calls and information ("9-1-1 Data") to public safety answering points. These circuits or equivalent data paths are defined as Critical 911 Circuits in 47 C.F.R. Section 12.4(a)(5). CenturyLink policies require tagging of any circuits or equivalent data paths used to transport 9-1-1 Data. Customer will cooperate with CenturyLink regarding compliance with these rules and

policies and will notify CenturyLink of all Services Customer purchases under this Agreement utilized as Critical 911 Circuits or for 9-1-1 Data.

CenturyLink explanation: Circuits that are used for 911 services need to be tagged as such so that they receive appropriate priority and treatment for service restoration in the event of an outage. CenturyLink needs our customers to commit to work with us on designating the circuits that they use to transport 911 Data.

W. Acceptable Use Policy and Data Protection. The State must comply with the CenturyLink Acceptable Use Policy ("AUP"), which is available at http://www.centurylink.com/legal, for Services purchased under this Agreement and acknowledge the CenturyLink Privacy Policy, which is available at http://www.centurylink.com/aboutus/legal/privacy-policy.html. CenturyLink may reasonably modify these policies to ensure compliance with applicable laws and regulations and to protect CenturyLink's network and customers.

CenturyLink explanation: Applicability of the CenturyLink AUP provides protection for all customers and the CenturyLink network.

III. CONTRACTOR DUTIES

A. INDEPENDENT CONTRACTOR / OBLIGATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink proposes changes to clarify that it is permitted to use affiliates, subcontractors, and third parties, since those relationships would be part of the solution proposed in our response. In addition, CenturyLink proposes to strike the last two sentences because our vendor contracts are already in place, and it is impractical to add customer-specific provisions into each contract. This should not impact the State because, regardless of CenturyLink's use of subcontractors, we remain responsible to the State for the delivery and performance of the services. CenturyLink agrees that the State may request personnel changes and CenturyLink will work with the State to address any concerns, but we must ultimately retain responsibility for how our employees are assigned to projects.

It is agreed that the Contractor is an independent contractor and that nothing contained herein is intended or should be construed as creating or establishing a relationship of employment, agency, or a partnership.

The Contractor is solely responsible for fulfilling the contract, subject to its permission to use affiliates, subcontractors, and third parties as set forth in the Contract. The Contractor or the Contractor's representative shall be the sole point of contact regarding all contractual matters.

The Contractor shall secure, at its own expense, all personnel required to perform the services under the contract. The personnel the Contractor uses to fulfill the contract shall have no contractual or other legal relationship with the State; they shall not be considered employees of the State and shall not be entitled to any compensation, rights or benefits from the State, including but not limited to, tenure rights, medical and hospital care, sick and vacation leave, severance pay, or retirement benefits.

By-name personnel commitments made in the Contractor's proposal shall not be changed without the ~~prior written approval~~ consent of the State, which shall not be unreasonably withheld. Replacement of these personnel, if approved by the State, shall be with personnel of equal or greater ability and qualifications.

All personnel assigned by the Contractor to the contract shall be employees of the Contractor or a subcontractor, and shall be fully qualified to perform the work required herein. Personnel employed by the Contractor or a subcontractor to fulfill the terms of the contract shall remain under the sole direction and control of the Contractor or the subcontractor respectively.

With respect to its employees, the Contractor agrees to be solely responsible for the following:

1. Any and all pay, benefits, and employment taxes and/or other payroll withholding;
2. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;
3. Damages incurred by Contractor's employees within the scope of their duties under the contract;
4. Maintaining Workers' Compensation and health insurance that complies with state and federal law and submitting any reports on such insurance to the extent required by governing law;

5. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,
6. All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination alleged against the Contractor, its officers, agents, or subcontractors or subcontractor's employees).

If the Contractor intends to utilize any subcontractor, the subcontractor's level of effort, tasks, and time allocation should be clearly defined in the bidder's proposal. The Contractor shall agree that it will not utilize any subcontractors not specifically included in its proposal in the performance of the contract without the prior written authorization of the State.

The State reserves the right to require the Contractor to reassign or remove from the project any Contractor or subcontractor employee for lawful reasons.

If the State receives a complaint about the behavior or conduct of Contractor's employees or any subcontractor employee, the State shall notify the Contractor and reserves the right to ask them to be reassigned or removed from the project.

~~Contractor shall insure that the terms and conditions contained in any contract with a subcontractor does not conflict with the terms and conditions of this contract.~~

~~The Contractor shall include a similar provision, for the protection of the State, in the contract with any subcontractor engaged to perform work on this contract.~~

B. EMPLOYEE WORK ELIGIBILITY STATUS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			**Please see CenturyLink's Attestation form provided as the Attachment "3.B I 9 Compliance Certification_Q1 2020_Letterhead"**

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of an employee.

If the Contractor is an individual or sole proprietorship, the following applies:

1. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html.
2. The completed United States Attestation Form should be submitted with the solicitation response.
3. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation

required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

4. The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified, or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

C. COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory)

The Contractor shall comply with all applicable local, state, and federal statutes and regulations regarding civil rights laws and equal opportunity employment. The Nebraska Fair Employment Practice Act prohibits Contractors of the State of Nebraska, and their subcontractors, from discriminating against any employee or applicant for employment, with respect to hire, tenure, terms, conditions, compensation, or privileges of employment because of race, color, religion, sex, disability, marital status, or national origin (Neb. Rev. Stat. §48-1101 to 48-1125). The Contractor guarantees compliance with the Nebraska Fair Employment Practice Act, and breach of this provision shall be regarded as a material breach of contract. The Contractor shall insert a similar provision in all subcontracts for goods and services to be covered by any contract resulting from this solicitation.

D. COOPERATION WITH OTHER CONTRACTORS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Contractor may be required to work with or in close proximity to other contractors or individuals that may be working on same or different projects. The Contractor shall agree to cooperate with such other contractors or individuals, and shall not commit or permit any act which may interfere with the performance of work by any other contractor or individual. Contractor is not required to compromise Contractor's intellectual property or proprietary information unless expressly required to do so by this contract.

E. PERMITS, REGULATIONS, LAWS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The contract price shall include the cost of all royalties, licenses, permits, and approvals, whether arising from patents, trademarks, copyrights or otherwise, that are in any way involved in the contract. The Contractor shall obtain and pay for all royalties, licenses, and permits, and approvals necessary for the execution of the contract. The Contractor must guarantee that it has

the full legal right to the materials, supplies, equipment, software, and other items used to execute this contract.

F. ~~OWNERSHIP OF INFORMATION AND DATA /~~ DELIVERABLES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink proposes edits to clarify the definition and scope of deliverable ownership.

The State shall have the ~~unlimited~~ right to publish, duplicate, use, and disclose all information and data developed or obtained by the Contractor on behalf of the State ("collectively, Deliverables") pursuant to this contract, if Deliverables are specifically contemplated in the Contract and paid for by the State.

The State shall own and hold exclusive title to any Deliverable developed as a result of this contract and paid for by the State. Contractor shall have no ownership interest or title, and shall not patent, license, or copyright, duplicate, transfer, sell, or exchange, the ~~design, specifications, concept, or~~ ~~d~~Deliverables.

G. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor shall throughout the term of the contract maintain insurance as specified herein and provide the State a current Certificate of Insurance/Acord Form (COI) verifying the coverage. The Contractor shall not commence work on the contract until the insurance is in place. If Contractor subcontracts any portion of the Contract the Contractor must, throughout the term of the contract, either:

1. Provide equivalent insurance for each subcontractor and provide a COI verifying the coverage for the subcontractor;
2. Require each subcontractor to have equivalent insurance and provide written notice to the State that the Contractor has verified that each subcontractor has the required coverage; or,
3. Provide the State with copies of each subcontractor's Certificate of Insurance evidencing the required coverage.

The Contractor shall not allow any subcontractor to commence work until the subcontractor has equivalent insurance. The failure of the State to require a COI, or the failure of the Contractor to provide a COI or require subcontractor insurance shall not limit, relieve, or decrease the liability of the Contractor hereunder.

In the event that any policy written on a claims-made basis terminates or is canceled during the term of the contract or within one (1) year of termination or expiration of the contract, the contractor shall obtain an extended discovery or reporting period, or a new insurance policy,

providing coverage required by this contract for the term of the contract and one (1) year following termination or expiration of the contract.

If by the terms of any insurance a mandatory deductible is required, or if the Contractor elects to increase the mandatory deductible amount, the Contractor shall be responsible for payment of the amount of the deductible in the event of a paid claim.

Notwithstanding any other clause in this Contract, the State may recover up to the liability limits of the insurance policies required herein.

1. WORKERS' COMPENSATION INSURANCE

The Contractor shall take out and maintain during the life of this contract the statutory Workers' Compensation and Employer's Liability Insurance for all of the contactors' employees to be engaged in work on the project under this contract and, in case any such work is sublet, the Contractor shall require the subcontractor similarly to provide Worker's Compensation and Employer's Liability Insurance for all of the subcontractor's employees to be engaged in such work. This policy shall be written to meet the statutory requirements for the state in which the work is to be performed, including Occupational Disease. The policy shall include a waiver of subrogation in favor of the State. The COI shall contain the mandatory COI subrogation waiver language found hereinafter. The amounts of such insurance shall not be less than the limits stated hereinafter. For employees working in the State of Nebraska, the policy must be written by an entity authorized by the State of Nebraska Department of Insurance to write Workers' Compensation and Employer's Liability Insurance for Nebraska employees.

2. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE

The Contractor shall take out and maintain during the life of this contract such Commercial General Liability Insurance and Commercial Automobile Liability Insurance as shall protect Contractor and any subcontractor performing work covered by this contract from claims for damages for bodily injury, including death, as well as from claims for property damage, which may arise from operations under this contract, whether such operation be by the Contractor or by any subcontractor or by anyone directly or indirectly employed by either of them, and the amounts of such insurance shall not be less than limits stated hereinafter.

The Commercial General Liability Insurance shall be written on an occurrence basis, and provide Premises/Operations, Products/Completed Operations, Independent Contractors, Personal Injury, and Contractual Liability coverage. The policy shall include the State, and others as required by the contract documents, Additional Insured(s). This policy shall be primary, and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory. The COI shall contain the mandatory COI liability waiver language found hereinafter. The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles.

REQUIRED INSURANCE COVERAGE	
COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Medical Payments	$10,000 any one person
Damage to Rented Premises (Fire)	$300,000 each occurrence

REQUIRED INSURANCE COVERAGE	
Contractual	Included
XCU Liability (Explosion, Collapse, and Underground Damage)	Included
Independent Contractors	Included
Abuse & Molestation	Included
If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.	
WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K
Statutory Limits- All States	Statutory - State of Nebraska
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$2,000,000 per occurrence
PROFESSIONAL LIABILITY	
All Other Professional Liability (Errors & Omissions)	$1,000,000 Per Claim / Aggregate
COMMERCIAL CRIME	
Crime/Employee Dishonesty Including 3rd Party Fidelity	$1,000,000
CYBER LIABILITY	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	$10,000,000
MANDATORY COI SUBROGATION WAIVER LANGUAGE	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
MANDATORY COI LIABILITY WAIVER LANGUAGE	
"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory as additionally insured."	

3. EVIDENCE OF COVERAGE

The Contractor shall furnish the Contract Manager, with a certificate of insurance coverage complying with the above requirements prior to beginning work at:

Public Service Commission
Attn: State 911 Director
PO Box 94927
Lincoln, NE 68509

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts and types of coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

Reasonable notice of cancellation of any required insurance policy must be submitted to the contract manager as listed above when issued and a new coverage binder shall be submitted immediately to ensure no break in coverage.

4. DEVIATIONS

The insurance requirements are subject to limited negotiation. Negotiation typically includes, but is not necessarily limited to, the correct type of coverage, necessity for Workers' Compensation, and the type of automobile coverage carried by the Contractor.

H. ANTITRUST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor hereby assigns to the State any and all claims for overcharges as to goods and/or services provided in connection with this contract resulting from antitrust violations which arise under antitrust laws of the United States and the antitrust laws of the State.

I. CONFLICT OF INTEREST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			CenturyLink is not aware of any conflicts of interest or relationships that would be considered a conflict of interest.

By submitting a proposal, bidder certifies that no relationship exists between the bidder and any person or entity which either is, or gives the appearance of, a conflict of interest related to this Request for Proposal or project.

Bidder further certifies that bidder will not employ any individual known by bidder to have a conflict of interest nor shall bidder take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its contractual obligations hereunder or which creates an actual or appearance of conflict of interest.

If there is an actual or perceived conflict of interest, bidder shall provide with its proposal a full disclosure of the facts describing such actual or perceived conflict of interest and a proposed mitigation plan for consideration. The State will then consider such disclosure and proposed mitigation plan and either approve or reject as part of the overall bid evaluation.

J. STATE PROPERTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor shall be responsible for the proper care and custody of any State-owned property which is furnished for the Contractor's use during the performance of the contract. The Contractor shall reimburse the State for any loss or damage of such property; normal wear and tear is expected.

K. SITE RULES AND REGULATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink can agree as modified below. CenturyLink agrees to comply with all reasonable site rules and regulations and requests that these be provided in advance, if possible, as it will better enable CenturyLink to be prepared in advance to comply.

The Contractor shall use its ~~best~~ reasonable efforts to ensure that its employees, agents, and subcontractors comply with reasonable site rules and regulations while on State or any government premises. Site rules will be provided to Contractor in advance whenever possible. If the Contractor must perform on-site work outside of the daily operational hours set forth by the State, it must make arrangements with the State or any government to ensure access to the facility and the equipment has been arranged. No additional payment will be made by the State on the basis of lack of access, unless the State fails to provide access as agreed to in writing between the State and the Contractor.

L. ADVERTISING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor agrees not to refer to the contract award in advertising in such a manner as to state or imply that the company or its goods or services are endorsed or preferred by the State. Any publicity releases pertaining to the project shall not be issued without prior written approval from the State.

M. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory)

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2-201.html and ensure that products and/or services provided

under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

N. DISASTER RECOVERY/BACK UP PLAN

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

The Contractor shall have a disaster recovery and back-up plan, of which a copy should be provided upon request to the State, which includes, but is not limited to equipment, personnel, facilities, and transportation, in order to continue delivery of goods and services as specified under the specifications in the contract in the event of a disaster.

O. DRUG POLICY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Contractor certifies it maintains a drug free workplace environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon request by the State.

P. WARRANTY; DISCLAIMER OF WARRANTIES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	Due to the high-risk nature of providing 911 services, CenturyLink requires a narrowed scope of warranties and clarifies that all warranties are expressly stated in the agreement, per the language proposed here.

~~Despite any clause to the contrary, t~~The Contractor represents and warrants that its services hereunder shall be performed by competent personnel and shall be of professional quality ~~consistent with generally accepted industry standards for the performance of such services~~ and shall comply in all respects with the requirements of this Agreement. For any breach of this warranty, the Contractor shall, for a period of ninety (90) calendar days from performance of the service, perform the services again, at no cost to the State~~, or if Contractor is unable to perform the services as warranted, Contractor shall reimburse the State all fees paid to Contractor for the unsatisfactory services. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without~~

~~limitation actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.~~

Disclaimer of Warranties. CENTURYLINK MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR NON-INFRINGEMENT, EXCEPT THOSE EXPRESSLY SET FORTH IN THIS AGREEMENT OR ANY APPLICABLE SERVICE ATTACHMENT. CUSTOMER ASSUMES TOTAL RESPONSIBILITY FOR USE OF THE SERVICE. IF CENTURYLINK INTEGRATES ANY RECORDS PROVIDED TO CENTURYLINK BY ANY OTHER DATA PROVIDER, FOR INCLUSION IN THE CUSTOMER'S 9-1-1 DATA, CENTURYLINK MAKES NO REPRESENTATION OR WARRANTY AND ASSUMES NO LIABILITY REGARDING THE ACCURACY OF THE DATA PROVIDED BY ANY OTHER DATA PROVIDER. IN ADDITION TO ANY OTHER DISCLAIMERS OF WARRANTY STATED IN THE AGREEMENT, CENTURYLINK MAKES NO WARRANTY, GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SERVICES WILL RENDER CUSTOMER'S SYSTEMS INVULNERABLE TO SECURITY BREACHES, OR THAT THE SERVICES WILL BE PROVIDED ERROR-FREE.

IV. PAYMENT

A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)

Neb. Rev. Stat. §§81-2403 states, "[n]o goods or services shall be deemed to be received by an agency until all such goods or services are completely delivered and finally accepted by the agency."

B. TAXES (Statutory)

The State is not required to pay taxes and assumes no such liability as a result of this solicitation. The Contractor may request a copy of the Nebraska Department of Revenue, Nebraska Resale or Exempt Sale Certificate for Sales Tax Exemption, Form 13 for their records. Any property tax payable on the Contractor's equipment which may be installed in a state-owned facility is the responsibility of the Contractor.

C. INVOICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Invoices for payments must be submitted by the Contractor to the agency requesting the services with sufficient detail to support payment. Public Service Commission State 911 Director 1200 N St. Lincoln, NE 68509. The terms and conditions included in the Contractor's invoice shall be deemed to be solely for the convenience of the parties. No terms or conditions of any such invoice shall be binding upon the State, and no action by the State, including without limitation the payment of any such invoice in whole or in part, shall be construed as binding or estopping the State with respect to any such term or condition, unless the invoice term or condition has been previously agreed to by the State as an amendment to the contract.

D. INSPECTION AND APPROVAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
SKB			

Final inspection and approval of all work required under the contract shall be performed by the designated State officials.

The State and/or its authorized representatives shall have the right to enter any premises where the Contractor or subcontractor duties under the contract are being performed, and to inspect, monitor or otherwise evaluate the work being performed. All inspections and evaluations shall be at reasonable times and in a manner that will not unreasonably delay work.

E. PAYMENT (Statutory)

Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2403). The State may require the Contractor to accept payment by electronic means such as ACH deposit. In no event shall the State be responsible or liable to pay for any goods and services provided by the Contractor prior to the Effective Date of the contract, and the Contractor hereby waives any claim or cause of action for any such services.

F. LATE PAYMENT (Statutory)

The Contractor may charge the responsible agency interest for late payment in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2401 through 81-2408).

G. SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS (Statutory)

The State's obligation to pay amounts due on the Contract for a fiscal year following the current fiscal year is contingent upon legislative appropriation of funds. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal year(s) for which such funds are not appropriated. The State will give the Contractor written notice thirty (30) calendar days prior to the effective date of termination. All obligations of the State to make payments after the termination date will cease. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

H. RIGHT TO AUDIT (First Paragraph is Statutory)

The State shall have the right to audit the Contractor's performance of this contract upon a thirty (30) calendar days' written notice. Contractor shall utilize generally accepted accounting principles, and shall maintain the accounting records, and other billing and service records and information relevant to the contract (Information) to enable the State to audit the contract. (Neb. Rev. Stat. §84-304 et seq.) The State may audit and the Contractor shall maintain, the Information during the term of the contract and for a period of five (5) years after the completion of this contract or until all issues or litigation initiated prior to the expiration of this records retention obligation are resolved, whichever is later. The Contractor shall make the Information available to the State at Contractor's place of business or a location acceptable to both Parties during normal business hours. If this is not practical or the Contractor so elects, the Contractor may provide electronic or paper copies of the Information. The State reserves the right to examine, make copies of, and take notes on any Information relevant to this contract, regardless of the form or the Information, how it is stored, or who possesses the Information. Under no circumstance will the Contractor be required to create or maintain documents not kept in the ordinary course of contractor's business operations, nor will contractor be required to disclose any information, including but not limited to product cost data, which is confidential or proprietary to contractor.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		SKB	CenturyLink requests a few edits to clarify that the parties will be responsible for their own costs of an audit and to clarify that the State has an obligation to review invoices in a timely manner and promptly raise any concerns about invoices.

The Parties shall pay their own costs of the audit ~~unless the audit finds a previously undisclosed overpayment by the State. If a previously undisclosed overpayment exceeds one-half of one percent (.5%) of the total contract billings, or if fraud, material misrepresentations, or non-performance is discovered on the part of the Contractor, the Contractor shall reimburse the State for the total costs of the audit.~~ Overpayments ~~and audit costs~~ owed to the State shall be paid within ninety (90) days of written notice of the claim, provided the Contractor shall have a right to vet and contest such findings. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit. Disputes must be submitted to Contractor in writing within 90 days from the date of the invoice or the right to dispute an invoice is waived.

V. PROJECT DESCRIPTION AND SCOPE OF WORK

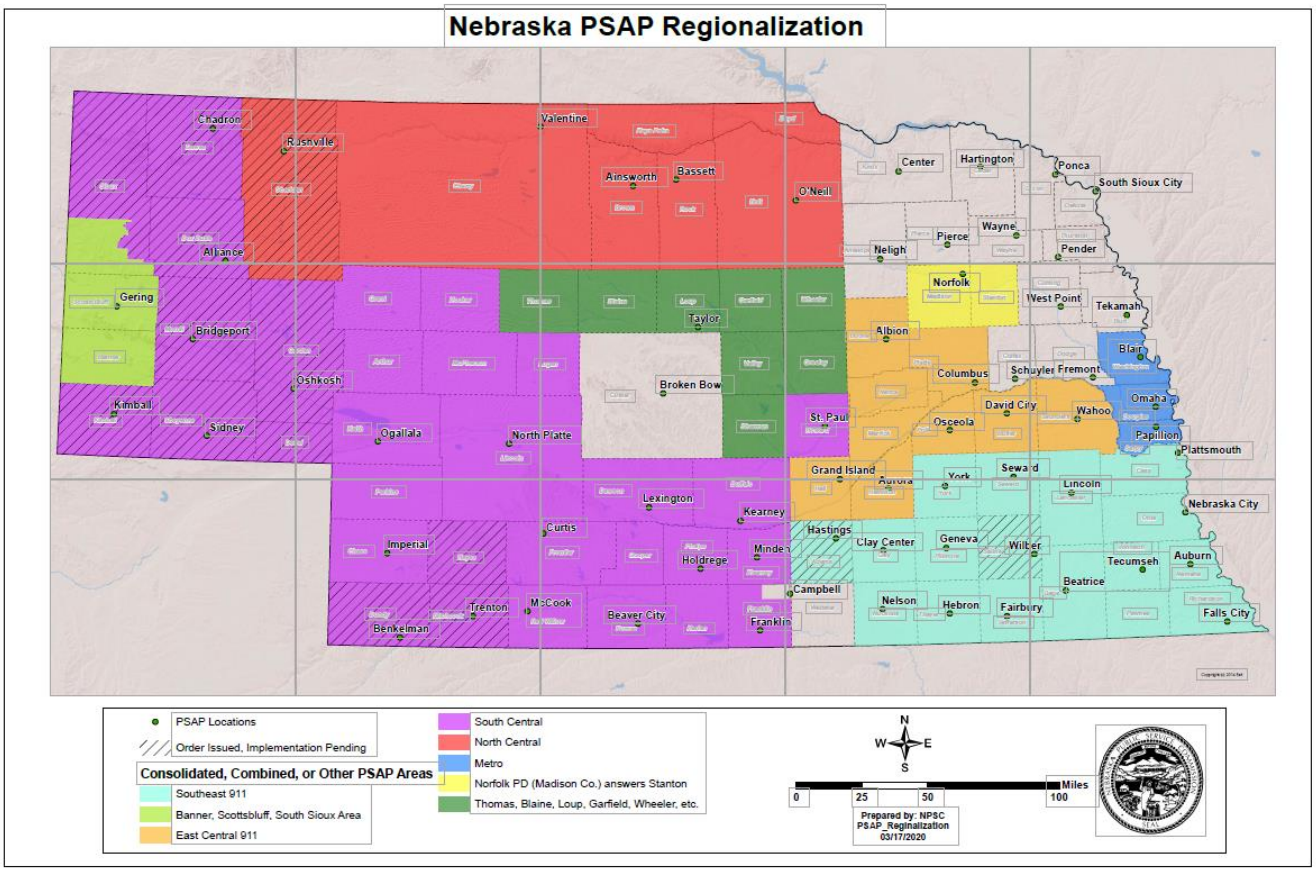
A. Background and Project Scope

The Nebraska Public Service Commission, State 911 Department (The Commission) is the statewide authority responsible for implementing and coordinating 911 service in the state. The Commission is seeking proposals for a statewide ESInet and NGCS to help advance Next Generation 911 (NG911) across the state.

Today, the local PSAPs manage and maintain independent relationships with 911 service provider and network providers. With this procurement, the Commission will establish and support a statewide ESInet and NGCS to provide 911 service to the regions throughout the state.

The state has 68 PSAPs that take approximately 1.13 million calls a year and serve a statewide population of 1.929 million people. The largest population centers are Douglas County (566,880) and Lancaster County (317,272). Many of the PSAPs throughout the state have joined together to form regions. Each region utilizes call-handling equipment (CHE) that operates in a host/remote configuration. The Commission is looking for the statewide ESInet to include physically redundant connections into each of the regional host systems. The current regional configuration is depicted in the diagram (Figure 1) below; however, it is anticipated that over the next 12 to 18 months, additional PSAPs will join one of the different regions or a new region may be formed. Updated regional information can be found on the Public Service Commission's website at www.psc.nebraska.gov.

FIGURE 1



Estimated Regions (subject to change): South Central/Panhandle=Region 1, Southeast 911=Region 2, East Central 911 (including Custer County)=Region 3, Metro=Region 4, North Central=Region 5, Norfolk PD=North East=Region 6, Metro West (anticipated Dodge, Colfax, Cuming, and Burt Counties)=Region 7

Response: CenturyLink has read and understands. The information presented in this RFP reflects our approach and solution to the above Scope of Work.

B. Composition of the Request for Proposal

This RFP is composed of two elements: Emergency Services Internet Protocol [IP] Network (ESInet) and Next Generation Core Services (NGCS). Bidders may respond to a single element (Option A- ESInet or Option B - NGCS) or both elements (Option C – ESInet and NGCS. The State will evaluate all conforming proposals. A highest scoring bidder will be identified for each of the options (A, B, and C) The State reserved the right to award any and all options at its sole discretion.

The statewide NG911 initiative will focus on two primary areas, the ESInet and NGCS.

1. Option A: Deployment of an ESInet

With the deployment of a statewide ESInet, the Commission is seeking a solution that connects each regional host to the statewide ESInet. Key project elements for ESInet deployment include, but are not limited to:

a. Deployment of a public safety-grade network that is monitored and managed to ensure security, reliability and high availability;
b. Implementation of a network that is affordable and provides a consistent level of service to all PSAPs throughout the state;
c. Development of a phased implementation approach that minimizes service impact to PSAP operations; and,
d. Cooperation and coordination with the NGCS provider throughout and after implementation.

2. **Option B: Deployment of Next Generation Core Services (NGCS)**
The Commission is seeking an NG911 call-delivery system that provides highly available call routing and delivery to the regional end points throughout the state. Key project elements for NGCS deployment include but are not limited to:

a. Deployment of monitored and managed core services that are redundant, resilient, sustainable, and provide an upgrade path to new technologies as NG911 services evolve;
b. Transition to the use of Geographic Information System (GIS) data for geospatial call routing;
c. Planned transition timelines that limit the overlap between the legacy selective router network and NGCS; and,
d. The ability to support various types of requests for assistance including calls, text messages, video messages, additional data, etc.

3. **Option C: Deployment of an ESInet and NGCS**
Includes all requirements of both Option A and Option B.

Please note that proposals may be submitted for all of the desired services or a portion of the services based on Bidder capabilities. For example, a network provider may bid only the ESInet portion of the proposal and not the NGCS.

The Commission's intent is to release an RFP soon after the release of the ESInet/NGCS RFP that addresses the connectivity from the host locations to the regional PSAP locations.

Response: CenturyLink has read, understands, and complies. CenturyLink's proposal incorporates Option C, deployment of both an ESInet and NGCS.

C. Bidder Requirements:

1. Bidders should include with their response:

a. Configuration Solution – A diagram showing the major components (hardware, software, and network layout) for the proposed system, accompanied by tables containing short descriptions of the diagrammed components in terms of their value or benefit to the Commission and the Public Safety Answering Points (PSAPs).

Response: The configuration solution diagram and the major components for the proposed solution are provided in the response to NGCS-1 in Attachment C, Option C.

b. Attachments – Cost Proposal, with a detailed description of its firm fixed pricing.

Response: The Cost Proposal is provided in a separate file per the instructions in Q&A response # 48 in Addendum Two. Please see the Cost Proposal in the file named "**RFP 6264 Z1 CenturyLink Proposal 1 Option C File 1 of 2**".

c. Appendices – The Bidder may include appendices and reference them from within the proposal response. This is particularly appropriate for lengthy responses on a single subject. Understanding the intent of the Bidder shall be possible without the reading of the appendices.

Response: CenturyLink has read, understands and complies.

d. Brochures – Hardware, software, or service brochures may be submitted with response where appropriate.

Response: CenturyLink has read, understands and complies.

D. General Requirements – Technical

1. General requirements – Commission Requirements

a. Industry Standards
The Commission seeks a standards-based solution that complies with nationally accepted standards and requirements applicable to ESInet architecture, security, and interface functionality. All aspects of the Bidder's proposed system design, deployment, operation, and security shall be in full compliance with the standards, requirements, and recommendations located in the Table 1: Adopted Standards. Standards Development Organizations (SDOs) include:

i. Association of Public Safety Communications Officials (APCO)
ii. The Monitoring Association (TMA)
iii. National Emergency Number Association (NENA)
iv. Alliance for Telecommunications Industry Solutions (ATIS)
v. Department of Justice (DOJ)
vi. Internet Engineering Task Force (IETF)
vii. North American Electric Reliability Corporation (NERC)
viii. National Institute of Standards and Technology (NIST)
ix. Telecommunications Industry Association (TIA)

Table 1: Adopted Standards

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
ATIS	ATIS-0500017	Considerations for an Emergency Services Next Generation Network (ES-NGN)	Identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next-generation telecommunications networks.	Version 1 June 2009

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
DOJ	CJISD-ITS-DOC-08140-5.6	Criminal Justice Information Services (CJIS) Security Policy	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information.	Version 5.6 June 5, 2017
IETF	RFC 3261	SIP: Session Initiation Protocol	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	Version 1 July 7, 2002
IETF	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Defines the generic URI syntax and a process for resolving URI references, along with guidelines and security considerations for the use of URIs on the Internet.	Version 1 January 2005
NENA/ APCO	REQ-001.1.2-2018	Next Generation 911 PSAP Requirements	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP.	Version 1.2 April 5, 2018
NENA/ APCO	INF-005	Emergency Incident Data Document (EIDD) Information Document	Provides a recommended list of data components, their relationships to each other, the data elements contained within each data component, and the registries that control the available values for appropriate data elements. Initiates the process to create a National Information Exchange Model (NIEM).	February 21, 2014 Scheduled to be replaced by a standards document
NENA	STA-015.10-2018	Standard Data Formats for 911 Data Exchange & GIS Mapping	Establishes standard formats for Automatic Location Identification (ALI) data exchange between service providers and Database Management System (DBMS) providers, a GIS data model, a data dictionary, and formats for data exchange between the ALI database and PSAP controller equipment.	Version 10 August 12, 2018
NENA	STA-008.2-2014	Registry System Standard	Describes how registries (lists of values used in NG911 functional element standards) are created and maintained.	Version 2 October 6, 2014

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
NENA	STA-010.2-2016	Detailed Functional and Interface Specifications for the NENA i3 Solution	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards.	Version 2 September 10, 2016
NENA	INF-016.2-2018	Emergency Services IP Network Design for NG911 (ESIND)	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInet.	Version 1 April 5, 2018
NENA	75-001	Security for Next Generation 911 (NG-SEC)	Establishes the minimal guidelines and requirements for levels of security applicable to NG911 entities.	Version 1 February 6, 2010
NENA	INF-015.1-2016	NG911 Security Information Document	Provides mechanisms and best practices for cybersecurity for i3 systems	Version 1 December 8, 2016
NERC	CIP 002-CIP 009	Critical Infrastructure Protection	Addresses the security of cyber assets essential to the reliable operation of the nation's critical infrastructure.	Version 1 December 16, 2009
NIST	FIPS 140-33	Security Requirements for Cryptographic Modules	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information.	Version 2 March 22, 2019
NIST	Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure.	Version 1.1 April 16, 2018
TIA	TIA-942-A	Telecommunications Infrastructure Standard for Data Centers	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers.	Revision A March 2014

As industry standards evolve, the Bidder's solution shall be upgraded to maintain compliance with the current version of established industry standards. The Bidder's solution shall support new ESInet, NGCS and security industry standards within 18 months of ratification of applicable industry standards at no additional cost to the State. Compliance requirements apply also to the supporting standards referenced within each standard. As solution updates are made to maintain compliance, the solution shall not abandon services or feature functionality in place at the time of the solution upgrade. The Bidder shall uncover any performance or feature changes prior to the upgrade and report them to the Commission for approval.

b. Public Safety-Grade Definition
The national standards listed in this document provide standards and requirements an IP network and core functions shall meet or exceed to be considered an ESInet. The term "public safety-grade" has been utilized to refer to

this level of standards compliance; however, a universal definition of this term has not been proposed by a Standards Development Organization (SDO) or accepted by the public safety community. For the purpose of the requirements associated with this ESInet and NGCS design and deployment, the following metric is used to define public safety-grade:

i. Reliability:
"Reliability" is the ability of a system or component to perform the required functions under stated conditions for a specified period of time. The traditional measure of system or component reliability is Mean Time Between Failure (MTBF). The required MTBF must result in system reliability of 0.99999 as recommended in NENA-INF-016.2-2018, Section 2.10.1.

ii. Availability:
"Availability" is the degree to which a system or component is operational and accessible when required for use. System availability is dependent upon the Mean Time to Repair (MTTR) calculation, which measures the time it takes to recover from component failure, a failed system upgrade, operator error, or other scheduled and unscheduled system interruption. Downtime must not exceed five (5) minutes per year, or 99.999 percent availability, as recommended in NENA-INF-016.2-2018, Section 2.10.1.

iii. Security:
Secure communications must be retained through the following measures, as recommended in NENA-INF-015.1-2016, Section 3.2:

- **a.** Rivest–Shamir–Adleman (RSA)-based public-key cryptography using X.509 certificates to authenticate elements, agencies, and agents. Mutual authentication must exist between both ends of a communication.
- **b.** An eXtensible Access Control Markup Language (XACML)-based Data Rights Management (DRM) system to control authorization.
- **c.** Advanced Encryption Standards (AES) based encryption to provide confidentiality.
- **d.** Secure Hash Algorithm (SHA)-based digest-based digital hashing to provide integrity protection.
- **e.** Dsig-based digital signatures to provide non-repudiation.

iv. Network Traffic Restrictions:
The established metrics in this definition can be achieved through system and component redundancy, diversity, resiliency, and other similar engineering methodologies. When the term "public safety-grade" is applied in this document, the Bidder shall describe how bidder's network and core service system and components for critical functions either meets or exceeds the standards-based, public safety-grade definition.

When this term is used in this document to describe the required level of service for the ESInet, and NGCS, functionality, the Bidder shall confirm that its service and components meet or exceed both the national standards listed in Table1 and the public safety-grade definition.

Response: CenturyLink has read, understands, and complies. CenturyLink's responses in Attachment C Option C show that we comply with and meet or exceed the standards listed above. Additional information about CenturyLink's NGCS and ESInet solution is provided in the Service Exhibits, SLAs, and Technical information provided in the Attachments, Addenda, Appendices, and Brochures attached to this response.

2. TECHNICAL APPROACH

The technical approach section of the Technical Proposal should consist of the following subsections:

a. Understanding of the project requirements;

Response: CenturyLink currently offers E9-1-1 services in 35 states where CenturyLink operates as a Local Exchange Carrier. Our E9-1-1 services include network management, local trunking, selective routing (using appropriate ESN data), and ALI database services. Additionally, CenturyLink offers a full range of PSAP applications in on-premise configurations.

CenturyLink currently offers NG9-1-1 services in Washington, Utah, North Dakota, Minnesota, and North Carolina over our IP-based, redundant, resilient, fault tolerant, and secure Public Safety grade ESInet. Powered by West Safety Services next generation core services, CenturyLink has been offering NG9-1-1 solutions for over 8 years.

CenturyLink has been designing and deploying public safety products and services based on the needs of the industry and our forward-looking view of 9-1-1. CenturyLink provides core 911 services to over 35 states in the US and has played a key role in defining, building, and maintaining the complex emergency communications infrastructure.

We listen to public safety officials, monitor new technology development, and participate in industry standards bodies to understand these needs and develop products that revolutionize the public safety industry.

CenturyLink has a proven track record of successfully integrating emerging technologies into the evolving emergency services network, and our proactive deployment of next generation technologies is helping to improve 9-1-1 system efficiency and increase interoperability throughout the emergency response community.

CenturyLink 911 systems and services support a high percentage of all 9-1-1 calls placed each day, totaling over 300 million calls to 9-1-1 each year. CenturyLink customers include all major U.S. wireline, wireless, Voice over IP (VoIP), Satellite, and Telecommunication Relay Services carriers, large international operators, and a growing number of public safety agencies and municipalities in the U.S. Built on a belief in work worth doing, our companies touch millions of lives every day and we take that responsibility very seriously.

CenturyLink is extensively involved in all aspects of 9-1-1, giving us a unique perspective on its required evolutionary path to support new technologies and expand citizen expectations. These insights have enabled CenturyLink to anticipate trends and help public safety agencies and telecommunications service providers proactively prepare for change.

CenturyLink's emergency communications excellence is built upon a strong foundation of the following:

- An unmatched knowledge of emergency communications and public safety operations
- A proven experience in the design, deployment, and operation of highly accurate, high-volume communication networks, equipment, software, and applications
- A solid reputation as a trusted and neutral custodian of sensitive data
- A passion for saving lives
- A thorough understanding of the needs of the State of Nebraska for NG911 Services.

i3 Products

CenturyLink's NG9-1-1 product suite is a complete, end-to-end manage hosted NG 9-1-1 solution that provides an i3 ESInet that is fully interoperable with legacy networks. The suite includes a broad range of premise-based and fully managed public safety solutions that align with the most commonly used industry standards. New products include interconnections with call handling solutions and managed and secure emergency IP network (ESInet) services.

Additional products in the i3 suite are:

- IP voice and data delivery to public safety answering points (PSAPs)
- Enterprise Geographic Information Services (GIS) data management services
- Comprehensive Geographic Information Services (GIS)
- Location Information Services (LIS)
- Advanced call routing services including ESRP, ECRF, BCF, LNG, and LPG
- Network and Application Security services
- Voice and data gateway services for interoperability with legacy and other next generation networks
- Advanced message switching services
- Call handling premise systems for the i3 capable PSAP
- Text-to-9-1-1

CenturyLink has been designing and implementing telephony networks since 1930. This includes 911 ALI database and selective routing and transport since the inception of 9-1-1. CenturyLink's NG9-1-1 solution is built on the basic principle of "no single point of failure." Our solution uses a fully redundant, multi-carrier, multi-location network linking all 9-1-1/E9-1-1 network elements and PSAPs. Within each redundant node, there are redundant network elements. Each of these facilities and nodes are equipped with physically redundant data communications and power equipment so that any component can be maintained without overall service impact. Failover within the system occurs automatically with no manual intervention. CenturyLink's network carriers enter each facility (minimum of two) via diverse facility transport paths and diverse points of interconnection. Where available, each carrier will have their 9-1-1 calls delivered over diverse facility routes.

The MPLS network is designed in a 100% capacity and 100% redundancy configuration so that if one MPLS carrier's network goes down, the redundant bandwidth can manage 100% of the PSAP's capacity. The result of this is a network that is truly public safety grade in terms of capacity, reliability, and redundancy.

CenturyLink's proven track record of successfully integrating emerging technologies into the evolving emergency services network and its proactive deployment of next generation technologies is helping to improve 9-1-1 system efficiency and increase interoperability throughout the emergency response community. Our network design is based on CenturyLink's extensive experience in deploying NG9-1-1 for hundreds of PSAPs and many statewide deployments covering the following areas.

b. Proposed development approach;

Response: CenturyLink follows a well-defined, repeatable, and disciplined system and software design, development, and implementation methodology. These are well planned and managed processes. The ESInet system design is a highly available and highly reliable distributed and redundant architecture with no single points of failure. Key components are redundant within a given geographic site and are also geographically redundant. The loss of any single element will not prohibit call processing functions. The architecture is also extremely scalable to meet current and future needs. The solution includes internal audits and background test capabilities to continuously ensure solution integrity and to detect abnormal conditions.

The overall implementation is highly secure and uses industry standard security best practices. The ESInet system is protected from external sources and practices internal security management best practices process and procedures.

The ESInet system design is a multi-tenant architecture with configuration to implement customer desired routing behavior and interface protocols. The resulting architecture is highly cost effective for individual customers and results in an ability to focus specialized resources, where smaller, completely localized solutions may struggle to deploy dedicated specialized resources.

Implementation has achieved a standard, highly repeatable, process as demonstrated by the numerous NG911 / PSAP deployments. Deployment is followed by an effective and constantly improving monitoring and management capability with a 24x7x365 support structure.

c. Attachment C - Technical Requirements Option A, B, and/or C;

Response: : CenturyLink has provided Attachment C Option C for this proposal version 2 in the electronic on-line filing as the file named "**RFP 6264 Z1 CenturyLink Proposal 1 Option C File 2 of 3"**

d. Proposed high-level project plan

Response:

A high-level Program Management Plan(PMP) has been provided as an appendix to this document. The Program Development Plan will be refined with input from all stakeholders after contract award during the planning phase of the project. The PMP outlines all areas of the project from planning through implementation and deployment and will serve as the guiding document throughout the lifecycle of the program. Please see the file named "**2.d_CenturyLink Sample Program Management Plan for Nebraska**"

During the planning phase of the project, the CenturyLink Program Manager will work with stakeholders to refine the PMP and ensure that it is inclusive of all aspects of both the project and overall program lifecycle. A final draft version of the PMP will be provided to all stakeholders for any revisions and signoff, then the final product will be distributed. As customer needs evolve, this document can, and should, be revised to reflect any changes to the project/program.

e. Schedule for the lifecycle of this project; and

Response:

A draft schedule has been provided as an appendix to this proposal. The schedule has been developed based on the timelines provided within the Request for Proposal and approaches the Implementation and Transition phases on a regional basis. A regional approach will allow the state to transition services in a manner that both reduces risk and allows for ample testing and acceptance prior to moving focus to the subsequent regions. The schedule that has been provided is to be considered a draft, with the finalized schedule to be provided after the planning phase has been completed. The CenturyLink Program Manager will update the schedule as the project progresses and provide it to the state as revisions occur, along with the regular status reporting. The schedule, although considered final after the planning phase, should be considered a "living" document as it will be adjusted throughout the lifecycle of the project. Please see the attachment named **"2.e Sample Nebraska_Draft Project Schedule_Gantt Chart Format**"

FORM A
BIDDER PROPOSAL POINT OF CONTACT

Request for Proposal Number 6264 Z1

Form A should be completed and submitted with each response to this solicitation. This is intended to provide the State with information on the bidder's name and address, and the specific person(s) who are responsible for preparation of the bidder's response.

Preparation of Response Contact Information	
Bidder Name:	CenturyLink Communications, LLC
Bidder Address:	118 South 19th Omaha Ne 68102
Contact Person & Title:	Jon Osborne
E-mail Address:	Jon.Osborne1@centurylink.com
Telephone Number (Office):	402 998 7392
Telephone Number (Cellular):	402 216 1009
Fax Number:	402 422 3545

Each bidder should also designate a specific contact person who will be responsible for responding to the State if any clarifications of the bidder's response should become necessary. This will also be the person who the State contacts to set up a presentation/demonstration, if required.

Communication with the State Contact Information	
Bidder Name:	CenturyLink Communications, LLC
Bidder Address:	125 S Dakota Ave. Sioux Falls, SD. 57104
Contact Person & Title:	Bjorn Johnson, Sr. Account Manager - SLED
E-mail Address:	Bjorn.Johnson@centurylink.com
Telephone Number (Office):	605 977 2820
Telephone Number (Cellular):	605 321 6188
Fax Number:	605 339 5652

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance with the procedures stated in this Solicitation, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free workplace.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

__X__ NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this Solicitation.

_____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. §71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD OR BY DOCUSIGN

FIRM:	CenturyLink Communications, LLC
COMPLETE ADDRESS:	931 14th Street, # 900 Denver, CO. 80202
TELEPHONE NUMBER:	720 779 8247
FAX NUMBER:	303 383 8275
DATE:	June 3, 2020
SIGNATURE:	Susan Baker
TYPED NAME & TITLE OF SIGNER:	Susan Baker, Manager Offer Management

ATTACHMENTS, ADDENDA, APPENDICES, AND BROCHURES

State Attachments and Required Uploaded Files

RFP 6264 Z1 CenturyLink Proposal 1 Option C File 2 of 4 (Cost Proposal)

RFP 6264 Z1 CenturyLink Proposal 1 Option C File 3 of 4 (Attachment C Option C)

RFP 6264 Z1 CenturyLink Proposal 1 Option C File 4 of 4 (PROPRIETARY INFORMATION)

State Issued Addenda

6264 Z1 Addendum One 3-25-2020

6264 Z1 Addendum Two 3-27-2020

6264 Z1 Addendum Three 4-16-2020

6264 Z1 Addendum Four Questions and Answers 4.22.20 final Q&A Answers - NE RFP

6264 Z1 Addendum Five 4-22-20 Revised SOE Revised Schedule - NE RFP NG911

6264 Z1 Addendum Six 5-7-2020 Questions and Answers Round Two final

6264 Z1 Addendum Seven 5-15-20 Questions and Answers additional question

CenturyLink Attachments and Supporting Documentation

6264 Z1 CC LLC NE Cert of Good Standing

1.A.1.i Key Employees ResumesNG911 Resumes_Combined

1_a_CC__LLC_Certificate_of_Name_Change__Incorporation

2.d_ CenturyLink Sample Program Management Plan for Nebraska

2.d ss15_SAMPLE Staging and Acceptance Checklist

2.d_Testing_Sample CenturyLink Test Plan

2.e Sample Nebraska_Draft Project Schedule_Gantt Chart Format

3.B I 9 Compliance Certification_Q1 2020_Letterhead

CenturyLink's Service Exhibits and SLA Attachments, as referenced in the Legal Statement included with this response:

Att A_MPLS (IPVPN and VPLS) VPN Service Schedule

Att B_Local Access Service Exhibit with Pricing Attachment

Att C_SLA_Local Access

Att D_Domestic Network Diversity Service Exhibit

Att E_SLA_Diversity

Att F_CenturyLink Select Advantage Service Exhibit

Att G_NextGen 911 Service Schedule Interim (Synergem)

Att H_SD WAN Service Schedule

Att I_Rental CPE Service Exhibit for MSA

Att J_Telecommunications Service Priority (TSP)

Att K_Data Security Addendum

Attachments and Brochures supporting attachment C Option C

SEC 3 Security Compliance Matrix

SLA 5 Brix_probe_PSAP_Troubleshooting

SLA 5 PSAP_Active_Test_V4-Example

Attachments and Brochures filed as PROPRIETARY INFORMATION and provided in a separate file:

CenturyLink-Proposal 1 PROPRIETARY INFORMATION Reasons

A.1.e NE Active Contracts Public Saftey & SoNE PROPRIETARY

ADDENDUM ONE

Date: March 25, 2020

To: All Bidders

From: Annette Walton / Nancy Storant, Buyers
Nebraska State Purchasing Bureau

RE: Addendum for RFP Number 6264 Z1 to be opened June 3, 2020 at 2:00:00 p.m. Central

The Change in Procurement Procedure allowing for electronic submission of bids through ShareFile has the following change:

The previous link did not request email information in order to send a confirmation email listing the items uploaded by a vendor for this RFP.

Please use the following Link to upload proposal documents:
https://nebraska.sharefile.com/r-r7e7e4b7a0264303a

This addendum will become part of the ITB/proposal and should be acknowledged with the Request for Proposal response.

ADDENDUM TWO

Date: March 27, 2020

To: All Bidders

From: Annette Walton / Nancy Storant, Buyers
Nebraska State Purchasing Bureau

RE: Addendum for RFP Number 6264 Z1 to be opened June 3, 2020 at 2:00:00 p.m. Central

Due to concerns around COVID-19, the State of Nebraska is allowing attendance of the Optional Pre-Proposal Scheduled for April 1, 2020 from 10am-12pm to only be via Skype. Please submit an Intent to Attend Form B for meeting information.

This addendum will become part of the ITB/proposal and should be acknowledged with the Request for Proposal response.

ADDENDUM THREE – REVISED SCHEDULE OF EVENTS

Date: April 16, 2020

To: All Bidders

From: Annette Walton / Nancy Storant, Buyers
Nebraska State Purchasing Bureau

RE: Addendum for RFP Number 6264 Z1 to be opened June 3, 2020 at 2:00:00 P.M. Central

Revised Schedule of Events

ACTIVITY		DATE/TIME
6.	State responds to written questions through Solicitation "Addendum" and/or "Amendment" to be posted to the Internet at: http://das.nebraska.gov/materiel/purchasing.html	April 22, 2020 ~~April 16, 2020~~
7.	Proposal Opening Location for mailed/hand delivered submissions: State Purchasing Bureau 1526 K Street, Suite 130 Lincoln, NE 68508 Electronic submissions: https://nebraska.sharefile.com/r-r11ba33e3ee24b63b	June 3, 2020 2:00: 00 PM Central Time
8.	Review for conformance to solicitation requirements	June 8, 2020
9.	Evaluation period	June 8, 2020 through June 29, 2020
10.	"Oral Interviews/Presentations and/or Demonstrations" (if required)	TBD –July 13-17
11.	Post "Notification of Intent to Award" to Internet at: http://das.nebraska.gov/materiel/purchasing.html	TBD
12.	Contract finalization period	TBD
13.	Contract award	TBD
14.	Contractor start date	TBD

This addendum will become part of the ITB/proposal and should be acknowledged with the Request for Proposal response.

ADDENDUM FOUR, QUESTIONS and ANSWERS

Date: April 22, 2020

To: All Bidders

From: Annette Walton/Nancy Storant, Buyers
AS Materiel State Purchasing Bureau

RE: Addendum for Request for Proposal Number 6264 Z1 to be opened June 3, 2020 at 2:00 P.M. Central Time

Questions and Answers

Following are the questions submitted and answers provided for the above-mentioned Request for Proposal. The questions and answers are to be considered as part of the Request for Proposal. It is the Bidder's responsibility to check the State Purchasing Bureau website for all addenda or amendments.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
1.	6264 Z1 Attachment C Technical Requirements Option A, B and C (Word doc)	SLA 1 through 9	General Operations - Service Level Agreements System Capacities and Performance	16	Option A, B, and C have the same SLA requirements; could the Commission please clarify how the SLA's apply to each option individually?	The SLA requirements apply as written. Even if a bidder is only responding to the NGCS, there is still a network component to that. The SLAs related to devices and capacity apply equally to network and NGCS devices.
2.	6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS (Word doc)	GEN SCEN 3	Scenario 3	25	Can the Commission clarify whether this scenario is referring to an SI or LDB change?	The reference is to a spatial interface (SI) change, but it could be either an SI or location database (LDB) in a transitional environment. The errors were discovered in the Contractor's validation process prior to updating either the SI or the LDB, with the understanding that the state will upload data to the Contractor and never have direct access to either the SI or the LDB.
3.	6264 Z1 ESInet and Core Services RFP Revision One and Cost Proposal (Word doc)	V.A	Background and Project Scope	28	Regions 1-6 are defined differently in Section V.A and in the Cost Proposal Summary; for example, Region 1 is defined as the South Central / Panhandle in RFP Section V.A and defined as SE in the Cost Proposal Summary. Could the Commission please clarify?	Section V.A. of the RFP is Correct. Please use the revised posted documents: 6264 Z1 Cost Proposal Option A ESInet Revision One, 6264 Z1 Cost Proposal Option B NGCS Revision One, and 6264 Z1 Cost Proposal Option C ESInet and NGCS Revision One.
4.	6264 Z1 ATTACHMENT A	PSAP Host Locations	-	-	Based on the description of each RFP element in section V.B of the main RFP document, the initial RFP solution will connect each regional host to the statewide ESInet. What does the Commission intend for the Standalone PSAPs and Regions 6 and 7 that do not have a host location defined in Attachment A? Can the Commission identify hosted location(s) for Regions 6	The creation and composition of PSAP regions is under local control. However, it is the State's expectation that the remaining standalone PSAPs will join either an existing region or one of two new regions, at the PSAPs discretion. The State anticipates that regions 6 & 7 will be comprised of PSAPs in the northeast corner of the state. The two regions are expected to form by mid-2021 and anticipated host locations have been added to Attachment A Revision One.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					and 7 to maintain consistency with pricing for Regions 1-5? Can the Commission indicate which Region the Standalone PSAPs intend to join?	For purposes of responding to this RFP, please assume the following: The State is of the understanding that the PSAPs in Custer and those included in 'Region 26' (Thomas, Blaine, Loup, Garfield, Wheeler, Valley, Greely and Sherman counties) will become a part of the East Central Region. ***Region 6 (Northeast)** Knox, Cedar, Dixon, Dakota, Thurston, Stanton, Madison (Host), Wayne, Pierce, and Antelope **Region 7 (Metro West)** Dodge (Host), Colfax (Host), Cuming and Burt *The Northeast region is finalizing host locations. Norfolk (Madison County) will be one host, while the second host may be one of the following three locations: South Sioux City (Dakota County), Wayne, or Hartington (Cedar County). The State anticipates that the second host will be known prior to the opening of the RFP and an Addendum will be posted once the locations are finalized.
5.	6264 Z1 ATTACHMENT A	PSAP Host Locations	-	-	Is there a timeframe that should be assumed for the deployment of the host locations for Regions 6 and 7 for purposes of developing the project implementation plan?	The State anticipates completion of regions 6 and 7 by the end of 2021. It is expected that all regions are transitioned to the statewide NG911 system by 2023.
6.	6264 Z1 ATTACHMENT A	PSAP Host Locations	-	-	If the requirement is for bidders to provide network to standalone PSAPs, what is the requirement for last-mile diversity and redundancy for standalone PSAPs?	All PSAPs on the NG911 system will be a part of a region. There will not be standalone PSAPs.
7.	6264 Z1 ATTACHME	PSAP Equipm	-	-	Can the Commission provide the call-handling position count at each PSAP?	See Attachment D Nebraska PSAP Trunk, Position, and Call Volume Information.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	NT A	ent				
8.	6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS (Word doc)	ESI 1	Emergency Services IP Network Diversity	30	Can the Commission please clarify whether diverse entrances already exist at any of the identified host locations due to the likelihood that bidders will not be able to perform site walks of the locations prior to bid submission? For sites that have diverse entrances, can the Commission provide information on which carriers are providing IP connectivity through those entrances?	It is the state's understanding that the majority of the host locations do not have diverse entrances into their facilities. The host locations that have diverse entrances are those serving the South East Region, with Windstream serving as the primary carrier in both host locations and the Metro Region, with CenturyLink serving as the primary carrier into both host locations. The North Central, South Central, East Central, Metro West, and North East do not have diverse entrances. The State asks that Bidders differentiate between primary and secondary connections both in the response and pricing matrix.
9.	6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS (Word doc)	NGCS 9	Next Generation Core Services Elements (NGCS) Legacy Network Gateway (LNG) Location Information	37	Are NGCS 8 and NGCS 9 duplicates?	Yes, NGCS 8 and NGCS 9 are duplicates NGCS 9 has been deleted in its entirety. Please see; Attachment C Option B Revision One, and Attachment C Option C Revision One.
10.	6264 Z1 Attachment C Technical	NGCS 67	Next Generation Core	59	What expectations does the Commission have for the interface between audio logging recording and i3 Event logging?	At this time, there is no requirement of audio logging occurring within NGCS. Audio logging is done at the host or PSAP level. i3 event logging must interface

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	Requirements Option C - ESInet and NGCS (Word doc)		Services Elements (NGCS) Event Logging and Management Information System (MIS)			with ECaTS.
11.	6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS (Word doc)	NGCS 62	Next Generation Core Services Elements (NGCS) Spatial Interface (SI) Use of the Commission's GIS Data Model	56	1. Describe how the Bidder's solution will use the Commission's GIS data model (Attachment D) without modification to the schema. Can the Commission confirm that this is actually referencing Attachment B?	Yes .NGCS 62 has been corrected. Please use: Attachment C Option B - NGCS Revision One and Attachment C Option C – ESInet and NGCS Revision One.
12.	6264 Z1 ESInet and Core Services RFP Revision One	-	Scope of Service	1	"The bidder must identify the proprietary information, mark the proprietary information according to state law, and submit the proprietary information in a separate container or envelope marked conspicuously using an indelible method with the words "PROPRIETARY INFORMATION" or if submitting the proposal or response electronically, as a separate electronic file that is named "PROPRIETARY INFORMATION". " As the proprietary information in bidder's responses may be in a number of	

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					different areas of the response and if bidders provide the bid as requested above, this would oblige the State evaluation team to reference back and forth between two documents as they go through the review of the completed responses. We would like to suggest for the benefit of the evaluation team that bidders provide two full set of response documents; One copy of the full submission for the evaluation team (not to be published publicly) and one redacted version of the completed response (for public publication).	Please submit all proprietary information as required in the RFP.
13.	Addendum 1	-	-	-	Can the State provide what the file size limitation are for bid submission via ShareFile, if any?	None known at this time.
14.			Attachment A	2,3	Will PSAP CPE be upgraded to be i3 capable or will this be an initial RFAI deployment?	The PSC will work with the regions to encourage i3 compatibility, but Bidders shall assume connectivity to CHE with the software versions noted in Attachment A Revision One.
15.			Attachment C	Page 65, SVAL-1	Can the State please confirm that SVAL-1 is an optional requirement?	SVAL-1 is not an optional requirement. Attachment C Option B NGCS - Revision One Attachment C Option C ESInet and NGCS - Revision One.
16.			6264 Z1 ESInet and Core Services RFP Revision	Page 29	Is the intent of the “Option A” network to be a standalone WAN for all host locations to communicate and share data; or is the “Option A” network exclusive to provide connectivity from the NGCS’s to the host locations?	It could potentially allow for traffic between PSAPs associated with different hosts; however, 911 requests for assistance shall have priority. The regional ESInets will handle traffic between PSAPs in the respective regions. Any non-911 traffic must be public-

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			One			safety-related (CAD, MIS, etc.). The State recognizes that there would need to be traffic engineering discussions before additional traffic could be added to the network.
17.			Attachment A	2-3	Can the State provide physical addresses for all the Stand Alone PSAPs so that vendors can determine diversity availability to each?	See response to Question 4.
18.			Attachment A	all	Can the State confirm there are no secondary PSAPs that will be connected to the ESInet/NGCS?	At this time, no secondary PSAPs will be connected to the ESInet/NGCS. If they connect in the future, they will connect via a regional host.
19.			Attachment C, Option C	10	NOC/SOC 10 - Does this requirement only apply to ESInet as NGCS is not indicated in this requirement?	It is a general requirement and applies to both ESInet and NGCS. Please use Attachment C – Option A ESInet Revision One; Attachment C Option B NGCS Revision One; and Attachment C Option C ESInet and NGCS Revision One.
20.			Attachment C, Option C	18	SLA 9 – Will the State please reference the Standards Document the 54ms network traffic convergence requirement is derived from?	ITU-T G.8031 and G.8032 implement sub-50ms failover in ethernet networks. Additionally, MPLS networks support Fast Re-Route (FRR) which also is sub-50ms.
21.			Attachment C, Option C	32	ESI 9 - Can the State provide additional documentation on the microwave network and other local/state-owned networks that are being proposed? Are these public safety grade	This requirement was to raise awareness of other networks in the state. Bidders should research all possible providers to provide service to the State. The PSC is unable to provide additional

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					networks?	information specific to the networks.
22.			Attachment C, Option C	33	ESI 11 - Can the state clarify the difference between ESI 10 and ESI 11?	ESI 10 specifies that the Contractor will support ESInet-to-ESInet interconnections. ESI 11 specifies that the Contractor will implement ESInet-to-ESInet and NGCS interconnections as the need arises.
23.			Attachment C, Option C	47	NGCS 38 - SCTP is listed as optional. NGCS 27 includes this and does not state as optional. Can the State clarify?	NGCS 27 refers to the border control function (BCF) and requires that the BCF be able to accept stream control transmission protocol (SCTP) traffic from outside. NGCS 38 refers to the emergency services routing proxy (ESRP), where SCTP traffic is desirable but not required.
24.			Attachment C, Option C	56	NGCS 62 - Reference to Attachment D. Currently no attachment D on the State's website, can the State provide?	See response to Question 11.
25.			Attachment C, Option C	59	NGCS 69 - State references MIS which is usually associated with CPE. Is the State asking for the NGCS provider to manage MIS or continue using the current ECaTs solution with their loggers for CPE?	The requirement is for the event logging in the NGCS to feed into the PSAPs' event logging (ECaTS) to provide a complete record of the call event.
26.			Attachment C, Option C	63	NGCS 77 - Can the State clarify the Ringdown Functionality. Ringdown is currently part of CPE, how does the State propose this be integrated with ESInet?	The requirement is that the NGCS support Ringdown functionality in the event that one or more CHE systems do not support it.
27.			Attachment A	2,3	Will you please add a "Total Position Count" column to the PSAP Table in	See response to Question 7.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					Attachment A?	
28.			6264 Z1 ESInet and Core Services RFP Revision One	all	What changes were made with the release of Revision One?	1. The Opening Date and time was corrected to: June 3, 2020 2:pm CT 2. Added to the Proprietary Paragraph on Page i. “if submitting the proposal or response electronically, as a separate electronic file that is named “PROPRIETARY INFORMATION”. 3. Schedule of Events Activity 2 added “Form B” 4. Schedule of Events, Activity 8 added “.00 (seconds)” to the time that bids are due.
29.			Attachment C, Option A, B, and C	all	Are there any Mandatory Requirements in Options A, B, or C?	Optional service is called out at NGCS 81. It is understood that Bidders may not have 100% compliance. The evaluation process is designed to select the best solution from those submitted.
30.			Attachment C, Option C	15	NOC/SOC 23 – State indicates they maybe find it beneficial to have a third party NOC/SOC service. Can the State provide additional details such as location, software used, and other technical capabilities on the 3rd party to allow vendors to price connecting to a 3rd party NOC/SOC?	This is a requirement to support such a connection in the future should the State determine it is in the State’s best interest. Bidders should describe their capabilities for establishing a data-sharing connection.
31.			Attachment C, Option C	25	GEN SCEN 3 – Can the state expand on the scenario described? What kind of changes has the bidder uploaded? Are these software updates? The assumption is that the	See response to Question 2. The reference is to a spatial interface (SI) change,

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					State is responsible for both MSAG and GIS data so they would be responsible for making updates to these. Not sure what kind of bidder updates would result in 15,000 errors being generated.	
32.			6264 Z1 ESInet and Core Services RFP Revision One, Section V.B.2.b	29	Can the State provide status of GIS data for the PSAP's throughout Nebraska? Will the State be going to i3 with geospatial day 1 or will it be a slower transition?	The statewide street centerline data is available for download from nebraskamap.gov (search 911) The State is currently working with each PSAP to create the statewide PSAP layer. This is a work in progress and the data is currently out to the PSAPs for input and updates. The State is looking to implement NG911 services as quickly as possible, so it is not required that geospatial routing be available with the initial deployments.
33.			Attachment A	2,3	Can you please provide the number of concurrent calls that each PSAP can currently support? As a follow on, is it the State's desire to maintain this capacity or is there a need to increase the number of concurrent calls for each PSAP? If so, please provide the desired number of concurrent calls by PSAP.	The number of concurrent calls that each PSAP can support is unknown. Please see Attachment D. At this time, it is the expectation of the State that the capacity for concurrent calls remains the same. As greater functionality becomes available (video, images, etc.), it is expected that network capacity can be adjusted to accommodate the additional traffic. Please refer to Req. GEN-4 and SLA-1.
34.			Attachment C	63	Make-Busy Functionality: Is the requirement to continue to use a	The functionality can be provided either way. Some PSAPs may desire the option of a

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					physical device for make-busy operation or can this capability be provided through a portal that would add more functionality and options for make-busy scenarios?	physical switch.
35.			Attachment A	3	Is it the intent of the State to connect each of the individual PSAPs (not currently part of a regional system) to the NGCS via ESInet or will those PSAPs remain on legacy routing until such time that they become part of an existing or new regional system?	See response to Question 4.
36.			6264 Z1 Cost Proposal Option A ESInet Final, 6264 Z1 Cost Proposal Option B-NGCS FINAL3.10.20, 6264 Z1 Cost Proposal Option C ESInet and NGCS final		The cost proposal worksheets require the breakout of fees to seven (7) regions. Section V. A of the Request for Proposal for Contractual Services (6264 Z1 ESInet and Core Services RFP final SONYAS.docx) and "Attachment A PSAP Host endpoints equipment and selective router locations" indicate the makeup of the seven (7) regions. Between those two data sources, twelve (12) of the "stand-alone" counties / PSAP locations from Attachment A are not accounted for in one of the seven (7) regions. How should fees for these twelve (12) unaccounted locations be included in the cost proposal? 1. Antelope County	See response to Question 4.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					2. Cedar County 3. City of South Sioux City 4. City of Wayne/Wayne County 5. Dawes County 6. Dixon County 7. Knox County 8. Mid Rivers 911 Center 9. Pierce County 10. Region 26 Council 11. Scottsbluff County 12. Thurston County	
37.			6264 Z1 Cost Proposal Option A ESInet Final, 6264 Z1 Cost Proposal Option B-NGCS FINAL3.10.20, 6264 Z1 Cost Proposal Option C		When will the remaining "stand-alone" entities join a specific region? Are there any circumstances that would allow a stand-alone to NOT be in a region, and if so, will each stand-alone be their own 'region'?	See response to Question 4.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			ESInet and NGCS final			
38.			6264 Z1 ESInet and Core Services RFP final SONYAS *Scope of Services I.J. Submission of Proposals*	i	How should bidders delineate proprietary information? Can bidders submit redacted copies to be used for FOIA requests? The RFP states that The Technical Proposal, Cost Proposal, and Proprietary information should be uploaded as separate files. We are concerned that by separating proprietary details from the Technical Proposal the full response context will not be understood and will therefore make proposal evaluation more difficult.	See response to Question 12.
39.			6264 Z1 ESInet and Core Services RFP final SONYAS *I.P. Request for Proposal / Proposal Requirements*	5	Should item #4 "Completed Sections II through IV" read "through VI" instead?	No. Please use the most recent version of the RFP: "6264 Z1 ESInet and Core Services RFP Revision One".
40.			6264 Z1 ESInet and Core	9-27	Are bidders required to indelibly initial the "Accept" or "Reject" boxes in ink, or can bidders type the company	Either is acceptable.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			Services RFP final SONYAS *II. Terms and Conditions* *III. Contractor Duties* *IV. Payment*		officer's initials?	
41.			6264 Z1 ESInet and Core Services RFP final SONYAS *V.B. Composition of the Request for Proposal*	29	The Commission's intent is to release an RFP soon after the release of the ESInet/NGCS RFP that addresses the connectivity from the host locations to the regional PSAP locations. Please provide the status of the intended RFP, and what the expected relationship with these services providers will be?	The status of releasing an RFP to address Host/Remote connectivity is still in discussion and a decision has not been finalized on the need for releasing such an RFP. Each region has a regional IP network today, and the expectation is that a possible Host/Remote RFP will not change the interaction between the Bidders and these regional IP providers. It is anticipated that the various service providers of the state and regional ESInets will advise one another of outages within their respective networks.
42.			6264 Z1 ESInet and Core Services RFP final SONYAS	29	Are there any plans to upgrade call handling equipment to NENA i3-ready call handling?	The PSC will work with the regions to encourage i3 compatibility, but Bidders shall assume connectivity to CHE with the software versions noted in Attachment A Revision One.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			V.B. Composition of the Request for Proposal			
43.			6264 Z1 Attachment C Technical Requirements Option C *GEN SCEN 4, Scenario 4*	25	Since the connectivity from the regional host controller to the PSAP's will be part of another RFP, what are the responsibilities of the service provider for this connectivity regarding monitoring, reporting, and maintenance actions?	The Regional IP network and monitoring of such networks is the responsibility of the Regional network service provider. It is anticipated that the various service providers of the State and regional ESInets will advise one another of outages within their respective networks.
44.			6264 Z1 Attachment C Technical Requirements Option C *ESI 9, Emergency Services IP Network (ESInet); Special Construction*	32	Can the State provide diagrams or schema for the existing network assets so bidder's understand what can be leveraged?	See response to Question 21.
45.			6264 Z1 Attachment C Technical	60	Please provide a copy or link to the existing data-sharing agreement (DSA).	Please see new 6264 Z1 Attachment E Nebraska ECaTs Data Sharing Agreement

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			Requirements Option C *NGCS 70, Next Generation Core Services Elements (NGCS)* *Event Logging and Management Information System (MIS); Access to Event Logging Data*			
46.			6264 Z1 Attachment C Technical Requirements Option C NGCS 71, Next Generation Core Services Elements	61	What needs to be provided for third-party certification proof?	Certification documents are not required. Please see NGCS 71.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			(NGCS) Event Logging and Management Information System (MIS); NENA Standards Compliance			
47.			RFP document, title page, top section:	Page i	The opening date and time says: "June 3, 3030, 2:00 P.M. Central Time". **Question**: Should the year be changed to 2020 instead of 3030? Or is there a reason its titled 3030?	See response to Question 28.
48.			RFP document, Section I. Procurement Procedure, part J. Submission of Proposals subsection 2 and Section VI Proposal	Pages 4 and 35	At section 1.J.2 of the RFP, the bid says: "The Technical, Cost Proposals, and Proprietary information should be uploaded as separate files." Additionally, section VI., Proposal Instructions, Part A Proposal Submission, number 2 Technical Approach says: " The technical approach section of the Technical Proposal should consist of the following subsections, which includes subpart f titled "Cost	

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			Instructions, Section 2.f		Proposal". **Question**: Should the cost proposal be included as subpart f in the Technical Approach/Technical Proposal electronic file document, or should it be submitted as a totally separate file?	Please submit the cost proposal as a separate excel file. VI.A.2.f. is hereby deleted.
49.			RFP document, Section I. Procurement Procedure, part P. Request for Proposal/Proposal Requirements, Subpart 4 and Section VI A. Proposal Instructions, Section 1 Corporate Overview & 2 Technical Approach	Pages 5 and 35	At Section 1.P.4, the proposal requirements say The proposals will first be examined to determine if all requirements listed below have been addressed and whether further evaluation is warranted. It goes on to include # 4 "Complete Sections II through IV." **Questions**: 1. In section VI Proposal Instructions, the location to include sections II through IV is not mentioned. Should those sections be included in Section VI, Part 1 for Corporate Overview, or in section VI part 2 for Technical Approach? 2. If in section VI.A.1, Corporate Overview, should the sections be in the order presented in the RFP, or do you want the	The State lists all required items in section I.P. The order of documents is not prescribed in the RFP document.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					Sections ii through IV after VI.A.1.j? 3. .If in Section VI.A.2 Technical Approach, where in the letter sequence a. to f. should sections II through IV be inserted?	
50.			ESInet & Core Services RFP Revision One	4	The RFP requests one hard copy labeled "original," but does not specify the number of hard copies. If bidders intend to submit hard copies, how many copies should be provided?	If a bidder chooses to submit a paper document, only one (1) copy marked “original” is needed.
51.			ESInet & Core Services RFP Revision One	20	If the primary contractor lists their subcontractors as additional insured on their insurance policy, does this satisfy the requirements in section G for subcontractors?	Yes, if the Contractor provides equivalent insurance for each subcontractor and verifies the coverage meets the requirements of the RFP.
52.			ESInet & Core Services RFP Revision One	15	Within Section VI. Proposal Instructions, Item 2. Technical Approach provides a list of the subsections that should be included in the Technical Proposal. Item c. states "Attachment C - Technical Requirements Option A, B, and/or C." If a bidder intends to submit a response for Technical Requirements Options A, B, and C, how does the state prefer all three options be submitted?	

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					Does the state want bidders to complete/return separate responses for Option A, B, and C? Or, does the state want only a response submitted for Option C and a separate cost proposal for each option? Please provide clarification. If the state does prefer bidders submit each option separately, should they be provided as separate binders?	Please submit a complete, separate response if responding to more than one option. Yes. Or if submitted electronically, as separate files using the naming convention stated in the RFP.
53.			Attachment C Option A / Attachment C Option B /Attachment C Option C	1	The instructions for Attachment C, Options A, B, and C include instructions indicating "the narrative should provide The Public Service Commission (PSC) with sufficient information to differentiate the bidder's business solution from other bidders' solutions. Bidder shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details shall be provided in the same paragraph as the requirement." However, ESInet & Core Services Revision One, page 29 indicates "The Bidder may include appendices and reference them from within the proposal response. This is particularly appropriate for lengthy responses on a single subject." The bidder believes this information is contradicting. Please provide clarification as to whether it is	Each Option being bid must include a response to each requirement. Bidders cannot reference a response submitted in another Option. While individual requirement responses may refer to additional documentation in appendices, attachments, etc., an answer may not be scored if it simply refers the reader to the response to an attachment or another requirement.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					acceptable for bidders to refer to appendixes within their response that are included later within the proposal?	
54.			Attachment C Option B Attachment C Option C	34 37	Req Identifier NGCS 8 and NGCS 9 are identical. Does the state want bidders to answer both requirements or will one be removed?	See response to Question 9.
55.			Attachment C Option B Attachment C Option B	35 38	Req Identifier NGCS 11 states "The bidder's BCF solution shall support transcoding of Baudot tones to real-time text (RTT), as described in IETF RFC 4103. Describe how the solution meets or exceeds the above requirements." Generally, this function is normally conducted by the legacy network gateway (LNG). Can the state please provide clarification on this requirement?	Describe how this functionality is implemented in the proposed solution, including the functional element or elements involved.
56.			Attachment C Option B Attachment C Option C	47 50	Regarding Req Identifier NGCS 45 “An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Describe the functionality of such an ECRF equivalent and document where this functional element resides within the proposed solution." If an origination network is using their own ECRF not provided by the bidder, how is the	This is in reference to originating service providers (OSPs) needing some means of making an initial routing decision. Whether this is implemented by the NGCS provider as an external (to the ESInet) ECRF or by the respective OSP depends on the bidder’s interop agreement with the OSP. Describe how the ECRF solution operates in a hierarchical environment.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					bidder expected to describe the functionality of said ECRF? Additionally, if it is in the origination network, how can the NGCS bidder document where this functional element resides? This same requirement is included in	For the remainder of the question, there is missing information. The State is unable to provide a response.
57.			Attachment C Option B Attachment C Option C	47 51	Part of Req Identifier NGCS 49 is a duplicate of NGCS 48. Both contain, at least in part, “Logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions.” Please provide clarification.	Req Identifier NGCS 48 deals specifically with rate-limiting queries and logging when those limits are exceeded. Req Identifier NGCS 49 is a more general list of requirements based on NENA-STA-010.2.
58.			Attachment C Option B Attachment C Option C	47 51	Part of Req Identifier NGCS 49 includes “Location error correction." It is the bidders belief that the ECRF should consume data and optionally detect errors, allowing the GIS staff to act on detected errors and resolve them in the source GIS data. An ECRF can’t, and should not, attempt to correct errors as this can introduce a number of problems. Can this requirement please be removed?	This requirement remains and should read, “location error identification.” Please use Attachment C Option B NGCS Revision One; and Attachment C Option B ESInet and NGCS Revision One.
59.			Attachment C Option B Attachment C Option C	41 51	Part of Req Identifier NGCS 49 includes “Compliance with NENA 02-010 and NENA 02-014." NENA 02-010 is a legacy schema for GIS and is incompatible with the NG9-1-1 GIS Data Model that is specified in	Bidder must be compliant with all current NENA standards, other industry standards and best practices.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					Attachment B. NENA 02-014 refers to GIS data collection and maintenance standards, of which the ECRF does not do. Can both of these requirements be removed, or updated, to reflect new NENA standards (such as the NG9-1-1 GIS Data Model)?	
60.			Attachment C Option B Attachment C Option C	51 51	Req Identifier NGCS 59 references legacy standards NENA 02-010 and NENA 02-014. Neither of these should apply to the SI. Can these be changed to the CLDXF standard and NG9-1-1 GIS Data Model?	Please see response to Question 59.
61.			Attachment C Option B Attachment C Option C	52 56	Req Identifier NGCS 63 states "Describe how the solution interfaces with other LDB solutions which may participate in or interface with bidder's solution." Please elaborate on how, and more importantly why, one LDB will need to interface with another? There is currently no NENA standard in place for this.	There will be a transition period between legacy routing and geospatial routing. Explain how the proposed solution would deal with multiple ALI/MSAG databases and the locations where ALI steering may be in place.
62.			Attachment C Option B Attachment C Option C	57 57	Req Identifier NGCS 64 states the LDB shall "Shall automatically detect, import and validate customer records (SOI records)." In order to load a legacy SOI record into an LDB, it must be converted to CLDXF. The NENA standards specify using an MSAG Conversion Service (MCS) functional element for this. Is an MCS part of the	The RFP seeks a complete solution. Please submit a response that best meets all current NENA and industry standards.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					requirements of this RFP?	
63.			Attachment C Option B Attachment C Option C	53 56	Req Identifier NGCS 62 refers to the Commission's GIS data model (Attachment D). Can the state please clarify if the GIS Data Model is Attachment B or D?	See response to Question 11.
64.			Cost Proposal Option C ESInet & NGCS Final	1	Each of the three pricing workbooks (including Cost Proposal Option A ESInet Final, Cost Proposal Option B NGCS Final, and Option C ESInet & NGCS Final) define seven regions. However, the diagram in ESInet & Core Services RFP Revision One, Section V. Project Description and Scope of Work (pg. 28) and Attachment A - PSAP Host EndPoints, Equipment, and Selective Router Locations do not definitively define or illustrate the regions to allow for pricing. Can the state please provide clarification as to how the regions should be defined including where the hosts are to be located for the Metro West and Northeast regions?	Please see response to Question 4.
65.			Attachment A - PSAP Host EndPoints, Equipment, and Selective Router	Page not numbered	Eighteen PSAPs are listed as "Stand Alone" in Attachment A. If anticipated regional hosts are not defined for the Metro West and Northeast regions, will ESInet providers be required to bid/provide layer 2 circuits to each of these PSAPs that are not part of a region? How will the state handle the	See response to Question 4.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			Locations		circuit costs for these sites if/when they join a region?	
66.	Optional Pre-Proposal Conference - Link to Listen to Conference			Media, Slide 5	Slide 5 of the pre-proposal conference presentation lists the proposal due date as June 2, 2020. All RFP documents and the procurement website lists June 3, 2020. Please confirm June 3, 2020 is the proposal due date.	See response to Question 28.
67.	Optional Pre-Proposal Conference - Link to Listen to Conference			Media, Slide 14	During the discussion of slide 14 of the pre-proposal conference presentation, MCP representative Milton Schober stated the RFP lists some older standards and bidders should state their compliance or non-compliance based upon the most current standards. Since the RFP will likely become part of resulting contract we ask that the State update the RFP to list the published standards that are required for compliance. We assume Mr. Schober was referring to Section V, D. General Requirements - Technical.	Please see response to Question 59.
68.			6264 Z1 Attachment C Technical Requirements Option B NGCS 62	53	Does the State plan to leverage the GeoComm Data Hub in place today for most of the regions?If so, how does the State envision GeoComm's Data Hub will interconnect to the required Spatial Interface (SI)?	The State intends to use the statewide aggregated data and will work directly with the PSAPs (or their designated GIS representative) to maintain this layer.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			Next Generation Core Services (NGCS) Spatial Interface (SI) Use of the Commission 's GIS Data Model			
69.	6264 Z1 ESInet and Core Services RFP Revision One Schedule of Events			2	Will vendors have the opportunity to ask follow-up questions to those answers released on or about April 16? If so, what is the deadline?	Bidders will be given an opportunity to ask question during a second round of Q&A. Please see posted Revised Schedule of Events.
70.	6264 Z1 ESInet and Core Services RFP Revision One Section I,			Page 6 and Page 11	Are the reference Vendor Performance Reports part of the RFP response evaluation process? If so, what is the derivation of the reports?	Vendor Performance Reports may be used for evaluation.. Bidders who have had a contract with the State of Nebraska may be evaluated on any performance reports submitted to State Purchasing Bureau.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	R. Evaluation of Proposals; and Section II, H. Vendor Performance Reports					
71.	V. PROJECT DESCRIPTION AND SCOPE OF WORK			Page 28	In order to assure proper sizing for traffic engineering, network bandwidth and data throughputs, we will need data on busy hour call attempts and average call durations. Can the State please provide this information?	The State is unable to provide this information at this time. The State is in the process of receiving 2019 call volume numbers from PSAPs statewide and will post the data with the 2nd round of Q&A.
72.	V. PROJECT DESCRIPTION AND SCOPE OF WORK			Page 28	During the pre-bid meeting there was mention of a new Metro West region with Colfax and Dodge Counties as participants. Can the State please provide a list of all the members that will be participating in this new region?	See response to Question 4.
73.	V. PROJECT DESCRIPTION AND SCOPE OF WORK			Page 28	During the pre-bid meeting there was mention of a new North East region with Wayne County, City of South Sioux City and City of Norfolk as participants. Can the State please provide a list of all the members that will be participating in this new	See response to Question 4.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					region?	
74.	Attachment C Technical Requirements – Option C			Requirement Identifier ESI 9 Page 32	Can the State please provide details and/or a diagram of the meet points of this microwave network?	See response to Question 21.
75.	Attachment C Technical Requirements – Option C			Requirement Identifier ESI 10 Page 33	Are there any plans or knowledge to support the connection to prospective neighboring ESInet's?	The State intends to implement this requirement in the future.
76.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 8 Page 37	Requirement Identifier NGCS 8 and NGCS 9 appear to be the same requirement. Are these duplicate requirements?	See response to Question 9.
77.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 32	Is there, or will there be, a Statewide geospatial project to position the PSAPs for true i3 geospatial routing? If yes, can you share those details relating to schedules, milestones,	See response to Question 32.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
				Page 45	etc.?	
78.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 1 Page 34	The RFP mentions transitional and end states for the NGCS network. What are the State's expectations regarding what defines the transitional state(s) and the end state?	The transitional period is the time between the start of routing on tabular data and the migration of the last region on tabular routing to full geospatial routing. Full geospatial routing is the end state.
79.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 1 Page 34	Does the State expect the NGCS network to receive calls directly from TDM trunks (i.e., is the contractor expected to provide the necessary gateways in this case)?	The State requires a complete solution. If gateways are necessary, the contractor must provide all equipment.
80.	Attachment A – PSAP Host EndPoints, Equipment and Selective Router Locations			Attachment A	Can the State provide detailed information on the downstream connection (i.e., PSAPs and regions) as to what terminating equipment is available at the regions, which PSAPs require direct connections and which directly connected PSAPs are IP-capable?	Only regions will be connecting to the statewide ESInet. The known call handling equipment type and model for each region is the level of detail that the State has listed on Attachment A – Revision One
81.	Attachment C Technical			Requirement	NGCS-14 requires the LNG to generate reports that can be loaded	This can be done through a central reporting function.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	Requirements – Option C			Identifier NGCS 14 Page 39	into a spreadsheet. Is it necessary for the LNG to do this directly or can this be done through a central reporting function?	
82.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 32 Page 45	Can the State provide more information on how many PSAPS – and for how long – tabular routing will be required? What is the limitation driving the need for tabular routing?	The State intends to transition to geospatial routing as soon as possible. The limiting factor at the moment is the current status of the statewide PSAP layer.
83.	Attachment C Technical Requirements – Option C			Requirement Identifier NGCS 70 Page 60	The RFP calls for both ECaTS and NENA i3 event reporting. Can the State provide any detail on how these are expected to interwork?	The RFP requires bidders to comply with NENA i3 event reporting. The requirements call for the proposed solution to interface with ECaTS. The contractor will be required to communicate with ECaTS to achieve this functionality.
84.	Attachment C, Option A Attachment C, Option B			12	Req Identifier NOC/SOC 15 describes that a NMIS – Management System should interface with the Incident Management System, and that the	Historical data includes but is not limited to, network and system performance data, bandwidth utilization, latency, jitter, packet loss, MOS scores, CPU and memory utilization, and outage-related data.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	Attachment C, Option C				Contractor shall maintain historical information for the term of the contract and provide copies of the data to the Commission at the end of the contract. Can the Commission clarify the scope of the historical information? Are we correct in interpreting this to mean the historical incident management information and related logging errors and not all logs?	
85.	Attachment C, Option B Attachment C, Option C			53 56	Req Identifier 62 refers to "regions." How many different regional GIS datasets can we expect to receive? Does the state envision these regional GIS datasets to be aggregated into a single statewide dataset for use in the ECRF/LVF?	The State currently anticipates 7 regions as part of the statewide ESInet. The State envisions these datasets will be aggregated into a statewide dataset. The State will provide the aggregated dataset to the Contractor.
86.	6264 Z1 Cost			summary	For clarification, will the five year total cost (cell	Yes.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	Proposal Option A, B, C Excel Workbooks			tab	B20 in the option C pricing workbook) be the figures that are used for cost comparison between vendors?	
					Or, does the renewal pricing also play a part in the cost scoring?	No.
				N/A	Will a faster implementation schedule save the State money on legacy costs? If so, are those cost savings going to be considered as part of the evaluation process when scoring the proposals? If it will be considered in scoring the proposals, will that be considered in the points awarded under Part 2 – Technical Approach or under Part 3 – Cost Proposal Points?	Cost evaluation is not weighted to include implementation timeline. The implementation timeline is evaluated on the technical response. N/A. Please see response above.
				N/A	Additionally, it is our interpretation that if these legacy cost	

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					savings are not factored in, the vendor with the slowest implementation schedule is likely to have the lowest cost proposal allowing them to score the maximum points in pricing. Is this interpretation correct?	
87.	Attachment A			page 1	Will the State provide location information for the 2 host sites for the Northeast Region? Locations of the host sites will both determine diversity and connection types that can be used to connect the ESInet to this region	See response to Question 4.
88.	Attachment C, Option C, SEC-3			pages 4-5	This requirement states: "The matrix shall identify whether the bidder's proposed solution Complies (C), Complies Partially (CP), Complies with Future Capability (CFC) or Does Not Comply (DNC), or Not Applicable (N/A) (as indicated in the NENA checklist) with the identified requirement(s) for each category included in the checklist." Each category contains varying numbers of requirements. Please explain how the	Please see Attachment C – Option A ESInet Revision One, Attachment C – Option B NGCS Revision One, and Attachment C – Option C ESInet and NGCS Revision One.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					State would like the bidders to determine the response. For example, suppose **Section 3. Authentication/Password Policy** has 54 requirements: 30 are Complies, 8 are Complies Partially , 0 are Complies with Future Capability, 1 is Does Not Comply, and 15 are N/A. For this example, can the State explain how bidders should determine which category to check for Section 3 in the checklist?	
89.	Attachment C, Option C, SEC-3			pages 4-5	This requirement states: "Bidder shall provide details to support the responses for each category in the response box below." What kind of details is the State requesting? Does the State want an explanation for each requirement in a section? Does the State want a breakdown of how many of each type of response is in each section? Please explain.	See response to Question 88.
90.	6264 Z1 Technical Requirements Option B NGCS 49 -	NGCS 49	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function	51	When logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions: What format of log file is required as well as any duration for retention, or settings to support such, requirements that may exist for the	The file format is not specified. The tools provided for viewing logs should be capable of reading the native format of each device, be it text, XML, JSON, or something else, and displaying the output in human-readable format. Records must be maintained for the length of the contract including all renewals and extensions. Please also see Section II.U. Contract Closeout.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
			(ECRF) Supported Functions		State?	
91.	6264 Z1 ATTACHMENT A	PSAP Equipment			Would the Commission provide the following 9-1-1 call volumes for each PSAP; Avg. Busy Hour, Peak Call Volume and and Annual Call Volume?	See response to Question 71.
92.	6264 Z1 ESInet and Core Services RFP Revision One and Cost Proposal (Word doc)	I.C	Schedule of Events	2	Please confirm that the bid due date is 6/3/20 per the RFP. 6/2/20 was shown during the pre-bid meeting.	See response to Question 66.
93.	6264 Z1 Attachment C Technical Requirements Option C -ESInet and NGCS (Word doc)	Gen SCEN	GEN SCEN 4	25	Vendors were request to provide connectivity to Host Sites for each of the regions. The scenario specifies connectivity to a PSAP. Would the State want to modify the Scenario using host site rather than a PSAP?	Yes, replace “PSAP” in Scenario 4 with “Host A”. Please use Attachment C Option A – ESInet, Attachment C Option B – NGCS, and/or Attachment C Option C – ESInet and NGCS.
94.	6264 Z1 Attachment C Technical Requiremen	NGCS 39	Next Generation Core Services Elements	47	Our understanding is that the i3 standard will soon be updated from i3 v2 to i3 v3, and furthermore that there are significant differences	Please see response to Question 59.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
	ts Option C -ESInet and NGCS (Word doc)		(NGCS) NENA Compliance Chart		between the two standards. Since no PSAP CPE supports v2 at this time, our expectation is that the State would prefer vendors be able to support i3 v3 once ratified, and therefore vendors could also address compliance to i3 v3 as an option?	
95.	Attachment C, Option C			Page 10	NOC/SOC 10: Does this requirement only apply to ESInet as NGCS is not indicated in this requirement?	See response to Question 19.
96.	Attachment C, Option C			Page 47	NGCS 38: Is SCTP a protocol which is optional or required?	See response to Question 23.
97.	Attachment C, Option C			Page 56	NGCS 62-1: Please provide or direct as to where Attachment D is located	See response to Question 11.
98.	Attachment C, Option C			Page 63	NGCS 77-2: Please provide the requirements and definition of an NGCS “ringdown” feature. This is typically a feature in Call Handling and in order to understand the request, please provide desired functionality.	See response to Question 26.
99.	6264 Z1 Cost Proposal Option C - ESInet and NGCS				Is it understood that complete pricing may not be provided until all locations are identified?	See Response to Question 4.
100.	Attachment C, Option C				There is no reference to the number of POI’s required. Can the State	Please provide a response that best meets the requirements of the RFP.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					provide guidance on this requirement?	
101.	Attachment C, Option C				Please provide a position count and/or concurrent call counts that need to be supported per Aggregated Call Handling location.	See Attachment D
102.	PROCUREMENT PROCEDURE, J. SUBMISSION OF PROPOSALS			4	The State is accepting either electronically submitted responses or paper responses for this RFP. For bidders submitting electronic responses: 1. Bidders submitting electronically can upload the response here: a. https://nebraska.sharefile.com/r-r11ba33e3ee24b63b **Questions:** In sections J. it discusses submitting each section of the RFP as well as lists the separate solutions Option A (ESInet), Option B (NGCS), and Option C (ESInet, & NGCS). 1. Will the state accept two solutions of the same service? How should a vendor submit these options? 2. Should there be two separate	 Yes. Submit a complete, separate, response, cost proposal, and Technical response for each. Yes.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					RFP submissions and two separate pricing options? 3. How do you want the separate RFP's named? 4. If a Vendor submits two options will the scoring be a weighted average or seen as a completely separate submission?	 Please see Section I.J.3. "Submission of Proposals" of RFP 6264 Z1 ESInet and Core Services RFP Revision One. Each proposal will be scored independently.
103.	**I. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH**			35	The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this solicitation….. ……..Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) b. SUBCONTRACTORS If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide: i. name, address, and telephone number of the	

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					subcontractor(s); i. specific tasks for each subcontractor(s); ii. percentage of performance hours intended for each subcontract; and iii. total percentage of subcontractor(s) performance hours. **Questions:** **1.** In section I. as apart of the resume section it states that you are requesting 3 personal references for each resume submitted. (name, address, and telephone number), this would be considered personal confidential information to these individuals. Knowing that the RFP is considered public information these individuals may not want their personal information publicized and attached to the RFP. Would the state accept the name of the reference omitting address, telephone number and upon award the vendor would provide additional information about the references so they may be contacted if the state feels it is	Question1:) The address and telephone numbers do not need to be submitted with the proposal, but must be submitted by the selected vendor upon award.

Question Number	Reference Document	RFP Section Reference	RFP Page Number	RFP Page Number	Question	State Response
					necessary? **2.** In the section outlined above "SUBCONTRACTORS If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:" name, address, and telephone number of the subcontractor(s). This too would be considered personal confidential information to these individuals. Knowing that the RFP is considered public information these individuals may not want their personal information publicized and attached to the RFP. Would the state accept the name of the reference omitting address, telephone number and upon award the vendor would provide additional information about the references so they may be contacted if the state feels it is necessary? **3.** Would the state accept the general corporate address and phone number of the subcontractors company to fulfill the requirement of this RFP in the outlined section.	Question 2:) The address and telephone numbers of subcontractors do not need to be submitted with the proposal, but must be submitted by the selected vendor upon award. Question 3: Yes, if the State would be able to contact the actual subcontractor(s) to be used to fulfill this contract using the given address and phone number.

This addendum will become part of the proposal and should be acknowledged with the Request for Proposal response.

ADDENDUM FIVE – REVISED SCHEDULE OF EVENTS

Date: April 22, 2020

To: All Bidders

From: Annette Walton / Nancy Storant, Buyers
Nebraska State Purchasing Bureau

RE: Addendum for RFP Number 6264 Z1 to be opened June 3, 2020 at 2:00:00 P.M. Central

Revised Schedule of Events

ACTIVITY		DATE/TIME
7.	Last day to submit second round written questions.	April 30, 2020
8.	State responds to second round written questions through Solicitation "Addendum" and/or "Amendment" to be posted to the Internet at: http://das.nebraska.gov/materiel/purchasing.html	May 7, 2020
9.	Proposal Opening Location for mailed/hand delivered submissions: State Purchasing Bureau 1526 K Street, Suite 130 Lincoln, NE 68508 Electronic submissions: https://nebraska.sharefile.com/r-r11ba33e3ee24b63b	June 3, 2020 2:00: 00 PM Central Time
10.	Review for conformance to solicitation requirements	June 8, 2020
11.	Evaluation period	June 8, 2020 through June 29, 2020
12.	"Oral Interviews/Presentations and/or Demonstrations" (if required)	TBD –July 13-17
13.	Post "Notification of Intent to Award" to Internet at: http://das.nebraska.gov/materiel/purchasing.html	TBD
14.	Contract finalization period	TBD
15.	Contract award	TBD
16.	Contractor start date	TBD

This addendum will become part of the ITB/proposal and should be acknowledged with the Request for Proposal response.

ADDENDUM SIX FOR QUESTIONS AND ANSWERS, ROUND TWO

Date: May 7, 2020

To: All Bidders

From: Annette Walton/Nancy Storant, Buyers
AS Materiel State Purchasing Bureau (SPB)

RE: Addendum for RFP 6264 Z1 to be opened June 3, 2020, 2:00 P.M. Central Time

Following are the changes made to the above mentioned RFP. The changes are to be considered as part of the RFP. It is the Bidder's responsibility to check the SPB website for all Addenda or Amendments.

Question Number	RFP Section Reference	RFP Page Number	Question	State Response
1.	6264 Z1 Attachment C Technical Requirements Option B: Requirement #NGCS 62, and Addendum Four – Questions & Answers; Question #68	6264 Z1 Attachment C Technical Requirements Option B NGCS, page 53; Addendum Four – Questions & Answers, page 25	Will the selected vendor be required to provide a solution and/or workflow for receiving GIS updates from the regions and aggregating the data into a statewide dataset? Or rather, will the State receive GIS data updates from the regions and deliver an aggregated statewide dataset to the selected vendor for ingestion into the ECRF and LVF via the SI? If this is the State's preferred method, how often does the State anticipate providing a statewide aggregated data set to the selected vendor? Further, if the State plans to deliver the statewide aggregated dataset for ingestion into the ECRF and LVF via the SI, will the State be	The Contractor will work directly with the State. The State will provide an aggregated statewide dataset for each of the required layers. Yes. The State anticipates providing data updates monthly. The State updates will be validated against topological errors and missing attribution. The Contractor will be required to provide their own

			performing any quality control and error checks prior to transmission to the selected vendor? If so, please elaborate on the planned checks.	validation prior to populating or updating the NGCS.
2.	6264 Z1 EsiNet and Core Services RFP final SONYAS Section II, H. Vendor Performance Reports	Page 11	The following requirement is in the terms and conditions: The State may document any instance(s) of products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or solicitation specifications. The State Purchasing Bureau may contact the Vendor regarding any such report. Vendor performance report(s) will become a part of the permanent record of the Vendor. What permanent record is the State referring to? Are these records available to the public?	Procedures for Vendor Performance Reports can be found in the Vendor manual at: http://das.nebraska.gov/materiel/purchase_bureau/vendor/vendor-info.html All performance reports received are kept on file. Yes.
3.	6264 Z1 Cost Proposal Option B-NGCS revision one.xlsx, 6264 Z1 Cost Proposal Option C ESInet and NGCS revision one.xlsx NRC Milestones tab	NRC Milestones tab	The total on the NRC Milestones tab of both the Option B (C11) and Option C (Cell C9 for ESInet and cell C19 for NGCS) workbooks is omitting the total NRC from Region 7. All totals are ignoring the region 7 value on NRC Milestones tab only. Is this an intentional omission or is this a formula error given that the instructions specify	Formula error. Please use 6264 Z1 Cost Proposal Option B Revision Two, 6264 Z1 Cost Proposal Option C Revision Two.

			NRC payments will be made as structured on the NRC milestones tab?	
4.	Document: 6264 Z1 Attachment A - PSAP HOST Endpoints equipment and selective router locations	Page. 1	Can the State verify the address for the Douglas County Call handling Host Site. Attachment A shows the address to be 151335 West Maple, Omaha. Douglas County Treasury is at 15335 W Maple. Can the State confirm that Douglas County Sheriff is on same property but faces west and has a 3601 N 156th St. address?	The address of the PSAP is 15335 West Maple, Omaha, NE. Please see Attachment A Revision Two – PSAP Host endpoints equipment and select router locations. The demarc for the back office/technology equipment is located at 3603 N 156 St, Omaha, NE.
5.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS.docx Section: ESI-9 and NGCS-1 Subsection: Network Design Documentation	Page. 32 and Page. 34	The RFP mentions transitional and end states for the NGCS network. What are the state's expectations regarding what defines the transitional state(s) and the end-state?	The transitional and end states apply to the NGCS only, not the ESInet. The transition state is the time when the NGCS is routing based on tabular data or a combination of tabular and geospatial data. The end state is the time at which all entities are routing based on geospatial data.
6.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS.docx Section: NGCS-4	Page. 36	Does the state expect the NGCS network to receive calls directly from TDM trunks (i.e. is the contractor expected to provide the necessary gateways in this case)?	Yes, the Contractor is required to provide a complete solution, including any necessary gateway functionality.

	Subsection: Next Generation Core Services Elements (NGCS), Legacy Network Gateway (LNG), LNG Description			
7.	General	General	Can the state provide detailed information on the downstream connection (i.e. PSAPs and regions) as to what terminating equipment is available at the regions, which PSAPs require direct connections and which directly connected PSAPs are IP-capable?	The call handling equipment for the regional host sites is included in Attachment A Revision Two – PSAP Host endpoints equipment and select router locations. There will not be any standalone PSAPs directly connected to the ESInet. All PSAPs will be part of a region. All connections to the ESInet will be from the host locations.
8.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS.docx Section: NGCS-14 Subsection: Next Generation Core Services Elements (NGCS), Legacy Network Gateway (LNG), Extraction of Log Files	Page. 39	Requires the LNG to generate reports that can be loaded into a spreadsheet. Is it necessary for the LNG to do this directly or can this be done through a central reporting function?	This can be done through a central reporting function.

9.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS.docx Section: NGCS-32 Subsection: Next Generation Core Services Elements (NGCS), Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF), Transition to Geospatial Routing	Page. 45	Can the state provide more information on how many PSAPS – and for how long – tabular routing will be required? What is the limitation driving the need for tabular routing?	The number of PSAPs is not known, each PSAP is controlled at the local level. It is the State's intent to transition to geospatial routing as soon as all PSAPs in a region are ready for geospatial routing. The limitation driving the need for tabular routing is that regional and statewide data still requires preparation.
10.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS.docx Section: NGCS-67 to NGCS-71 Subsection: Multiple	Pages. 59-61	The RFP calls for both ECaTS and NENA i3 event reporting. Can the state provide any detail on how these are expected to interwork?	The requirements call for the proposed solution to interface with ECaTS. The Contractor will be required to work with ECaTS to achieve this.
11.	Document: 6264 Z1 Attachment C Technical Requirements Option C - ESInet and	Page. 62	What is the current situation with PSAPs in the State of Nebraska and Text-to-9-1-1? Do all PSAPs support integrated text handling	There are approximately 42 PSAPs that have text-to-911 capabilities. No, not all PSAPs support integrated text, some rely

	NGCS.docx Section: NGCS-76 Subsection: Next Generation Core Services Elements (NGCS), Message Session Relay Protocol Text (MSRP) Integration		capabilities, or do some still rely on an Over-the-Top solution? Will the new NGCS network be required to support the OTT approach? Will the existing OTT solution (if any) be left in place?	on an OTT solution. The State intends to integrate text-to-911 into NGCS and have text available to all PSAPs. NGCS will not be required to support OTT. No OTT solutions will not remain.
12.			Are ISPs allowed to bid this RFP with/through partners?	Yes.
13.	Attachment C, Option, Option B Revision One Attachment C, Option C Revision One	59 62	NGCS 76 - How is (SMS)-to-911 service delivered to PSAPs today? What integration to existing service is expected to be provided by the ESInet provider? Is the intent for the NGCS and/or ESInet provider to become the primary SMS-to-911 provider for PSAPs in Nebraska?	See question 11. Integration to existing service is not required. Yes.
14.	Cost Proposal Option A ESInet Revision One Cost Proposal Option B NGCS Revision One Cost Proposal Option C ESInet Revision One	1 1 1	Within the revised Cost Proposal spreadsheets, regions were adjusted to match the Nebraska PSAP Regionalization map (Figure 1) within the 6264 Z1 EsiNet and Core Services RFP Revision One. Regions 1 and 2 were switched to reflect the desired project schedule. However, in doing so, the associated	Yes. Please use 6264 Z1 Cost Proposal Option A Revision Two; 6264 Z1 Cost Proposal Option B Revision Two; and/or 6264 Z1 Cost Proposal Option C revision Two.

			populations were not adjusted. Will the state modify the Cost Proposal spreadsheets to reflect the correct populations? Or, should Bidder's work from the existing Cost Proposals (Options A, B, and C)?	
15.	6264 Z1 Attachment C Technical Requirements Option C - ESInet and NGCS, NGCS 77	63	Please provide a full definition of the NGCS requirement to provide ringdown circuits. Traditional Ringdown functionality typically involves legacy technological solutions not provided within a typical IP network. Please describe the functionality requested so that the ESInet vendor can describe the IP and NGCS infrastructures capability to support requirement.	The requirement is that the NGCS support Ringdown functionality in the event that one or more CHE systems do not support it.
16.	6264 Z1 Attachment CTechnical Requirements Option C - ESInet and NGCS, NGCS 67	59	Please clarify the i3 Logging request of the ESInet provider. It is generally understood that delivery of the State/PSAP facing report is the responsibility of the MIS vendor. The process of establishing these reports typically occurs in two stages. a. Aggregation of i3 element record logs and delivery of that data (interface) to the MIS reporting vendor (EcATS) b. Establishment of reports of specified i3 elements on ECaTS	

			platform. It is the understanding of the ESInet vendor that the solution will include the resources/time/effort for item a.. For Item b. it is understood that the resources, time effort and pricing would be a separate agreement between the state/PSAP and ECaTS and the ESINET vendor should not account for additional cost of ECaTS to support those reports. Please confirm	The requirement is only for the delivery of the data to ECaTS. The ESInet/NGCS contractor must coordinate this with ECaTS. For item 'b,' the State works directly with ECaTS for the reports and formatting of the reports, so yes, the ESInet vendor should not account for additional cost to support these reports.
17.	Attachment A, Attachment D	All	Please identify which potential Host Region the following PSAP's will be affiliated with: • Scottsbluff County Custer County	Scottsbluff County will become a part of the South Central region. The State anticipates that Custer County will become a part of the East Central region.
18.	Attachment A	1	Please confirm the address for the Douglas County PSAP Host location.	See response to Question 4.
19.	Attachment C, Option C	6	SEC 5 – Please provide use case of a device/carrier outside of the IP network not provided credentials.	The State wants to ensure that a network that connects to the ESInet or NGCS has a valid reason for interconnection. If that is the case, credentials are issued. The State requires that if no valid reason for interconnection exists, credentials are not issued.
20.	Attachment C,	63	NGCS 77 – Will the	The State is not looking

	Option C		PSAPs be providing ringdown phones if their CPE does not support this functionality?	for any party to provide equipment. We are looking for support of the functionality via the NGCS.

This Addendum will become part of the RFP and should be acknowledged with the RFP.

ADDENDUM SEVEN FOR QUESTIONS AND ANSWERS, ADDITIONAL QUESTIONS

Date: May 14, 2020

To: All Bidders

From: Annette Walton/Nancy Storant, Buyers
AS Materiel State Purchasing Bureau (SPB)

RE: Addendum for RFP 6264 Z1 to be opened June 3, 2020, 2:00 P.M. Central Time

Following are the changes made to the above mentioned RFP. The changes are to be considered as part of the RFP. It is the Bidder's responsibility to check the SPB website for all Addenda or Amendments.

Question Number	RFP Section Reference	RFP Page Number	Question	State Response
1.	6264 Z1 Cost Proposals Option A ESInet Revision Two; 6264 Z1 Cost Proposal Option B NGCS Revision Two; 6264 Z1 Cost Proposal Option C ESInet and NGCS Revision Two		The revision two version of the cost workbooks corrected the 2019 estimates of population for the first two regions. However, in doing so, the calculation of the MRC for Regions One and Region Two is now pulling the incorrect population figure (i.e. the Region One MRC is multiplying the price per pop. by Region Two's population and vice versa). This is making the MRC for Region One larger than the MRC for Region Two when using the same per pop price because the formulas in "NRC/MRC Region 1 Total" and "NRC/MRC Region 2 Total" on all input tabs have an incorrect cell reference. Will the State be issuing revision three?	Yes. Please use 6264 Z1 Cost Proposal Option A ESInet Revision Three; 6264 Z1 Cost Proposal Option B NGCS Revision Three; 6264 Z1 Cost Proposal Option C ESInet and NGCS Revision Three.

This Addendum will become part of the RFP and should be acknowledged with the RFP.

STATE OF NEBRASKA

United States of America, } ss.
State of Nebraska }

Secretary of State
State Capitol
Lincoln, Nebraska

I, Robert B. Evnen, Secretary of State of the State of Nebraska, do hereby certify that

CENTURYLINK COMMUNICATIONS, LLC

a Delaware limited liability company is authorized to transact business in Nebraska;

all fees, taxes, and penalties due under the Nebraska Uniform Limited Liability Company Act or other law to the Secretary of State have been paid;

the Company's most recent biennial report required by section 21-125 has been filed by the Secretary of State;

the Secretary of State has not revoked the Company's Certificate of Authority and has not filed a notice of cancellation.

This certificate is not to be construed as an endorsement, recommendation, or notice of approval of the entity's financial condition or business activities and practices.

In Testimony Whereof,

I have hereunto set my hand and affixed the Great Seal of the State of Nebraska on this date of

May 20, 2020

Secretary of State

Verification ID a5b4884 has been assigned to this document. Go to ne.gov/go/validate to validate authenticity for up to 12 months.

BJORN JOHNSON
SENIOR ACCOUNT MANAGER

Experience Summary

Bjorn Johnson oversees all aspects of the regional 9-1-1 accounts, including South Dakota, North Dakota, Nebraska, and Illinois. He actively participates in implementation tasks including planning development, execution, quality control, customer facing meetings, and account-related documentation. He serves as the overall account director and point of contact for the Public Service Commission and all Public Service Answering Points (PSAPs). Mr. Johnson is a proven Account Manager with 20 years of demonstrated of experience and success in management, marketing, and strategic business development. Mr. Johnson is a progressive, decisive, innovative professional who is highly valued for expertise interpreting corporate vision and strategy, translating objectives into actionable plans, and providing decisive leadership to multi-functional team members. Mr. Johnson has a strong work ethic and track record of success with a history of developing long-lasting relationships based on a foundation of trust, integrity, and reliability. Mr. Johnson has gained deep expertise in public safety networks, 9-1-1 call handling, sales engineering, 9-1-1 technologies, strategic planning, managing complex projects, team building, state budget optimization, and risk management.

Role and Understanding of the Process

Mr. Johnson serves as the first point of escalation for any account-related issues. His professional interest ranges from Business Development through Public Safety NG-911 Telecommunications Solution implementation. Mr. Johnson has provided leadership that has raised customer retention levels through effective client management and by delivering effective solutions. Mr. Johnson engages state and local leadership through establishing CenturyLink C-Level and Director level relationships within multiple market verticals. He facilitates business development through client acquisition, effective marketing strategies, and by driving sales through consistent follow-up activities. Mr. Johnson cultivates and nurtures relationships with clients to educate them on services or product specifications, including design, features, advantages, and benefits. He works effectively with customers and delivers outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, Mr. Johnson has focused on deployment of 9-1-1 initiatives and strict adherence to and conformance with customer needs. Mr. Johnson is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Computer Science, University of Nebraska, Omaha, Nebraska, Attended 1987-1990

Computer Science, Community College of the Air Force, San Antonio, Texas, 1984-1988

Relevant Employment/Project History

CenturyLink . Sioux Falls, South Dakota 2013-Present
Senior Account Manager

As Senior Account Manager, Mr. Johnson responsible for 9-1-1 in North Dakota and South Dakota, Nebraska, and Illinois. Involved in moving an enhanced 9-1-1 to NG-911 in his respective states. His responsibilities include working with customers to design solutions that resolve customer pain points, works with CTL product team to develop products that meet customer specific requirements, works with CTL orders team to ensure customer orders are installed on-time/timely, attended National 9-1-1 community conference and meetings to stay abreast of 9-1-1 innovations. In 2019, Mr. Johnson moved South Dakota to a hosted state-wide NG-911 solution.

Mitel/DataNet **Sioux Falls, South Dakota** **2011-2013**
Sales Manager

As Sales Manager at Mitel/DataNet, Mr. Johnson manages the Local Group consisting of 6 Sales Professionals that included sales of Server and Desktop Virtualization, Storage, and Telecommunications. He is Responsible for a 21-million-dollar annual quota.

CenturyLink . **Sioux Falls, South Dakota** **2007-2011**
Premier Account Manager

As Premier Account Manager, Mr. Johnson managed Government, Education, and Medical Accounts for the entire State of South Dakota. He promoted telecommunication and business solutions to CenturyLink clientele and hosted Customer meetings to provide customer service and promote CenturyLink Products and Services. He also hosted and attended CenturyLink tradeshows and provide presentations. Mr. Johnson provided routine account management to CenturyLink Customers. He was responsible for a Monthly Total Billed Revenue Quota of $720,000.00 and a Total Billed Revenue of $6.8 Million dollars annually.

Communication Service for the Deaf. **Sioux Falls, South Dakota** **2002-2007**
Assistant Chief Technology Officer

As Assistant Chief Technology Officer, Mr. Johnson designed, implemented and managed CSD's VRS (video relay systems). This system provided relay services to the Deaf community through H.323 and SIP video across the public internet. He designed and implemented a nationwide converged IP network that supports voice, data and video and worked with Qwest engineers to develop a nation-wide ATM network supporting video and data. Utilizing OC3 to DS1 level circuits. Mr. Johnson implemented Qwest SHNS OC12 network supporting voice, video and data. He was responsible 15 employees and accountable for a 5 million dollar a year budget, coordinated and managed several projects from concept to completion. These projects were completed on time and within budget constraints and developed relationships with many communication and equipment providers to develop unconventional solutions to communication barriers for the deaf and hard of hearing community.

Qwest Communications **Sioux Falls, South Dakota** **1998-2002**
Data Applications Sales Engineer

As Data Applications Sales Engineer, Mr. Johnson was the Principal network architect in the design and installation of Governor Janklow's statewide school video network. He designed extensive Voice, LAN and WAN networks for Governmental and commercial Agencies. Including the use of Private line, ISDN, Frame Relay, ATM and MPLS networks and coordinated the installation of communication services and equipment to support clients' networks.

Certifications / Training

None

Professional Memberships / Associations

None

JON OSBORNE
CENTRAL REGION ACCOUNT DIRECTOR
PUBLIC SAFETY

Experience Summary

Jon Osborne oversees all aspects of the Nebraska's 9-1-1 accounts, including overall solutioning. He actively participates in implementation tasks including planning development, execution, quality control, customer facing meetings, and account-related documentation. He serves as the overall account director and point of contact for the Public Service Commission and all Public Service Answering Points (PSAPs). Furthermore, Mr. Osborne is a voting board member on the Nebraska 9-1-1 Service System Advisory Committee. Mr. Osborne is a proven Account Director with 17 years of demonstrated of experience and success in management, marketing, and strategic business development. He is a dedicated, energetic, and versatile professional with expansive technical skill set and an advanced degree in educating clients on company services or products, acquiring new accounts, expanding the client base, and ultimately generating higher levels of revenue. Mr. Osborne is a progressive, decisive, innovative professional who is highly valued for expertise interpreting corporate vision and strategy, translating objectives into actionable plans, and providing decisive leadership to multi-functional team members. He leverages eco-centric thinking and relationship building to steer clients towards a mutually beneficial outcome. Articulate and persuasive with exceptional communication and training skills, Mr. Osborne has a strong work ethic and track record of success with a history of developing long-lasting relationships based on a foundation of trust, integrity, and reliability. He has gained deep expertise in public safety networks, 9-1-1 call handling, sales engineering, 9-1-1 technologies, strategic planning, managing complex projects, team building, state budget optimization, and risk management.

Role and Understanding of the Process

Mr. Osborne acts as overlay support to provide state 9-1-1Account Managers who are focused on delivering customer 9-1-1 solutions. He serves as the first point of escalation for any account-related issues. His professional interest ranges from Business Development through Public Safety NG-911 Telecommunications Solution implementation. Mr. Osborne has provided leadership that has raised customer retention levels through effective client management and by delivering effective solutions.

Mr. Osborne engages state and local leadership through establishing CenturyLink C-Level and Director level relationships within multiple market verticals, including a voting board member on the Nebraska 9-1-1 Service System Advisory Committee. He facilitates business development through client acquisition, effective marketing strategies, and by driving sales through consistent follow-up activities. Mr. Osborne cultivates and nurtures relationships with clients to educate them on services or product specifications, including design, features, advantages, and benefits. He works effectively with diverse individuals and delivers outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, Mr. Osborne has focused on deployment of 9-1-1 initiatives and strict adherence to and conformance with customer needs. Mr. Osborne is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master Business Administration, Bellevue University, Bellevue, Nebraska, 2018

Master of Science, Management Information Systems, Bellevue University, Bellevue, Nebraska, 2016

Bachelor of Science, Management, Bellevue University, Bellevue, Nebraska, 2008

Relevant Employment/ Project History

CenturyLink **Omaha, Nebraska** **2017-Present**
Senior Global Relationship Manager / Central Region Director Public Safety

As Senior Global Relationship Manager for Central Region Director Public Safety at CenturyLink, Mr. Osborne is responsible for strategically engaging with state and local leadership through establishing C-Level and Director level relationships within multiple market verticals. Specifically, he solves customer business challenges through technology solutions by understanding customer's business model, funding mechanisms, engaging in creative research and investigation, and aligning challenges to potential technology solutions. Mr. Osborne collaborates with public safety support team to deliver optimal services and experience, effective planning, maintaining engagement during the sales process, and using effective communications. He provides services that targets line of public sector leadership to identify challenges, collaborating with vendors/partners to identify optimal solution for clients, attending and participating in conferences and national work groups APCO/NENA to stay current on technology trends, building adaptive relationships, maintaining a strong ability to consult the customer, and tailoring conversations to their needs. Highlights of Mr. Osborne's key significant accomplishments include the following:

- NENA/APCO National Member
- NENA/NG911 S&BP
- MPLS Network Specifics

Executive Technologies, Inc. **Sioux City, Iowa** **2015-2017**
Director of Sales & Client Services

As Director of Sales & Client Services, Mr. Osborne contributed individually through establishing C-Level and Director level relationships within multiple market verticals. Specifically, Enterprise and Government agencies. He directed corporate sales training, led development, conducted performance reviews, monitored account executives & sales managers progress toward reaching development goals. Mr. Osborne consistently promoted the company's culture of a team-based work environment to elevate sales across business lines and encourage employee and customer retention. He established and adjusted selling prices by monitoring costs, competition, and supply and demand.

Mr. Osborne's significant accomplishments include providing critical input on several key projects. Highlights of his key significant accomplishments include the following:

- Directed the hardware and software sales of teams to meet and/or exceed targeted unit placement and revenue
- Maintained 30% margin in gross profit/net operating income
- Generating $4M in annual revenue

Encartele, Inc. **Omaha, Nebraska** **2013-2015**
Director of Business Development/Director of Sales & Marketing

As Director of Business Development, Mr. Osborne was responsible for providing the company direction of sales and marketing focused on SaaS, CPE, and cloud-based storage. that was specifically focused in Law Enforcement and Public Safety. He determined annual unit and gross-profit plans by implementing marketing strategies and analyzing trends. Mr. Osborne established C-Level and Director level relationships within multiple nationwide law enforcement agencies.

Mr. Osborne's significant accomplishments include several key initiatives which were critical to customer's operations. As the Lead Sales Engineer, Highlights of Mr. Osborne's key significant accomplishments include the following:

- Restructured sales and RFP process resulting in $4.8M in total contract revenue in 18-month time frame
- Increasing sales revenue by 9.5% in 2013; 14.5% in 2014; 15.2% in 2015
- Increased overall revenue by 23.8% during tenure
- Successfully launched new brand via social media outlets and obtained 20,000+ followers

White Lotus Group **Omaha, Nebraska** **2012-2013**
Sales Manager & Marketing

As Sales Manager, Mr. Osborne was responsible for developing and maintaining strong relationships with tier 1 corporate accounts C-Level contacts. His responsibilities include launching and managing market specific CRM, developed marketing and hunting process, built and maintained CRM data base. Mr. Osborne facilitated sales and marketing presentations for prospective clients, evaluated trends within specific markets, and established priorities for focus on revenue generating activities. He directed brand management, Public Relations, media relations, corporate positioning, product launches, advertising, and sales collateral. He also produced media sales kits that demonstrated key marketing analytics and demographics. Highlights of Mr. Osborne's key significant accomplishments include the following:

- Restructured Sales packets resulting in 4.7% quarterly sales
- Implemented Client Relationship Management (CRM) Sales Pro improving sales Funnel
- Restructured RFP and Contract response format cutting down on reply and acceptance timelines

CenturyLink **Omaha, Nebraska** **2002-2012**
Sales & Sales Support Manager

As Sales and Sales Support Manager at CenturyLink, Mr. Osborne functioned as the Manager of Mass Markets Telecommunications Sales and Support Office, Manager of Client Services and National Markets Center for Off-line and Sales Support. His responsibilities included interviewing, developing, training, motivating sales center of 250+ Senior Sales Consultants and 175+ Sales Support Specialists. Highlights of Mr. Osborne's key significant accomplishments include the following:

- Collaborated with cross functional channels to ensure maximum efficiency, productivity, and order accuracy for 45,000+ accounts.
- Successfully coached all teams to maintain 100+% of productivity metrics.

Certifications / Training

- NENA/NG911 S&BP
- Miller Heiman Strategic Selling
- RFP Development
- Contract Interpretation
- MPLS Network Specifics
- Buyer-Seller Relationships
- Train the Trainer
- Fair Hiring Practices
- Prevention of Harassment Policies
- Sales Processes
- Best Practices in Management
- Gaining Sales Commitment
- Qwest 360 Executive Professional Development Program

Professional Memberships / Associations

- Tangier Shriner – Omaha Nebraska
- Waterloo Masonic Lodge – Omaha Nebraska
- Sigma Phi Epsilon National Alumni Board - Omaha Nebraska
- Sigma Phi Epsilon National Alumni Association – Omaha Nebraska

CARLOS SIMMONDS
NATIONAL DIRECTOR, PUBLIC SAFETY

Experience Summary

Carlos Simmonds is a proven Director with 19 years of demonstrated experience in management, marketing, and strategic business development. He is a strategic, results-driven professional who is focused on team leadership, performance analysis, and business management, ensuring profit and sales maximization. Mr. Simmonds is a proven leader at reversing non-performing operations by installing new processes, leading ecosystems, and translating vision into action. Over his career, he has gained deep expertise in sales engineering, strategic planning, overseeing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Simmonds manages and oversees the national CenturyLink Public Safety team and all sales disciplines including revenue projections and conversion of market opportunities to new revenue for the organization. He works with CenturyLink leadership to develop the strategic direction and implement new initiatives. Mr. Simmonds has executed key tasks that led to the inception of an internal group who established and identified the key players in the development of the Public Safety Group at CenturyLink, which provides 9-1-1 service nationally. He engages state and local leadership to strengthen relationships, resolves any type of escalated issue, and develops CenturyLink go-to market strategy, which includes strategic partnering.

Mr. Simmonds is an advocate for CenturyLink's customers and serves as a conduit to facilitate communications between internal and external ecosystem partners for ensuring positive customer experiences, on-time project completions with his programs, and market penetration. Over his career at CenturyLink, Mr. Simmonds has focused on deployments of various 9-1-1 and company strategic initiatives.

Education

Bachelor of Science, Business Administration, University of Phoenix, Phoenix, Arizona, 2011

Relevant Employment/ Project History

CenturyLink **Phoenix, Arizona** **2019-Present**
National Director, Public Safety

As Director in Public Safety at CenturyLink, Mr. Simmonds manages and oversees the national CenturyLink Public Safety team and all sales discipline including revenue projections and conversion of market opportunities to new revenue for the organization. His responsibilities include implementing the company's vision and strategies by maintaining focus on CenturyLink's core values, developing and establishing relationships with industry partners, and conducting weekly staff and ecosystem meetings that focus on project deliverables and overcoming obstacles to ensure both customer and channel success. Highlights of Mr. Simmonds's key significant accomplishments include the following:

- Sponsored and provided the vision and strategic direction for the product development of NG 911 solution for CenturyLink that was first implemented for the State of Arizona
- Executed key tasks that led to the inception of an internal group who established and identified the key players in the development of the new Public Safety Group at CenturyLink, which provides 9-1-1 service nationally

CenturyLink **Phoenix, Arizona** **2015-Present**
Senior Relationship Manager

As Senior Relationship Manager for 9-1-1 Public Safety at CenturyLink, Mr. Simmonds was accountable for developing successful business relationships by actively seeking new business influencers within assigned territory in the Public Safety sector (9-1-1). His responsibilities included targeting line of business leadership to identify

business challenges and cultivate a foundation of trust/partnership, providing guidance and leadership to extended sales support team to ensure CenturyLink's success in the market and overseeing all day to day sales operations. He collaborated and built relationships with vendors and partners. He led CenturyLink's efforts with contract language, design components, integration into the legacy 9-1-1 system, and negotiating discounts with the manufacturers to increase CenturyLink's margin in the NG-911 space. Highlights of Mr. Simmonds's key significant accomplishments include the following:

- Negotiated and received award for NG-911 managed service contract (TCV over $80 million)
- Earned the company COE award 2016-2018. Monthly Recurring Revenue (MRR) attainment 2015- 361%, 2016- 134%, 2017- 593%, 2018- 372%

Integra **Boise, Idaho** **2013-2015**
Government /Education Solutions Manager

As Solutions Manager at Integra, Mr. Simmonds was accountable for developing and growing the Idaho and Eastern Washington markets in the government and education sector through the successful coaching and leadership of direct reports. He developed profitable and long-term relationships with heads of state agencies, school districts, and local municipal governments, and oversaw all day to day sales operations. Highlights of Mr. Simmonds's key significant accomplishments include the following:

- Successful negotiated of statewide purchasing contracts generating over $10 million in new contract revenue
- Earned the company Elev8 award as the #1 Solutions Manager for 4th quarter 2013 and 1st quarter 2014 with blended results of 238% of quota

Frontier Communications **Boise, Idaho** **2012-2013**
Strategic Territory Manager

As Strategic Territory Manager at Frontier Communications, Mr. Simmonds was accountable for meeting and exceeding assigned monthly sales objectives and revenue quotas in the commercial, government, and education sectors. He developed profitable relationships with the various levels of management across the company from the C-Level to IT management. His recognitions include top West Enterprise Sales Executive 1st, 2nd and 3rd quarter 2012 and he earned the company red carpet start award for achieving a 36% quarter over quarter territory growth.

CenturyLink **Boise, Idaho** **2008-2012**
Strategic Account Manager

As Strategic Account Manager at CenturyLink, Mr. Simmonds was accountable for meeting and exceeding assigned monthly sales objectives and revenue quotas in the Enterprise business market groups through the successful management of customer base. He developed profitable relationships with the various levels of management across the company from the C-Level to IT management. Mr., Simmonds was responsible for building and maintaining a sales funnel by hunting for new prospects on a daily basis through telemarketing, knocking on doors, cold calling, working resources such as Chamber of Commerce, Hart Hanks, Hoover's list, vendor contacts and customer referrals. He was accountable for providing outstanding customer service daily as well as development of customer presentations according to their business requirements, trends and emerging technologies. He partnered with new and existing customers through a consultative sales approach in order to better understand their business strategies and needs. He was responsible for the monthly acquisition of 12 new logos. Mr. Simmonds was recognized as Destination Beyond winner 2010 & 2011. 110% club quarterly branch excellence awards (2010-2011) and received Branch recognition for high achievement in sales YTD 149%, retention 195% and blended 192% (2010-2011). Mr. Simmonds also received numerous monthly top MRC branch sales leader awards (2009-2011).

Certifications / Training

The Real ABC's of selling advanced leadership certification

Miller Heiman Conceptual & Strategic Selling certification.

Salesforce certification.

Summit 2 strategic selling certification.

Culture Selling training and certification.

Cisco CSE certification.
Avaya product certifications including AURA, Contact Centers, and Unified Communications.
ShoreTel UC and IP platform certifications.
Mitel product training and partner certifications.

Professional Memberships / Associations

NENA, member since 2013

STEVE DELOACH
SENIOR SALES ENGINEER

Experience Summary

Steve Deloach is a proven Senior Sales Engineer with over 33 years of demonstrated Telecommunications experience in both Telecommunications and Public Safety. Mr. Deloach is a dedicated, energetic, and versatile professional with expansive technical skill set supported by an advanced degree in multiple telecommunication platforms. He has gained deep expertise in sales engineering, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

As Senior Sales Engineer, Mr. Deloach is responsible for design and architecture of world-class Public Safety networking solutions. He is an accomplished Sales Engineer with a unique combination of strong communication and presentations skills along with technical acumen. Mr. Deloach possesses over 35 years of Sales Engineering Management experience in the telecommunications industry and over 20 of those years directly supporting regional and National Public Safety Sales and Engineering teams for a Fortune 500 telecommunications company. He has built a repertoire that is based upon solid experience with CRM, Marketing Automation tools and applications with over 25 years of B2B Sales and Engineering experience. Mr. Deloach has spent the last 18 months working directly with Public Safety Agencies in the State of Nebraska assisting them in solving Public Safety 9-1-1 Equipment and Network Challenges utilizing the vast portfolio of solutions offered by CenturyLink. He has intimate knowledge of the design and implementation of a Next Generation 9-1-1 (NG 911) Solution on a Statewide basis and has met with several customers in the State to discuss the requirements of designing and implementing NG-911. Mr. Deloach completely understands the Network Design/Call Delivery (ESINet), Call Routing/Processing (NGCS) and all the backend touchpoints required for the successful implementation of a Statewide ESInet. He attends Public Safety Conferences and stays abreast of NENA Standards for NG-911to ensure the solutions CenturyLink offer and deploy meet and exceed NENA and Customers expectations and standards. Mr. Deloach is passionate about Public Safety and Emergency Communications and have worked in the Public Safety technology field for over 20 years engineering solutions utilizing and integrating wireless or wireline networks to enhance the delivery of Public Safety Services by our First Responders.

Mr. Deloach is an articulate communicator who works effectively with customers and delivers outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, he focuses on initiatives and strict adherence to and conformance with customer needs. Mr. Deloach is a skilled communicator who broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master Business Administration, University of Phoenix, Cary, NC

Bachelor of Arts, Computer Science, University of North Carolina at Charlotte, Charlotte, NC

Relevant Employment/ Project History

CenturyLink **Rocky Mount, NC** **2014-Present**
Senior Sales Engineer

As Sales Engineering Manager at CenturyLink, Mr. Deloach is responsible for designing and engineering Public Safety Solutions for Government customers in NC, TN, VA, PA, NJ, NE, IA. His responsibilities include project coordination, gross margin analysis, pricing, customer presentations, technical support and design of complex 9-1-1 Network (NG-911) and CPE solutions. Mr. Deloach works closely with Product and Marketing organizations and Vendors to ensure that CenturyLink solutions exceeded customers and company's expectations.

Mr. Deloach's significant accomplishments include providing critical input on several key projects that supported 9-1-1 Network (NG-911) and CPE solutions. Highlights of Mr. Deloach's key significant accomplishments include the following:

- Design of Backup Network for Public Safety Critical Solutions
- Designed and Implemented Largest Call Handling Equipment Solutions in PA
- Implemented 1st Clustered Call Handling Solution within CenturyLink

SPRINT **Cary, NC** **2008-2014**
Manager – Solutions Engineer

As Manager and Solutions Engineer at SPRINT, Mr. Deloach was responsible for leading a team of Solutions Engineers with technical expertise supporting Wireline and Wireless solutions for all market segments in Eastern NC and Southern Virginia. His primary objective was to coordinate and manage activities and efforts to ensure that all assigned area and regional sales revenue objectives were met. His job responsibilities included managing a team of 7 Solutions Engineers that provided pre-sales design and technical support to the Sales Organization and Customers for MPLS, Dedicated IP, SIP trunking, IaaS, SaaS, UCaaS, Managed Network Services, Customer Premise Equipment (CPE) and wireless devices, solutions and applications. Highlights of Mr. Deloach's key significant accomplishments include the following:

- Nominated- Public Sector SE Manager of the Year
- Led a Group of Engineers that assisted in the generating of over $100M in annual revenues

SPRINT NEXTEL **Cary, NC** **2005-2008**
Manager – Solutions Engineer, Public Sector

As Manager and Solutions Engineer at SPRINT, Mr. Deloach was responsible for leading a team of Solutions Engineers with technical expertise covering SPRINT NEXTEL Wireless products and services for customers in the Public Sector Market Segments in NC/SC/TN/AL/MS/AR/LA/GA. Mr. Deloach's primary objective was to coordinate and manage activities and efforts to ensure that all assigned area and regional sales revenue objectives were met. He managed a team of 8 Solutions Engineers that provided pre-sales design and technical support to the Sales Organization and Customers for wireless devices, solutions and applications. Highlights of Mr. Deloach's key significant accomplishments include the following:

- Led a Group of Engineers that assisted in the generating of over $75M in annual revenues

SPRINT **Tarboro, NC** **2008-2014**
Manager – Technical Solutions Sales

As Manager at SPRINT, Mr. Deloach was responsible for Public Safety National Sales and Engineering Support for CPE and Network products and services. He oversaw the engineering, design and pricing of CPE and Network Public Safety solutions to customers in the Business Sales In- Franchise markets. He managed a team of Sales Engineers who were responsible for end to end Public Safety solutions including pre-sales support for CPE, long distance, PCS and network/database opportunities. He managed a group of 22 Network/Database/CPE Engineers covering 13 States. Highlights of Mr. Deloach's key significant accomplishments include the following:

- Generated over $50M in 9-1-1 Non-Regulated and Regulated sales revenue
- Outstanding SE Manager of the Year Award

SPRINT **Tarboro, NC** **2008-2014**
General Manager – Sales and Service

As General Manager of Sales and Service at SPRINT, Mr. Deloach was responsible for the sales and engineering of Non-Regulated Public Safety products and services in the Mid-Atlantic Region. He managed three E911 Engineers and six E911 Account Executives, one Sales Assistant, and one E911 Area Manager. He managed a team that was dedicated to engineering and selling Public Safety integrated 9-1-1 solutions. Mr. Deloach participated in technical sales presentations to prospective clients for both 9-1-1 CPE and Network technologies and solutions. He also provided consultation for strategic approaches to RFP's and RFI's. Highlights of Mr. Deloach's key significant accomplishments include the following:

- Generated over $11M in CPE sales for Sprint National Public Safety

Certifications / Training

Solution Selling Workshops
Leadership Development Seminars
NG-911Conferences
Advanced 9-1-1 CPE Design and Implementation Training
Learning to Lead Seminars
Kenan Flagler Executive Leadership Training

Professional Memberships / Associations

NC911 Board Member
Credit Union Board Member
Team Excellence Award
IP Telephony Strategy Migration Team Member
SpinCo Integration Team Member
Presidents /Masters Club
Who's Who Among College Students
Member of Kappa Alpha Psi Fraternity
Nominated- Public Sector SE Manager of the Year

STEVEN KLOCEK
SENIOR SALES ENGINEER

Experience Summary

Steven Klocek is a proven Senior Sales Engineering Manager with 36 years of demonstrated Telecommunications experience. Mr. Klocek is dedicated primarily to the support of large business and government customers. He demonstrated strong performance in delivering Next Generation 9-1-1 systems, Sales, Design Engineering, Project Management and Customer Service through leadership, teamwork and personal attention to quality. He managed large complex projects, SME CenturyLink Next Generation 9-1-1 Network, bid proposals, Staff, offices and operations, all with a focus on helping customers achieve their business objectives.

Role and Understanding of the Process

Mr. Klocek is responsible for design and architecture of world-class networking solutions. Mr. Klocek provided technical consulting Sales Engineering teams who are focused on the technical aspects of the solution. Mr. Klocek has provided technical leadership on a range of projects that raised customer retention levels while reducing maintenance costs. He has been a sound resource for providing direction on technical aspects of solutions on various E911 projects. He has provided critical design and development support on Next Generation E911 solutions and provides customer service support for the Public Service Answering Points (PSAP's) in Minnesota, South Dakota & North Dakota. Mr. Klocek is an articulate communicator who works effectively with diverse individuals and delivers outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, Mr. Klocek has demonstrated a keen focus on deployment of E911 initiatives and strict adherence to and conformance with customer needs. Mr. Klocek is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Associate in Computer Maintenance, Mankato Area Vocational Technical Institute (MAVTI) Mankato, MN 1983

- Basic and Digital Electronics. Specialized Study Computer Maintenance & Programming.
- Use of Electronic Test Equipment.

US WEST Communications Inc. Learning Systems, Minneapolis, MN

- Quality Process Management 4/97
- Success Principles for Project Management 7/96
- Kepner/Tregoe Project Management, 12/94
- Microsoft Project 4.0 for Windows, 10/94

Relevant Employment/ Project History

CenturyLink **Minneapolis, Minnesota** **2011-Present**

Senior Sales Engineering-Solution Architecture Team – 9-1-1 Public Safety

As Senior Sales Engineering Manager for 9-1-1 Public Safety at CenturyLink, Mr. Klocek provides Professional System Engineering and direction to CenturyLink Sales department on products and services for Government & Education clients. His primary focus is on E911 CPE and Network. Mr. Klocek's responsibilities include providing customer service for the Public Service Answering Points (PSAP's) in Minnesota, South Dakota & North Dakota as well as designing and pricing CenturyLink products for specific for customer applications, communication plans, project status meetings and written recommendations along with customer presentations. Mr. Klocek has gained a deep knowledge based upon his experienced in Next Generation E911 Network, 9-1-1 Hosting Platforms, LAN, WAN, VOIP, Positron, Plant/Cassidian, E911, Nortel, Avaya, NEC, Adtran, DS0, DS1, DS3, SHARP & SHNS, CPE and Video networks. Highlights of Mr. Klocek 's key significant accomplishments include the following:

- Developed National Programs for CenturyLink E911 Services which dictated the method by which CenturyLink standardizes the installation of Next Generation E911 CPE equipment, Pricing and Installation

standards from pre-sale to post sale, and incorporated all documents into a listed CenturyLink Technical Publication

- Functioned as a Qwest Next Generation Emergency 9-1-1 Subject Matter Expert for Minnesota State-Wide NextGen 9-1-1 Platform RFP and the ND State-Wide NextGen 9-1-1 Platform for ND, which both were awarded to Qwest

BAILIWICK DATA SYSTEMS **Eden Prairie, Minnesota** **2002-2006**
Manager, Engineered Design and Development

As Manager at Bailiwick Data Systems, Mr. Klocek provided Program Development, System Engineering and direction to support Sales and Operations of Bailiwick products and services for clients. He responsibilities included designing and pricing of Bailiwick products specific for customer applications, communication plans, project status meetings and written documentation along with customer presentations. Highlights of Mr. Klocek 's key significant accomplishments include the following:

- Developed a deployment design using Computer Aided Design Software (CAD) to realize an overlay of a Big Box store, which standardized the overlay of the store and placed the proper amount of voice/data locations in the proper departments; the overlay worked very well for receiving bids as well as release for the installers to deploy and resulted in significant savings by streamlining the process

QWEST Global National Sales **Minneapolis, Minnesota** **1998-2002**
System Engineer III

As System Engineer at QWEST, Mr. Klocek provided System Engineering support and direction to Qwest's Sales department on Qwest products and services for global clients. His job functions included supporting design and pricing of Qwest products specific for customer applications, communication plans, project status meetings and written recommendations along with customer presentations. Through performing his duties, Mr. Klocek built a deep repertoire of experience in LAN, WAN, VOIP, Positron, Plant, E911, Nortel, Avaya, NEC, DS0, DS1, DS3, SHARP & SHNS, CPE and Video networks. Highlights of Mr. Klocek's key significant accomplishments include the following:

- Special Project to protect our network and PSAP's in a preparation for Y2K time clock changes.
- Managed a 3-year project to deploy the new Campus at ADC Telecommunications, included underground plant, physical layer fiber and copper facilities and wireless communications.

US West Professional & Technical Services **Minneapolis, Minnesota** **1994-1998**
Project Manager

As Project Manager at QWEST, Mr. Klocek provide Project Management, leadership and direction to Sales of U S West products and services for Sales and Carrier clients. His responsibilities included coordinating internal U S West departments, external clients and subcontractor organizations. Highlights of Mr. Klocek's key significant accomplishments include the following:

- Managed significant installations that included major hospitals and colleges in several states

U S West Official Company Services **Minneapolis, Minnesota** **1983-1994**
Assistant Area Manager

As Assistance Area Manager at US West, Mr. Klocek managed 15 field technicians, 4 Supply Room Attendants and 3 Data Specialist, employed in multiple states. Supervisor of installation and maintenance crews for complex US West company services. He also coordinated service for Internal U S West Customers for Minnesota & North Dakota's base for Customer Premise Equipment & Data Network Services. His job functions included the coordination of internal U S West departments, external clients and subcontractor organizations. He also provided support for developing design and pricing of Qwest products specific for customer applications, communication plans, project status meetings and written recommendations along with customer presentations. Highlights of Mr. Klocek 's key significant accomplishments include the following:

- Designed and developed the project base line for building U S West Mega Centers in MN and CO. Mega Centers were monitoring centers for repair tickets, workload planning, new construction routes and climate monitoring to plan for store damage throughout the United States

Certifications / Training

Motorola E911 product training, 8/2018
Intrado E911 product training, 5/2018
Cassidian Sales Engineering 9-1-1 Certification on E911 product, 8/2014
SAVIS Cloud training, 2014
Cassidian Sales Engineering 9-1-1 Certification on E911 product, 2/2012
Adtran Sales Engineering Certification on E911 product, 7/2010
Plant/CML Sales Engineering Certification on E911 product, 9/2010
Nortel VoIP/BCM Training Certification, 2/07
Anoka- Ramsey Community College. Anoka, MN. Cisco Certified Design Associate (CCDA), 12/01
BICSI, Tampa FL. Designing Telecommunications Systems, 12/99

Professional Memberships / Associations

Minnesota Ducks Unlimited – Zone Chairman, 2005 to present.
Carver County Ducks Unlimited - Chairman, 1992 to 2005.
Project Management Institute - Member 1997 to 2004
Carver County Ducks Unlimited - Committee Member, 1988 to 1992

MS. CATHY ATKIN
SENIOR SALES ENGINEER – PUBLIC SAFETY 9-1-1

Experience Summary

Ms. Cathy Atkin is a proven Senior Sales Engineer with 45 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. Ms. Atkin is a dedicated, energetic, and versatile professional with expansive technical skill set, advanced degree and certifications in multiple 9-1-1 telecommunication platforms including 9-1-1 Call Handling Equipment designs, Data Center and Cloud designs, Enterprise Network WAN/LAN management. She has gained deep expertise in sales engineering, 9-1-1 technologies, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

As Senior Sales Engineer at CenturyLink, Ms. Atkin manages Sales Engineers who are focused on the technical aspects of the solution. She serves as first point of escalation for any design-related issues. She holds several certifications, which include VMWare, Cisco CCNA/CCDA, and Cyber-Security Solutions. Ms. Atkin has provided input into NENA standards, engineering designs, and solutions to Public Safety over 45 years. She has provided expertise on the evolution of Public Safety solutions throughout her career and technical leadership on a range of projects that raised customer retention levels while reducing overall costs. She has performed installations, configurations, and special services "grooming" 9-1-1 Public Safety Network and Call Handling solutions. Ms. Atkin designed and implemented Next Generation solutions several States including Arizona, Minnesota, Colorado, Washington, South Dakota and Utah. She has designed, installed, and maintained internal databases, systems and Public Safety systems. Ms. Atkin holds several product certifications that include Cisco, Avaya, Mitel, Vesta, and Viper. She is an articulate communicator who works effectively with diverse individuals and delivers outstanding customer service through consistent, on-time, and on-budget project delivery. Over her career at CenturyLink, Ms. Atkin focuses on deployment of NG-911 initiatives and strict adherence to and conformance with customer requirements. Ms. Atkin is a skilled communicator as she broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Degree, Computer Engineering, University of Phoenix, Tucson Arizona, January 1994

Relevant Employment/ Project History

CenturyLink **Salt Lake City, Utah and Tucson, Arizona** **1990-Present**
Senior Sales Engineering – 9-1-1 Public Safety, Government and Federal Services

As a Senior Sales Engineer for 9-1-1 Public Safety at CenturyLink, Ms. Atkin is responsible for developing and delivering NG-911 Core, ESInet and I3 solutions for our NG-911 Managed solutions. Her responsibilities include identifying customer business requirements and developing solutions that addressed customer needs with a focus on engineering designs and solution selling. Ms. Atkin analyzes NG-911 and Public Safety Call Center Operations to determine best practice applications and designs. She delivers solution presentations that encourage customer collaboration. She spearheads network security resource requisitioning, installation, configuration, and monitoring. Ms. Atkin develops and documents new system configurations, processes, security, maintenance, backup, and reporting procedures for effective record keeping. Ms. Atkin delivers technical training to associates and customers to promote proper system configuration and designs. She promotes a productive collaboration environment through interfacing with vendors, such as CAD, Radio and Logging providers, 9-1-1 stakeholders, and project teams to drive solution development and testing. She prepares reports to track service issues, customer support business cases, and communicate project costs and status to both the customer (PSAP/State) and Public Safety teams.

Ms. Atkin's significant accomplishments include the successful deployment of several key 9-1-1 systems which were critical to customer's operations. As the Lead Sales Engineer, Ms. Atkin led the development and

implementation multi-million-dollar 9-1-1 delivery systems. Highlights of Ms. Atkin's key significant accomplishments include the following:

- Collaborated with Product Management and 9-1-1 vendors to create new NG-911 Managed Services offering for both the State of Arizona and 9-1-1 Public Safety in Arizona that can be deployed throughout the CenturyLink US wide territories
- Deployed Statewide MPLS deployment for State of NM 9-1-1 system which includes managed IQ Data Bundle, Network Based Security, and Co-location
- Assisted with the State of Arizona (AZnet) Managed Services deployment which accomplished over 770 sites Cisco, Juniper, MPLS and statewide migration
- Created focus teams with individual contributors to improve internal processes and build new public safety product offerings, including new 9-1-1 Public Safety managed services and onboarding new vendor partners
- Capitalized on the many diverse skills of direct reports to deliver customer solutions resulting in over 100% revenue goals attainment and customer satisfaction
- Established clear and concise individual and team goals, significantly increasing the quality of engineering designs, customer design, and public safety team morale
- Directed Tucson Police Department's Plant CML, Vesta, and Nortel Meridian ACD project as Technical Project Leader; resolved challenging Nortel design flaws to meet customer's system acceptance requirements.
- Played integral role in planning, design, and implementation of Enterprise Mapping and Enterprise Magic for nine Pima County E9-1-1 call centers; equipped multiple call centers with full suite of systems, including telecommunication platforms, servers, workstations, CTI applications, databases, GIS mapping applications, and voice and data networks

Certifications / Training

Cisco CCNA/CCDA

VMWare, Juniper- JNCIP-SEC

CenturyLink Sales Academy

Security DDOS and others

Professional Memberships / Associations

Arizona Women in Engineering Support Group, 2000

Project Management Institute, Member, 1994

NANCY C. SERAFINO
SENIOR SALES ENGINEER

Experience Summary

Nancy C. Serafino possesses 25 years of experience at CenturyLink serving 9-1-1 customers. She is a proven Sales Engineer with 32 years of demonstrated 9-1-1 systems development management experience, in both the commercial and State and Local Government environments. She has demonstrated client engagement leadership and change management results, effecting multi-million dollars in annual cost reductions and in hard benefits. Her expertise ranges from overseeing the implementation of E911 solutions to providing customer service and client facing. Ms. Serafino proven experience in strategic management and keen sense for completing implementations of E911 technology, systems integration, and business processes has gained her recognition with her customers and within CenturyLink.

Responsibility and Understanding of the Process

Ms. Serafino is responsible for the design and architecture of world-class networking solutions. Ms. Serafino is certified as a certified Emergency Number Professional (ENP) and has served on the Ohio State 9-1-1 Technical Advisory Committee for over 5 years. As Senior Sales Engineer, she effectively interfaces with various customers to provide 9-1-1 systems throughout the USA, including at the State level. As a proven leader, Ms. Serafino builds consensus, effects change, and delivers with consistent results on delivering E911 implementation projects. She served on the original ESINet Steering Committee for the States of Ohio and Pennsylvania as appointment by the Governors of these States. Real experience, such as this, has deepened Ms. Serafino's understanding of the importance of Nebraska's mission to implement their State-wide 9-1-1 system with next generation network capabilities that are necessary to save lives.

Ms. Serafino possesses over 25 years of Sales Engineering Management experience in the telecommunications industry and over 20 of those years directly supporting regional and national Public Safety Sales and Engineering teams for a Fortune 500 telecommunications company. Over her entire 34-year career at CenturyLink, Ms. Serafino has gained a deep knowledge of implementing 9-1-1 initiatives with strict adherence to and conformance with commercial and State and Local Government requirements. Ms. Serafino is an articulate communicator who works effectively with customers and delivers outstanding customer service through consistent, on-time, and on-budget project delivery. As a senior staff member, Ms. Serafino effectively achieves objectives by broadly communicating initiatives, receiving affirmation, and implementing plans across the entire program to achieve customer and end-user goals. As a senior staff member working at CenturyLink, she continues to augment her sound foundation in implementing and deploying 9-1-1 systems and develop her passion as a Senior Sales Engineer at CenturyLink.

Education

Bachelor of Science, Youngstown State University, 1988

Relevant Employment/ Project History

CenturyLink **Mansfield, Ohio** **1988-Present**
Senior Sales Engineer

As Senior Sales Engineer at CenturyLink, Ms. Serafino is responsible for overseeing development of 9-1-1 solutions. Her responsibilities and duties include managing implementation teams to ensure requirements are met; supporting the CenturyLink's Sales Organization and customers in configuring 9-1-1 solutions based on customer requests and State RFPs; and supporting implementations, configuring solutions, and selling legacy 9-1-1 systems until the transition to NG-911 systems. She also conducts training for Customer Service Managers (CSMs) and implementation team members; scheduling and tracking implementation teams progress while monitoring and reporting progress, roadblocks, and risks to stakeholders. She provides leadership through functioning as a liaison between clients and internal and external project team members to ensure cohesion and enhances team collaboration.

Ms. Serafino's significant accomplishments include providing critical oversight and team management that led to the delivery of several E911 solutions. Ms. Serafino's deep understanding the State of Nebraska's objective was gained from her experience in managing a year-long transition for the State of Indiana to their selected NG911 state-wide solution as a Project Manager who coordinated tasks, set agenda and schedules to implement network, and billing for E911 systems.

Sales Engineer

As Sales Engineer, Ms. Serafino performed various duties as a Regional Subject Matter Expert. Her responsibilities included generating and retaining E911 revenue by supporting CenturyLink's E911 Sales organization. Ms. Serafino technical contributions on E911 projects included developing and delivering solutions and quotes for CPE and Network buildouts. She also drafted, prepared, and delivered effective customer focused solutions presentations and demonstrations that were critical for communication project statuses.

Customer Service Operations E911 Area Manager

As E911 Area Manager, Ms. Serafino functioned as the primary interface for E911 PSAP Customers, Country and State agencies, and external stakeholders for Ohio, Pennsylvania, and New Jersey. Her responsibilities included managing major network configurations, overseeing delivery of 911 solutions, and functioning as the primary interface for internal CenturyLink departments during project execution. Ms. Serafino's significant accomplishments include providing oversight and management of development activities over several project implementation lifecycles. Ms. Serafino received an award by the State of Ohio for providing effective custom service to the State for coordinating PSAP vendor activities.

Certifications / Training

Emergency Number Professional (ENP)

Professional Memberships / Associations

Ohio Technical Advisory Committee, member

National Emergency Number Association (NENA), member

Ohio Telephone Association (OTA), member

STEPHEN E. DOYLE
MANAGER SALES ENGINEERING – SPECIALIZED SALE

Experience Summary

Stephen E. Doyle is a proven Sales Engineering Manager with 41 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. Mr. Doyle is a dedicated, energetic, and versatile professional with expansive technical skill set, advanced degree and certifications in multiple 9-1-1 telecommunication platforms and WAN/LAN management. He has gained deep expertise in sales engineering, 9-1-1 technologies, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Doyle manages Sales Engineers who are focused on the technical aspects of the solution. He serves as first point of escalation for any design-related issues. He holds several product certifications. Mr. Doyle has provided technical leadership on range of projects that raised customer retention levels while reducing maintenance costs. He has performed installations, configurations, and special services "grooming" of Digital Loop Carrier (DLC) systems. He has also installed and maintained telephony high-voltage protection equipment in power generating plants and similar tech-heavy environments.

His deep understanding of the process and the State of Nebraska's 9-1-1 mission is demonstrated in the experience he has gained over his career. Mr. Doyle architected the Arizona Next Generation 9-1-1 (NG-911) managed services solution which included NG-911 cores services and managed emergency call handling equipment, employing Vesta and Viper. The Arizona NG-911 solution was designed to meet the financial constraints and provide next generation capabilities using an Operating Expense (OPEX) model to deploy NG core services within budget. He collaborated with the State of Arizona 9-1-1 emergency office and State-hired consultants to develop mission critical requirements and specifications CenturyLink implemented and deployed the NG9-1-1 solution that exceeded customer expectations. He led his solution architect team in designing and developing a new NG9-1-1 cores services ESINet solution for California Office of Emergency Services (CALOES), resulting in CenturyLink being selected as one of four Regional Network Service Provider (RNSPs) for the Southern California region.

Mr. Doyle is skilled and an articulate communicator who works effectively with customers and delivers outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, Mr. Doyle's keen focus on deployment of 9-1-1 initiatives and strict adherence to and conformance with customer needs.

Education

Master of Science, Information Management, University of Phoenix, Tucson AZ, 2006

Bachelor of Science, Business Information Systems, University of Phoenix, Tucson, AZ, 2004

Relevant Employment/ Project History

CenturyLink **Tucson, Arizona** **2017-Present**
Sales Engineering-9-1-1Public Safety, GES/Manager

As Sales Engineering Manager for 9-1-1 Public Safety at CenturyLink, Mr. Doyle is responsible for managing the CenturyLink's centralized National 9-1-1 Public Safety Sales Engineering team. His responsibilities include focusing on leveraging individual expertise to distribute workloads, establish best practices, collaborate with product management to drive 9-1-1 product offerings, and improve the customer experience. Worked with internal and external partners) all business processes and procedures.

Mr. Doyle's significant accomplishments include providing critical input on several key projects that supported Arizona's Emergency Communications Services development lifecycles. Highlights of Mr. Doyle's key significant accomplishments include the following:

- Deployed Arizona's NG-911 solution through a collaboration with the State of Ariziona 9-1-1 office and State-hired consultants to develop mission critical requirements and specs that exceeded customer expectations.
- Designed, developed, and deployed solutions that met the customer financial constraints to provide NG capabilities using Operating Expense (OPEX) model and within budget.
- Created focus teams with individual contributors to improve internal processes and build new public safety product offerings, including new 9-1-1 Public Safety managed services and onboarding new vendor partners
- Capitalized on the many diverse skills of direct reports to deliver customer solutions resulting in over 100% revenue goals attainment
- Established clear and concise individual and team goals, significantly increasing the quality of engineering designs, customer wins, and team morale

CenturyLink **Tucson, Arizona** **2010-2017**
Sales Engineering-9-1-1Public Safety, GES/Lead Sales Engineer

As Lead Sales Engineer for 9-1-1Public Safety at CenturyLink, Mr. Doyle was responsible for developing and delivering E911Managed Service and GES solutions. His responsibilities include identifying customer business requirements and developing solutions that addressed customer needs with a focus on solution selling. Mr. Doyle analyzed E911and GES call center operations to determine requirements. He also collaborated interactively through solution presentations. He spearheaded network security resource requisitioning, installation, configuration, and monitoring. Mr. Doyle developed and documented new system configurations, maintenance, backup, and reporting procedures for effective record keeping. He delivered technical training to associates and customers to promote proper system usage. He promoted a productive environment through interfacing with vendors and project teams to drive solution development and testing, while preparing reports to track service issues, support business cases, and communicate project costs and status to senior management.

Mr. Doyle's significant accomplishments include the successful deployment of several key 9-1-1systems which were critical to customer's operations. As the Lead Sales Engineer, Mr. Doyle led the development and implementation multi-million-dollar 9-1-1delivery systems. Highlights of Mr. Doyle's key significant accomplishments include the following:

- Collaborated with Product Management and 9-1-1vendors to create new NG-911Managed Services offering for Arizona that can be deployed throughout the CenturyLink territories
- Deployed Statewide MPLS deployment for State of NM 9-1-1system which includes managed IQ Data Bundle, Network Based Security, and Co-location
- Assisted with the Tucson Unified School District deployment which accomplished a 110 sites Avaya CS1000 migration

CenturyLink **Tucson, Arizona** **2002-2010**
Tier II Technical Support Specialist

As Tier II Technical Support Specialist for Arizona Emergency Communication Services, Mr. Doyle participated in all phases of various project life cycles from design through delivery and ongoing maintenance. He designed, installed, and maintained complex telecommunication and data network platforms, which included PBX, VM (Voice Mail), computer telephony integrated systems (CTI), databases, advanced Geographical Information Systems (GIS) applications, TCP / IP networks, Cisco routers and firewalls, frame relay circuits, T1 (DS1), ISDN, and various DSO-type circuits and carrier platforms. His responsibilities include providing input regarding support functions that was included all business processes and procedures.

Mr. Doyle's significant accomplishments include providing critical input on several key projects that supported Arizona's Emergency Communications Services development lifecycles. Highlights of Mr. Doyle's key significant accomplishments include the following:

- Directed Tucson Police Department's Plant CML, Vesta, and Nortel Meridian ACD project as Technical Project Leader; resolved challenging Nortel design flaws to meet customer's system acceptance requirements.

- Played integral role in planning, design, and implementation of Enterprise Mapping and Enterprise Magic for nine Pima County E9-1-1call centers; equipped multiple call centers with full suite of systems, including telecommunication platforms, servers, workstations, CTI applications, databases, GIS mapping applications, and voice and data networks.
- Designed and implemented enhanced functionality that eased management of 9-1-1emergency calls by increasing efficiency and accuracy of transfers.

Certifications / Training

Vesta
Viper

Professional Memberships / Associations

National Emergency Number Association (NENA), member 2005
Association Public-Safety Communications Official (APCO), member 2005

JOHN ROBERT SHUTTLEWORTH
SENIOR DIRECTOR – SALES ENGINEERING & SOLUTIONS ARCHITECTURE

Experience Summary

Mr. John Shuttleworth is a proven Sales Engineering Director with 38 years of demonstrated Telecommunications experience in both Federal and State Government and Education Services support. Mr. Shuttleworth is a dedicated, energetic, and versatile professional with expansive technical skill set including Management and networking in both the wireline and wireless industries. He has gained deep expertise in Pre-Sales Engineering, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

As Senior Director – Sales Engineering and Solutions Architecture at CenturyLink, Mr. Shuttleworth manages Sales Engineers and Solutions Architects who are focused on the technical aspects of the solution. He reports directly to the Senior Vice President of CenturyLink's Public Sector Government focused vertical. Mr. Shuttleworth has provided technical leadership over multiple teams that support the Department of Defense, Civilian Agencies, Special Programs and Government related systems integrators. He has covered a range of projects in both the wireline and wireless technologies. He has built technical teams in support of complex technical solutions and works to align skillsets and resources effectively. Mr. Shuttleworth is an articulate communicator who works effectively with diverse individuals and delivers outstanding customer service through consistent communications and team management. Over his career at CenturyLink, Mr. Shuttleworth has focused on Network Development, the design of complex networks with strict adherence to and conformance with customer needs. Mr. Shuttleworth is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Bachelor of Science, Business Management, Indiana University of Pennsylvania, Indiana, PA - 1980

Relevant Employment/ Project History

CenturyLink **Herndon, Virginia** **2017-Present**
Senior Director/Director – Sales Engineering & Solutions Architecture

As Senior Director for Sales Engineering and Solutions Architecture at CenturyLink, Mr. Shuttleworth is responsible for managing the CenturyLink's Pre-Sales Engineering and Solutions Architecture teams. His responsibilities include managing 130 pre-sales engineers and solutions architects supporting Public Sector customers. Mr. Shuttleworth's team is responsible for ensuring compliant solutions for tactical product requirements as well as complex technical solutions.

Mr. Shuttleworth's significant accomplishments include leading technical teams and driving solutions in support of CenturyLink's major Public Sector contracts including, but not limited to:

- The General Services Administration's Enterprise Infrastructure Services (EIS) Contract.
- Multiple contracts in support of the Department of Defense.
- Multiple contracts in support of the Intelligence Community.

Mr. Shuttleworth's team consists of 11 Sales Engineering Managers reporting directly to him who focus on the individual Public Sector verticals in Public Safety, State and Local, Dept of Defense, Civilian and the IC.

- Combined the former CenturyLink and Level 3 Communications Pre-Sales Federal Government Technical teams as a result of the acquisition of Level 3 by CenturyLink to create the current team of 130 Sales Engineering professionals.
- Optimized diverse skills of the team to ensure delivery of complex technical solutions.

- Works with Product Management, Service Delivery and Program Management to ensure appropriate handoffs to internal Corporate ecosystem.
- Work with Government agencies and Government focused customers to transform networks and technical requirements.
- Ensure technical compliance with customer requirements.
- Continues to develop team talent and ensure alignment of appropriate technical resources.

Level 3 Communications (now CenturyLink) **Herndon and McLean, Virginia** **2009-2017**
Director/Manager - *Sales Engineering*

As Director for the former Level 3 Communications, Mr. Shuttleworth led a team of Pre-Sales Engineers and Solutions Architects. He also collaborated interactively through solution presentations. He spearheaded network security resource requisitioning, installation, configuration, and monitoring. Mr. Shuttleworth developed and documented new system configurations, maintenance, backup, and reporting procedures for effective record keeping. He delivered technical training to associates and customers to promote proper system usage. He promoted a productive environment through interfacing with vendors and project teams to drive solution development and testing, while preparing reports to track service issues, support business cases, and communicate project costs and status to senior management.

Level 3 Communications **Herndon and McLean, Virginia** **2002-2009**
Sales Engineer

As a Sales Engineer, Mr. Shuttleworth closely aligned and collaborated with his Sales counterpart to develop technical solutions serving customer needs and requirements. His key technical accomplishments during this time were leading and supporting a mission critical technical solution for a DoD dark fiber network and a mission critical network that required significant backup and redundancy.

Level 3 Communications **McLean, Virginia** **1998-2002**
Network Developer

As a Network Developer, Mr. Shuttleworth was responsible for planning new networks in specified markets including fiber optic cable route planning and technical facility selection within the markets. This included close coordination with the Sales, Construction, and Operations teams to ensure maximum market penetration and opportunity benefits. Mr. Shuttleworth worked with the Finance team to ensure appropriate cost management throughout Planning and Construction.

Certifications / Training

None

Professional Memberships / Associations

None

CAROLINE BUSSELL
CLIENT SUPPORT MANAGER

Experience Summary

Caroline Bussell is a proven Client Support Manager (CSM) with 3 years of demonstrated Telecommunications back office support expertise in both Global Enterprise Customers and Government and Education Services support. Ms. Bussell is a dedicated, energetic, and versatile professional with expansive technical skill set and degree. She has gained deep expertise in personnel management, customer service, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Ms. Bussell is responsible for supporting Sales Account Managers within Iowa and Nebraska territories. She performs retention management of customer contracts, executes move order changes, serves as customer advocate for billing issues, and handles lifecycle management needs. Ms. Bussell supports the Nebraska Account Manager through resolving billing and invoicing disputes and performing move order changes. Her responsibilities include responding to billing inquiries, resolving billing disputes, pulling internal reporting, aiding with supporting customers, and assisting her team with order processing group to minimize billing errors.

Ms. Bussell is an articulate communicator who works effectively with customers and delivers outstanding customer service. Over her career at CenturyLink, Ms. Bussell's is focused on strict adherence to and conformance with customer needs. Ms. Bussell is a skilled communicator as she broadly communicates her initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Bachelor of Art, Liberal Studies with minor in Telecommunications and Sociology, Indiana University, Bloomington, IN, 2017

Relevant Employment/ Project History

CenturyLink **Chicago, Illinois** **2019-Present**
Client Support Manager

As Client Support Manager at CenturyLink, Ms. Bussell proactively serves as customer advocate and handles lifecycle management needs for over 200 accounts. Her responsibilities include serving as a liaison to my customers and between all internal business groups, working to identify and resolve any/all issues, devising and implementing customer retention and revenue growth plans, and coordinating monthly and quarterly business reviews and customer contact evaluations.

CenturyLink **Charlotte, North Carolina** **2018-2019**
Account Manager

As Account Manager at CenturyLink, Ms. Bussell built and managed customer relationships by identifying and qualifying their business needs and provided them with network solutions that meet their criteria utilizing CenturyLink's ecosystem effectively. She gained deep understanding of internal systems and effectively utilized go-forward products and platforms to perform daily tasks of a sales professional. The understanding she gained assisted her with augmenting the customer experience with CenturyLink services.

CenturyLink **Indianapolis, Indiana** **2017-2011**
Logistics Account Executive

As Logistics Account Executive, Ms. Bussell was responsible for coordinating all shipping needs necessary for each client by finding a reliable carrier and eliminated fall out by maintaining strong communication with the drivers. She successfully networked and developed strong relationships with both customers and

carriers and effectively negotiated profitable rates with both the shipper and the carrier through independent research and kept up to date with changing lane rates. She functioned as the single point of contact for customers and carriers to efficiently solve daily problems.

Certifications / Training

Sales Academy College Connect
Social Selling Index Achievement

Professional Memberships / Associations

None

MARY ANDERSON
MANAGER BASE MANAGEMENT

Experience Summary

Mary Anderson is a proven Manager with 15 years of demonstrated Telecommunications back office support expertise in both Global Enterprise Customers and Government and Education Services support. Ms. Anderson is a dedicated, energetic, and versatile professional with expansive technical skill set and degree. She has gained deep expertise in personnel management, customer service, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Ms. Anderson is responsible for the all Client Support Managers (CSMs) that support Strategic Accounts within CenturyLink's territory. She is a point of escalation and is ultimately responsible for overall customer satisfaction. Ms. Anderson responds to billing inquiries and resolves billing disputes. Her responsibilities include in assisting her CSMs and proactively monitors service provider-billing accuracy through resolving escalations, managing day-to-day administrative tasks, pulling internal reporting, providing assistance with supporting customers and assisting her team with order processing group to minimize billing errors on the front end. Ms. Anderson managed her team through their involvement in the implementation of the South Dakota NG-911 project. Ms. Anderson is an articulate communicator who works effectively with customers and delivers outstanding customer service through consistent, on-time, and on-budget project delivery. Over her career at CenturyLink, Ms. Anderson's keen focus on deployment of customer-driven initiatives and strict adherence to and conformance with customer needs. Ms. Anderson is a skilled communicator as she broadly communicates her initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Bachelor of Science, Computer Information Management, College of Saint Mary's, Omaha, NE, 2002

Relevant Employment/ Project History

CenturyLink **Omaha, Nebraska** **2017-Present**
Manager Base Management

As Manager in Base Management at CenturyLink. Ms. Anderson drives consistency throughout day-to-day operations: standards, tools, best practices, process knowledge and communication. She provides escalation assistance and situation management to drive for internal and external issue resolution coordinating across sales, service delivery, billing and service management. She ensures CSM team partners closely with Account Director/Sales Engineering (AD/SE) teams in order to grow revenue and provide superior customer experience. Ms. Anderson also ensures coordination and cross alignment with Client Support Management across the sales organization while implementing best practice and solutions to channel's business and customer needs. As a manager, Ms. Anderson promotes positive on-boarding experience for new hires (such as tools, training, and resources) and drives optimal ramp time to full productivity. She manages resource allocation to ensure assigned account bases allow appropriate sales and client support and oversees Key Performance Indicators such as revenue, revenue retention, sales, quoting, client survey feedback.

Ms. Anderson's significant accomplishments include providing critical input on several key projects. Highlights of Ms. Anderson's key significant accomplishments include the following:

- Contributed on CenturyLink internal projects to streamline the customer experience in upfront ordering
- Assisted several large implementations for high profile customers
- Participated in a select group of managers for CenturyLink's company-wide Leadership Experience Program for Front Line Leaders

CenturyLink **Omaha, Nebraska** **2014-2017**
Account Consultant

As Account Consultant at CenturyLink, Ms. Anderson functioned as Account Consultant Subject Matter Expert for SD WAN, IQ Networking, IQ SIP products. She participated in several ongoing Time Interval Reduction projects as well as new product deployment trials. Ms. Anderson was responsible for High Cost Work-In-Progress (WIP) to drive orders to completion. Her responsibilities included maintaining dedicated, high profile customer base and assisting with complex solution delivery and escalations. Her daily duties included present a positive image of CenturyLink during client meetings and communications, assisting management in resolving escalated customer issues. Ms. Anderson functioned as acting Interim Manager during CenturyLink re-organization after Level 3 merger and maintained good rapport with team members. Highlights of Ms. Anderson's key significant accomplishments include the following:

- Received the CenturyLink COE Award for customer account support and assistance to internal Sales Team to improve CenturyLink's customer experience

Evolving Solutions, Inc. **Omaha, Nebraska** **2007-2014**
Senior Account Manager

As Senior Account Manager for Evolving Solutions, Inc., Ms. Anderson was responsible for delivery of projects on time for customers on a national scale. She managed vendors, carrier provisioners, subagent support, and client support resources. She participated in all phases of various project life cycles from design through delivery and ongoing maintenance to deliver complex carrier solutions to new sites for clients with aggressive timelines. Her daily duties included developing and maintaining project documentation and conducting meetings with the clients to fully assess client needs and expectation setting. Ms. Anderson delivered status reports and client communications and coordinated with project team members. She developed training manuals for Operations Department. Highlights of Ms. Anderson's key significant accomplishments include the following:

- Contributed to company's growth through improving the quoting process and client retention.

Certifications / Training

Deep understanding of carrier network offerings, including Ethernet, SIP, MPLS, and many others
Proficient with CORE, SFA, Host Applications
Proficient in MS Office including Excel and Outlook

Professional Memberships / Associations

None

MICHELE L. WOLF
DIRECTOR – BASE MANAGEMENT

Experience Summary

Michele L. Wolf is a proven Director with demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support and 21 years at CenturyLink. Her deep expertise in managing large, complex telecommunications programs empowers Ms. Wolf to execute her role as an effective program manager. She employs her problem-solving skills and the ability to quickly gather information to manage project implementation plans across the lifecycle of her programs. Ms. Wolf's education and professional development accomplishments include holding a Master of Business Administration. Ms. Wolf is a dedicated, energetic, and versatile professional with expansive technical skill set, advanced degree and certifications in managing telecommunications and WAN/LAN initiatives. She has gained deep expertise in strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Ms. Wolf is responsible for the all Client Support Managers (CSMs) nation-wide for all national 9-1-1 accounts. She serves as a point of escalation for any all implementation and billing issues. Her responsibilities include in assisting her managers and proactively monitors service provider-billing accuracy through resolving escalations, managing day-to-day administrative tasks, pulling internal reporting, providing assistance with supporting customers and assisting her team with order processing group to minimize billing errors on the front end. Ms. Wolf managed her team through their involvement in the implementation of the South Dakota, Arizona, and California NG-911 systems and fully understands the State of Nebraska's 9-1-1 mission and the process to implement it. Through experience, Ms. Wolf has developed a deep understanding the process of installing and implementing PSAPs.

Ms. Wolf is highly accomplished, solutions-driven professional with enterprise support expertise and demonstrated track record of commitment to customer leading teams, driving improvement and is focused on getting the best out of employees. She holds an MBA and Six Sigma Green Belt certification. Ms. Wolf is an expert in analysis and documentation of existing business processes, requirements, and technical specifications. Ms. Wolf is an articulate communicator who works effectively with customers and delivers outstanding customer service through consistent, on-time, and on-budget project delivery. Over her career at CenturyLink, Ms. Wolf focuses on deployment of 9-1-1 initiatives and strict adherence to and conformance with customer needs. She is a skilled communicator as she broadly communicates her initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master of Business Administration, Augsburg College, Minneapolis, MN, 2012

Bachelor of Arts, Economics and Management, Augsburg College, Minneapolis, MN, 2009

Relevant Employment/ Project History

CenturyLink **Minneapolis, Minnesota** **2017-Present**
Director-Base Management

As Director in Base Management at CenturyLink, Ms. Wolf is the leader of an organization of 100 Account Consultants, Project Managers, Program Managers, and 7 Post Sales Managers nationwide, who support the growth and retention of our existing customer base and also the acquisition of new clients. Her responsibilities include managing and ensuring her team address all post-sale service issues relating to ordering, provisioning, billing, analysis, performance, and reliability of CenturyLink products and services. She conducts RFP analysis, develops proposals, and delivers RFP presentations to customers. Ms. Wolf assists the CenturyLink Sales Organization in driving sales goals by assisting with pricing, developing a technically sound solution, and drafting contracts.

Ms. Wolf's significant accomplishments include providing critical input on several key project. Highlights of Ms. Wolf's key significant accomplishments include the following:

- Received Circle of Excellence Winner for outstanding performance – top 10% performer in the CenturyLink; received award 2017 & 2018
- Exceeded Sales Target Every month in 2018

CenturyLink **Minneapolis, Minnesota** **2013-2017**
Post Sales Engineering Manager II

As Post Sales Manager at CenturyLink, Ms. Wolf managed a team of 21 Account Consultants and 1 service manager across 8 states for the Midwest region, who supported the growth and retention of our existing customer base and the acquisition of new clients. She ensured her team addressed all post-sale service issues relating to ordering, provisioning, billing, analysis, performance, and reliability of CenturyLink products and services. She hired and trained 13 Account Consultants in 8 different states in 3 months. Ms. Wolf performed RFP analysis, developed proposals, and delivered RFP presentations to customers. She assisted CenturyLink's Sales Organization in driving sales goals by assisting with pricing, creating a technically sound solution, and drafting contracts. Highlights of Ms. Wolf's key significant accomplishments include the following:

- Hired a new team of 13 employees and had them fully ramped up in 3 months
- Contributed to sales region revenue increase of 4.2% over the first 3 quarters of last year through implementing new processes and more aggressive timelines for installs to recognize revenue sooner

CenturyLink **Minneapolis, Minnesota** **2011-2013**
Account Consultant

As Account Consultant, Ms. Wolf supported achievement of sales objectives by partnering with sales team and executing on sales opportunities by developing and maintaining customer relationships. She advocated on behalf of the customer to ensure specific quality improvement strategies and goals were met in service delivery. Ms. Wolf analyzed revenue and expense trends and performed revenue and expense forecasts and prepared annual plans and field budgets. She prepared spreadsheets, graphs, and charts to illustrate financial trends and presented to leadership. Highlights of Ms. Wolf's key significant accomplishments include the following:

- Conducted account records cleanup and conciliation to identify and correct billing errors, resulting in a direct and immediate revenue increase of 3%
- Contributed to sales team revenue increase of $200,000 through implementing product upgrading and pricing strategies for customers

CenturyLink **Minneapolis, Minnesota** **2010-2011**
Service Delivery Coordinator

As Service Delivery Coordinator, Ms. Wolf provided excellent customer service to over 300 large business customers, by serving as a single point of contact. She resolved complex customer billing and service issues. Sold a variety of telecommunications products including data lines, T1 lines, networking, and phone systems. Ms. Wolf acted as a peer coach and trained newly hired representatives. She served as in-charge for managers and handled customer escalations and supervision of representatives. Highlights of Ms. Wolf's key significant accomplishments include the following:

- Maintained outstanding order accuracy for 14 consecutive months as evidenced by 100% quality audits for 14 consecutive months
- Scored 100% on all customer service goals during call observations
- Successfully managed a team of 12 employees for a four-month period, balancing peer relationships in a union environment while fulfilling managerial duties

Certifications / Training

Six Sigma Green Belt Certification, 2018

Professional Memberships / Associations

None

RACHEL G. RENTERIA
SENIOR POST SALES ENGINEER

Experience Summary

Rachel G. Renteria is a proven Senior Post Sales Engineer with 25 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. Her deep expertise in managing technically divers customer networks, that range from VoIP, DATA, Cloud, Security, MPLS, and Hosting empowers Ms. Renteria to execute her role as an effective Post Sales Engineer. She employs her problem-solving skills and very customer oriented with strong understanding of sense of urgency at any customer level. Ms. Renteria holds several certifications, including Cisco Certified Network Associate (CCNA) and the Six Sigma Basic Certificate. Ms. Renteria is a dedicated, energetic, and versatile professional. she has gained deep expertise in managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Ms. Renteria is a Senior Post Sales Engineer at CenturyLink who is responsible for fortune 500 customer networks, providing 24x7 SLA management on multiple types of service including VoIP, MPLS, SIP, IP DATA, Hosting, SD-WAN, Frame relay. She possesses deep expertise in troubleshooting customer networks and providing solutions to outages, providing solution's to all types of network technologies from DATA, VoIP, MPLS, VPN, SIP trunk, supporting C-level customers to resolve critical outages. Ms. Renteria responsibilities include working with account managers and their leadership teams, and closely with Sales Engineers to design and implement customer solutions. She oversees network operations projects including budgeting, planning, implementation, maintenance, administration, staffing and provides day to day leadership of call center employees, both on-shore and off-shore. Ms. Renteria has been supporting 9-1-1 system for 15 months for the of states of Nebraska, Missouri, and Iowa. For Nebraska, she escalates repairs, monitor network technician responses, supports PSAPs to full capacity. She reviews work that was performed in a post-sales capacity to ensure network stability. She coordinates technical visits with the customers and ensures PSAPs overflow call capacity is set up correctly for call handling in cases of surge.

Ms. Renteria is a results-oriented business professional with proven abilities in team building, managing projects, and improving efficiency of operations. She possesses a keen ability to identify areas of organizational strength and weakness and implement company policies, standards, operational processes and systems that optimize productivity and bottom line. She motivates staff to perform at optimal effectiveness. Over her career at CenturyLink, Ms. Renteria focuses on strict adherence to and conformance with customer needs. Ms. Renteria is a skilled communicator as she broadly communicates her initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

2 years IT course work at International Business College

Relevant Employment/ Project History

CenturyLink **Dallas, Texas** **2014-Present**
Senior Post Sales Engineer/Senior Client Service Manager/Senior Service Manager

As Senior Post Sales Engineer at CenturyLink, Ms. Renteria is responsible for fortune 500 customer networks, providing 24x7 SLA management on multiple types of service including VoIP, MPLS, SIP, IP DATA, Hosting, SD-WAN, Frame relay and manage technical teams across the globe. Her duties include managing customer networks and ticket escalation and providing all ticket updates to customers. She supports the Sales Organization in customer negotiations to drive new sales and design customer networks and collaborates with account managers and sales engineers to grow and improve customer networks. Ms. Renteria identifies new opportunities within the customer's network. She provides superior customer care by proactively communicating with C-level customers on outages and working with CNOC engineers to proactively monitor customer networks and resolve customer network issues. Ms. Renteria received recognition as CenturyLink's top 12 sales rep for 2018.

Bank of America **Frisco, Texas** **2010-2013**

Associate Vice President

At Bank of American in her various roles, Ms. Renteria oversaw day to day operations of MCCA Managed Contact Center Applications over the Mortgage call center telephony systems. Her responsibilities included providing 24/7 infrastructure management and monitoring, incident management. She provided superior service delivery by consistently meeting all SLA's. Ms. Renteria managed, led, and supported a team of 2 Managers and 32 technicians including overseas staff. She oversaw and supported 42 Aspect ACD call centers, Aspect Primitive Dialer, VOIP, and UIP and managed and support the Vendor management team of 6 electronic Workflow Management (eWFM). Ms. Renteria managed the NICE call recording team and was responsible for ensuring all customer calls are recorded. She provided training to all new associates and ensure current employees remain up to date on all training material. Training of RTI rollout. She also managed NICE Call Recording Projects to complete implementation and turn over to operation team and line of business (LOB). Ms. Renteria worked closely with CenturyLink's PMO and cross functional teams to deliver projects in a timely manner and within project scope and budgets exceeding 5 million in budget. She defined project scope goals and deliverables, which support business goals. She also maintained vendor relationships, negotiating, and contracting, monitored vendors performance. Ms. Renteria worked closely with CenturyLink's IVR team on all projects and outages to ensure steadfast resolution. She was responsible for all system stability across all Mortgage call centers, to not impact our customer and ultimately their customer by providing daily system monitoring and ensure employees understand the importance of maintaining system stability. She was responsible for all Vendor Management and third-party vendors, to ensure Priority tickets are handled quickly and within the SLA. Her experience with all Life cycle project management and implementation and Delivery, which includes planning, tracking, and execute the operational disaster recovery plan, overseeing 24x7 support of all incident tickets and project delivery, and supporting all change management process and implementation. Her responsibilities also included supporting all RCA-Postmortem Management by all teams and liaising between C-level and Line of Business Team.

Verizon Business **Richardson, Texas** **2003-2009**

Senior Technical Service Manager, Network Operations Manager, CRM Project Manager

At Verizon Business in her various roles, Ms. Renteria oversaw multiple customer Networks, across a global sales region with emphasis on the US and Latin America. Her responsibilities included functioning as a 24x 7 emergencies on call Manager for the duration of time at Verizon, meeting all customers Service Level Agreements (SLAs), managing ticket escalation and providing all ticket updates to customers within a timely manner. She worked with the Sales team to increase sales and continue to grow customer base revenue. Ms. Renteria proactively communicated with C-level customers on outages and worked with CNOC engineers to proactively monitor customer networks. She managed Field technicians on outage repairs for field and Colocations and led Technical teams to quick resolve on technical outages. She worked closely with Sales teams to grow accounts and maintain client focus.

Verizon Business **Richardson, Texas** **1998-2002**

Network Operations Manager

Ms. Renteria ensured complete customer satisfaction by creating a help desk program which successfully met customer needs for 24-hour customer service and resulted in a $2 million cost savings to the company by drastically reducing extended customer outages and subsequent requests for credit reimbursement. She annualized data to improve customer networks and ultimately improve profits within a competitive market and beat out competitors and ensured customer Network outages remain minimal and provide constant feedback to customer during the outage. Ms. Renteria managed the acquisition team during all new acquisitions until fully implemented into the Verizon Business Model. She led staff by focusing on empowering and motivating employees to be successful and exceed quarterly goals. Directly increased sales by developing a team incentive program to motivate the post sales team in delivering timely results during outages. She performed as an account manager, managing global accounts such as Continental Airlines, BOA, JCPenney, PepsiCo. She maintained and managed all contractual equipment agreements for customers under account team as well as processed all Managed Service Provided agreements for customers on their CPE and Network. Ms. Renteria was responsible for vendor management of multimillion-dollar account negotiations, including playing an instrumental role in creating a partnership with Cisco and Nortel which resulted in the ability to provide direct customer service and increased customer satisfaction. She recruited, hired and promoted staff including discipline of employees as well as conducted yearly reviews and continuous training

sessions for cross functional teams. She also implemented Policies and Procedure for both Sales and Network Operations.

Verizon Business **Richardson, Texas** **1996-2008**

CRM Project Manager

Ms. Renteria was responsible for customer quarterly review of network performance and quarterly customer growth reports. She managed customer accounts by meeting with customers on a monthly or quarterly basis to strategically go over their network and review all changes that could be implemented. She developed new business growth plans and ideas for driving quarterly sales for all existing customers globally and implemented new billing software to provide better customer service by allowing the billing department to work more closely with order fulfillment, credits, installs and expedites. Ms. Renteria maintained all customer Equipment Lease agreements and contracts on CPE. She managed all account hot cuts and installations along with expedite and provided customer network diversity by reviewing customer's network monthly. She communicated effectively with all levels of staff and upper management including C-Level

Certifications / Training

Six Sigma Basic Certificate

Cisco Certified Network Associate (CCNA)-Certificate

Professional Memberships / Associations

None

JOHN ATKINSON
MANAGER POST SALES ENGINEERING II

Experience Summary

John Atkinson is a proven Manager of Post Sales Engineers with 34 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. He possesses a proven track record of supporting mission critical applications, and unique, customized solutions for a base of strategic, 9-1-1 and Public Sector accounts. He employs his problem-solving skills and is very customer oriented with strong understanding of sense of urgency at any customer level. Mr. Atkinson is a dedicated, energetic, and versatile professional. He has gained deep expertise in managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Atkinson is a Manager of Post Sales Engineering (PSE) at CenturyLink who is responsible for Manager Post Sales Engineering responsible for overall operational performance for regional clients within the Public Sector. Mr. Atkinson responsibilities include managing his team of Post Sales Engineers who work with account managers and their leadership teams, and closely with Sales Engineers to design and implement customer solutions. He is responsible for 9-1-1 and Public Sector customers in 36 states. He manages his team to assist them in executing their responsibilities, which include event management, change management, design and RFP support. He assists his PSEs and proactively monitors repair performance through supporting escalations, managing day-to-day administrative tasks, pulling internal reporting, and aiding with supporting customers. Mr. Atkinson managed his team who supports NG-911 systems for State and Local Governments in central midwestern States from South Dakota to Texas and all eastern States. He fully understands the criticality of State of Nebraska's 9-1-1 mission and the process to support it.

Mr. Atkinson is a results-oriented business professional with proven abilities in team building, managing projects, improving efficiency of operations and financial analysis. He possesses a keen ability to identify areas of organizational strength and weakness and implement company policies, standards, operational processes and systems that optimize productivity and bottom line. He motivates staff to perform at optimal effectiveness, while controlling costs through efficient use of human and operational resources. Over his career at CenturyLink, Mr. Atkinson focuses on strict adherence to and conformance with customer needs. Mr. Atkinson is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Hill Associates, Burlington VT, Advanced Telecommunications Studies, 1997

Dakota County Technical, Minneapolis MN, Telecommunications study, CSS Labs, 1995

University of Phoenix, Seattle WA, Electronics, 1993

Minneapolis Community College – Small Business Administration, 1990-1992

University of MN, Duluth MN, General Studies, 1983-87

Relevant Employment/ Project History

CenturyLink **Phoenix, Arizona** **2018-Present**

Post Sales Engineering Manager II

As Manager of Post Sales Engineering at CenturyLink, Mr. Atkinson is responsible for leading a team of 10 Post Sales Engineers with responsibility for 9-1-1 and Public Sector customers in 36 states. Team responsibilities include event management, change management, design and RFP support. In his current role, Mr. Atkinson's significant

accomplishment that includes South Dakota NG-911 implementation on an accelerated timeline to achieve customer objectives.

CenturyLink **Phoenix, Arizona** **2007-2018**

Lead Post Sales Engineer

At CenturyLink, Mr. Atkinson was responsible for post-sales relationship management for several Arizona and New Mexico-based premier customers. He led 24x7 escalations and event management, prepared network metrics, and facilitated service meetings with customers. He regularly interfaced with leadership teams, both with customers and internally.

Qwest Communications **Tempe Arizona** **2006-2007**

Supervisor Network Operations

As a Supervisor in Network Operations at CenturyLink, Mr. Atkinson supervised the work of two Customer Data Technician crews. His overall responsibility for designed services installation and repair and span recovery efforts for the southeast Phoenix metro.

Qwest/US West Communications **Minneapolis, Minnesota** **1996-2006**

Customer Service Specialist

As a Customer Service Specialist at CenturyLink, Mr. Atkinson functioned as a NOC technician who supported customers with Frame Relay & ATM services. He diagnosed and repaired coordination including testing with customers and other internal departments, field technicians and other carriers such as Verizon and Sprint. For most of the ten years in this role, Mr. Atkinson was dedicated to the State of Oregon government and their Frame network that covered over 7000 locations. He was single point of contact for all repair issues and test/turn-up activity for all locations. He achieved TIER III on the technical career ladder.

Certifications / Training

None

Professional Memberships / Associations

None

DAVID C. MUELLER
SENIOR MANAGER

Experience Summary

David C. Mueller is a proven Senior Manager with 19 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. His deep expertise in managing large, complex telecommunications programs empowers Mr. Mueller to execute her role as an effective program manager. He employs her problem-solving skills and the ability to quickly gather information to manage project implementation plans across the lifecycle of her programs. Mr. Mueller's education and professional development accomplishments include holding a Master of Business Administration. Mr. Mueller is a dedicated, energetic, and versatile professional. He has gained deep expertise in managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Mueller is a Senior Manager in Operations Service Management at CenturyLink who is responsible for overall operational performance for all clients supported by Operations Service Managers (OSMs) and Post Sales Engineers (PSEs) within the Public Sector, which includes Federal, State, and Local Agencies. His responsibilities include assisting his managers and proactively monitoring repair performance through supporting escalations, managing day-to-day administrative tasks, pulling internal reporting, providing assistance with supporting customers. Mr. Mueller manages his team in supporting the South Dakota, Arizona, and California NG-911 systems and fully understands the State of Nebraska's 9-1-1 mission and the process to support it. He earned a Master of Business Administration in Management and a Six Sigma Green Belt certification as well as an advanced degree. Mr. Mueller is a results-oriented business professional with proven abilities in team building, managing projects, improving efficiency of operations and financial analysis. He possesses a keen ability to identify areas of organizational strength and weakness and implement company policies, standards, operational processes and systems that optimize productivity and bottom line. He motivates staff to perform at optimal effectiveness, while controlling costs through efficient use of human and operational resources. Over his career at CenturyLink, Mr. Mueller focuses on strict adherence to and conformance with customer needs. Mr. Mueller is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master of Business Administration, Management, University of Colorado, Denver, CO, 2001

Bachelor of Arts, Political Science, Colorado State University, Fort Collins, CO, 1993

Relevant Employment/ Project History

CenturyLink **Broomfield, Colorado** **2008-Present**
Senior Manager-Service Management, Federal and SLED

As Senior Manager at CenturyLink, Mr. Mueller develops partnership between Account Teams, PMO and Service Assurance organizations in support of our clients. He manages a team of Service Managers that support agencies and clients in the Federal and SLED channels. His duties require his leadership and management aptitude to lead his team on tasks that require operational support through KPI assessment, performance analysis, SIP identification and reviews. He supports the client with engaging various CenturyLink Repairs Centers during exceptional service outages. Mr. Mueller develops relationships with key client personnel to ensures proper individuals are notified with outage updates.

Mr. Mueller assumed his role at the end of 2019, with key significant accomplishments that include the following:

- Reorganized the Federal Service Managers to more effectively support the customer base by aligning with high level agencies and sales directors, building better familiarity and responsiveness.

- Reorganizing SLED Service Managers by experience and skill sets to provide the correct individuals with newer, more detailed 9-1-1 training

Senior Manager – Enterprise Repair for Data. IP Infrastructure

As Senior Manager at CenturyLink, Mr. Mueller recruited, developed, evaluated and motivated a high performing, 24x7 team including six managers and 100+ technicians. He developed, documented, communicated, and implemented strategic and tactical operational improvement initiatives at both the team and larger organizational level. Mr. Mueller produced metric reporting, headcount modeling, scheduling and team performance read outs. He was the primary liaison with partner carriers, providing performance feedback at monthly meetings, as well as engaging escalation contacts during executive escalations. Mr. Mueller represented the Enterprise Repair organization at customer get well meetings and merged legacy company Offnet teams into a single Offnet team. Highlights of Mr. Mueller's key significant accomplishments include the following:

- Improved MTTR for one legacy company team by 42% during 2018
- Improved three the month rolling average Top Box CSAT score from 40% to 60% during 2018

Project Manager – Business Operations, Managed and IP Service Assurance

As Project Manager, Mr. Mueller prepared executive level reporting that communicates team performance. He produced budget forecasting, metric reporting, headcount modeling and business cases and tracked strategic and tactical operational improvement initiatives.

Senior Analyst – Internal Audit

As Senior Analyst, Mr. Mueller assisted in the planning of financial, operational and IT audits. He identified opportunities for improving business processes, enhancing revenue, reducing costs or improving internal controls - ensure integrity and reliability of the controls. He communicated with business process owners to document processes, risks and controls of audit areas. Mr. Mueller developed, executed and documented detailed audit testing procedures that measured compliance to established internal control policies, procedures, laws, and regulations and drafted audit reports and communicated audit findings to business process owners.

University of Denver, Division of Athletics and Recreation **Denver, Colorado** **2004-2008**

Director of Joy Burns Arena

As Director, Mr. Mueller hired, managed, developed and evaluated several teams that included 3 exempt employees, 20 full-time employees, 75+ part-time employees, and 100+ volunteers. He developed programming and space utilization through observation, daily activities, data analysis, weekly staff meetings and quarterly department head retreats – developed and documented policies and procedures. He oversaw staff and program scheduling in main venues, including supporting training, meeting, and locker rooms. His job responsibilities included directing overall logistical operations of recreational programming – hiring coaches, scheduling practices/games/officials, assigning support staff, procurement of equipment and supplies. Mr. Mueller developed and implemented risk management policies and procedures. He coordinated facility and equipment maintenance to ensure quality and safe programs and managed a facility and equipment depreciation account. Highlights of Mr. Mueller's key significant accomplishments include the following:

- Improved "Learn to Skate" program retention during peak season from 62% in FY05 to 76% in FY06
- Increased net revenue by 14% from FY05 ($372K) to FY07 ($423K)

Time Warner Telecom, Network Operations Center **Greenwood, Colorado** **1998-2004**

Project Manager – Inventory Assurance

As Project Manager, Mr. Mueller partnered with outside consultants and vendors to develop and implement new customized communication network inventory system that integrated with company's legacy systems. He led development of the workflow systems within new network inventory system. Mr. Mueller consulted with operational SME's to provide accurate and complete information to the project team and reported project progress or roadblocks to senior management as appropriate. He developed process flow charts and M & P documents that highlighted user roles and tasks and coordinated change control and release management. He participated a tool development project that audited actual network against inventory databases. Mr. Mueller developed and

implemented processes and supporting documentation to address required manual clean-up of data bases resulting from network audits. Mr. Mueller's key significant accomplishment was managing a single phase of one project (approx. 16% of network) captured $1.1M in stranded equipment to be re-deployed.

Certifications/Training

Six Sigma Green Belt - Acuity Institute, December 2008

Professional Memberships/Associations

None

ERIC B PETERSON
DIRECTOR – OPERATIONS SERVICE MANAGEMENT

Experience Summary

Eric B. Peterson is a proven Director with 22 years of demonstrated Telecommunications experience in both Global Enterprise Customers and Government and Education Services support. His deep expertise in overseeing and managing large, complex telecommunications programs empowers Mr. Peterson to execute his role as Director. He employs his problem-solving skills and the ability to quickly gather information to guide and manage project implementation plans across the lifecycle of his programs. Mr. Peterson's education and professional development accomplishments include holding a Master of Business Administration. Mr. Peterson is a dedicated, energetic, and versatile professional. He has strong Operations Science based analytical measurement experience and has gained deep expertise in managing teams, team building, talent development, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Peterson is a Director in Operations Service Management at CenturyLink who leads a 170-person Operations Service Management organization company-wide. He is responsible for leading Operations Service Managers (OSMs) and Post Sales Engineers (PSEs) within the Public Sector, which includes Federal, State, and Local Agencies. Mr. Peterson is responsible for all aspects of Operations Service Management processes and post-install support. He is directly responsible for the Operations Service Management (OSM) organization and, by extension, individual contributors. Mr. Peterson is a point of escalation both internally and customer-facing, to ensure appropriate operations support. For the Nebraska NG-911, Rachel Renteria is part of Mr. Peterson's organization. With CenturyLink, Mr. Peterson is currently managing the NG-911 system operations for the State of California. This includes the deployment of Next Generation Core Services (NGCS), ESINet, and the aggregation network to all Originating Service Providers (OSP). Mr. Peterson specializes in the following product solutions: E911/NG-911, UCaaS, Contact Center, VoIP, Managed Security Services, Dark Fiber, Private Dedicate Rings/Networks (PDR/PDN), Wavelength Services, TDM T1/T3 Services, Ethernet Private Lines, Ethernet Virtual Private Line Service, Multi-Protocol Label Switching Service and Internet.

He earned a Master of Business Administration and a Bachelor of Science in Finance. Mr. Peterson is a results-oriented business professional with proven abilities in team building, managing projects, improving efficiency of operations and financial analysis. He possesses a deep understanding of Operations Service Management, Assurance, Sales, and Product Lifecycles. He applies his skills in Critical thinking and execution of big ideas to enable transformation for promoting innovative thinking across his organization. He motivates staff to perform at optimal effectiveness, while controlling costs through efficient use of human and operational resources. Over his career at CenturyLink, Mr. Peterson focuses on strict adherence to and conformance with customer needs. Mr. Peterson is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master of Business Administration, University of Tulsa, Tulsa, OK, 2002

Bachelor of Science, Finance, Oklahoma State University, Stillwater, OK, 2000

Relevant Employment/ Project History

CenturyLink **Tulsa, Oklahoma** **2019-Present**
Director – Operations Service Management

As Director in Operations Service Management (OSM) at CenturyLink, Mr. Peterson leads a 170-person Operations Service Management organization companywide. Our mission and goal are to provide Industry Leading Customer Experience to those we serve by being the service assurance experts and resource center for internal and external customers as well as to alleviate pressure placed on the Repair Center. We do this through relationships and our

core competencies, which include providing Operations Reviews, Service Improvement Plans, critical outage support, post-incident RFO discussion support, ticket and GCR contact management, and project management for process exceptions. Our relationship with Repair, the Sales Organization, and directly with Customers is key to our success and is something that differentiates us from our competitors.

Mr. Peterson's significant accomplishments include providing critical input on several key projects that supported several State Emergency Communications Services development lifecycles. Highlights of Mr. Peterson's key significant accomplishments include the following:

- Leading Digital Transformation efforts within repair through the use of Power BI and other analytics tools to give our OSMs better insights into customer performance and areas to improve upon
- Developed Mobile applications to allow our OSM's have up to the minute information regarding customer network ticketing to improve customer experience
- Successfully merged 5 different OSM organizations into 1 company-wide organization

CenturyLink **Tulsa, Oklahoma** **2015-2019**
Senior Manager – Operations Service Management

As Senior Manager at CenturyLink, Mr. Peterson managed and led most groups within the Operations Service Management organization including most of GAM, Federal, GEAR and parts of Wholesale at times. He effectively led and developed team members across multiple companies from various backgrounds and led multiple teams including two teams with 25 directs for over 9 months. Mr. Peterson accomplished process improvement project that led to building a SharePoint site for team collaboration and improving the digital account management process. He capitalized on opportunities to innovate that led his team to better ways of accomplishing their job through technology and data analytics. Mr. Peterson effectively partnered and developed strong relationships with Assurance, Sales, and Customer leader as well as individual contributors and worked to develop and recognize talent within the organization. Highlights of Mr. Peterson's key significant accomplishments include the following:

- Pioneered the use of Power BI, Power Apps, Flow, and SharePoint to transform the entire OSM Organization as well as share with other organizations
- Developed and rolled out our new Metric and Marketing platforms which includes Power BI and OSM University

CenturyLink **Tulsa, Oklahoma** **2003-2015**
Service Manager Lead

As Service Manager, Mr. Peterson responsible for over $140 million in complex annual revenue. His responsibilities included addressing overall customer satisfaction, billing maintenance, service maintenance, revenue retention, Operations Science based operations reviews and analysis, and both tactical and strategic process development. He effectively led when managing a diverse group of people and departments in a matrix management environment to achieve goals and objectives important to the company and the customer. Mr. Peterson developed and maintained operations science-based operations reviews that include complex data analysis, root cause identification, and service improvement plans. To promote interdepartmental synergies, he initiated and implemented multiple cross-department process improvements many of which involved new revenue opportunities and assisted in cross-functional development teams for creation and release of new products to existing customers. His actions resulted in sales growth revenue base in a market with steady price declination. Mr. Peterson's key significant accomplishments included recovering over $1.2 million in cost savings by reviewing complex financial operating data, developing technical plans to migrate services, and implementing the plan.

CenturyLink **Tulsa, Oklahoma** **2000-2003**
Project Manager IV

As Project Manager, Mr. Peterson managed the ordering and provisioning of telecommunication circuits and projects for a large and wide-ranging customer base including large cable companies and government sub-contracts. His responsibilities included delivering multimillion-dollar services to telecom customers, providing custom presentations for customers to assist the sales process, and managing a group of people and processes for delivering results. Mr. Peterson's significant accomplishment in this position included developing new processes that netted over $20 million.

Certifications / Training

None

Professional Memberships / Associations

None

EARL STAN WATERMAN
REGIONAL OPERATIONS MANAGER

Experience Summary

Earl Stan Waterman is a proven Regional Operations Manager with over 35 years of demonstrated experience in Telecommunications at CenturyLink. Mr. Waterman is a self-motivated, organized professional with demonstrated success in management, interpersonal and communication skills, and the ability to manage numerous tasks simultaneously. He is a dedicated, energetic, and versatile professional with expansive technical skill set that is built upon a technical degree and certifications in best industry management practices and information security policy development. The deep expertise in managing large, complex telecommunications programs Mr. Waterman has gained over his career has resulted in his strong problem-solving skills and the ability to quickly gathers information and implement plans of action. He functions as Secretary on the Nebraska One-Call Board Member and is pursuing an Associate Degree.

Role and Understanding of the Process

Mr. Waterman manages a team of six supervisors, one administrative assistant, and a base of 94 central offices, fields, and design/9-1-1 union technicians that install and maintain broadband, POTS, Gigabit Passive Optical Network (GPON), Ethernet, and 9-1-1. He serves as a point of contact, ensuring compliance with contract terms and objectives are incorporated consistently throughout the project implementation. Mr. Waterman is full responsibility for multi-million-dollar budgets and executing complex projects on time and on budget. He fully understands the critical role Operations play in maximizing the uptime of the Nebraska 9-1-1 system and possesses expertise in risk analysis and management and incident response oversight. Mr. Waterman understands the importance of excellent customer service and has successfully managed his team. He addressed customer concerns promptly and pass on customer "Thank You Feedback" directly to his technicians. Over his career at CenturyLink, Mr. Waterman has keenly focus on deployment of E911 initiatives and strict adherence to and conformance with customer needs. He is a skilled communicator who effectively communicates initiatives and implements plans across the entire program to achieve customer goals.

Education

Associate Degree, Western Nebraska Community College, Scottsbluff, Nebraska, Candidate

Relevant Employment/ Project History

CenturyLink **Scottsbluff, Nebraska** **1988 – Present**
Regional Operations Manager

As a Regional Operations Manager at CenturyLink, Mr. Waterman is responsible for executing and completing telecommunications projects that include voice and data service delivery, network expansions, site activations, outside plant, and fiber builds according to strict deadlines and within budget. His responsibilities include managing a team of six supervisors, an administrative assistant, and a base of 94 central office, field, and design/9-1-1 union technicians that install and maintain broadband, POTS, GPON, Ethernet, and 9-1-1. He manages a $3M expense budget by prioritizing jobs and workload with his supervisors on the best agreed-upon approach to spend the funding on projects, resulting project completion below or at budget each year. He monitors damage claims to ensure money is recouped from the damaging party and manages line extension contractor that preforms construction maintenance activities, including the status of cable repair projects, installation of buried drops, and hold them accountable for on-time performance and quality. He produces maintenance packages by exchange with cost analysis for pedestal replacement/rehab projects and submit cable replacement projects with characterization analysis to support the replacement. Mr. Waterman works with the CenturyLink Public Policy Team to submit Nebraska Universal Service Fund projects. He promotes a corporate employee engagement survey and develop action plans to address the issues and concerns. He administers quarterly point awards to acknowledge fellow employees for work well done.

Area Plant Supervisor

As Area Plant Supervisor at CenturyLink, Mr. Waterman was responsible for directing technicians to maintain OSP/Network facilities in a productive and effective manner. He supervised the conversion of Nortel DMS 100 and DMS 10 products to the Nortel C2P switching technology and performed in-charge duties during the manager's absence and for extended periods when vacancies occurred at the manager level. Mr. Waterman managed $1.5 million employee budgets, coming in below or meeting budget each year. He partnered with internal departments to ensure customer trouble or service order Key Service Measurements were achieved and partnered with engineering on projects to ensure a wider scope of work was reviewed to ensure bad facilities and growth opportunities were identified. Mr. Waterman participated in three Union contract negotiations in 2004, 2007, and 2010 and is an active participant in a Nebraska PSC hearing in January 2011.

Network Supervisor

As Network Supervisor at CenturyLink, Mr. Waterman was responsible for the network facilities in 17 exchanges (35,000 households), including performing monthly central office quality inspections. As part of his duties. Mr. Waterman managed the eight technicians that were responsible for the routine maintenance and repair of special services and the analog and digital switching equipment. He honed his teamwork and communication skills by providing feedback to the team and manager.

Outside Plant Supervisor

As Network Supervisor at CenturyLink, Mr. Waterman was responsible for eight outside plant technicians that served seven exchanges in the Southern and Eastern part of the Sprint territory in Nebraska and supervised 28 departmental personnel, hired new employees, and scheduled work shifts. As part of his duties. Mr. Waterman provided exceptional service to our customers and frontline associates. He maintained budget and promoted teamwork by loaning out employees to supervisors to help with results as well as preformed monthly quality inspections on outside plant technicians and shared the results with each individual.

CenturyLink **Glasco, Kansas** **1981-1988**
Installation and Repair Technician

As Installation and Repair Technician, Mr. Waterman was responsible for the installation of phone lines and the maintenance of customer service in four exchanges. He maintained aerial cable and buried cable independently and executed in-charge duties when the local supervisor was on vacation or away for extended meetings.

Certifications / Training

North Central Kansas Technical College, Beloit, KS Plumbing, Heating, and Air Conditioning Certificate

Professional Memberships / Associations

Nebraska One-Call Board Member, Secretary, 2007 – Present

Volunteer for the Festival of Hope, 2017 - Present

CORY M. SKOUMAL
REGIONAL OPERATIONS MANAGER

Experience Summary

Cory M. Skoumal is a proven Regional Operations Manager with over 20 years of demonstrated experience in Telecommunications at CenturyLink. Mr. Skoumal is a self-motivated, organized professional with demonstrated success in management, interpersonal and communication skills, and the ability to manage numerous tasks simultaneously. He is a dedicated, energetic, and versatile professional with expansive technical skill set that is built upon best industry management practices. Mr. Skoumal possesses strong problem-solving skills and the ability to quickly gathers information and implement plans of action. He holds a degree in Business Administration and Management Marketing.

Role and Understanding of the Process

Mr. Skoumal is responsible for the continuous operation of the network transmission equipment, and infrastructure as well as construction, maintenance, installation and repair of outside plant. and manages a team that executes the tasks. He serves as a point of contact for escalation to ensure compliance with contract terms and objectives are incorporated consistently throughout the project implementation. Mr. Skoumal is full responsibility for multi-million-dollar budgets and executing complex projects on-time and on-budget. He fully understands the critical role Operations play in maximizing the uptime of the Nebraska 9-1-1 system and possesses expertise in risk analysis and management and incident response oversight as well as the importance of excellent customer service. Over his career at CenturyLink, Mr. Skoumal has keenly focused on deployment of 9-1-1 initiatives and strict adherence to and conformance with customer needs. Mr. Skoumal is a skilled communicator who effectively communicates initiatives and implements plans across the entire program to achieve customer goals.

Education

Bachelor of Science, Business Administration & Management Marketing, University of Nebraska, Omaha, NE, 1999

Relevant Employment/Project History

CenturyLink **Omaha, NE** **2011 – Present**
Regional Operations Manager

As a Regional Operations Manager at CenturyLink, Mr. Skoumal is responsible the continuous operation of the network transmission equipment, and infrastructure as well as construction, maintenance, installation and repair of outside plant. He developed and managed an annual $30 million expense budget for the area for all employee and non-employee expenses. His duties include providing product marketing information to facilitate meeting the market's sales unit and net gain forecast while delivering exemplary customer service; maintaining high visibility in the community by being active in local organizations and service groups; ensuring compliance with all company and industry standards and safety procedures; and staying abreast of changing technology to determine the best long term solutions for the company. Mr. Skoumal contributes to the annual capital budget plan development by collaborating with local Engineering organization to ensure the market's needs are met.

CenturyLink **Omaha, NE** **2010-2011**
Manager – Design/Field Engineering

As Manager in Design/Field Engineering at CenturyLink, Mr. Skoumal was responsible for Design and Field Engineering functions specific to the local loop for wire centers in Nebraska and Western Iowa. He led, coach, and develop Outside Plant Engineers to meet and exceed performance targets while continuously improving processes. He performed regular audits on employee job requirements to ensure compliance to company policy. Mr. Skoumal managed operations budgets through authorization of work orders, monitor, and track results. He observed and coached performance of team members against defined metrics and scorecard initiating improvement plans as

needed and partnered with internal and external organizations to ensure that work is completed in an accurate and efficient manner to better serve Qwest customers. He established a team environment to facilitate and improve communications, cooperation, and employee attitude to better serve the team and Qwest customers.

CenturyLink **Omaha, NE** **2005-2010**
Network Operations Manager

As Network Operations Manager at CenturyLink, Mr. Skoumal oversaw the 175 employee Installation and Maintenance, Cable Maintenance, and Construction daily operation for Omaha and Western Iowa. His responsibilities included establishing and ensuring adherence to budgets, work plans, and performance requirements. He was accountable for operational results, methods & procedures, and staffing of the functional area and ensured proper scheduling of daily Construction workload to achieve critical completion dates. His other duties included developing the supervisor team and their subordinates through constant feedback and coaching, building successful relationships with Communications Workers of America (CWA) union officials to help foster positive interactions, and improving relationships with key internal departments to share ideas and facilitate communications. Mr. Skoumal strengthened his department's financial position by controlling expenses through overtime and material management and strived to increase efficiency in employee's daily work through developing employees as well as identifying process improvements to improve workflow.

CenturyLink **Omaha, NE** **2003-2005**
Network Operations Supervisor

As Network Supervisor at CenturyLink, Mr. Skoumal was responsible for the installation and maintenance of Designed Services circuits and equipment including DS0, DS1, E911, Pair gain systems, and Multiplexers. He developed employee performance through training and individual coaching to ensure efficiency and effectiveness while performing daily work functions. He regularly interacted with customers to ensure satisfaction in the products and services received and exercised financial responsibility by managing tool and equipment inventories as well as overtime. Mr. Skoumal was appointed to interview a committee that was charged with assisting in selecting new employees and worked with various departments within Qwest to ensure that all critical service order dates were met. He coordinated initial deployment and turn up of Broadband DSLAM's in the Omaha area and directed the chronic and noise mitigation crew for the states of Nebraska and Iowa.

CenturyLink **Des Moines, IA** **2001-2003**
Senior Design Engineer

As Senior Design Engineer at CenturyLink, Mr. Skoumal used resources to provide telephone and internet cable facilities to new developments (such as a Sub-Division or Campus). He issued engineering work packages for copper and fiber systems including workprints in OSP-FM or Cimage databases. He was responsible for providing specifications for cable placing and splicing, as well as equipment selection and safety guidelines and working to create the most economically feasible solutions while meeting budgetary guidelines. He provided extensive technical expertise in resolving customer held orders in a timely matter and interact with customers to coordinate cable facility placement that meets the customer due date.

CenturyLink **Omaha, NE** **2000-2001**
Customer Experience Manager

As Customer Experience Manager at CenturyLink, Mr. Skoumal managed end-to-end customer experience for 150 to 200 customers simultaneously. His responsibilities included interacting with and directed managers at all levels to prioritize and meet customer issues, initiating alternative solutions and atonement, managing data and information flow on numerous business computer systems, following-up with customer to ensure satisfaction, analyze and document results, and identifying and implemented process improvements to increase departmental productivity.

Certifications / Training/Achievements

Completed Leadership Omaha program through the Omaha Chamber of Commerce.

Nominated for the Ten Outstanding Young Omahans award through the Omaha Jaycees.

Appointed to the Board of Directors for the following organizations:

- Omaha Children's Museum
- Douglas County Sheriff Foundation
- Millard Athletic Association

Assigned to various key corporate teams for process and business improvements:

- Modem Management Team
- Corporate Force to Load Implementation Team
- Nebraska Leadership Team
- Chronic Repair Reduction Team
- Net Promoter Customer Satisfaction Implementation Team

Professional Memberships/Associations

None

MARGARET A. COOK
SENIOR FEDERAL PROGRAM MANAGER

Experience Summary

Margaret A. Cook is a proven Federal Program Manager with over 10 years of demonstrated Program Management experience in Telecommunications. She is a dedicated, energetic, and versatile professional with an expansive technical skill set that is built upon a technical degree and certifications in industry-standard management practices and information security policy development. Her deep expertise in managing large, complex telecommunications programs empowers Ms. Cook to execute her role as an effective program manager. She employs her problem-solving skills and the ability to quickly gather information to manage project implementation plans across the lifecycle of her programs. Ms. Cook's education and professional development accomplishments include holding a Bachelor of Science in Information Systems, maintaining an active Project Management Professional (PMP™) certification since 2005, and acquiring the Certified Information Systems Security Professional (CISSP) certification.

Role and Understanding of the Process

Ms. Cook oversees all aspects of the program lifecycle and overall implementation phases, namely, project planning development, project execution, quality, change control, meeting coordination, and documentation. She serves as the main customer point of contact and integrator, ensuring that compliance with contract terms and objectives are consistently met throughout a project implementation. Ms. Cook has built a 26-year career in the telecommunication industry, with over 15 years focused on mission critical Department of Defense networks. She managed the implementation and operations of the NY, PA, & MD National Guard networks during the September 11, 2001 crisis in September 2001. Real experience, such as this, has deepened Ms. Cook's understanding of the importance of Nebraska's 9-1-1 system moving to the next generation network capabilities that are necessary to save lives. To accomplish Nebraska's mission, Ms. Cook understands that managing all transition risk is paramount to ensuring a seamless service transition while maintaining uninterrupted service throughout the transition. Furthermore, Ms. Cook is committed, as she is on all her programs, to overseeing a timely Nebraska 9-1-1 system implementation, which fulfills customer expectations by meeting the project plan and deploying the system on-time and within budget.

Ms. Cook is fully responsibility for multi-million-dollar budgets, developing multi-year corporate strategies, and executing complex projects on time and on budget. Her expertise in risk analysis and management, information security policy development, compliance governance, IT auditing, and incident response oversight equips her with the requisite knowledge, skills, and experience to properly manage the Nebraska 9-1-1 system implementation. Additionally, she has successfully managed projects that featured penetration testing, configuration of change control, and disaster recovery planning. Over her career at CenturyLink, Ms. Cook has keenly focused on initiatives that are comparable to the Nebraska's 9-1-1 initiative, which demands strict adherence to and conformance with customer needs. She is a skilled communicator who effectively communicates initiatives and implements plans across the entire program to achieve customer goals.

Education

Bachelor of Science, Computer Information Systems, Florida Institute of Technology, Melbourne, FL, 2016

Relevant Employment/ Project History

CenturyLink **Herndon, Virginia** **2015 – Present**
Senior Federal Program Manager

As a Senior Program Manager who is dedicated to support the Harris Corporation portfolio of projects within CenturyLink Communications Government Markets Group, Ms. Cook is responsible for executing and completing telecommunications projects that include voice and data service delivery, network expansions, site activations, outside plant, and fiber builds according to strict deadlines and within budget. Her responsibilities include acquiring

resources and coordinating the efforts of team members and third-party vendors, contractors, or consultants in order to complete projects according to project plan and schedule. Ms. Cook is directly responsible for managing quality control and project objectives that is based on critical path throughout the lifecycle of the entire program. Ms. Cook directs and manages all implementation phases from beginning to end across the entire lifecycle of projects. In the role of the lifecycle program management, Ms. Cook defines project scope, goals, and deliverables that support business objectives in collaboration with senior management and key stakeholders. She develops full-scale project plans and associated communications documents as well as liaise with project stakeholders on an ongoing basis. Ms. Cook estimates the resources and participants that are required to achieve project goals. She develops and submits budget proposals with recommendations and modify budget where necessary. She sets, manages, and continually communicates project expectations with team members and other stakeholders. Ms. Cook identifies and resolves issues that arise and manages program and project dependencies as well as critical path drivers using the schedule project timelines and milestones. Ms. Cook daily duties involve developing and delivering progress reports to customers and stakeholders, participating in proposal support activities, developing requirements documentation, and delivering presentations. Ms. Cook maintains an important role in supporting the sales channel as she builds, develops, and grows any business relationships vital to the success of the program.

Ms. Cook's significant accomplishments include providing effectively program management on a portfolio of key projects that supported Harris Corporation's business objectives. Highlights of Ms. Cook's key significant accomplishments include the following:

- Continuous improvement for the Harris Corporation portfolio of services, valued at $4.5 million MRC, resulting in the award of new business on a continual basis.
- Assisted with development and implementation of the Proof of Concept for CenturyLink's Managed Trusted Internet Protocol (MTIPs) gateway

AMTRAK / National Passenger Railroad Corp. **Washington, DC** **2012-2015**
Senior Security Engineer/Senior System Architect

As Information System Security Manager at AMTRAK, Ms. Cook was responsible for architecting network solutions for nationwide video surveillance, as well as, executing PSIM integration and Network Security. She developed and implemented the Continuous Monitoring Program to maintain the authority to operate (ATO) to ensure proper vulnerability discovery and mitigation, boundary scope, and overall network security of the program, while maintaining FISMA compliance as defined by FIPs 199, 200 and OMB-circular A-130. She managed all Federal Regulatory Compliance reporting for Secure Network, including Plans of Actions and Milestones (POA&M) reporting. She advised Security and Network Engineers on configuring, implementing, and managing network components, such as servers, data storage systems, security software systems, applications software, camera data review systems, new MPLS sites, CCTV, and applications. Ms. Cook supervised A&A documentation, including monthly, quarterly and annual reporting and performed monthly vulnerability scanning for discovery and mitigation strategy development and execution.

Ms. Cook's significant accomplishments include the successful security management of AMTRAK IT systems which were critical to customer's operations. Highlights of Ms. Cook's key significant accomplishments include the following:

- Delivered implementation and migration of 300 cameras and other video surveillance equipment 2 weeks ahead of schedule through close collaboration with vendor and completion of network configuration.
- Increased productivity of staff utilizing standardized process for accessing camera systems, control systems, alarms, and sensors regardless of brand, across enterprise, by leading largest Physical Security Information Management (PSIM) implementation within transportation sector integrating thousands of cameras across the United States from different manufacturers into one common operating platform.
- Facilitated federal agency information sharing for organization by executing initial and on-going A&A activities, achieving ATO for Amtrak FISMA certification project.

CenturyLink **Fairfax, Virginia** **2007-2012**
Program Manager – Federal Programs

Ms. Cook led daily operations for Amtrak Police Department Secure Network (ROMAN), including supporting equipment such as MPLS, Colocated Hosting/Data Centers, Managed Firewall/Intrusion Detection Prevention

Services, vulnerability management, Managed Network Services, CCTV, Internet Hosting and mobile VPN. Highlights of Ms. Cook's key significant accomplishments include the following:

- Captained Physical Infrastructure Security Program for Amtrak conducting vulnerability assessments, risk analysis, and counter-terrorism risk management strategies protecting critical infrastructure assets, as well as, managing $10M budget constructing 65 node network with Total Cost of Ownership savings of 35% against existing business network; complete with fully redundant bi-coastal data centers.
- Maintained 87% win rate serving as Technical Writer/Program Management SME for government RFPs.

MCI WORLDCOM / VERIZON Business **McLean, Virginia** **1999-2007**
Engineer / Engineering Program Manager

Ms. Cook served as the dedicated Program Manager to the Department of State Telecommunications Program Office (DTS-PO) for Spectrum program. She managed day-to-day activities, collaborated with sales team on proposal development and submission via SPECTRUM contract vehicle, and delivered scope, time estimation, implementation plan, and cost for various phases of project lifecycle. She developed and managed customer relationships at all levels of agency providing expertise and leadership regarding telecommunications technology implementation and project execution. Ms. Cook created and established an operational framework for projects that included detailed project plans, project organization and administration. Her duties included monitoring and adjusting project performance against key metrics such as budget, service delivery, and network performance. Ms. Cook identified, assessed, and resolved network infrastructure implementation issues. She also reviewed customer deliverables for content and quality. Ms. Cook drove the Department of Defense FTS2001 transition as Dedicated Program Manager and lead engineer furnishing full lifecycle program management, pairing with GSA and DoD migrating 25k+ voice and data circuits in over 800 global locations. Highlights of Ms. Cook's key significant accomplishments include the following:

- Implemented first International Naval Exercise Private IP (PIP) network for Navy Communications Management Office (NCMO) facilitating United States Navy exercises with international partners such as Australia, Germany, Japan, the United Kingdom and Canada.
- Established telecommunications trailers and other posts in theater during wartime for US DoD allowing service members to maintain contact with stateside relatives.

Certifications / Training

Project Management Professional (PMP™), active since 2005
Certified Information System Security Professional (CISSP) certification, since 2010
Certified Cloud Computing Security Knowledge (CCSK), since 2012
ITILv3 certification, since 2016

Professional Memberships / Associations

Project Management Institute (PMI)
International Information System Security Certification Consortium $(ISC)^2$
Society of Women Engineers
American Society for Industrial Security (ASIS)
Cloud Security Alliance

GORDON L. GEE
DIRECTOR, FEDERAL PMO

Experience Summary

Gordon L. Gee is a proven Director within CenturyLink's Program Management Office with 30 years of demonstrated Telecommunications experience. Mr. Gee is a dedicated, energetic, and versatile professional with expansive technical skill set built from holding technical and advanced degrees that are used to focus on telecommunications and security solutions. He has gained deep expertise in sales engineering, strategic planning, managing complex projects and teams, team building, cost optimization, and risk management.

Role and Understanding of the Process

Mr. Gee is responsible for all aspects of Program/Project Management processes and lifecycle management. He is directly responsible for PMO managers and, by extension, individual contributors. Mr. Gee is a point of escalation both internally and customer-facing, to ensure appropriate project support and project deliverables. For the Nebraska NG-911 implementation, Margaret Cook reports directly to Mr. Gee. He has managed installations, testing, and internal teams and contractors on various project implementations. He is responsible for the quality of the systems, implementation of processes and endeavors to deliver high-quality products that meet and exceed customer requirements and expectations. With CenturyLink, Mr. Gee is currently managing the NG-911 system implementation for the State of California. This includes the deployment of Next Generation Core Services (NGCS), ESINet and the aggregation network to all Originating Service Providers (OSP). Mr. Gee specializes in the following product solutions: E911/NG-911, UCaaS, Contact Center, VoIP, Managed Security Services, Dark Fiber, Private Dedicate Rings/Networks (PDR/PDN), Wavelength Services, TDM T1/T3 Services, Ethernet Private Lines, Ethernet Virtual Private Line Service, Multi-Protocol Label Switching Service and Internet.

Mr. Gee leverages his expertise and experience to promote the application of program and project management standards to ensure deliverables consistently meet contractual requirements and satisfy high-quality standards for the customer and CenturyLink. His objective is to deliver outstanding customer service through consistent, on-time and on-budget project delivery. Over his career at CenturyLink, Mr. Gee's keen focus on deployment of telecommunications solutions with strict adherence to and conformance with customer needs. Mr. Gee is a skilled communicator as he broadly communicates his initiatives, receives affirmation, and implements plans across the entire program to achieve customer goals.

Education

Master of Business Administration, Finance, Johns Hopkins University – Carey School of Business, Baltimore, MD, 2009

Bachelor of Science, Electrical Engineering, University of Alberta, Edmonton, Alberta, Canada 1998

Relevant Employment/ Project History

CenturyLink **Herndon, Virginia** **2018-Present**
Director, Federal PMO

Mr. Gee manages the project and program management teams that deploy telecommunications and professional service solutions to Federal, State and Local government agencies, Research and Education and Large System Integrators. Mr. Gee is responsible for managing and documenting complex projects, planning and managing staff resources, managing risks and communicating and coordinating with all internal and external stakeholders. He is responsible for executing projects or project components from inception to implementation. For ongoing programs, he develops the operational support model. He establishes the appropriate project team structure, reporting, and metrics to measure performance against plan while ensuring processes are in place to support the products. Mr. Gee develops, interprets and implements financial business concepts for business planning and control. He drives

product development or operational processes to meet program and project objectives. Highlights of Mr. Gee's key significant accomplishments include the following:

- Developed the PMO team to oversee and manage all NG-911 solutions
- Implemented a dedicate PMO team for the Commonwealth of Pennsylvania that manages and supports the customer's DWDM, Routing and Switching networks; , including a comprehensive suite of Manage Security Services (MSS). This implementation resulted in significant cost savings for the Commonwealth

Level 3 Communication **McLean, Virginia** **2012-2017**
Manager, Federal PMO

As Manager in the Federal PMO at Level 3, Mr. Gee specialized in outside plant (OSP) fiber design, implementation and testing. He managed contractors and field resources throughout the project to ensure quality and on time delivery. Mr. Gee interpreted project requirements and communicated project scope to clients and eco-teams ensure milestones were met. He managed dependencies across projects and leads project meetings involving customers, partners and cross-functional teams. His other key responsibilities included reporting regular status updates to senior executives and key project stakeholders; performing technical analysis to determine present and future business performance; driving metrics to all layers of the organization (end-to-end and sub-pieces, organization and by individual). He identified areas of process and drove system improvement based on data. Highlights of Mr. Gee's key significant accomplishments include the following:

- Managed and oversaw the deployment resilient Fiber Optic rings for the US Government
- Developed and productized a new FedRAMP UCaaS product offering for Government customers and oversaw the first implementation for a Federal Agency

ASM Research **Fairfax, Virginia** **2012-2012**
Technical Consultant

As a Technical Consultant, Mr. Gee was a member of proposal team who assisted in the development and writing of the T4 proposal for US Department of Veterans Affairs. He defined Program Management Office management structure, resources and execution strategy as well as examined the technical feasibility of a VoIP solution and specified implementation resources.

OCEUS Networks (F/K/A Ericsson Federal) **Reston, Virginia** **2010-2011**
Technical Consultant

As a Technical Consultant, Mr. Gee engineered and proposed telecommunication solutions that include the various technologies, including Tactical 3G/4G Wireless (network in a box), Ericsson 3G (WCDMA/HSPA) QuicLINK and Oceus Networks 4G (LTE) Xiphos, Commercial 3G/4G Wireless: Ericsson RAN (RBS) and Evolved Packet Core, Optical: Ericsson/Marconi MHL-3000 DWDM/CWDM and Ericsson WDM PON, Data/TDM: Ericsson OMS 800, OMS 1200, OMS/SPO 1400, OMS 1600, OMS 2400, Distributed Antenna System: Powerwave FBU and Nexus FT, and Microwave Radio: Ericsson Mini-Link short-haul and Marconi long-haul microwave radios.

Mr. Gee engineered WDM networks using Ericsson's LDT, INTERplan, INTERconfig, and Autorack optical software planning tools. He served as solutions lead for the DISA account team and proposed a migration strategy to move from ATM to IP. He designed microwave links using Pathloss 5 software. Mr. Gee attended customer meetings to gather requirements and assess business opportunities. He created network design and solutions for RFI/RFPs, developed Mobile Virtual Network Operator (MVNO) value proposition and marketing collateral; and created a winning proposal for a distributed antenna system (DAS) solution for the United Nations.

NEC America **Fairfax, Virginia** **2012-2012**
Director of Product Management / Systems Engineering

As a Director of Product Management, Mr. Gee managed the telecommunication product line that consisted of fiber optic transport (CWDM and DWDM), hybrid TDM/Ethernet switches, MPLS-TP data transport, and Passive Optical Network (PON) access technologies for the US and Canadian markets. He designed and engineered optical and data networks for clients based on their requirements and applications. He assembled a systems engineering organization from scratch for which he defined all its processes and job functions. Mr. Gee expanded the product portfolio by establishing third-party OEM and reseller agreements. He conducted market research and competitive analysis; developed marketing collateral, white papers, and training program for sales/marketing teams and clients.

Mr. Gee wrote and presented business cases to executive management to justify new product development. He managed product certification such as NEBS, MEF and UL and presented product and network solutions to clients. He responded to customer's RFI/RFP/RFQs and managed the installation of new DWDM and transport networks in labs and First Field Applications. Mr. Gee managed department budgets and ensured compliance to corporate regulations. He developed a systems integration model featuring NEC professional services and non-NEC products to generate new revenue streams. Highlights of Mr. Gee's key significant accomplishments include the following:

- As Program Manager, he successfully managed the certification and product acceptance of NEC's DWDM equipment in AT&T's lab for North American backbone deployment.
- He won a systems integration contract with The Port Authority of New York and New Jersey to upgrade their DCE communication network at all PATH stations.

Certifications / Training

None

Professional Memberships / Associations

P. Eng. Professional Engineers Ontario

Delaware

The First State

I, JEFFREY W. BULLOCK, SECRETARY OF STATE OF THE STATE OF DELAWARE, DO HEREBY CERTIFY THE ATTACHED IS A TRUE AND CORRECT COPY OF THE CERTIFICATE OF AMENDMENT OF "QWEST COMMUNICATIONS COMPANY, LLC", CHANGING ITS NAME FROM "QWEST COMMUNICATIONS COMPANY, LLC" TO "CENTURYLINK COMMUNICATIONS, LLC", FILED IN THIS OFFICE ON THE TWENTY-FIFTH DAY OF MARCH, A.D. 2014, AT 1:44 O'CLOCK P.M.

AND I DO HEREBY FURTHER CERTIFY THAT THE EFFECTIVE DATE OF THE AFORESAID CERTIFICATE OF AMENDMENT IS THE FIRST DAY OF APRIL, A.D. 2014, AT 12:01 O'CLOCK A.M.

Jeffrey W. Bullock, Secretary of State

0642301 8100

AUTHENTICATION: 1237671

140376224

DATE: 03-25-14

You may verify this certificate online at corp.delaware.gov/authver.shtml

State of Delaware
Secretary of State
Division of Corporations
Delivered 01:44 PM 03/25/2014
FILED 01:44 PM 03/25/2014
SRV 140376224 - 0642301 FILE

CERTIFICATE OF AMENDMENT

to the

CERTIFICATE OF FORMATION

of

QWEST COMMUNICATIONS COMPANY, LLC

This Certificate of Amendment to the Certificate of Formation of Qwest Communications Company, LLC, a Delaware limited liability company, dated as of March 13, 2014, is being duly executed and filed by Stacey W. Goff, as an authorized person, acting pursuant to Section 18-202 of the Delaware Limited Liability Company Act, to amend the Certificate of Formation to change the name of the limited liability company to "CenturyLink Communications, LLC."

FIRST. Prior to the amendment adopted hereby, the name of the limited liability company is Qwest Communications Company, LLC.

SECOND. The Certificate of Formation of the limited liability company, executed and filed with the Delaware Secretary of State effective January 2, 2009, is hereby amended by restating the first article thereof in its entirety as follows:

> "The name of the limited liability company formed hereby is CenturyLink Communications, LLC."

This Certificate of Amendment shall be effective on April 1, 2014 at 12:01 a.m. Eastern Daylight Time

IN WITNESS WHEREOF, the undersigned has executed this Certificate of Amendment to the Certificate of Formation on March 13, 2014.

Stacey W. Goff
Authorized Person

CenturyLink

State of Nebraska

Next Generation 911 Emergency Services
IP Network (ESInet) and Next Generation Core Services (NGCS)

RFP No.: 6264 Z1

Sample Program Management Plan (PMP)

June 3, 2020

CenturyLink

Table of Contents

1. Document Control

Ownership of the *Program Management Plan* (PMP) belongs to the CenturyLink Program Management Office.

CenturyLink Program Manager	CenturyLink Program Director
Maggie Cook 571.730.3096 Margaret.Cook@CenturyLink.com	Gordon L. Gee 571.730.6591 Gordon.Gee@centurylink.com

2. Revision History

Date of Release	Version	Modification
May 5, 2020	1.0	Original Document Draft Completed.

3. Introduction

The *Program Management Plan (PMP)* outlines how CenturyLink works with the State of Nebraska to, deliver and implement Next Generation 911 (NG-911) services in Nebraska. The PMP is the controlling document regarding project process and procedures and is revised in conjunction with input from all stakeholders. In the event a change needs to be made to the PMP, the CenturyLink Program Manager completes the revision and provides a revised copy of the PMP to all stakeholders for review and agreement. The PMP describes the tasks necessary to execute project outcomes and shows the overlap and dependencies of each activity.

4. Project Management Approach

CenturyLink has mobilized several internal teams to address the many aspects of this project. These teams are comprised of Engineers, Technicians, and Subject Matter Experts (SMEs) devoted to implementing the Nebraska NG-911 solution successfully. Each team has specific responsibilities and duties to perform for the overall project. The CenturyLink Program Manager is responsible for the oversight of all personnel assigned to this project and maintains reach back across the organization when additional resources are needed, or escalations become necessary to achieve the goal. The combined effort of these teams allows for a smooth delivery of services associated with the NG-911 project.

Prior to the deployment stage, CenturyLink holds Project Kickoff meetings with each team separately and with all teams together to ensure complete understanding of the project goals and contracted outcomes. CenturyLink also holds Discovery meetings within each group to determine who would be best suited to provide the services necessary to meet the timelines and requirements of the NG-911 project. A Kickoff meeting is then held with the state to inspire further discussion, answer questions, and gain a mutual understanding of all expectations going forward.

5. Key Personnel

Designation of Key Staff is one of the first deliverables for the project. The following table represents an expanded form of the initial version. The team shown below is responsible for over program success.

5.1 Account Team

CenturyLink's account team, under the guidance of the Director of Sales provides the State of Nebraska with information about CenturyLink services and serves as the overall point of contact for CenturyLink sales. Our account team is responsible for gathering and confirming NG-911 all specifications and requirements necessary to submit an order. Our account team works closely with stakeholders to execute all quotes and orders for new and additional CenturyLink services, and assists them through the credit application process.

Name	Title	Phone/Mobile	Email
Bjorn Johnson	**Sr. Account Manager**	**605 977 2820**	**Bjorn.Johnson@CenturyLink.com**
Jon Osborne	**Account Director**	**402 998 7392**	**Jon.Osborne1@centurylink.com**
Carlos Simmonds	**Account Director**	**602 512 2535**	**Carlos.Simmonds@CenturyLink.com**
Stephen Doyle	**Sales Director**	**520-292-5618**	**Stephen.Doyle@centurylink.com**
John Shuttleworth	**Senior Director Sales**	**571 730 6522**	**John.Shuttleworth@centurylink.com**

5.2 Sales Engineer (SE) –

CenturyLink's SEs work with the State of Nebraska's stakeholders to identify technical options and define technical requirements for implementing the services. Our SEs are responsible for understanding the existing network, key locations and potential need or the customer. With technical knowledge and information about CenturyLink services, our SEs manage the engineering portion of the service quote the inventory and the capacity process for the new order.

	Contact	Title	Office	Mobile	Email
Level 1	Steve Deloach	Sales Engineer	434 971 3871		Steve.Deloach@centurylink.com
Level 1	Steve Klocek	Sales Engineer	763 400 5492		Steven.Klocek@centurylink.com
Level 1	Cathy Atkin	Sales Engineer	520 526 1877		Cathy.Atkin@CenturyLink.com
Level 1	Nancy Serafino	Sales Engineer	567 345 0814		Nancy.C.Serafino@centurylink.com
Level 2	Stephen Doyle	Mgr, Sales Engineer	520-292-5618		Stephen.Doyle@centurylink.com
Level 3	John Shuttleworth	Dir, Sales Engineers	571 730 6522		John.Shuttleworth@centurylink.com
Level 4	David Young	VP Sales, Government	571 730-6516	202 253-0452	David.Young@CenturyLink.com

5.3 Program Management – Maggie Cook, PMP, CISSP, CCSK and ITIL certified

CenturyLink's Program Manager (PM) is responsible for the oversight of the implementation and life cycle management of NG911 solutions. The Program Manager serves as a primary point of contact for all post sales activities, including program and service delivery issues and general program questions. The Program Manager also serves as a point of escalation for program issues, tracking and resolution has reach-back across all levels of CenturyLink, and acts as the customer advocate within our organization.

	Contact	Title	Office	Mobile	Email
Level 1	Maggie Cook	Senior Federal Program Manager	571-730-3096	703-867-2095	Margaret.Cook@CenturyLink.com
Level 2	Gordon Gee	Director, Federal PMO	703-386-2475	703-728-2834	Gordon.Gee@CenturyLink.com
Level 3	Seana Gilliland	VP, Federal PMO	571-730-6577	703-966-8701	Seana.Gilliland@CenturyLink.com
Level 4	David Young	VP Sales, Government	571-730-6516	202 253-0452	David.Young@CenturyLink.com

5.4 Customer Care Manager (CCM) -

The CCM serves as the point of contact for the CenturyLink Customer Care organization and is responsible for planning, directing, and coordinating service delivery activities to ensure the project goals and objectives remain on track. The CCM manages new install orders as soon as the sales representative promotes the quote to an actionable order in our systems. More specifically, CenturyLink's CCM reviews documents to make sure all necessary technical and contact information has been received and oversees the assignment of capacity, testing, and activation of the service. Our CCM ensures that required documents are properly filed, tracked the status of the order to support on-time delivery, and proactively communicates updates throughout the service activation process.

The Customer Care Management Contact and Escalation Matrix specifically for State of Nebraska is listed below:

	Contact	Title	Office	Mobile	Email
Level 1	Caroline Bussell	Customer Care Manager	317-697-4499		Caroline.Bussell@centurylink.com
Level 2	Mary Anderson	Mgr, Customer Service	402 998 7386		Mary.Anderson1@CenturyLink.com
Level 3	David Nguyen	Dir, Customer Service	872 759-9241	469 667-4023	David.Nguyen@CenturyLink.com

5.5 Operations Service Manager (OSM) –

CenturyLink's Operations Service Manager (OSM) serves as the customer advocate responsible for providing Operations Reviews including Metrics, Event and Escalation Management, and Reason For Outage (RFO) Management. It is important to note that the OSM is an addition to the primary escalation processes. Escalations should only be routed to the Operations Service Manager if the primary process has not achieved desired results to avoid confusion of information and ensure communication updates through resolution are provided to State of Nebraska as quickly as possible.

Name	Title	Phone/Mobile	Email
Rachel Renteria	Operations Service Manager	214-533-9452	Rachel.Renteria@CenturyLink.com
John Atkinson	Post Sales Engr Manager	602 563 3292	John.Atkinson@CenturyLink.com
David Mueller	Senior Manager: MAS	720 888 2634	Dave.Mueller@CenturyLink.com
Chris Noble	Director, Operations Management	918 547 9799	Chris.Noble@CenturyLink.com

6. Project Schedule

CenturyLink will build a detailed Project Schedule using Microsoft Project, which lists the Milestones for the project, along with detailed steps for each of those Milestones. The schedule will also provide the means for CenturyLink and the State of Nebraska to monitor the implementation of the project throughout all stages. Once a schedule is agreed on, detailed dates and anticipated days for performance will be added. Through a series of meetings with State designees CenturyLink Program Management will finalize the schedule and track the completion of the following milestones:

1. System Design
2. Development and Finalization of a Statement of Work
3. Build out and testing of the network and deployment of the Functional Elements
4. Interconnection with Originating Service Providers
5. Interconnection with Ancillary systems
6. Gateway/network interface
7. ALI format and interface testing
8. Comprehensive test and acceptance plans for all network connections, verifying all functionality with the PSAP and/or Call Handling Equipment provider solutions
9. Functional specifications testing
10. Final acceptance testing
11. 30-Day reliability testing
12. Solution acceptance

CenturyLink tracks major Milestones in the NG-911 management plan using the Project Schedule. Each of these Milestones represent significant progress during the program. Please refer to the sample project schedule in the attachment file named: "**2.e Sample Nebraska_Draft Project Schedule_Gantt Chart Format**".

7. Site Surveys

External Dependency: If necessary. Approved by the State of Nebraska Survey and Coordination Schedule

Task Name	% Complete	Duration	Start	Finish
Site Surveys				
Submit site survey to STATE for review		5 days		
STATE returns survey		5 days		
Authorization to Proceed with surveys		1 day		
Conduct Site surveys		32 days		

CenturyLink completes a Site Survey at each PSAP/location where the stakeholders determine Network terminations and Network Interfacing Device (NID) Equipment Installation. The CenturyLink Implementation Project Manager coordinates each site visit with the State of Nebraska.

CenturyLink arrives onsite at a predetermined time and date and uses the Site Survey Template provided by CenturyLink. We note all findings on the Site Survey form, along with pictures taken at the PSAP. To ensure accuracy when compiling documents, all pictures include dates and the PSAP name.

CenturyLink provides the Site Survey form and detailed supporting documentation to the State of Nebraska for approval prior to starting this project.

We provide a priority list we built that is based on the Site Survey results. PSAP's that require additional corrective actions (i.e., fiber extension to demarcation, additional power to racks, additional rack placement, etc.) are moved to the bottom of the installation schedule if needed to avoid delays in schedules.

Not all locations require site surveys due to the site nature, i.e. data center. In this case the site demark information are documented, and the team proceeds with installation.

Sites and planned dates for each site are as follows:

Task Name	Duration	Start	Finish
Site Surveys			
South Central Region (VIPER)			
Buffalo	1 day	TBD	TBD
Dawson	1 day	TBD	TBD
Dawes	1 day	TBD	TBD
South Eastern Region (Motorola)			
Data Center 1	1 day	TBD	TBD
Data Center 2	1 day	TBD	TBD
East Central Region (Motorola)			
Hall	1 day	TBD	TBD
Saunders	1 day	TBD	TBD
North Central Region (Ztron)			
Cherry	1 day	TBD	TBD
Holt	1 day	TBD	TBD
East Central Region (VIPER)	1 day	TBD	TBD
Douglas	1 day	TBD	TBD
Pottawattamie	1 day	TBD	TBD
Metro West (VIPER)			
Dodge	1 day	TBD	TBD
Colfax	1 day	TBD	TBD
North Eastern Region			
Madison	1 day	TBD	TBD
Wayne	1 day	TBD	TBD
Cedar	1 day	TBD	TBD
Dakota	1 day	TBD	TBD

8. Network Requirements and Final Design Solution

External Dependency: Complete Network requirements and final design requirements with STATE

Task Name	% Complete	Duration	Start	Finish
Product Development				
Design POI and Aggregation Points				
Design and build NGCS				
Design and build Ingress Circuits				
Design and build Egress Circuits				
Design and order NG-911 Trunk Services				
Develop and Document Interfaces				
Document Database Integration				
Dashboard Development				

8.1 Design Point of Interface (POI) and Aggregation

External Dependency: OSP LATA requirements

CenturyLink determines POI locations and trunk count based on dialog with the State, OSP and wireless carriers. Dialog diversity from each POI are established based on the amount of physical connectivity required to support trunking and network interconnections.

8.2 Design and Build-Out Next Generation Core Services (NGCS)

External Dependency: None

CenturyLink deploys physical hardware and necessary software in our geo-diverse datacenters.

8.3 Design and order NG-911 (Egress) Services

External Dependency: PSAP Access, Availability of Power, Space and Entrance Facilities.

CenturyLink will identify the appropriate access providers with the State of Nebraska who are available to build out diverse connectivity to each required location. When confirmed by the State, CenturyLink will order the circuits necessary to maintain diversity to each PSAP/datacenter.

8.4 Database Integration Design

External Dependency: Input from PSAPs

CenturyLink will work with the State on database design.

8.5 Dashboard Development

External Dependency: Input from stakeholders

CenturyLink works with the stakeholders to develop a dashboard that encompasses all the pertinent information needed.

9. Originating Service Providers (OSPs) Aggregation Connectivity

External Dependency: OSPs

Task Name	% Complete	Duration	Start	Finish
OSP Aggregation Connectivity	0%			
Letter of Agency (LOA)	0%			
Validate trunk count w/OSPs and other carriers	0%			
Establish POI	0%			
Establish LNG	0%			
Establish trunking w/OSPs and other carriers	0%			

CenturyLink's NG-911 Aggregations Services Coordinator works with the Originating Service Providers (OSPs) and other carriers to order and install trunks to support the ingress and aggregation of 9-1-1 traffic. Tracking and testing are completed by internal CenturyLink teams (i.e., provisioning, OSP, etc.).

- Letter of Agency (LOA) provided to the OSPs and carriers from CenturyLink
- Validate trunk count from serving End offices with OSPs and carriers
- Establish POI – CenturyLink Trunk Services Coordinator works with OSP to deliver T-1 circuits to Carrier Facility Access Points; this depends on Local Access Transport Area (LATA) restriction and are reviewed with the OSP as well as the State of Nebraska.
- Establish LNG – connect POI to diverse Legacy Network Gateways via diverse connectivity.
- Establish Time Division Multiplexing (TDM) (ISUP) trunks over T-1 links with OSP.

10. Interface and implementation

External Dependency: PSAP Facilities

Task Name	% Complete	Duration	Start	Finish
Infrastructure Build				
Finalize PSAP site list with the state of Nebraska				
Determine on-net/off-net sites				
ID logical network addresses				
Complete Network/circuit Design				
Order materials				
Review & approve w/State of Nebraska for PSAP Delivery				

10.1 Ordering:

CenturyLink will submit circuit orders for the ESINet and manage their delivery against the master project schedule. However, there may be delays caused by the following:

- Capacity issues – CenturyLink makes every effort to ensure that circuit capacity is available to support the new ESInet. However, capacity can occasionally become consumed during the timeframe from quote to customer order request. In these instances,CenturyLink advises the customer of the issue and works to find available capacity. If new construction is needed, CenturyLink Program Manager and CCM will work with internal engineering and construction teams to expedite delivery to keep the project on schedule. If delay is caused by construction or equipment upgrade for an offnet circuit, CenturyLink will escalate with the third party carrier using well established processes.
- Circuit Diversity Type (physical path, electronics, etc.) and avoidance(s) criteria not met
- Unknown connector types LC versus the CenturyLink standard SC, Fiber types requested such as Multi-mode versus the CenturyLink standard Single mode fiber.
- Deficient panel termination information such as specific ports or next available on which panel.
- Unclear availability of DC or AC Power types,amperages & termination requirements.
- Cabinet or rack types and dimension requirements.

When an order is submitted, it is the responsibility of the CenturyLink Customer Care Manager to ensure implementation is accurate and on time. The CenturyLink CCM, Caroline Bussell, provides order status, via spreadsheet, no less than three times per week. Status calls are held every Monday and can be moved or cancelled at the discretion of the customer.

Implementation time frames are built upon standard intervals for each service type. The draft Project Schedule included as an attachment to this document has been built on standard intervals.

Expedite orders:

In some cases, the standard interval may not meet the customer's need for implementation timeframes. In this case, an expedite request may be attached to the order. If the expedite is made at the request of the customer, an expedite charge may apply. However, if there is an issue that is beyond the customer's control, CenturyLink may submit an expedite request on the customer's behalf at no additional charge to the customer. All expedite implementations are handled as a priority by the Service Delivery Project Manager. However, all expedite orders, while they may result in a shortened implementation timeframe, are considered best effort and may vary depending upon the local provider. In other words, CenturyLink makes every effort to deliver the circuit(s) in a timeframe shorter than standard interval, however, if capacity or other issues exist, the timeframe may not be able to be shortened.

Order Information Verification and FOC Notification:

In order to ensure that all implementations go through the process smoothly the CCM attempts to verify all information on the order at the time of receipt. The CCM sends the provided point of contact the email below. The email has been standardized to address all service types and contains the pertinent information required. If the information on the email notification differs from that on the TSO or if the local point of contact has information that is contrary to that provided, the CCM, along with the rest of the team, should be notified as quickly as possible.

During the order entry process, an ASR must be issued to the local exchange carrier. If the address information is incorrect or the local point of contact provides information that differs from the TSO, CenturyLink requires a supplement to the TSO. All intervals are restarted upon receipt of the supplemental order by CenturyLink.

The notification email is re-sent to all parties upon receipt of a Firm Order Commitment or install date from CenturyLink or the third party carrier. Upon receipt of the FOC date notification, CenturyLink requests that the State of Nebraska and/or PSAP confirm the receipt and demark the location and availability of the local point of contact (LCON) for the PSAP. CenturyLink makes every effort to ensure that the operations field tech for CenturyLink or the third party carrier reaches out to the local point of contact prior to arriving at the site, however this is does not always happen. To ensure the LCON is kept aware of circuit delivery time and demark location, this notification and acknowledgement is a valuable tool.

11. Infrastructure Build

11.1 Finalize PSAP Site List with the State of Nebraska

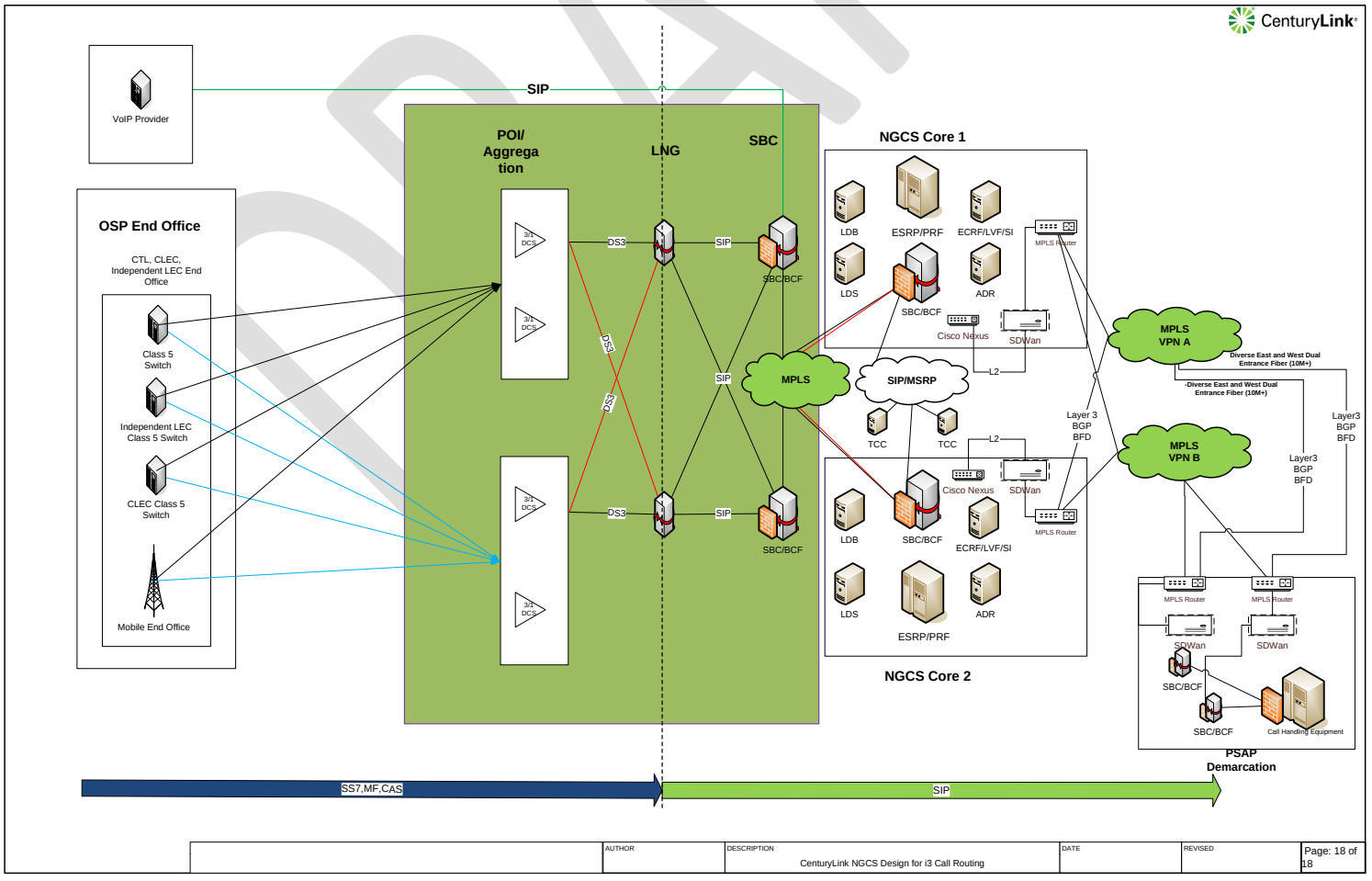
CenturyLink received the PSAP list with address and contact information from the State of Nebraska. Additional missing detail for sites are updated prior to starting this project.

11.2 Determine On-net/Off-net sites

CenturyLink has evaluated the network locations for the entire state of Nebraska and has selected access providers for network. In this list, we have designated locations which already have CenturyLink facilities and sites that CenturyLink provides construction for fiber plant.

11.3 Complete Network Design

CenturyLink's network design is segmented into 3 parts: Ingress/Aggregation, NGCS, and NG-911 trunk or ESINet. Each segment has its own appropriate services that are documented as details are established to facilitate these designs. An initial diagram for the network design is provided below.



11.4 Order Materials

All hardware for delivery of PSAP endpoint is ordered, inventoried, and stored for PSAP implementation, by CenturyLink.

11.5 Review and Approve with State of Nebraska for PSAP Delivery

CenturyLink Program Manager will receive confirmation from the state of Nebraska to proceed with implementation.

12. Implement NG-911 Egress Circuits/Trunks at PSAPs

External Dependency: The State of Nebraska and CenturyLink need to compile an accurate contact list, identify unknown outside plant build requirements, and agree upon a Logical IP schema.

Task Name	% Complete	Duration	Start	Finish
PSAP Connectivity	**0%**			
Deliver and Test Circuits to all PSAPs	0%			
NG9-1-1 NGCS	**0%**			
NG-911 NGCS Connectivity	0%			
NG-911 Functional Element Provisioning	0%			
NG-911 Solution	0%			

12.1 Receive, Create and Verify IP Assignments

CenturyLink establishes logical address assignment (IPv4 or IPv6) based on the agree design terms. Based on these design terms, CenturyLink creates a record for the deployment and WAN assignments are ordered with the NG-911 trunk services that contain the routing and blocks associated with each specific site.

12.2 Order, Install, and Test NG-911 Trunks for PSAP

Upon completion of the site surveys and an evaluation of available CenturyLink, Local Exchange Carrier (LEC) and 3rd party providers, the CenturyLink Project team places all circuit orders for each of the PSAP's and Data Centers in Nebraska. The orders are placed in the same priority order as the site surveys were completed. Circuit orders are tracked to their completion by CenturyLink personnel in our circuit provisioning team. Then, CenturyLink sends a formal notice of circuit installation completion to the end customer once a circuit has been successfully installed, tested for Layer 1 connectivity, and is ready for use. We also track completion of each site and report our progress to the State of Nebraska office in our weekly status meetings.

12.3 Activate NG-911 Trunk

The CenturyLink NG-911 Trunk Services Coordinator is responsible for serving as the point of contact to facilitate the circuit installation at each PSAP in Nebraska and providing updates to the CenturyLink Program Manager. The CenturyLink NG-911 Trunk Services Coordinator also works closely with the CenturyLink NG-911 Core Services Coordinator to schedule circuit turn-ups at each of the PSAP's and backup Center sites. All work is coordinated between the CenturyLink Program Coordinator and the State of Nebraska.

12.3.1 **Network Services Connectivity Confirmation**: The CenturyLink NG-911 Trunk Services Coordinator verifies that the network is deployed to each defined location on a "location-by-location" basis. From this confirmation, a dispatch leads the installation of extended demarcation wiring and associated hardware to the location identified during the site survey.

12.3.2 **Turn-up Network Services**: Activation of Multi-Protocol Labeling Service (MPLS) network to the edge device.

12.3.3 **Test Network Services**: Validation of routing and throughput to the NGCS locations from each diverse circuit.

12.4 Design & Implementation (This section may change and will require discussions with OSP's and the State of Nebraska upon award of this contract.)

12.4.1 Integration of local jurisdictional GIS and configuration of NGCS

Our CenturyLink NG911 Solution uses the ESRP/PRF and ECRF/LVF services built into NGCS (Next Gen Core Services) to replace the ALI and selective routing functions of the legacy 9-1-1 network. In addition to providing the routing of the calls based on the Customer's requirements, our NGCS also provides geolocation data for any jurisdiction to serve as the LDB in a true NG9-1-1 deployment or as an ALI-DBMS in a migration strategy.

Our CenturyLink NG911 solution has been provisioned with the functional elements (Core Services) defined by the end-state architectural specifications in NENA-STA-010.2 (Originally 08-003). CenturyLink and our core provider work with the state of Nebraska to populate the required location information into the LDB and maintain links to OSPs to allow this information to be updated. CenturyLink and our core provider also develop and maintain the PSAP routing rules appropriate to Customer's jurisdiction.

12.4.2 Interconnecting selective routers

Nebraska wants to eliminate the incumbent selective router as the source for calls inbound to this system. In addition, the state desires to establish capabilities for transferring calls between the NGCS and PSAPs still served by legacy selective routers.

We can provide unidirectional interconnectivity to selective routers in neighboring state, which will allow calls to be delivered to the selective router. This service is available on a per call basis. Bi-directional interconnectivity is required to receive 9-1-1 calls from neighboring selective routers. Bi-directional interconnectivity requires mileage sensitive TDM circuits to be provisioned between any of our existing POIs and the selective router.

At a high level, selective router interconnectivity involves the following areas of effort:

1. Providing and installing sufficient gateway (PIF) capacity for the project
2. Establishing general, multipurpose SS7 interworking capability at both of the POI sites in each LATA, including CLLIs and point codes.
3. Establishing bidirectional tandem-to-tandem connectivity with the current Legacy Selective

Router Gateways (LSRG's).

4. Provide ongoing professional services to operate the PIFs, maintain SS7 capabilities, and facilitate ongoing interoperation

Our team is responsible for engineering, provisioning, and maintaining the SS7 signaling capabilities at each POI. We coordinate with the OSPs to facilitate their installation of bearer T1s to the POIs and engineer and order the bearer circuits between the POIs and the LSRG's, leveraging their status as a CLEC in Nebraska and as the designated 9-1-1 service provider for the state to accomplish these tasks.

13. NG-911 NGCS

13.1 NG-911 Next Generation Core Services Connectivity

External Dependency: Final PSAP list

CenturyLink creates infrastructure orders for the network to the NGCS datacenters via *Session Border Controllers* (SBCs). This network includes the following topology:

13.1.1 Diverse MPLS connections to the CenturyLink LNGs for Ingress SIP traffic to each of the listed datacenters.

13.1.2 Diverse MPLS connections to the diverse CenturyLink MPLS cores that are used to egress traffic destined for State of Nebraska PSAPs.

13.1.3 Diverse connectivity to the NGCS datacenters:

- Cross-connect orders for each datacenter are issued to extend the connectivity to the location of the hardware.

14. NG-911 Functional Element provisioning

External Dependency: Updates from OSP

14.1 Border Control Function (BCF)

CenturyLink installs and tests Highly Available Session Border Controllers for security policies and SIP call anchoring. SIP headers can be manipulated to meet the format of the NGCS at this anchor point.

14.2 Emergency Call Routing Function/Location Validation Function

Upon receipt of an updated Geographic Information System (GIS) dataset, CenturyLink loads the *Emergency Call Routing Function/Location Validation Function* (ECRF/LVF) using the *Spatial Interface* (SI). CenturyLink works to define a process for adjudicating instances where there is a conflict in validity determination between CenturyLink systems and the GIS dataset received.

At a high level, CenturyLink's recommended approach for this resolution is as follows:

14.2.1 Determine the type of discrepancy.

14.2.2 Assess the source of the conflict.

14.2.3 Apply automated and human intelligence (where necessary) to resolve.

14.2.4 Implement the resolution.

Validation of GIS: When changes are submitted, a quality control process begins immediately checking the data for errors, which are then rated for severity and flagged for follow-up. This solution includes configurable quality control thresholds that can be used to block publishing to the ECRF/LVF. CenturyLink collaborates with the state to define a process for communicating such cases when they arise in order to resolve the underlying discrepancy and effectively resolve each case.

14.3 Policy Routing Function (PRF) Provisioning

CenturyLink gathers alternate routing information from individual PSAP management and, from the State for this function based on this information Policy Routing Rules are loaded into the PRF for each PSAP. This information is detailed to include timers and destined paths for emergency calls based on stipulated criteria that would impede normal call delivery.

15. System Acceptance Testing

External Dependency: STATE and PSAP readiness

Task Name	% Complete	Duration	Start	Finish
System Acceptance Testing				

CenturyLink has provided a comprehensive Sample Test Plan in the attachment "**2.d_Testing_Sample CenturyLink Test Plan"** to illustrate the steps that our technical staff will take prior to releasing the system for testing in conjunction with the state. For ease of use, when the system is ready for final testing the Sample Staging and Final Acceptance Plan checklist must be completed and agreed to by both the CenturyLink technical team and the state. These checklists are provided in attachment named "**2.d ss15_SAMPLE Staging and acceptance checklist**". Similar documents are presented at the program/project planning kickoff meeting and discussed in the project planning sessions to finalize the steps that both parties have agreed upon.

16. Preliminary Staging Plan

Staging Acceptance Test Plan (SATP)

- CenturyLink PM ships Equipment to location. CenturyLink Technician confirms all equipment is included in the shipment and inventories serial numbers. CenturyLink Field Technician provides handoffs for PSAP equipment (CAD, etc. as applicable) CenturyLink Field Technician connects System to network.

Staging Hardware, Software

- PSAP premigration activities
- Prep system for Field Engineer to install NID
- Final equipment configurations and testing (Software/Firmware Updates, network/NID devices only)
- Pre-cutover call: Customer approval to proceed

Staging for Final Acceptance Test Plan (FATP)

- Final test of network components
- Network migration to new system
- Complete migration

Final Procedure Steps: Observation and Acceptance

- Execute ATP
- Provisional acceptance accorded by state
- Perform 30-day observation period
- Perform 30-day Test
- Close punch list
- Update location profile in CenturyLink system for NG911 NOC
- Transition to operational environment
- Final acceptance by state – Customer Acceptance Form

After completion of the final network test and cutover, the CenturyLink Program Manager will provide the State of Nebraska with the results of final testing to include what is listed below and request formal acceptance from the State.

Final Documentation of Test - CenturyLink Project Manager will provide the State of Nebraska and PSAP of final results of test.
Network Connectivity (Can be run simultaneously)
NGCS – DNS
NG911 Aggregation – NGCS network

NGCS – network
NG911 Trunk – ESInet for each PSAP and CenturyLink lab
System Components
Integration – Policy DB
Integration – Location DB
Integration – State GIS (Utilizes a common NG9-1-1 GIS data set available for all PSAPs when a common NG9-1-1 GIS data set is established
NGCS - ECRF
NGCS – ESRP
NG911 Aggregation - LIF/NIF
NGCS – i3 Logging
System Monitoring
Exfo Probe to PSAP – CenturyLink lab
Pre-Cut PSAP Testing – CenturyLink lab
Call Testing
Exfo Probe to PSAP – per PSAP
Pre-cut PSAP testing - per PSAP.

Upon completion and receipt of Customer Acceptance, the CenturyLink engineering team provides “As-Built” PSAP drawings for the state.

17. Monthly Billing and SLA

External Dependency: None

Task Name	% Complete	Duration	Start	Finish
Monthly Billing and SLA Plan				
Billing*				
Operational SLA in Effect**				

** Potentially the start of billing for circuits*
*** SLA in effect following system acceptance*

Invoices are submitted per the instructions outlined in the contract. Invoicing of project Milestones only begin after testing and acceptance of systems by the State. NRC and MRC are submitted on separate invoices for total monthly services following the month in which the charges accrue. Any issues or questions with invoicing are brought to the attention of the State finance person assigned and to the attention of the CenturyLink PM for resolution. Invoices are submitted via email.

17.2 Billing Disputes

All CenturyLink customer billing inquiry and disputes may be submitted by one of the following methods:

Please refer to the customer's invoice for the contact email address that is most pertinent for their account type, otherwise there are continuously monitored mailboxes that provide an additional method for submitting requests. The customer receives confirmation of the request submitted and the assigned case tracking number within 72 hours. Below are details on the different mailboxes:

CenturyLink Enterprise accounts - Care.Inquiry@CenturyLink.com.

CenturyLink Wholesale accounts - Wholesale.Dispute@CenturyLink.com

Legacy CenturyLink Kenan accounts - Billing@CenturyLink.com

A Customer Financial Services Billing Coordinator contacts the customer within five (5) days of their submission. At that time, they request any additional information that may be needed to process the customer's request. It is the responsibility of the customer to provide all pertinent information requested with fifteen (15) calendar days of the Billing Coordinator's request. In order to expedite the request, it is important to provide all the required information at the time of the request submission and any supporting documentation that may help us resolve the request.

Please note: In the event CenturyLink does not receive further information after the third (3rd) request from the customer that is required in order to process their submission, it may be necessary to cancel the customer's request. The customer would then need to resubmit their request once they have the information required to process their request. Once the customer submits all necessary information, CenturyLink determines a resolution of the inquiry or dispute. The customer can then expect to receive a resolution notification from the Billing Coordinator that includes an explanation to their inquiry or dispute. Disputes should be submitted within 90 days of the invoice date unless otherwise stated in the Customer's MSA.

18. PSAP Training

The NG-911 *Training Plan* outlines the objectives, requirements, strategy, and methodology that is used when providing NG training to the PSAP users. The purpose of this training is to provide information about commonly used tools and the operation of the new NG-911 systems.

The *Training Plan* defines the following:

- Needs and Skills Analysis
- Training Methodology and Delivery Methods
- Training Schedule and Milestones

18.1 Needs and Skills Analysis

The State identified the need for its PSAP users to transition to a new Next Gen 9-1-1 service that is controlled and coordinated by the State office to ensure always-on service. To successfully implement this service, CenturyLink develops a training course and materials for State identified users in order to familiarize management and operators with the new functionality.

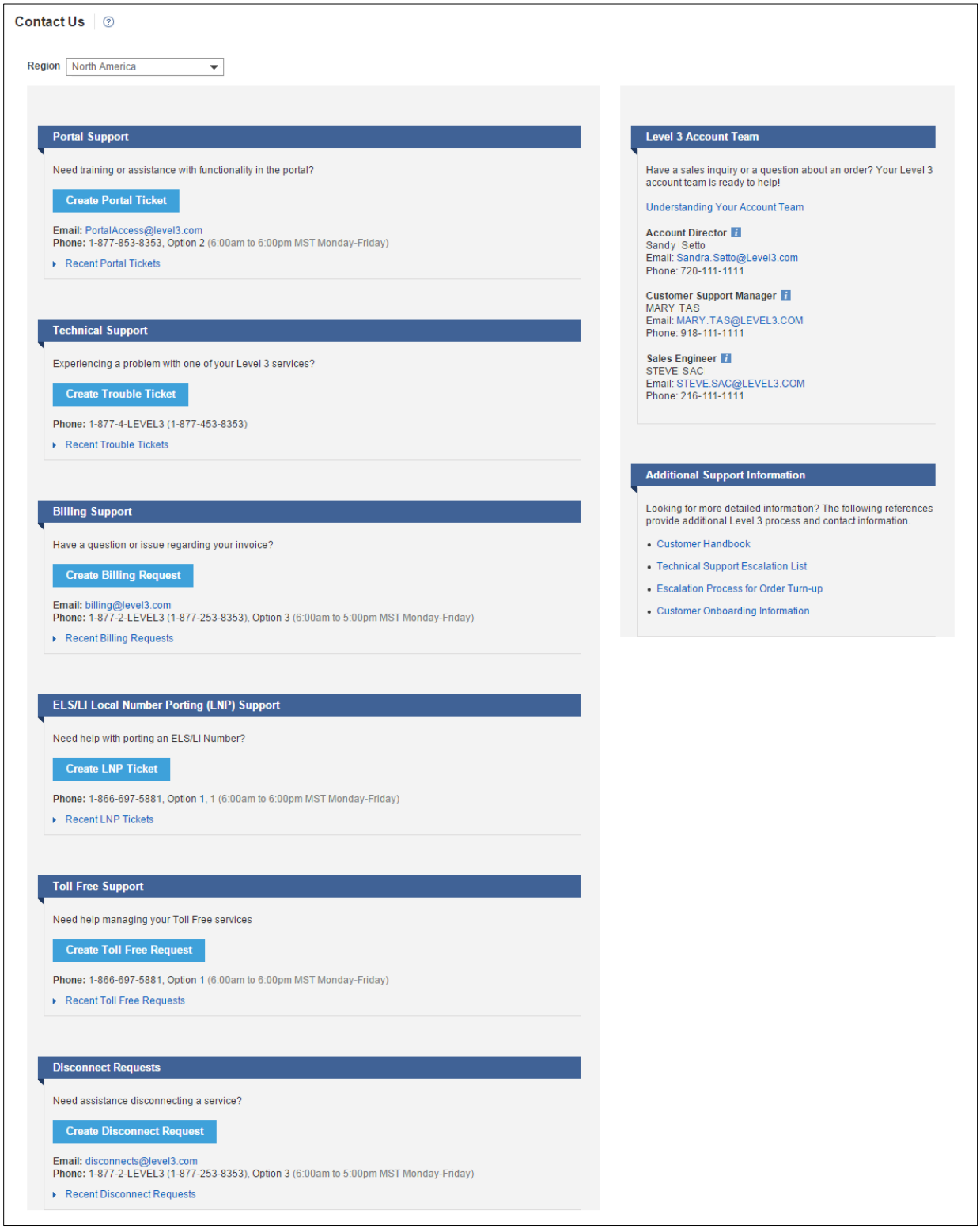
18.2 Training Schedule and Milestones CenturyLink issues

Communications about training content and sessions will be provided approximately thirty (30) days prior to the cutover for each site in conjunction with or via the State office. A training schedule and training sessions are developed for and coordinated with each site. We include a live 2-hour session to provide training on the CenturyLink Customer Portal.

CenturyLink's Customer portals are designed to help monitor and manage CenturyLink services during the ordering, implementation, and post-implementation phases. Through points of secure access, the portals provide direct line of communication, 24x7, from virtually anywhere in the world.

The customer portal includes a context-sensitive and searchable online help system with detailed description, step-by-step instructions for each portal feature, and online tutorials and webinars. Our Portal Support Center is available to assist with a broad range of issues, including general application questions, setup and management of Delegated Administrators, and capability questions and issues.

Important customer notifications are also posted to the portal's Home page and sent via email to keep users well informed so they can prepare for impacting events. In addition, the portal contains a Contact Us page that provides email and phone information by region for each CenturyLink support team, as well as the contact information for the specific account team.


Contact Us
Region
North America
Portal Support
Need training or assistance with functionality in the portal?
Create Portal Ticket
Email: PortalAccess@level3.com
Phone: 1-877-853-8353, Option 2 (6:00am to 6:00pm MST Monday-Friday)
Recent Portal Tickets
Technical Support
Experiencing a problem with one of your Level 3 services?
Create Trouble Ticket
Phone: 1-877-4-LEVEL3 (1-877-453-8353)
Recent Trouble Tickets
Billing Support
Have a question or issue regarding your invoice?
Create Billing Request
Email: billing@level3.com
Phone: 1-877-2-LEVEL3 (1-877-253-8353), Option 3 (6:00am to 5:00pm MST Monday-Friday)
Recent Billing Requests
ELS/LI Local Number Porting (LNP) Support
Need help with porting an ELS/LI Number?
Create LNP Ticket
Phone: 1-866-697-5881, Option 1, 1 (6:00am to 6:00pm MST Monday-Friday)
Recent LNP Tickets
Toll Free Support
Need help managing your Toll Free services
Create Toll Free Request
Phone: 1-866-697-5881, Option 1 (6:00am to 6:00pm MST Monday-Friday)
Recent Toll Free Requests
Disconnect Requests
Need assistance disconnecting a service?
Create Disconnect Request
Email: disconnects@level3.com
Phone: 1-877-2-LEVEL3 (1-877-253-8353), Option 3 (6:00am to 5:00pm MST Monday-Friday)
Recent Disconnect Requests
Level 3 Account Team
Have a sales inquiry or a question about an order? Your Level 3 account team is ready to help!
Understanding Your Account Team
Account Director
Sandy Setto
Email: Sandra.Setto@Level3.com
Phone: 720-111-1111
Customer Support Manager
MARY TAS
Email: MARY.TAS@LEVEL3.COM
Phone: 918-111-1111
Sales Engineer
STEVE SAC
Email: STEVE.SAC@LEVEL3.COM
Phone: 216-111-1111
Additional Support Information
Looking for more detailed information? The following references provide additional Level 3 process and contact information.
Customer Handbook
Technical Support Escalation List
Escalation Process for Order Turn-up
Customer Onboarding Information

Contact Us

Benefits of Using the Customer Portal

- **Convenience**—CenturyLink handle all tickets and requests with the same level of care whether our customers open them through the portal or call us directly. Our free online portal provides our customers with an easy and convenient way to manage tickets and requests that saves them time.
- **Support and Communications** —Customers have access to comprehensive portal user support and education tools. Users can take advantage of our Portal Support Center or learn more about the portal capabilities with tutorials, webinars and user guides.
- **Security**— Our portal is designed to provide secure and private access with three tiers of authentication to help ensure the protection and integrity of network data.
- **Reliability**—Our portal serves as a dependable management tool. It provides transparent interactions with back-office source systems for timely delivery of information throughout a service lifecycle and fast resolution and response times to issues.
- **Personalization**—Users can customize views to see the information that is most important to them, save pages as favorites, assign personal IDs to tickets, manage their subscriptions, and more.

19. PSAP Cutover Plan

External Dependency: STATE and PSAP readiness

Task Name	% Complete	Duration	Start	Finish
PSAP Cutover				
Wireline Carrier 1				
Wireline Carrier 1				
Selective Router Decommissioning				

The CenturyLink NG-911 Program Manager and Aggregation Coordinator will host an OSP/Carrier Translations call that shifts traffic from the OSPs to the tested and established POIs. During this transition, calls are delivered over the NGCS to the destined PSAP via the new NG-911 network services. This migration strategy allows for all affected PSAPs to be migrated individually and in stages. Another option would be to have all the traffic switched by OSPs and wireless carriers at one time allowing the NG-911 Aggregation services to deliver to all PSAPs.

After the pre-cutover testing is complete, the cutover can proceed and calls will traverse to the CenturyLink NGCS and then routed to the PSAP via i3 SIP directly to the call handling equipment or Legacy PSAP Gateway.

The recommended cutover approach is as follows:

Cutover Approach

- In preparation for the cutover, CenturyLink will pre-test and loop-up the circuit in the customer equipment rooms at all locations.
- CenturyLink encourages customer participation in pre-testing, where feasible. Potential technical problems can be identified and resolved prior to the official

cutover by pre-testing the new CenturyLink circuits and new or reconfigured customer equipment.

- CenturyLink pre-tests circuits through the NID.
- The recommended approach is for CenturyLink to pre-test through their equipment with a remote CenturyLink/LEC tester.
- Once CenturyLink and the customer have agreed that sites are ready, the customer schedules the test and turn up with the CenturyLink Program Manager.
- Activations may be scheduled up to one day in advance; off-hours must receive CenturyLink authorization in advance. Normal hours of activation are 7 a.m. – 11 p.m. EST.
- OPTIONAL: A conference bridge is set up for the activations.
- Participants for site activations based on the scope of the cutover activity and can include:
- Customer technical contact, remote or onsite
- Customer site contact – required
- CenturyLink technician
    - CenturyLink/LEC remote tester
    - CenturyLink Program Manager
- Confirm Calls through legacy network are completing correctly (no known issues Wireless & Wireline)
- Run test calls to confirm call path
- Confirm NGCS is Ready
- Confirm Network is Ready
- Confirm Site Ready (call taker in place, site not busy with active 911 calls)
- Execute cutover
- Make a wireless 911 test call
- Make a wireline 911 test call
- Validate incoming call queue is playing appropriate ring back tones or hold message
- Test 3 Digit Star Code Transfer(s). Transfer to a PSAP on net and off net PSAP and Transfer back into PSAP migrating
- Validate transfer to 10 digit PSTN number
- Validate transfer to translation service

- Caller Hang up test - ring once and hang up
- Test alternate routing (optional)
- Test Abandonment Route (optional)
- Unabandon - Verify calls are back to the PSAP
- Release NGCS and CenturyLink Translations Resources

Front Room

- CAD Spill tested- Receiving Data
- Validate PSAP display and mapping
- Recording Tested * Analog recording
- Other requested tests

Final Acceptance

- Sign off and acceptance by PSAP and State

At time of activation, CenturyLink provides premises equipment ready to accept the new circuit. CenturyLink is prepared to run loops to the premise, and confirms connectivity is established. The Customer contact will provide verbal acceptance.

Formal service acceptance is required by the customer to close out the install order. The circuit will not move to 24 x 7 post install monitoring until the circuit has been accepted by the customer.

After 48 hours of customer circuit acceptance, the install order is closed and services are handed to the 24 x 7 post-install support team.

Upon cutover of each site, the Program Manager will ensure that the customer has the appropriate contact and escalation list.

Contingencies are discussed as part of the cutover plan and could include:

- If the data migration is not successful, the CenturyLink implementation group will follow the issue through to resolution;
- If new equipment is in use, this event will not impact service;
- The Customer responsibilities will include providing access to the site and equipment vendor support if applicable.

Assumptions:

Delivery of some circuits may be delayed outside of CenturyLink standard intervals due to provisioning and/or facility issues;

- Parallel system will be in place prior to cutover
- Activations are scheduled per the project scope and negotiated between customer and CenturyLink project managers;
- Further understanding of the network, equipment and site-specific requirements is necessary before detailed scope of work and project plan are developed;
- Phases will overlap to meet implementation timeframes;
- The customer will request extended demark on CenturyLink/LEC ordered loops.

20. Selective Router Decommissioning Plan

External Dependency: Successful PSAP cutover and OSP cooperation CenturyLink works with all OSPs in Nebraska to decommission their selective routers.

21. Project Management Approach

21.1 Review and Validate all Technical Requirements with STATE

One of the first tasks for the project is the review and validation of the technical requirements for NG-911 Services early in the project. This effort will minimize the implementation of incorrect requirements, change orders, schedule delays, and cost increases.

22. Execution

22.1 Communication, Tracking and Escalation Plan

The designated CenturyLink Program Manager, Maggie Cook, is responsible for the overall success of this project. As such, all project related questions, concerns, or issues should be directed to the Program Manager. During the project planning phase, the CenturyLink Program Manager meets with all stakeholders to establish a project status and issues tracking document, a weekly communications cadence and methodology for addressing any issues that may arise outside of these weekly meetings. An escalation matrix will be provided for both implementation and service issues should the customer feel that additional focus is necessary.

22.2 Technical Escalation Matrix

The following table outlines the escalation steps for any technical issues with the contract, implementation, or documentation required during the buildout phase of the NG-911 project. The Program Manager should always be the first line of contact.

CenturyLink	Title / Role	Office Phone	Cell Phone	email address
Rachel Renteria	Sr. Post Sales Engr. – Data Escalations (1st lvl)	214 989 3577	214 989 3577	Rachel.Renteria@centurylink.com
John Atkinson	Mgr, Post Sales Engr II – Data Escalations (2nd lvl)	602-563-3292	480-888-5104	John.Atkinson@centuryLink.com
Caroline Bussell	Client Support Manager – Order/Billing (1st lvl)	N/A	317 697 4499	Caroline.Bussell@centurylink.com
Mary Anderson	Mgr, Sales Support – Data Escalations (2nd lvl)	402-998-7386	402-215-2282	Mary.Anderson1@CenturyLink.com

23. Change Management

The established Change Management (CM) process is one of the many tools used to assist the Program Manager to provide systematic control of all changes and better overall project management. Comprehensive change management is vital to the success of complex projects and is necessary to ensure adequate control over the triple constraints of money, time, and scope while maintaining overall project execution.

The Program Manager (PM) tracks changes as part of the every-day process of project implementation. The PM will document and manage changes to ensure that changes do not affect the project negatively. Scope, budget, schedule, and documentation will all be tracked against the contract. Changes in any of these areas will be vetted within the CenturyLink tea. Once approved by the internal CenturyLink Change Management Board, they will be forwarded to the State for review and approval/rejection.

The PM will provide a change management form to the State of Nebraska for approval prior to implementing the CM process.

23.1. Planned Maintenance

CenturyLink performs scheduled maintenance to ensure the successful growth of the network. Scheduled maintenance is planned with as little customer impact and as much advance notice as possible. We are committed to using standardized methods and procedures for efficient and prompt handling of all changes to minimize the adverse impact of change-related incidents upon service quality.

CenturyLink sends customers email notifications with:

- Description of the work
- Date & time (GMT) of the scheduled maintenance
- List of the impacted services
- Location of the maintenance
- Status of the maintenance

Contact information for questions or concerns:

CenturyLink uses a Global Change Request (GCR) number as the unique identifier for network maintenance.
Call 855.CGH.MGMT (855.244.6468) option 1
Direct dial call 720-888-0229 or 01256 731731
Email change.Management.na@CenturyLink.com

24. Risk Management Plan

24.1 Risk Identification

Risks to a project are presented in many ways. There are internal risks with the project team and external risks that are outside of the project scope. The PM will manage and present these risks to the team to ensure they are considered and addressed as the project progresses.

CenturyLink identifies, analyzes, and responds to all possible risks to ensure delivery of service is not interrupted. During the planning phase of the project, the Program Manager reviews each step of the project/program to establish if it presents an "at risk" situation that may delay the project or create unreasonable downtime for each PSAP. As risks are identified throughout the life cycle of the project, the Program Manager develops a mitigation or contingency plan to ensure a successful transition of all contracted services. The next section illustrates some the potential risks.

24.2 Potential Risks and Avoidance Measures

Below are the known risks that may affect the execution and schedule of the project. Each risk identified is associated with a mitigation and contingency plan.

Example of Risk Assessment and Avoidance Matrix.

Area of Risk	Probability	Responsible Parties	Impact	Mitigation Strategy
Pre-configuration of Equipment and Pre-testing is not successful.	High *(when site is moving to a different vendor, equipment, new hardware, and software)*	CenturyLink, Vendor and (possibly) Customer	If customer information received or entered for configuration is incomplete or inaccurate or non-compatible it will delay cutover until resolved. If discovered during cut over it could result in stopping cut over and moving back to previous hardware and software.	Obtain technical support from Vendor as needed.
Purchase Order Errors	Avoidable	CenturyLink and State	Installation interval not met.	Conduct a complete inventory when equipment gets on site.
Others				

25. Public Safety NOC

CenturyLink is dedicated to providing the State of Nebraska with ongoing support for all of the installed services. We embrace a strong operational philosophy that is customer-focused and highly responsive. Strict performance metrics drive our internal organizations to deliver quality service to the customer on a consistent basis. In the event an issue arises with the service, CenturyLink works to rapidly respond to inquiries and quickly resolve any problems. The Public Safety team is responsible for your experience at critical times, such as when your service is having an outage or impairment. We strive to combine our technical expertise with a positive and pleasant customer experience.

25.1 NG911 PSS NOC Technicians

Once the CenturyLink Service has been installed, a NG911 PSS NOC technician becomes point of contact for service-related issues. The NG911 PSS NOC technician is trained to quickly address technical issues related to the CenturyLink service. The primary objectives of a NG911 PSS NOC technician are to provide start-to-finish accountability for network service performance and to drive resolution of issues based on the first call.

25.2 Trouble ticket handling for State of Nebraska Tickets

When the State of Nebraska NOC opens a trouble ticket directly with CenturyLink NG911 PSS NOC for services covering State of Nebraska Technologies circuits, CenturyLink sends a ticket notification via email to individuals within the State of Nebraska Program Management team notifying that a ticket has been opened by the NOC. This is the same ticket notification that is sent to the State of Nebraska NOC. Subsequent auto ticket notifications via email will continue to be sent, giving status on the progress of the fix action hourly until the ticket is closed. Normal ticket escalation process that has been established on tickets opened by the NOC for State of Nebraska tickets will need to occur from the State of Nebraska NOC to the CenturyLink Government Solutions Control Center.

25.3 Trouble Management

To report an issue, a ticket will need to be opened via the CenturyLink Portal. This ensures that the customer will receive the most up-to-date status as soon as it becomes available. The Portal also improves accuracy in routing tickets to the appropriate team by identifying what is impacting the service. Tickets can also be opened by calling our Public Safety NG911 NOC at **1-800-357-0911.**

25.4 Trouble Ticket Classifications

The priority for the ticket is based on the information provided while opening the ticket. It determines whether the ticket is classified as **Out of Service** (a complete disruption of service which renders it unusable) **or Impaired (**a problem which disrupts quality or connectivity of a service or feature).

25.5 Escalation Procedures

The escalation path is product and equipment agnostic and is exclusively for CenturyLink's valued NG911 clients.

CenturyLink Public Safety Service (PSS) Network Operations Center (NOC)				
Group	Name	Title	Contact	Number
PSS NOC	PSS Network Operations Center	24x7	PSS NOC Center Main Number	800-357-0911
PSS NOC	1st Level Escalation	1st Level Escalation	PSS NOC Center Main Number	800-357-0911 – request a first level escalation
PSS NOC	2nd Level Escalation	PSS NOC Supervisor – Monday – Friday 7am to 3pm CST	Linda Capetz	612-256-6357 (O)
		PSS NOC Supervisor – Monday – Friday 3pm to 11pm CST	Will Cave	612-439-8968 (O)
		PSS NOC Duty Supervisor After hours, weekends and holidays	Duty Supervisor	833-291-4450
PSS NOC	3rd Level Escalation	PSS NOC Manager	Carl Klein	612-439-8841 (O)
				651-442-5999 (M)
PSS NOC	4th Level Escalation	PSS NOC Director	Sally Bakarich	720-888-8988 (O)
				303-507-4367 (M)
PSS NOC	5th Level Escalation	VP Centralized Services	Jorge Magana	404-526-4428 (O)
				404-384-1576 (M)

updated 2/19/2020

25.6 Entrance Criteria for a Defect/Chronic ticket:

All of the following entrance criteria for a Defect and Chronic ticket must be met:

1. A Service Identifier (SID) has had three (3) or more Customer Trouble tickets, worked to resolve, in the past 45 days. Or, the SID has had five (five) Customer Trouble tickets, worked to resolve, in the past 6 months.

2. Each Customer Trouble ticket has been worked on a legitimate service issue. Tickets reporting on non-Customer Trouble issues should not be taken into consideration (i.e. duplicate tickets, GCR related tickets, Customer Power, etc.).

3. A Customer contact has requested that a Chronic ticket be opened on their circuit.

4. A Defect or Chronic ticket is not already open on the SID.

25.7 Reason for Outage (RFO) Request

RFO's can be requested one of the following three ways:

1. Initiate the request by calling the CenturyLink Service Center – 1-877-453-8353 and select the appropriate option (Transport, IP, Voice, etc.). Provide the technician with the ticket number associated to the closed case and let them know that you are the customer and request an RFO.

2. From the My CenturyLink Customer Portal go to "Service Management" > "Trouble Ticketing" > "View Trouble Tickets." A list of trouble tickets is displayed, select the ticket in question by locating it in the list or by typing it into the search box. Once the ticket in question has been selected, click the "Request Reason for Outage" button. Enter the requested information and hit "Submit."

3. Send an email to the assigned Customer Support Manager with the following information:
    - Contact name of the person to whom the RFO should be addressed
    - Email address of the person(s) to whom the RFO should be sent
    - CenturyLink Ticket number that corresponds with the RFO request
    - Reason for the RFO request
    - Any specific questions that need to be addressed in the RFO
    - RFO's are not provided for the following:
        - A service impairment or outage caused by the customer's network or equipment.
        - Open trouble tickets (requests can be opened once the ticket is closed).
        - Tickets closed to no trouble found, cleared before testing, cleared during testing.
        - "Switch hits," "latency"," or "failed calls" for which the issue has not been investigated and documented within a previous trouble ticket.

Receiving the RFO:

CenturyLink is committed to providing all valid RFOs within five business days of the initial request. The Service Level Objective (SLO) is measured from official request time (in queue start time) to the time the RFO is sent out (service restoral time). Weekends and holidays, as well as any time spent gathering follow-up information pertaining to questions, are not included in the SLO timeframe.

26. Vocabulary

Acronym	Definition
ACD	Automatic Call Distribution
API	Application Program Interface
ATP	Acceptance Test Plan
BCF	Border Control Function
CAD	Computer Aided Dispatch
STATE	Nebraska Communications Authority
CCM	Customer Care Manager
CenturyL	CenturyLink
DNS	Domain Name Server
ECRF	Emergency Call Routing Function
ESRP	Emergency Services Routing Proxy
FCC	Federal Communications Commission
FQDN	Fully qualified domain name
GIS	Geographic Information System
GUI	Graphical User Interface
ICMP	Internet control messaging protocol
ISUP	Integrated services digital network
ITIL	Infrastructure Technology Information Library
LATA	Local area transport area
LDB	Location Database
LEC	Local Exchange Carrier
LNG	Legacy Network Gateway
LPG	Legacy PSAP Gateway
LVF	Location Validation Function
MPC	Mobile provisioning center
NENA	National Emergency Number Association
NG-911	Next Generation 911 Services
NGCS	Next Generation Core Services
NGS	Next Generation Services
NOC	Network Operations Center
STATE	Nebraska State Authority
OSP	Originating Service Provider
PIF	Protocol Internetworking Function
PM	Program Manager

Acronym	Definition
PMP	Program Management Plan
PNSP	Primary Network Service Provider
POI	Point of Interface
POP	Point of Presence
PRF	Policy Routing Function
PSAP	Public Safety Answering Point (911 center)
RNSP	Regional Network Service Provider
SBC	Session Border Control
SD-WAN	Software-Defined Wide Area Network
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Subject Matter Expert
SOW	Statement of Work
TDM	Time Domain Multiplexer
URI	Uniform Resource Identifier
URN	Uniform resource name
VPC	VoIP Provisioning Center

SAMPLE NG911 STAGING & ACCEPTANCE CHECKLIST

PSAP NAME

PROJECT TASK	COMPLETE	CONFIRMED BY	DATE	Notes:
HOST NETWORK COMPLETE (PROJECT PLAN)				
UPS Testing				
Physical Network Connections Complete				
Circuit 1				
Network CUG confirmed				
Circuit Confirmed Up/Up				
BFD Established				
Able to Ping HLR and PHX and tunnels are up				
QOS confirmed				
EX1's can ping both sites				
PSAP EX1 - Monitoring online				
Circuit 2				
Network CUG confirmed				
Circuit Confirmed Up/Up				
BFD Established				
Able to Ping HLR and PHX and tunnels are up				
QOS confirmed				
EX1's can ping both sites				
Premigration Tasks Complete (Equipment testing)				
1.) Call Routed to PSAP through IEN - Test call sent to PSAP. Caller confirms routing and audio quality				
2.) Alternate Route via all trunks manual OOS- Set all trunks out of service and send test call.				
3.) Test both call paths to the PSAP - Force a test call to route through Englewood and Miami				
4.) Abandonment Routing- Intrado resource manually puts PSAP into abandoned state - test call made				
5.) Un-abandonment routing - Intrado resource manually unabandons PSAP.				
6.) Ring no answer timer- Test call sent to PSAP. Call is allowed to ring continuously until rolling over to alternate route.				
7.) Caller Hang Up - test call sent to PSAP, caller Hangs up prior to the PSAP answering. Confirm CPE abandon call feature works as designed.				
8.) Fixed Bridge conferencing confirmation - 3 digit star codes. - Test call sent to PSAP and transferred to 3 digit star code. All parties on the bridge talk to confirm conferencing is established. Call taker at PSAP disconnects. Caller confirms that caller and call taker are still bridged.				
9.) Manual Transfer to valid local TN - Test call sent to PSAP Manual Transfer to local TN				
10.) Manual Transfer to a Long distance Cell- Test call sent to PSAP , Manual Transfer to local TN				
11.) Test EXFO EX1				
Viper				
Premigration for xxxxxxxx Milestones Met (xxxxxxxy Project Log)				
Front Room				
Workstations configured and ready				
Viper to Host				
Admin Lines Make/Receive Calls				
Admin Transfers. * Hook Flash (3 way calling on lines) Can add conferencing on the lines. (Would need to use two admin lines) Ellen L to add the 3 way calling on lines.				
CAD Spill				
Radio Cable Tested				

PUNCH LIST ITEM	COMPLETE	DESCRIPTION

AGENCY	AUTHORIZED BY	VOTE

Test Plan

Introduction

The acceptance test plan (ATP) contained here is intended to demonstrate that the solution developed by CenturyLink meets all of the requirements set by the State of Nebraska for a Statewide ESInet and NG911 Solution. This will cover the following major areas:

- NG911 Aggregation network
- NG911 NG Core Services (NGCS)
- Integration
- System Monitoring (Dashboard SD-WAN controller)
- NG911 PSAP Trunk testing.
- EXFO probes to PSAP
- Pre-cut PSAP Testing

This Sample test plan was written based on the understanding of the CenturyLink RFP response for a Statewide ESInet and next Generation Core Services Solution requirements. CenturyLink will provide a custom test plan and submit to the State of Nebraska for approval prior to starting this project and upon award of contract.

Test Tools and Equipment Utilzed to Conduct Test and Test Facilities

The test tools used to execute the ATP consist of:
Networking tools – ping, traceroute, dns query etc.
System specific tools – policy editor and viewer, GIS data viewer …
Exfo Active Assurance (AA) call generator and probe – generates test calls from aggregation network through NGCS to probe at PSAP location

Manual calls – call initiated from aggregation network through NGCS core to PSAP call taker
CentuiryLink lab PSAP – used to validate core functionality prior to testing with production PSAPs.

Simulators and process for simuation of test calls (Refer to each tab for info in this workbook)

Test thresholds

Pass, Fail, Restart Test

Configuration of tests - Custom to be determined

Test Strategy & Environment

The primary objective is to demonstrate system readiness leading to a migration of traffic from the current systems to the new one. Based on the approach taken by State of Nebraska to minimize legacy integration all of the PSAP in the entire state must be ready to accept traffic prior to any traffic migration. Test execution will be sequenced starting with network connectivity followed by major system components and finishing with full call testing with each PSAP. The sections in the ATP correspond to the functional areas previously mentioned. The three sections related to the PSAP are templates. They will be repeated for each PSAP. The start of acceptance testing assumes that the component hardware and software has been installed and the CenturyLink has completed our internal Network Readiness Testing (NRT). ATP execution can be sequenced as follows:

Final Documenation of Test - CenturyLink Project Manager will provide the State of Nebraska and PSAP of final results of test.

Network Connectivity (Can be run simultaneously)
- NGCS – DNS
- NG911 Aggregation – NGCS network
- NGCS – network
- NG911 Trunk – ESInet for each PSAP and CTL lab

System Components
- Integration – Policy DB
- Integration – Location DB
- Integration – State GIS (Utilizes a common NG9-1-1 GIS data set available for all PSAPs when a common NG9-1-1 GIS data set is established
- NGCS - ECRF
- NGCS – ESRP
- NG911 Aggregation - LIF/NIF
- NGCS – i3 Logging
- System Monitoring
- Exfo Probe to PSAP – CTL lab
- Pre-Cut PSAP Testing – CTL lab

Call Testing
- Exfo Probe to PSAP – per PSAP
- Pre-cut PSAP testing - per PSAP.

Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Execution Date	Result PassFail	Tester (print name)	Status
OSP Trunking								
1	SS7 ISUP COT testing on trunk group 1	COT testing passes	CTL/OSP	N				
2	SS7 ISUP COT testing on trunk group 2	COT testing passes	CTL/OSP	N				
3	CenturyLink disables multiple DS0s to TDM gateway 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL/OSP	N				
4	CenturyLink disables multiple DS0s to TDM gateway 2	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL/OSP	N				
5	CenturyLink disables DS1 to TDM gateway 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL/OSP	N				
6	CenturyLink disables DS1 to TDM gateway 2	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL/OSP	N				
NGCS Network								
7	CTL disables GigE 1 between CTL aggregation network and NGCS	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
8	CTL disables GigE 2 between CTL aggregation network and NGCS	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
9	CTL completely disables aggregation network SBC 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
10	CTL completely disables aggregation network SBC 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
Network								
11	CTL disables GigE 1 between CTL aggregation network	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
12	CTL disables GigE 2 between CTL aggregation network a	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
13	CTL completely disables aggregation network SBC 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				
14	CTL completely disables aggregation network SBC 1	9-1-1 OPS sees alarm / Regional Dashboard indicates alarm/ Prime Dashboard indicates alarm	CTL	N				

Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Date	Result	Tester (print name)	Status
DNS								
1	From network element run DNS A and SRV queries for all NGCS elements		CTL	N				
ESRP								
2	Disable an ESRP. Test call	Cal still completes with second ESRP.	CTL	N				
LIF/NIF								
3	Disable an LIF/NIF. Test call	Cal still completes with second LIF/NIF.	CTL	N				
ECRF								
4	Disable an ECRF. Test call	Cal still completes with second ECRF.	CTL	N				
LDB								
5	Disable an LDB. Test call	Cal still completes with second LDB.	CTL	N				
i3 Logging								
6	Retrieve logs for test calls and validate.		CTL	N				
Notes:								

Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Date	Result	Tester (print name)	Status
Policy								
1	For each PSAP in the State of Nebraska + CTL lab load PSAP policy viapolicy editor tool. Verify Policy rules are transferred to all copies of the Policy Store.	Policy rules for each PSAP are transtered from CTL to the policy store	CTL	N				
2	Use the Policy editor tool to perform an update on the CTL lab PSAP policy. Verify update is transferred to all copies of the State of Nebraska Policy Store.	Policy update for CTL lab PSAP are updated from the policy store	CTL	N				
Location DB								
3	Create SOI records for test telephone numbers used in ATP. Have prime process them and needed data to populate the r Location DB.	Telephone numbers populated in LDB.	CTL	N				
State GIS								
4	Validate all state GIS data has been replicated to all copies in the NGCS core.	Initial GIS data loaded	CTL	N				
5	Generate a GIS update and validate that it is updated in all copies of the regional GIS.	Update populated in regional GIS DB	CTL	N				
Aggregation Failover								
6	Disable side-A connectivity to the core and run a test call.	Call will successfully route through the regional NGCS. Alarms will be generated.	CTL/PSAP	Y				
7	Disable side-A and side B connectivity to the core and run a test call.	Call will successfully route through the prime NGCS. Alarms will be generated.	CTL/PSAP	Y				
Core Failover								
8	Disable side-A connectivity to the NGCS core from the aggregation network and run call.	Call will successfully route through the regional NGCS. Alarms will be generated.	CTL/PSAP	Y				
9	Disable side-A and side-B connectivity to the NGCS core from the aggregation network and run call.	Call will successfully route through the prime NGCS. Alarms will be generated.	CTL/PSAP	Y				
PSAP transfer								
10	Ctl make test call with known call party number for given PSAP. Call is routed to PSAP and answered. Caller identifies call as a test call. Have call-taker transfer call to another PSAP ourside the region. After connecting have first PSAP call taker hang up. Then have second PSAP call taker hang up.	Original call is answered and call is successfully transferred to second PSAP via the Primer ESInet	CTL/PSAP	Y				
Notes:								

Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Date	Result	Tester (print name)	Status
Dashboard								
1	Verify user accounts for logging into dashboard	Login successful and dashboard displayed		N				
2	Verfiy status of each of the monitored functional elements	Status are updated		N				
3	During testing that disables a network element or link verify that the status of the network element changes in the dashboard	Network element status enabled		N				
4	Verify Call statistics are updated after test calls.	statistics are updated		N				
SD-WAN Controller								
5	Verify user accounts for logging into SD-WAN controller	login successful		N				
6	Utilize SD-WAN controller to configure SD-WAN connections.			N				
Ticketing								
7	Verify user accounts for logging into ticketing system	Login successful		N				
Notes								

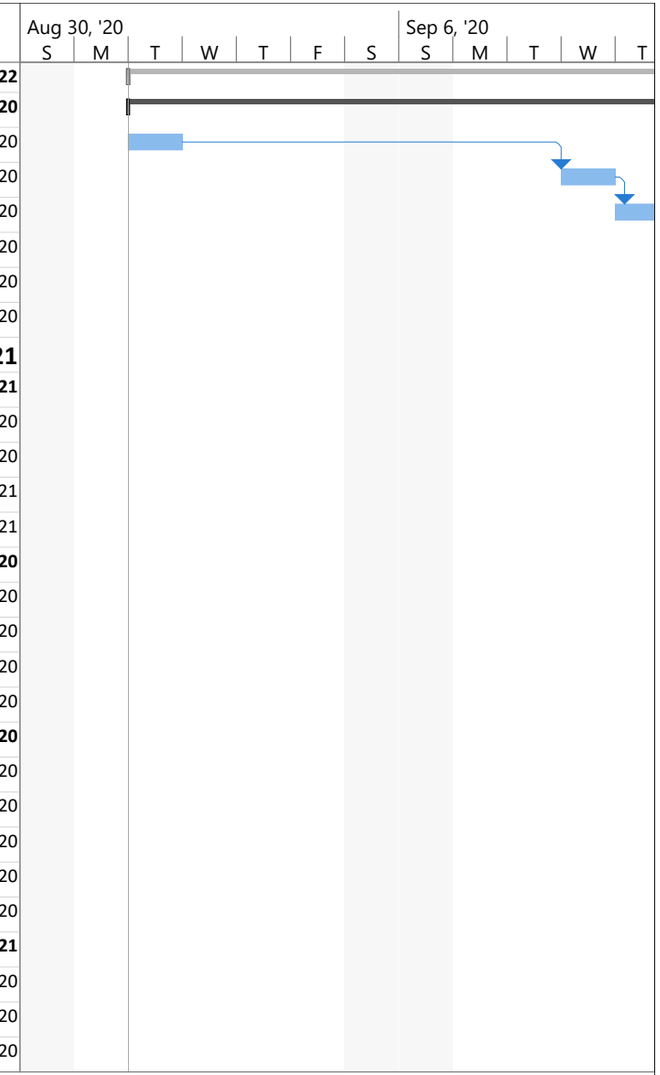
Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Date	Result	Tester (print name)	Status
ESInet	For each PSAP							
1	CPE-SD-WAN Device 1 ping from Priv Router 1 TBD IP Address = Ethernet-1 IP PSAP end		CTL	N				
2	CPE-SD-WAN Device 1 ping from Priv Router 2 TBD IP Address = Ethernet-1 IP PSAP end		CTL	N				
3	CPE-SD-WAN Device 2 ping from Priv Router 1 TBD IP Address = Ethernet-2 IP PSAP end		CTL	N				
4	CPE-SD-WAN Device 2 ping from Priv Router 2 TBD IP Address = Ethernet-2 IP PSAP end		CTL	N				
5	Tracert to SD-WAN Device 1 - confirm and document network path from Priv Router 1. On Ethernet 1 via IP TBD		CTL	N				
6	Tracert to SD-WAN Device 1 - confirm and document network path from Priv Router 2. On Ethernet 1 via IP TBD		CTL	N				
7	Tracert to SD-WAN Device 2 - confirm and document network path from Priv Router 1. On Ethernet 1 via IP TBD		CTL	N				
8	Tracert to SD-WAN Device 2 - confirm and document network path from Priv Router 2. On Ethernet 1 via IP TBD		CTL	N				
9	Tracert to SBC1 - confirm and document network path from Priv Router 1. On Ethernet 1 via IP TBD		CTL	N				
10	Tracert to SBC1 - confirm and document network path from Priv Router 2. On Ethernet 1 via IP TBD		CTL	N				
11	Tracert to SBC2 - confirm and document network path from Priv Router 1. On Ethernet 1 via IP TBD		CTL	N				
12	Tracert to SBC2 - confirm and document network path from Priv Router 2. On Ethernet 1 via IP TBD		CTL	N				
13	Ping LPG1 from SBC1		CTL	N				
14	Ping LPG2 from SBC2		CTL	N				
15	NGCS BCF1 traceroute to PSAP SBC1		CTL	N				
16	NGCS BCF1 traceroute to PSAP SBC1		CTL	N				
17	NGCS BCF2 traceroute to SBC1		CTL	N				
18	NGCS BCF2 traceroute to PSAP SBC1		CTL	N				
MGMT Network								
19	SSH to SD-WAN Device 1 login, confirm and document network path from Priv Router 1.		CTL	N				

Test #	Test Procedure	Expectations	Test Team	PSAP Resource	Date	Result	Tester (print name)	Status
20	SSH to SD-WAN Device 1 login, confirm and document network path from Priv Router 2.		CTL	N				
21	SSH to SD-WAN Device 2 login, confirm and document network path from Priv Router 1.		CTL	N				
22	SSH to SD-WAN Device 2 login, confirm and document network path from Priv Router 2.		CTL	N				
23	SSH to SBC1 login, confirm and document network path from Priv Router 1.		CTL	N				
24	SSH to SBC1 login, confirm and document network path from Priv Router 2.		CTL	N				
25	SSH to SBC2 login, confirm and document network path from Priv Router 1.		CTL	N				
26	SSH to SBC2 login, confirm and document network path from Priv Router 2.		CTL	N				
27	HTTPS to SD-WAN 1 login, confirm and document network path from Priv Router 1.		CTL	N				
28	HTTPS to SD-WAN 1 login, confirm and document network path from Priv Router 2.		CTL	N				
29	HTTPS to SD-WAN 2 login, confirm and document network path from Priv Router 1.		CTL	N				
30	HTTPS to SD-WAN 2 login, confirm and document network path from Priv Router 2.		CTL	N				
Notes:								

Test #	Test Procedure	Expectations	Test Team	PSAP Resourc	Date	Result	Tester (print name)	Status
1	Run SIP Active Assurance call on side-A; verify test completes; Observe Exfo call reporting.	Call completes as expected	CTL	N				
2	Run SIP Active Assurance call on side-B; verify test completes; Observe Exfo call reporting.	Call completes as expected	CTL	N				
3	Disable ethernet port to EX1 probe for side-A. Run SIP Active Assurance call on side-A; Verify test call fails. Check for alarm	Call failed, alarm raised	CTL	N				
4	Disable ethernet port to EX1 probe for side-a and side-B. Run SIP Active Assurance call on side-B; Verify test call fails. Check for alarm	Call failed, alarm raised	CTL	N				
Notes:								

Test #	Test Procedure	Expectations	Test Team	Prime NOC Resource	Date	Result	Tester (print name)	Status
DNS								
1	Query (AAAA and SRV) DNS for all FQDNs associated with the PSAP.	Query successful	CTL					
2								
Policy								
3	Retrieve PSAP specific policy from policy store and verify it is correct.	PSAP policy validated	CTL					
Test Calls								
4	Ctl make test call with known call party number for given PSAP. Call is routed to PSAP and answered. Caller identifies call as a test call. Have call taker hang up.	Call is routed to PSAP and answered.	CTL/PSAP					
5	Ctl make test call with known call party number for given PSAP. Call is routed to PSAP and answered. Caller identifies call as a test call. Have call-taker transfer call to another PSAP. After connecting have first PSAP call taker hang up. Then have second PSAP call taker hang up.	Original call is answered and call is successfully transferred to second PSAP	CTL/PSAP					
6	Ctl make test call with known call party number for given PSAP. . Caller identifies call as a test call. Have call-taker transfer call to known PSTN destination. After connecting have first PSAP call taker hang up. Then have second PSAP call taker hang up.	Original call is answered and call is successfully transferred to known PSTN destination	CTL/PSAP					
7	Disable side-A link to PSAP. Ctl make test call with known call party number for given PSAP. Caller identifies call as a test call. Have call taker hang up.	Call is routed to PSAP and answered. Alarms are generated.	CTL/PSAP					
8	Disable side A and side-B link to PSAP. Ctl make test call with known call party number for given PSAP. Caller identifies call as a test call. Have call taker hang up.	Call is routed to overflow PSAP as defined in Policy Store for PSAP. Alarms are generated and status of PSAP changes in Dashboard	CTL/PSAP					
Notes:								

ID	Task Name	Duration	Start	Finish
0	**Nebraska NGCS Notional Project Plan**	**515 days**	**Tue 9/1/20**	**Mon 8/22/22**
1	**Phase I: Planning and Design**	**17 days**	**Tue 9/1/20**	**Wed 9/23/20**
2	Sign contract	1 day	Tue 9/1/20	Tue 9/1/20
3	Receive PO	1 day	Wed 9/9/20	Wed 9/9/20
4	Publish preliminary PM Plan for stakeholder review	1 day	Thu 9/10/20	Thu 9/10/20
5	Schedule stakeholder kickoff meetings	1 day	Fri 9/11/20	Fri 9/11/20
6	Meet with state and begin mobilization	2 days	Mon 9/21/20	Tue 9/22/20
7	Publish revised PM Plan and FSB	1 day	Wed 9/23/20	Wed 9/23/20
8	**South Central Region**	**81 days**	**Thu 9/24/20**	**Thu 1/14/21**
9	**OSP Connectivity Planning**	**77 days**	**Thu 9/24/20**	**Fri 1/8/21**
10	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Thu 9/24/20	Fri 10/2/20
11	Conduct OSP discussions	60 days	Mon 10/5/20	Fri 12/25/20
12	Develop Draft OSP connectivity plan	10 days	Mon 12/28/20	Fri 1/8/21
13	Draft Aggregation plan and circulate for comment	10 days	Mon 12/28/20	Fri 1/8/21
14	**Survey (TBD) PSAPs and Dispatch Centers**	**15 days**	**Mon 10/5/20**	**Fri 10/23/20**
15	Publish survey form	1 day	Mon 10/5/20	Mon 10/5/20
16	schedule visits	5 days	Tue 10/6/20	Mon 10/12/20
17	Conduct visits, compile data and revise plans accordingly	15 days	Tue 10/13/20	Mon 11/2/20
18	Publish revised PM Plan	1 day	Tue 11/3/20	Tue 11/3/20
19	**Enhance datacenters as needed**	**7 days**	**Wed 11/4/20**	**Thu 11/12/20**
20	Confirm rack space and other DC needs satisfied	5 days	Wed 11/4/20	Tue 11/10/20
21	Plan for deploying ECRF, LVF and other GIS components	5 days	Wed 11/4/20	Tue 11/10/20
22	Identify enhancements needed in datacenters	5 days	Wed 11/4/20	Tue 11/10/20
23	Order new components and schedule labor	2 days	Wed 11/11/20	Thu 11/12/20
24	Identity and provision POIs	5 days	Wed 11/11/20	Tue 11/17/20
25	**Revise network design IAW tasks above**	**52 days**	**Wed 11/4/20**	**Thu 1/14/21**
26	Confirm network typology and provisioning plans	5 days	Wed 11/4/20	Tue 11/10/20
27	ID need for legacy gateways and provision	3 days	Wed 11/4/20	Fri 11/6/20
28	Complete NENA checklist 75-002	2 days	Wed 11/18/20	Thu 11/19/20



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

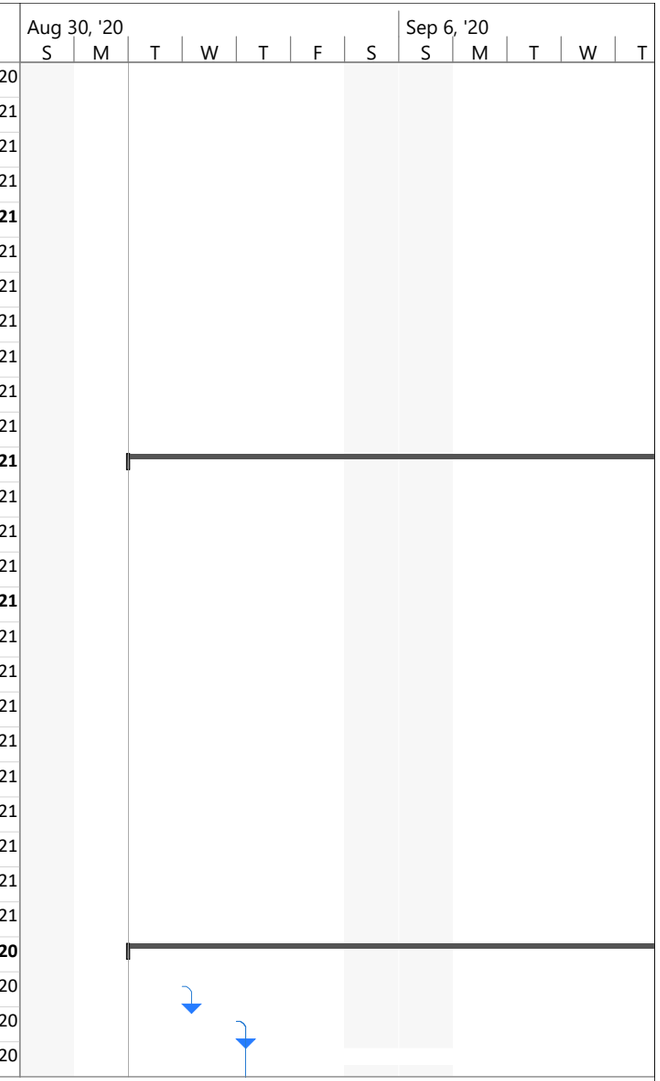
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
29	Confirm compliance with network security plan	2 days	Fri 11/20/20	Mon 11/23/20
30	Confirm transport independence and diversity	5 days	Tue 11/24/20	Mon 11/30/20
31	Prepare circuit plan and place orders	5 days	Tue 11/24/20	Mon 11/30/20
32	**ID changes to standard dashboard required for this project**	**30 days**	**Wed 11/4/20**	**Tue 12/15/20**
33	**ID PSAP needs and place orders**	**30 days**	**Wed 11/4/20**	**Tue 12/15/20**
34	Schedule installs and establish links to PSAP CPE vendors	30 days	Wed 11/4/20	Tue 12/15/20
35	Develop test plans with all vendors to ensure interface effectiveness	30 days	Wed 11/4/20	Tue 12/15/20
36	**Provision Monitoring**	**52 days**	**Wed 11/4/20**	**Thu 1/14/21**
37	Program OCOM	10 days	Wed 12/16/20	Tue 12/29/20
38	Program FortiSIEM	10 days	Wed 12/16/20	Tue 12/29/20
39	Plan E-Bonding capability	10 days	Wed 12/16/20	Tue 12/29/20
40	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Wed 12/16/20	Tue 12/29/20
41	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Wed 11/11/20**	**Thu 1/14/21**
42	Provision two geographically diverse cores capable of 99.999% availability	30 days	Wed 11/18/20	Tue 12/29/20
43	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Wed 12/30/20	Wed 12/30/20
44	**Design GIS solution**	**47 days**	**Wed 11/11/20**	**Thu 1/14/21**
45	Finalize plans for ECRF, LVF and other GIS components	45 days	Wed 11/11/20	Tue 1/12/21
46	Identify and provision GIS elements for use in datacenters	1 day	Wed 1/13/21	Wed 1/13/21
47	Confirm two instances of ECRF/PRF	1 day	Wed 1/13/21	Wed 1/13/21
48	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Thu 1/14/21	Thu 1/14/21
49	Publish training plan for stakeholder comment	50 days	Wed 11/4/20	Tue 1/12/21
50	**Phase II: Deployment**	**140 days**	**Wed 11/11/20**	**Tue 5/25/21**
51	**Complete OSP integration**	**50 days**	**Mon 1/11/21**	**Fri 3/19/21**
52	Execute interconnect agreements	10 days	Mon 1/11/21	Fri 1/22/21
53	Deploy i3-Interconnect where needed	30 days	Mon 1/25/21	Fri 3/5/21
54	Execute POI and datacenter interconnection	10 days	Mon 3/8/21	Fri 3/19/21
55	**Install datacenter links and enhancements**	**124 days**	**Wed 11/11/20**	**Mon 5/3/21**
56	Complete rack installs	7 days	Wed 11/11/20	Thu 11/19/20
57	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Fri 11/20/20	Thu 12/31/20

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

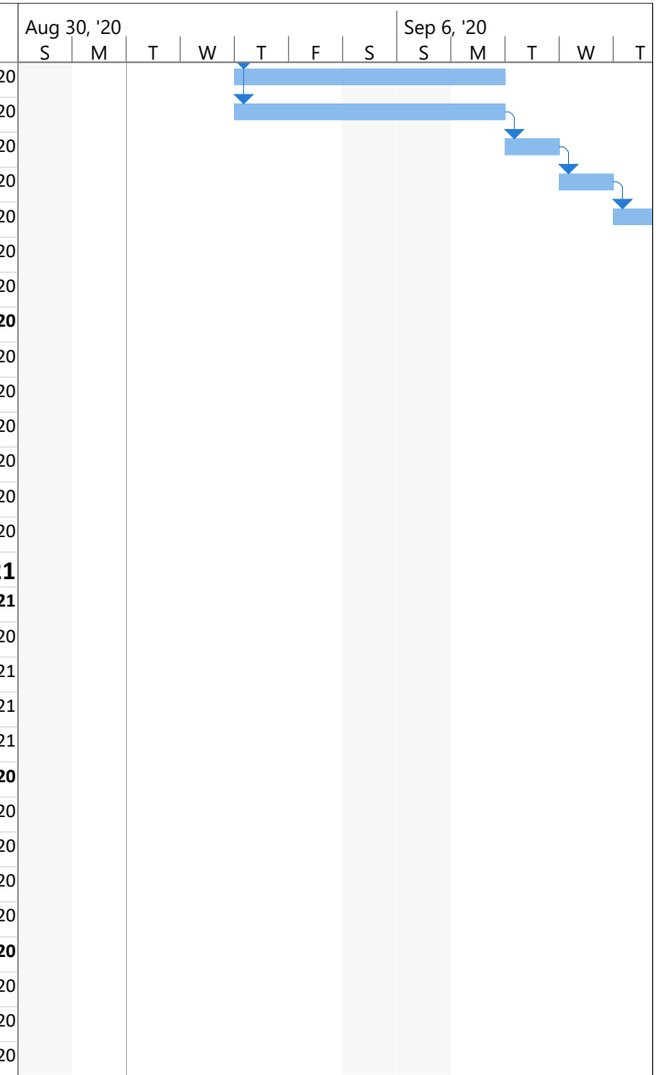
ID	Task Name	Duration	Start	Finish
58	Install GIS components	30 days	Fri 11/20/20	Thu 12/31/20
59	Install circuits, cross-connects and FOC	30 days	Mon 3/22/21	Fri 4/30/21
60	Confirm datacenter readiness	1 day	Mon 5/3/21	Mon 5/3/21
61	Install network connections and gateways	70 days	Mon 1/25/21	Fri 4/30/21
62	**Complete PSAP configurations**	**6 days**	**Mon 5/3/21**	**Mon 5/10/21**
63	Test CPE interfaces	5 days	Mon 5/3/21	Fri 5/7/21
64	Test circuits	5 days	Mon 5/3/21	Fri 5/7/21
65	Execute interface agreements if needed with CPE vendors	1 day	Mon 5/10/21	Mon 5/10/21
66	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Tue 5/11/21	Tue 5/11/21
67	Standup POIs	1 day	Wed 5/12/21	Wed 5/12/21
68	Publish and review cutover plan with stakeholders	10 days	Wed 5/12/21	Tue 5/25/21
69	**Phase III: Cutover**	**214 days**	**Tue 9/1/20**	**Fri 6/25/21**
70	Execute training plan	3 days	Wed 5/26/21	Fri 5/28/21
71	confirm readiness for cutover	1 day	Mon 5/31/21	Mon 5/31/21
72	Obtain state and local concurrence to cutover PSAP 1	5 days	Tue 6/1/21	Mon 6/7/21
73	**Prepare PSAP 1 for cutover**	**12 days**	**Tue 6/8/21**	**Wed 6/23/21**
74	Confirm fail-back plan in place	1 day	Tue 6/8/21	Tue 6/8/21
75	Confirm CPE interfaces operational	5 days	Tue 6/8/21	Mon 6/14/21
76	Confirm OSP readiness	2 days	Tue 6/15/21	Wed 6/16/21
77	Confirm training completed	1 day	Thu 6/17/21	Thu 6/17/21
78	Confirm PSAP ready for flash network cutover	1 day	Fri 6/18/21	Fri 6/18/21
79	Notify state PSAP 1 ready for flash cutover	1 day	Fri 6/18/21	Fri 6/18/21
80	Perform cutover	2 days	Mon 6/21/21	Tue 6/22/21
81	Confirm success	1 day	Wed 6/23/21	Wed 6/23/21
82	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Thu 6/24/21	Fri 6/25/21
83	**Perform flash network cutover**	**14 days**	**Tue 9/1/20**	**Fri 9/18/20**
84	Confirm fail-back plan in place	1 day	Tue 9/1/20	Tue 9/1/20
85	Turn-up core services	1 day	Wed 9/2/20	Wed 9/2/20
86	Activate interface between core services and legacy network	3 days	Thu 9/3/20	Mon 9/7/20



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
87	Migrate OSPs to i3 network	3 days	Thu 9/3/20	Mon 9/7/20
88	Onboard carriers into location database	3 days	Thu 9/3/20	Mon 9/7/20
89	Link core services to ESInet	1 day	Tue 9/8/20	Tue 9/8/20
90	Perform flash network cutover	1 day	Wed 9/9/20	Wed 9/9/20
91	Confirm carrier services	1 day	Thu 9/10/20	Thu 9/10/20
92	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Fri 9/11/20	Thu 9/17/20
93	Cutover confirmed to state	1 day	Fri 9/18/20	Fri 9/18/20
94	**Phase IV: Observation and Acceptance**	**39 days**	**Mon 9/21/20**	**Thu 11/12/20**
95	Execute ATP	5 days	Mon 9/21/20	Fri 9/25/20
96	Provisional acceptance accorded by state	1 day	Mon 9/28/20	Mon 9/28/20
97	Perform 30-day observation period	30 days	Tue 9/29/20	Mon 11/9/20
98	Close punch list	30 days	Tue 9/29/20	Mon 11/9/20
99	Final acceptance by state	2 days	Tue 11/10/20	Wed 11/11/20
100	Transition to operational environment	1 day	Thu 11/12/20	Thu 11/12/20
101	**South Eastern Region**	**226 days**	**Mon 10/5/20**	**Mon 8/16/21**
102	**OSP Connectivity Planning**	**77 days**	**Fri 11/13/20**	**Mon 3/1/21**
103	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Fri 11/13/20	Mon 11/23/20
104	Conduct OSP discussions	60 days	Tue 11/24/20	Mon 2/15/21
105	Develop Draft OSP connectivity plan	10 days	Tue 2/16/21	Mon 3/1/21
106	Draft Aggregation plan and circulate for comment	10 days	Tue 2/16/21	Mon 3/1/21
107	**Survey (TBD) PSAPs and Dispatch Centers**	**15 days**	**Mon 10/5/20**	**Fri 10/23/20**
108	Publish survey form	1 day	Mon 10/5/20	Mon 10/5/20
109	schedule visits	5 days	Tue 10/6/20	Mon 10/12/20
110	Conduct visits, compile data and revise plans accordingly	15 days	Tue 10/13/20	Mon 11/2/20
111	Publish revised PM Plan	1 day	Fri 11/13/20	Fri 11/13/20
112	**Enhance datacenters as needed**	**7 days**	**Mon 11/16/20**	**Tue 11/24/20**
113	Confirm rack space and other DC needs satisfied	5 days	Mon 11/16/20	Fri 11/20/20
114	Plan for deploying ECRF, LVF and other GIS components	5 days	Mon 11/16/20	Fri 11/20/20
115	Identify enhancements needed in datacenters	5 days	Mon 11/16/20	Fri 11/20/20



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
116	Order new components and schedule labor	2 days	Mon 11/23/20	Tue 11/24/20
117	Identity and provision POIs	5 days	Mon 11/23/20	Fri 11/27/20
118	**Revise network design IAW tasks above**	**52 days**	**Mon 11/16/20**	**Tue 1/26/21**
119	Confirm network typology and provisioning plans	5 days	Mon 11/16/20	Fri 11/20/20
120	ID need for legacy gateways and provision	3 days	Mon 11/16/20	Wed 11/18/20
121	Complete NENA checklist 75-002	2 days	Mon 11/30/20	Tue 12/1/20
122	Confirm compliance with network security plan	2 days	Wed 12/2/20	Thu 12/3/20
123	Confirm transport independence and diversity	5 days	Fri 12/4/20	Thu 12/10/20
124	Prepare circuit plan and place orders	5 days	Fri 12/4/20	Thu 12/10/20
125	**ID changes to standard dashboard required for this project**	**30 days**	**Mon 11/16/20**	**Fri 12/25/20**
126	**ID PSAP needs and place orders**	**30 days**	**Mon 11/16/20**	**Fri 12/25/20**
127	Schedule installs and establish links to PSAP CPE vendors	30 days	Mon 11/16/20	Fri 12/25/20
128	Develop test plans with all vendors to ensure interface effectiveness	30 days	Mon 11/16/20	Fri 12/25/20
129	**Provision Monitoring**	**52 days**	**Mon 11/16/20**	**Tue 1/26/21**
130	Program OCOM	10 days	Mon 12/28/20	Fri 1/8/21
131	Program FortiSIEM	10 days	Mon 12/28/20	Fri 1/8/21
132	Plan E-Bonding capability	10 days	Mon 12/28/20	Fri 1/8/21
133	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Mon 12/28/20	Fri 1/8/21
134	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Mon 11/23/20**	**Tue 1/26/21**
135	Provision two geographically diverse cores capable of 99.999% availability	30 days	Mon 11/30/20	Fri 1/8/21
136	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Mon 1/11/21	Mon 1/11/21
137	**Design GIS solution**	**47 days**	**Mon 11/23/20**	**Tue 1/26/21**
138	Finalize plans for ECRF, LVF and other GIS components	45 days	Mon 11/23/20	Fri 1/22/21
139	Identify and provision GIS elements for use in datacenters	1 day	Mon 1/25/21	Mon 1/25/21
140	Confirm two instances of ECRF/PRF	1 day	Mon 1/25/21	Mon 1/25/21
141	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Tue 1/26/21	Tue 1/26/21
142	Publish training plan for stakeholder comment	50 days	Mon 11/16/20	Fri 1/22/21
143	**Phase II: Deployment**	**168 days**	**Mon 11/23/20**	**Wed 7/14/21**
144	**Complete OSP integration**	**50 days**	**Tue 3/2/21**	**Mon 5/10/21**

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
145	Execute interconnect agreements	10 days	Tue 3/2/21	Mon 3/15/21
146	Deploy i3-Interconnect where needed	30 days	Tue 3/16/21	Mon 4/26/21
147	Execute POI and datacenter interconnection	10 days	Tue 4/27/21	Mon 5/10/21
148	**Install datacenter links and enhancements**	**152 days**	**Mon 11/23/20**	**Tue 6/22/21**
149	Complete rack installs	7 days	Mon 11/23/20	Tue 12/1/20
150	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Wed 12/2/20	Tue 1/12/21
151	Install GIS components	30 days	Wed 12/2/20	Tue 1/12/21
152	Install circuits, cross-connects and FOC	30 days	Tue 5/11/21	Mon 6/21/21
153	Confirm datacenter readiness	1 day	Tue 6/22/21	Tue 6/22/21
154	Install network connections and gateways	70 days	Tue 3/16/21	Mon 6/21/21
155	**Complete PSAP configurations**	**6 days**	**Tue 6/22/21**	**Tue 6/29/21**
156	Test CPE interfaces	5 days	Tue 6/22/21	Mon 6/28/21
157	Test circuits	5 days	Tue 6/22/21	Mon 6/28/21
158	Execute interface agreements if needed with CPE vendors	1 day	Tue 6/29/21	Tue 6/29/21
159	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Wed 6/30/21	Wed 6/30/21
160	Standup POIs	1 day	Thu 7/1/21	Thu 7/1/21
161	Publish and review cutover plan with stakeholders	10 days	Thu 7/1/21	Wed 7/14/21
162	**Phase III: Cutover**	**197 days**	**Fri 11/13/20**	**Mon 8/16/21**
163	Execute training plan	3 days	Thu 7/15/21	Mon 7/19/21
164	confirm readiness for cutover	1 day	Tue 7/20/21	Tue 7/20/21
165	Obtain state and local concurrence to cutover PSAP 1	5 days	Wed 7/21/21	Tue 7/27/21
166	**Prepare PSAP 1 for cutover**	**12 days**	**Wed 7/28/21**	**Thu 8/12/21**
167	Confirm fail-back plan in place	1 day	Wed 7/28/21	Wed 7/28/21
168	Confirm CPE interfaces operational	5 days	Wed 7/28/21	Tue 8/3/21
169	Confirm OSP readiness	2 days	Wed 8/4/21	Thu 8/5/21
170	Confirm training completed	1 day	Fri 8/6/21	Fri 8/6/21
171	Confirm PSAP ready for flash network cutover	1 day	Mon 8/9/21	Mon 8/9/21
172	Notify state PSAP 1 ready for flash cutover	1 day	Mon 8/9/21	Mon 8/9/21
173	Perform cutover	2 days	Tue 8/10/21	Wed 8/11/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
174	Confirm success	1 day	Thu 8/12/21	Thu 8/12/21
175	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Fri 8/13/21	Mon 8/16/21
176	**Perform flash network cutover**	**14 days**	**Fri 11/13/20**	**Wed 12/2/20**
177	Confirm fail-back plan in place	1 day	Fri 11/13/20	Fri 11/13/20
178	Turn-up core services	1 day	Mon 11/16/20	Mon 11/16/20
179	Activate interface between core services and legacy network	3 days	Tue 11/17/20	Thu 11/19/20
180	Migrate OSPs to i3 network	3 days	Tue 11/17/20	Thu 11/19/20
181	Onboard carriers into location database	3 days	Tue 11/17/20	Thu 11/19/20
182	Link core services to ESInet	1 day	Fri 11/20/20	Fri 11/20/20
183	Perform flash network cutover	1 day	Mon 11/23/20	Mon 11/23/20
184	Confirm carrier services	1 day	Tue 11/24/20	Tue 11/24/20
185	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Wed 11/25/20	Tue 12/1/20
186	Cutover confirmed to state	1 day	Wed 12/2/20	Wed 12/2/20
187	**Phase IV: Observation and Acceptance**	**39 days**	**Thu 12/3/20**	**Tue 1/26/21**
188	Execute ATP	5 days	Thu 12/3/20	Wed 12/9/20
189	Provisional acceptance accorded by state	1 day	Thu 12/10/20	Thu 12/10/20
190	Perform 30-day observation period	30 days	Fri 12/11/20	Thu 1/21/21
191	Close punch list	30 days	Fri 12/11/20	Thu 1/21/21
192	Final acceptance by state	2 days	Fri 1/22/21	Mon 1/25/21
193	Transition to operational environment	1 day	Tue 1/26/21	Tue 1/26/21
194	**Metro Region**	**197 days**	**Wed 1/27/21**	**Thu 10/28/21**
195	**OSP Connectivity Planning**	**77 days**	**Wed 1/27/21**	**Thu 5/13/21**
196	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Wed 1/27/21	Thu 2/4/21
197	Conduct OSP discussions	60 days	Fri 2/5/21	Thu 4/29/21
198	Develop Draft OSP connectivity plan	10 days	Fri 4/30/21	Thu 5/13/21
199	Draft Aggregation plan and circulate for comment	10 days	Fri 4/30/21	Thu 5/13/21
200	**Survey (TBD) PSAPs and Dispatch Centers**	**21 days**	**Fri 2/5/21**	**Fri 3/5/21**
201	Publish survey form	1 day	Fri 2/5/21	Fri 2/5/21
202	schedule visits	5 days	Mon 2/8/21	Fri 2/12/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
203	Conduct visits, compile data and revise plans accordingly	15 days	Mon 2/15/21	Fri 3/5/21
204	Publish revised PM Plan	1 day	Mon 3/8/21	Mon 3/8/21
205	**Enhance datacenters as needed**	**7 days**	**Tue 3/9/21**	**Wed 3/17/21**
206	Confirm rack space and other DC needs satisfied	5 days	Tue 3/9/21	Mon 3/15/21
207	Plan for deploying ECRF, LVF and other GIS components	5 days	Tue 3/9/21	Mon 3/15/21
208	Identify enhancements needed in datacenters	5 days	Tue 3/9/21	Mon 3/15/21
209	Order new components and schedule labor	2 days	Tue 3/16/21	Wed 3/17/21
210	Identity and provision POIs	5 days	Tue 3/16/21	Mon 3/22/21
211	**Revise network design IAW tasks above**	**52 days**	**Tue 3/9/21**	**Wed 5/19/21**
212	Confirm network typology and provisioning plans	5 days	Tue 3/9/21	Mon 3/15/21
213	ID need for legacy gateways and provision	3 days	Tue 3/9/21	Thu 3/11/21
214	Complete NENA checklist 75-002	2 days	Tue 3/23/21	Wed 3/24/21
215	Confirm compliance with network security plan	2 days	Thu 3/25/21	Fri 3/26/21
216	Confirm transport independence and diversity	5 days	Mon 3/29/21	Fri 4/2/21
217	Prepare circuit plan and place orders	5 days	Mon 3/29/21	Fri 4/2/21
218	**ID changes to standard dashboard required for this project**	**30 days**	**Tue 3/9/21**	**Mon 4/19/21**
219	**ID PSAP needs and place orders**	**30 days**	**Tue 3/9/21**	**Mon 4/19/21**
220	Schedule installs and establish links to PSAP CPE vendors	30 days	Tue 3/9/21	Mon 4/19/21
221	Develop test plans with all vendors to ensure interface effectiveness	30 days	Tue 3/9/21	Mon 4/19/21
222	**Provision Monitoring**	**52 days**	**Tue 3/9/21**	**Wed 5/19/21**
223	Program OCOM	10 days	Tue 4/20/21	Mon 5/3/21
224	Program FortiSIEM	10 days	Tue 4/20/21	Mon 5/3/21
225	Plan E-Bonding capability	10 days	Tue 4/20/21	Mon 5/3/21
226	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Tue 4/20/21	Mon 5/3/21
227	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Tue 3/16/21**	**Wed 5/19/21**
228	Provision two geographically diverse cores capable of 99.999% availability	30 days	Tue 3/23/21	Mon 5/3/21
229	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Tue 5/4/21	Tue 5/4/21
230	**Design GIS solution**	**47 days**	**Tue 3/16/21**	**Wed 5/19/21**
231	Finalize plans for ECRF, LVF and other GIS components	45 days	Tue 3/16/21	Mon 5/17/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

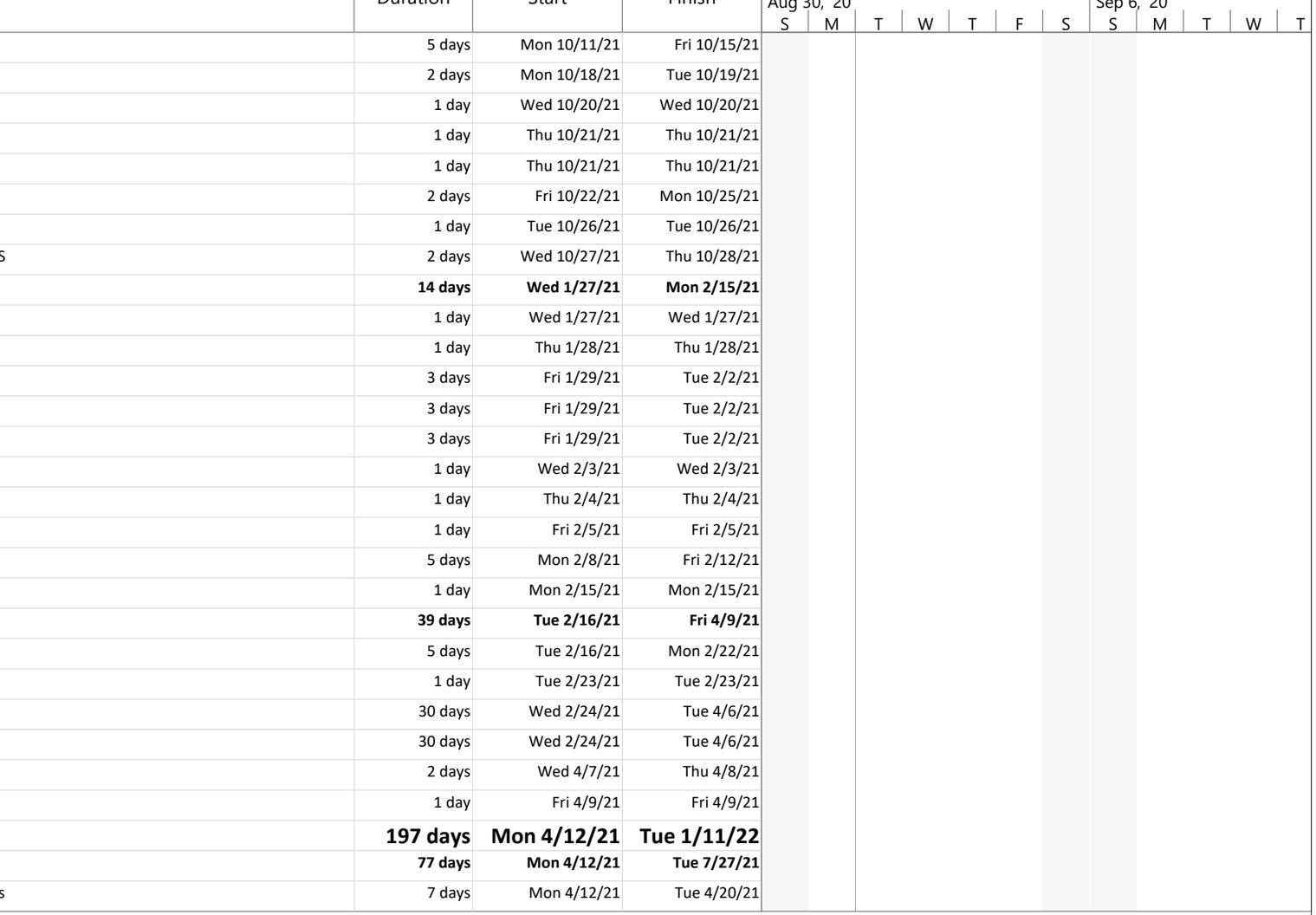
Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
232	Identify and provision GIS elements for use in datacenters	1 day	Tue 5/18/21	Tue 5/18/21
233	Confirm two instances of ECRF/PRF	1 day	Tue 5/18/21	Tue 5/18/21
234	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Wed 5/19/21	Wed 5/19/21
235	Publish training plan for stakeholder comment	50 days	Tue 3/9/21	Mon 5/17/21
236	**Phase II: Deployment**	**140 days**	**Tue 3/16/21**	**Mon 9/27/21**
237	**Complete OSP integration**	**50 days**	**Fri 5/14/21**	**Thu 7/22/21**
238	Execute interconnect agreements	10 days	Fri 5/14/21	Thu 5/27/21
239	Deploy i3-Interconnect where needed	30 days	Fri 5/28/21	Thu 7/8/21
240	Execute POI and datacenter interconnection	10 days	Fri 7/9/21	Thu 7/22/21
241	**Install datacenter links and enhancements**	**124 days**	**Tue 3/16/21**	**Fri 9/3/21**
242	Complete rack installs	7 days	Tue 3/16/21	Wed 3/24/21
243	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Thu 3/25/21	Wed 5/5/21
244	Install GIS components	30 days	Thu 3/25/21	Wed 5/5/21
245	Install circuits, cross-connects and FOC	30 days	Fri 7/23/21	Thu 9/2/21
246	Confirm datacenter readiness	1 day	Fri 9/3/21	Fri 9/3/21
247	Install network connections and gateways	70 days	Fri 5/28/21	Thu 9/2/21
248	**Complete PSAP configurations**	**6 days**	**Fri 9/3/21**	**Fri 9/10/21**
249	Test CPE interfaces	5 days	Fri 9/3/21	Thu 9/9/21
250	Test circuits	5 days	Fri 9/3/21	Thu 9/9/21
251	Execute interface agreements if needed with CPE vendors	1 day	Fri 9/10/21	Fri 9/10/21
252	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Mon 9/13/21	Mon 9/13/21
253	Standup POIs	1 day	Tue 9/14/21	Tue 9/14/21
254	Publish and review cutover plan with stakeholders	10 days	Tue 9/14/21	Mon 9/27/21
255	**Phase III: Cutover**	**197 days**	**Wed 1/27/21**	**Thu 10/28/21**
256	Execute training plan	3 days	Tue 9/28/21	Thu 9/30/21
257	confirm readiness for cutover	1 day	Fri 10/1/21	Fri 10/1/21
258	Obtain state and local concurrence to cutover PSAP 1	5 days	Mon 10/4/21	Fri 10/8/21
259	**Prepare PSAP 1 for cutover**	**12 days**	**Mon 10/11/21**	**Tue 10/26/21**
260	Confirm fail-back plan in place	1 day	Mon 10/11/21	Mon 10/11/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
261	Confirm CPE interfaces operational	5 days	Mon 10/11/21	Fri 10/15/21
262	Confirm OSP readiness	2 days	Mon 10/18/21	Tue 10/19/21
263	Confirm training completed	1 day	Wed 10/20/21	Wed 10/20/21
264	Confirm PSAP ready for flash network cutover	1 day	Thu 10/21/21	Thu 10/21/21
265	Notify state PSAP 1 ready for flash cutover	1 day	Thu 10/21/21	Thu 10/21/21
266	Perform cutover	2 days	Fri 10/22/21	Mon 10/25/21
267	Confirm success	1 day	Tue 10/26/21	Tue 10/26/21
268	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Wed 10/27/21	Thu 10/28/21
269	**Perform flash network cutover**	**14 days**	**Wed 1/27/21**	**Mon 2/15/21**
270	Confirm fail-back plan in place	1 day	Wed 1/27/21	Wed 1/27/21
271	Turn-up core services	1 day	Thu 1/28/21	Thu 1/28/21
272	Activate interface between core services and legacy network	3 days	Fri 1/29/21	Tue 2/2/21
273	Migrate OSPs to i3 network	3 days	Fri 1/29/21	Tue 2/2/21
274	Onboard carriers into location database	3 days	Fri 1/29/21	Tue 2/2/21
275	Link core services to ESInet	1 day	Wed 2/3/21	Wed 2/3/21
276	Perform flash network cutover	1 day	Thu 2/4/21	Thu 2/4/21
277	Confirm carrier services	1 day	Fri 2/5/21	Fri 2/5/21
278	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Mon 2/8/21	Fri 2/12/21
279	Cutover confirmed to state	1 day	Mon 2/15/21	Mon 2/15/21
280	**Phase IV: Observation and Acceptance**	**39 days**	**Tue 2/16/21**	**Fri 4/9/21**
281	Execute ATP	5 days	Tue 2/16/21	Mon 2/22/21
282	Provisional acceptance accorded by state	1 day	Tue 2/23/21	Tue 2/23/21
283	Perform 30-day observation period	30 days	Wed 2/24/21	Tue 4/6/21
284	Close punch list	30 days	Wed 2/24/21	Tue 4/6/21
285	Final acceptance by state	2 days	Wed 4/7/21	Thu 4/8/21
286	Transition to operational environment	1 day	Fri 4/9/21	Fri 4/9/21
287	**North Central Region**	**197 days**	**Mon 4/12/21**	**Tue 1/11/22**
288	**OSP Connectivity Planning**	**77 days**	**Mon 4/12/21**	**Tue 7/27/21**
289	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Mon 4/12/21	Tue 4/20/21



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

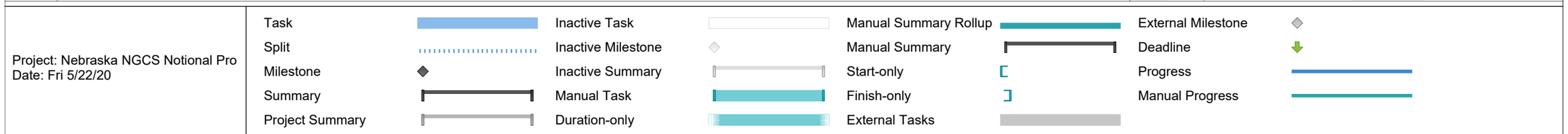
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
290	Conduct OSP discussions	60 days	Wed 4/21/21	Tue 7/13/21
291	Develop Draft OSP connectivity plan	10 days	Wed 7/14/21	Tue 7/27/21
292	Draft Aggregation plan and circulate for comment	10 days	Wed 7/14/21	Tue 7/27/21
293	**Survey (TBD) PSAPs and Dispatch Centers**	**96 days**	**Wed 4/21/21**	**Wed 9/1/21**
294	Publish survey form	1 day	Wed 4/21/21	Wed 4/21/21
295	schedule visits	5 days	Thu 4/22/21	Wed 4/28/21
296	Conduct visits, compile data and revise plans accordingly	90 days	Thu 4/29/21	Wed 9/1/21
297	Publish revised PM Plan	1 day	Thu 9/2/21	Thu 9/2/21
298	**Enhance datacenters as needed**	**7 days**	**Fri 9/3/21**	**Mon 9/13/21**
299	Confirm rack space and other DC needs satisfied	5 days	Fri 9/3/21	Thu 9/9/21
300	Plan for deploying ECRF, LVF and other GIS components	5 days	Fri 9/3/21	Thu 9/9/21
301	Identify enhancements needed in datacenters	5 days	Fri 9/3/21	Thu 9/9/21
302	Order new components and schedule labor	2 days	Fri 9/10/21	Mon 9/13/21
303	Identity and provision POIs	5 days	Fri 9/10/21	Thu 9/16/21
304	**Revise network design IAW tasks above**	**52 days**	**Fri 9/3/21**	**Mon 11/15/21**
305	Confirm network typology and provisioning plans	5 days	Fri 9/3/21	Thu 9/9/21
306	ID need for legacy gateways and provision	3 days	Fri 9/3/21	Tue 9/7/21
307	Complete NENA checklist 75-002	2 days	Fri 9/17/21	Mon 9/20/21
308	Confirm compliance with network security plan	2 days	Tue 9/21/21	Wed 9/22/21
309	Confirm transport independence and diversity	5 days	Thu 9/23/21	Wed 9/29/21
310	Prepare circuit plan and place orders	5 days	Thu 9/23/21	Wed 9/29/21
311	**ID changes to standard dashboard required for this project**	**30 days**	**Fri 9/3/21**	**Thu 10/14/21**
312	**ID PSAP needs and place orders**	**30 days**	**Fri 9/3/21**	**Thu 10/14/21**
313	Schedule installs and establish links to PSAP CPE vendors	30 days	Fri 9/3/21	Thu 10/14/21
314	Develop test plans with all vendors to ensure interface effectiveness	30 days	Fri 9/3/21	Thu 10/14/21
315	**Provision Monitoring**	**52 days**	**Fri 9/3/21**	**Mon 11/15/21**
316	Program OCOM	10 days	Fri 10/15/21	Thu 10/28/21
317	Program FortiSIEM	10 days	Fri 10/15/21	Thu 10/28/21
318	Plan E-Bonding capability	10 days	Fri 10/15/21	Thu 10/28/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
319	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Fri 10/15/21	Thu 10/28/21
320	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Fri 9/10/21**	**Mon 11/15/21**
321	Provision two geographically diverse cores capable of 99.999% availability	30 days	Fri 9/17/21	Thu 10/28/21
322	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Fri 10/29/21	Fri 10/29/21
323	**Design GIS solution**	**47 days**	**Fri 9/10/21**	**Mon 11/15/21**
324	Finalize plans for ECRF, LVF and other GIS components	45 days	Fri 9/10/21	Thu 11/11/21
325	Identify and provision GIS elements for use in datacenters	1 day	Fri 11/12/21	Fri 11/12/21
326	Confirm two instances of ECRF/PRF	1 day	Fri 11/12/21	Fri 11/12/21
327	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Mon 11/15/21	Mon 11/15/21
328	Publish training plan for stakeholder comment	50 days	Fri 9/3/21	Thu 11/11/21
329	**Phase II: Deployment**	**97 days**	**Wed 7/28/21**	**Thu 12/9/21**
330	**Complete OSP integration**	**50 days**	**Wed 7/28/21**	**Tue 10/5/21**
331	Execute interconnect agreements	10 days	Wed 7/28/21	Tue 8/10/21
332	Deploy i3-Interconnect where needed	30 days	Wed 8/11/21	Tue 9/21/21
333	Execute POI and datacenter interconnection	10 days	Wed 9/22/21	Tue 10/5/21
334	**Install datacenter links and enhancements**	**49 days**	**Fri 9/10/21**	**Wed 11/17/21**
335	Complete rack installs	7 days	Fri 9/10/21	Mon 9/20/21
336	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Tue 9/21/21	Mon 11/1/21
337	Install GIS components	30 days	Tue 9/21/21	Mon 11/1/21
338	Install circuits, cross-connects and FOC	30 days	Wed 10/6/21	Tue 11/16/21
339	Confirm datacenter readiness	1 day	Wed 11/17/21	Wed 11/17/21
340	Install network connections and gateways	70 days	Wed 8/11/21	Tue 11/16/21
341	**Complete PSAP configurations**	**6 days**	**Wed 11/17/21**	**Wed 11/24/21**
342	Test CPE interfaces	5 days	Wed 11/17/21	Tue 11/23/21
343	Test circuits	5 days	Wed 11/17/21	Tue 11/23/21
344	Execute interface agreements if needed with CPE vendors	1 day	Wed 11/24/21	Wed 11/24/21
345	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Thu 11/25/21	Thu 11/25/21
346	Standup POIs	1 day	Fri 11/26/21	Fri 11/26/21
347	Publish and review cutover plan with stakeholders	10 days	Fri 11/26/21	Thu 12/9/21

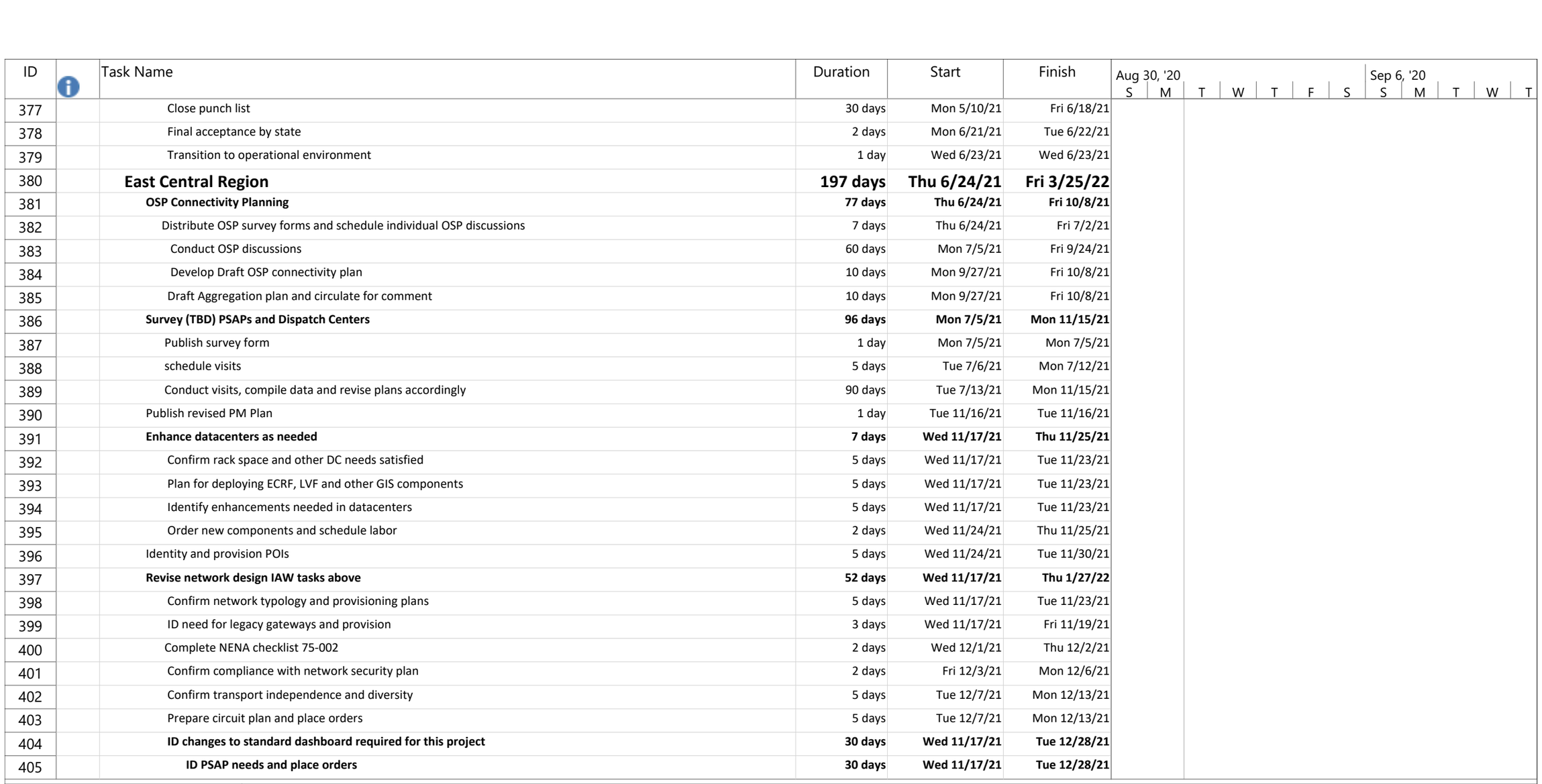


ID	Task Name	Duration	Start	Finish
348	**Phase III: Cutover**	**197 days**	**Mon 4/12/21**	**Tue 1/11/22**
349	Execute training plan	3 days	Fri 12/10/21	Tue 12/14/21
350	confirm readiness for cutover	1 day	Wed 12/15/21	Wed 12/15/21
351	Obtain state and local concurrence to cutover PSAP 1	5 days	Thu 12/16/21	Wed 12/22/21
352	**Prepare PSAP 1 for cutover**	**12 days**	**Thu 12/23/21**	**Fri 1/7/22**
353	Confirm fail-back plan in place	1 day	Thu 12/23/21	Thu 12/23/21
354	Confirm CPE interfaces operational	5 days	Thu 12/23/21	Wed 12/29/21
355	Confirm OSP readiness	2 days	Thu 12/30/21	Fri 12/31/21
356	Confirm training completed	1 day	Mon 1/3/22	Mon 1/3/22
357	Confirm PSAP ready for flash network cutover	1 day	Tue 1/4/22	Tue 1/4/22
358	Notify state PSAP 1 ready for flash cutover	1 day	Tue 1/4/22	Tue 1/4/22
359	Perform cutover	2 days	Wed 1/5/22	Thu 1/6/22
360	Confirm success	1 day	Fri 1/7/22	Fri 1/7/22
361	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Mon 1/10/22	Tue 1/11/22
362	**Perform flash network cutover**	**14 days**	**Mon 4/12/21**	**Thu 4/29/21**
363	Confirm fail-back plan in place	1 day	Mon 4/12/21	Mon 4/12/21
364	Turn-up core services	1 day	Tue 4/13/21	Tue 4/13/21
365	Activate interface between core services and legacy network	3 days	Wed 4/14/21	Fri 4/16/21
366	Migrate OSPs to i3 network	3 days	Wed 4/14/21	Fri 4/16/21
367	Onboard carriers into location database	3 days	Wed 4/14/21	Fri 4/16/21
368	Link core services to ESInet	1 day	Mon 4/19/21	Mon 4/19/21
369	Perform flash network cutover	1 day	Tue 4/20/21	Tue 4/20/21
370	Confirm carrier services	1 day	Wed 4/21/21	Wed 4/21/21
371	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Thu 4/22/21	Wed 4/28/21
372	Cutover confirmed to state	1 day	Thu 4/29/21	Thu 4/29/21
373	**Phase IV: Observation and Acceptance**	**39 days**	**Fri 4/30/21**	**Wed 6/23/21**
374	Execute ATP	5 days	Fri 4/30/21	Thu 5/6/21
375	Provisional acceptance accorded by state	1 day	Fri 5/7/21	Fri 5/7/21
376	Perform 30-day observation period	30 days	Mon 5/10/21	Fri 6/18/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
377	Close punch list	30 days	Mon 5/10/21	Fri 6/18/21
378	Final acceptance by state	2 days	Mon 6/21/21	Tue 6/22/21
379	Transition to operational environment	1 day	Wed 6/23/21	Wed 6/23/21
380	**East Central Region**	**197 days**	**Thu 6/24/21**	**Fri 3/25/22**
381	**OSP Connectivity Planning**	**77 days**	**Thu 6/24/21**	**Fri 10/8/21**
382	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Thu 6/24/21	Fri 7/2/21
383	Conduct OSP discussions	60 days	Mon 7/5/21	Fri 9/24/21
384	Develop Draft OSP connectivity plan	10 days	Mon 9/27/21	Fri 10/8/21
385	Draft Aggregation plan and circulate for comment	10 days	Mon 9/27/21	Fri 10/8/21
386	**Survey (TBD) PSAPs and Dispatch Centers**	**96 days**	**Mon 7/5/21**	**Mon 11/15/21**
387	Publish survey form	1 day	Mon 7/5/21	Mon 7/5/21
388	schedule visits	5 days	Tue 7/6/21	Mon 7/12/21
389	Conduct visits, compile data and revise plans accordingly	90 days	Tue 7/13/21	Mon 11/15/21
390	Publish revised PM Plan	1 day	Tue 11/16/21	Tue 11/16/21
391	**Enhance datacenters as needed**	**7 days**	**Wed 11/17/21**	**Thu 11/25/21**
392	Confirm rack space and other DC needs satisfied	5 days	Wed 11/17/21	Tue 11/23/21
393	Plan for deploying ECRF, LVF and other GIS components	5 days	Wed 11/17/21	Tue 11/23/21
394	Identify enhancements needed in datacenters	5 days	Wed 11/17/21	Tue 11/23/21
395	Order new components and schedule labor	2 days	Wed 11/24/21	Thu 11/25/21
396	Identity and provision POIs	5 days	Wed 11/24/21	Tue 11/30/21
397	**Revise network design IAW tasks above**	**52 days**	**Wed 11/17/21**	**Thu 1/27/22**
398	Confirm network typology and provisioning plans	5 days	Wed 11/17/21	Tue 11/23/21
399	ID need for legacy gateways and provision	3 days	Wed 11/17/21	Fri 11/19/21
400	Complete NENA checklist 75-002	2 days	Wed 12/1/21	Thu 12/2/21
401	Confirm compliance with network security plan	2 days	Fri 12/3/21	Mon 12/6/21
402	Confirm transport independence and diversity	5 days	Tue 12/7/21	Mon 12/13/21
403	Prepare circuit plan and place orders	5 days	Tue 12/7/21	Mon 12/13/21
404	**ID changes to standard dashboard required for this project**	**30 days**	**Wed 11/17/21**	**Tue 12/28/21**
405	**ID PSAP needs and place orders**	**30 days**	**Wed 11/17/21**	**Tue 12/28/21**



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
406	Schedule installs and establish links to PSAP CPE vendors	30 days	Wed 11/17/21	Tue 12/28/21
407	Develop test plans with all vendors to ensure interface effectiveness	30 days	Wed 11/17/21	Tue 12/28/21
408	**Provision Monitoring**	**52 days**	**Wed 11/17/21**	**Thu 1/27/22**
409	Program OCOM	10 days	Wed 12/29/21	Tue 1/11/22
410	Program FortiSIEM	10 days	Wed 12/29/21	Tue 1/11/22
411	Plan E-Bonding capability	10 days	Wed 12/29/21	Tue 1/11/22
412	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Wed 12/29/21	Tue 1/11/22
413	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Wed 11/24/21**	**Thu 1/27/22**
414	Provision two geographically diverse cores capable of 99.999% availability	30 days	Wed 12/1/21	Tue 1/11/22
415	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Wed 1/12/22	Wed 1/12/22
416	**Design GIS solution**	**47 days**	**Wed 11/24/21**	**Thu 1/27/22**
417	Finalize plans for ECRF, LVF and other GIS components	45 days	Wed 11/24/21	Tue 1/25/22
418	Identify and provision GIS elements for use in datacenters	1 day	Wed 1/26/22	Wed 1/26/22
419	Confirm two instances of ECRF/PRF	1 day	Wed 1/26/22	Wed 1/26/22
420	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Thu 1/27/22	Thu 1/27/22
421	Publish training plan for stakeholder comment	50 days	Wed 11/17/21	Tue 1/25/22
422	**Phase II: Deployment**	**97 days**	**Mon 10/11/21**	**Tue 2/22/22**
423	**Complete OSP integration**	**50 days**	**Mon 10/11/21**	**Fri 12/17/21**
424	Execute interconnect agreements	10 days	Mon 10/11/21	Fri 10/22/21
425	Deploy i3-Interconnect where needed	30 days	Mon 10/25/21	Fri 12/3/21
426	Execute POI and datacenter interconnection	10 days	Mon 12/6/21	Fri 12/17/21
427	**Install datacenter links and enhancements**	**49 days**	**Wed 11/24/21**	**Mon 1/31/22**
428	Complete rack installs	7 days	Wed 11/24/21	Thu 12/2/21
429	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Fri 12/3/21	Thu 1/13/22
430	Install GIS components	30 days	Fri 12/3/21	Thu 1/13/22
431	Install circuits, cross-connects and FOC	30 days	Mon 12/20/21	Fri 1/28/22
432	Confirm datacenter readiness	1 day	Mon 1/31/22	Mon 1/31/22
433	Install network connections and gateways	70 days	Mon 10/25/21	Fri 1/28/22
434	**Complete PSAP configurations**	**6 days**	**Mon 1/31/22**	**Mon 2/7/22**

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

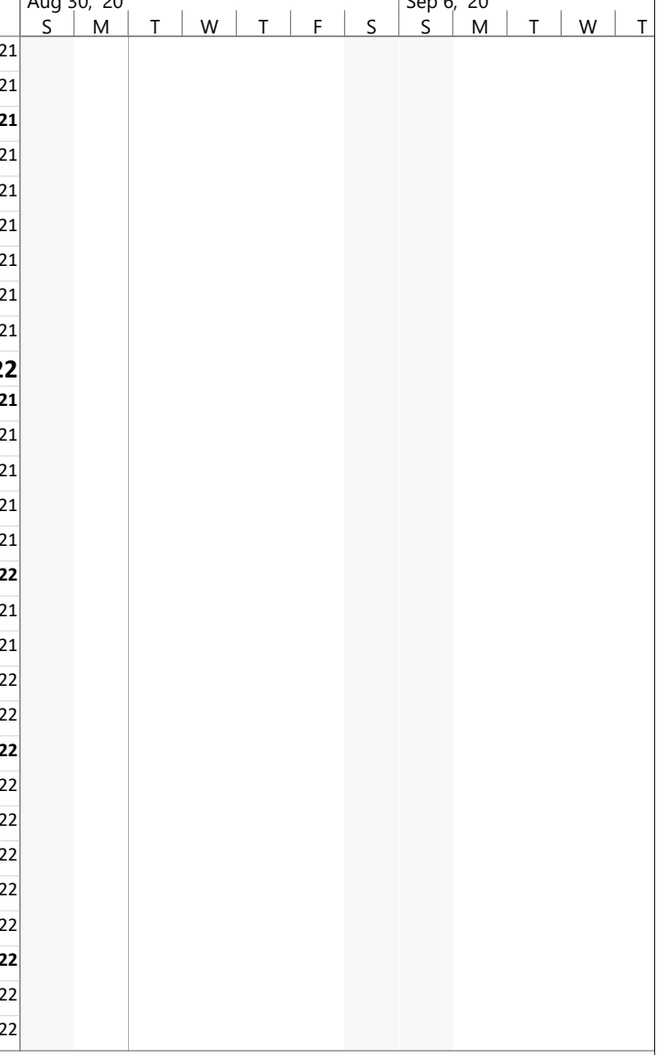
Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
435	Test CPE interfaces	5 days	Mon 1/31/22	Fri 2/4/22
436	Test circuits	5 days	Mon 1/31/22	Fri 2/4/22
437	Execute interface agreements if needed with CPE vendors	1 day	Mon 2/7/22	Mon 2/7/22
438	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Tue 2/8/22	Tue 2/8/22
439	Standup POIs	1 day	Wed 2/9/22	Wed 2/9/22
440	Publish and review cutover plan with stakeholders	10 days	Wed 2/9/22	Tue 2/22/22
441	**Phase III: Cutover**	**197 days**	**Thu 6/24/21**	**Fri 3/25/22**
442	Execute training plan	3 days	Wed 2/23/22	Fri 2/25/22
443	confirm readiness for cutover	1 day	Mon 2/28/22	Mon 2/28/22
444	Obtain state and local concurrence to cutover PSAP 1	5 days	Tue 3/1/22	Mon 3/7/22
445	**Prepare PSAP 1 for cutover**	**12 days**	**Tue 3/8/22**	**Wed 3/23/22**
446	Confirm fail-back plan in place	1 day	Tue 3/8/22	Tue 3/8/22
447	Confirm CPE interfaces operational	5 days	Tue 3/8/22	Mon 3/14/22
448	Confirm OSP readiness	2 days	Tue 3/15/22	Wed 3/16/22
449	Confirm training completed	1 day	Thu 3/17/22	Thu 3/17/22
450	Confirm PSAP ready for flash network cutover	1 day	Fri 3/18/22	Fri 3/18/22
451	Notify state PSAP 1 ready for flash cutover	1 day	Fri 3/18/22	Fri 3/18/22
452	Perform cutover	2 days	Mon 3/21/22	Tue 3/22/22
453	Confirm success	1 day	Wed 3/23/22	Wed 3/23/22
454	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Thu 3/24/22	Fri 3/25/22
455	**Perform flash network cutover**	**14 days**	**Thu 6/24/21**	**Tue 7/13/21**
456	Confirm fail-back plan in place	1 day	Thu 6/24/21	Thu 6/24/21
457	Turn-up core services	1 day	Fri 6/25/21	Fri 6/25/21
458	Activate interface between core services and legacy network	3 days	Mon 6/28/21	Wed 6/30/21
459	Migrate OSPs to i3 network	3 days	Mon 6/28/21	Wed 6/30/21
460	Onboard carriers into location database	3 days	Mon 6/28/21	Wed 6/30/21
461	Link core services to ESInet	1 day	Thu 7/1/21	Thu 7/1/21
462	Perform flash network cutover	1 day	Fri 7/2/21	Fri 7/2/21
463	Confirm carrier services	1 day	Mon 7/5/21	Mon 7/5/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
464	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Tue 7/6/21	Mon 7/12/21
465	Cutover confirmed to state	1 day	Tue 7/13/21	Tue 7/13/21
466	**Phase IV: Observation and Acceptance**	**39 days**	**Wed 7/14/21**	**Mon 9/6/21**
467	Execute ATP	5 days	Wed 7/14/21	Tue 7/20/21
468	Provisional acceptance accorded by state	1 day	Wed 7/21/21	Wed 7/21/21
469	Perform 30-day observation period	30 days	Thu 7/22/21	Wed 9/1/21
470	Close punch list	30 days	Thu 7/22/21	Wed 9/1/21
471	Final acceptance by state	2 days	Thu 9/2/21	Fri 9/3/21
472	Transition to operational environment	1 day	Mon 9/6/21	Mon 9/6/21
473	**Metro West Region**	**197 days**	**Tue 9/7/21**	**Wed 6/8/22**
474	**OSP Connectivity Planning**	**77 days**	**Tue 9/7/21**	**Wed 12/22/21**
475	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Tue 9/7/21	Wed 9/15/21
476	Conduct OSP discussions	60 days	Thu 9/16/21	Wed 12/8/21
477	Develop Draft OSP connectivity plan	10 days	Thu 12/9/21	Wed 12/22/21
478	Draft Aggregation plan and circulate for comment	10 days	Thu 12/9/21	Wed 12/22/21
479	**Survey (TBD) PSAPs and Dispatch Centers**	**96 days**	**Thu 9/16/21**	**Thu 1/27/22**
480	Publish survey form	1 day	Thu 9/16/21	Thu 9/16/21
481	schedule visits	5 days	Fri 9/17/21	Thu 9/23/21
482	Conduct visits, compile data and revise plans accordingly	90 days	Fri 9/24/21	Thu 1/27/22
483	Publish revised PM Plan	1 day	Fri 1/28/22	Fri 1/28/22
484	**Enhance datacenters as needed**	**7 days**	**Mon 1/31/22**	**Tue 2/8/22**
485	Confirm rack space and other DC needs satisfied	5 days	Mon 1/31/22	Fri 2/4/22
486	Plan for deploying ECRF, LVF and other GIS components	5 days	Mon 1/31/22	Fri 2/4/22
487	Identify enhancements needed in datacenters	5 days	Mon 1/31/22	Fri 2/4/22
488	Order new components and schedule labor	2 days	Mon 2/7/22	Tue 2/8/22
489	Identity and provision POIs	5 days	Mon 2/7/22	Fri 2/11/22
490	**Revise network design IAW tasks above**	**52 days**	**Mon 1/31/22**	**Tue 4/12/22**
491	Confirm network typology and provisioning plans	5 days	Mon 1/31/22	Fri 2/4/22
492	ID need for legacy gateways and provision	3 days	Mon 1/31/22	Wed 2/2/22



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
493	Complete NENA checklist 75-002	2 days	Mon 2/14/22	Tue 2/15/22
494	Confirm compliance with network security plan	2 days	Wed 2/16/22	Thu 2/17/22
495	Confirm transport independence and diversity	5 days	Fri 2/18/22	Thu 2/24/22
496	Prepare circuit plan and place orders	5 days	Fri 2/18/22	Thu 2/24/22
497	**ID changes to standard dashboard required for this project**	**30 days**	**Mon 1/31/22**	**Fri 3/11/22**
498	**ID PSAP needs and place orders**	**30 days**	**Mon 1/31/22**	**Fri 3/11/22**
499	Schedule installs and establish links to PSAP CPE vendors	30 days	Mon 1/31/22	Fri 3/11/22
500	Develop test plans with all vendors to ensure interface effectiveness	30 days	Mon 1/31/22	Fri 3/11/22
501	**Provision Monitoring**	**52 days**	**Mon 1/31/22**	**Tue 4/12/22**
502	Program OCOM	10 days	Mon 3/14/22	Fri 3/25/22
503	Program FortiSIEM	10 days	Mon 3/14/22	Fri 3/25/22
504	Plan E-Bonding capability	10 days	Mon 3/14/22	Fri 3/25/22
505	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Mon 3/14/22	Fri 3/25/22
506	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Mon 2/7/22**	**Tue 4/12/22**
507	Provision two geographically diverse cores capable of 99.999% availability	30 days	Mon 2/14/22	Fri 3/25/22
508	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Mon 3/28/22	Mon 3/28/22
509	**Design GIS solution**	**47 days**	**Mon 2/7/22**	**Tue 4/12/22**
510	Finalize plans for ECRF, LVF and other GIS components	45 days	Mon 2/7/22	Fri 4/8/22
511	Identify and provision GIS elements for use in datacenters	1 day	Mon 4/11/22	Mon 4/11/22
512	Confirm two instances of ECRF/PRF	1 day	Mon 4/11/22	Mon 4/11/22
513	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Tue 4/12/22	Tue 4/12/22
514	Publish training plan for stakeholder comment	50 days	Mon 1/31/22	Fri 4/8/22
515	**Phase II: Deployment**	**97 days**	**Thu 12/23/21**	**Fri 5/6/22**
516	**Complete OSP integration**	**50 days**	**Thu 12/23/21**	**Wed 3/2/22**
517	Execute interconnect agreements	10 days	Thu 12/23/21	Wed 1/5/22
518	Deploy i3-Interconnect where needed	30 days	Thu 1/6/22	Wed 2/16/22
519	Execute POI and datacenter interconnection	10 days	Thu 2/17/22	Wed 3/2/22
520	**Install datacenter links and enhancements**	**49 days**	**Mon 2/7/22**	**Thu 4/14/22**
521	Complete rack installs	7 days	Mon 2/7/22	Tue 2/15/22

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
522	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Wed 2/16/22	Tue 3/29/22
523	Install GIS components	30 days	Wed 2/16/22	Tue 3/29/22
524	Install circuits, cross-connects and FOC	30 days	Thu 3/3/22	Wed 4/13/22
525	Confirm datacenter readiness	1 day	Thu 4/14/22	Thu 4/14/22
526	Install network connections and gateways	70 days	Thu 1/6/22	Wed 4/13/22
527	**Complete PSAP configurations**	**6 days**	**Thu 4/14/22**	**Thu 4/21/22**
528	Test CPE interfaces	5 days	Thu 4/14/22	Wed 4/20/22
529	Test circuits	5 days	Thu 4/14/22	Wed 4/20/22
530	Execute interface agreements if needed with CPE vendors	1 day	Thu 4/21/22	Thu 4/21/22
531	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Fri 4/22/22	Fri 4/22/22
532	Standup POIs	1 day	Mon 4/25/22	Mon 4/25/22
533	Publish and review cutover plan with stakeholders	10 days	Mon 4/25/22	Fri 5/6/22
534	**Phase III: Cutover**	**197 days**	**Tue 9/7/21**	**Wed 6/8/22**
535	Execute training plan	3 days	Mon 5/9/22	Wed 5/11/22
536	confirm readiness for cutover	1 day	Thu 5/12/22	Thu 5/12/22
537	Obtain state and local concurrence to cutover PSAP 1	5 days	Fri 5/13/22	Thu 5/19/22
538	**Prepare PSAP 1 for cutover**	**12 days**	**Fri 5/20/22**	**Mon 6/6/22**
539	Confirm fail-back plan in place	1 day	Fri 5/20/22	Fri 5/20/22
540	Confirm CPE interfaces operational	5 days	Fri 5/20/22	Thu 5/26/22
541	Confirm OSP readiness	2 days	Fri 5/27/22	Mon 5/30/22
542	Confirm training completed	1 day	Tue 5/31/22	Tue 5/31/22
543	Confirm PSAP ready for flash network cutover	1 day	Wed 6/1/22	Wed 6/1/22
544	Notify state PSAP 1 ready for flash cutover	1 day	Wed 6/1/22	Wed 6/1/22
545	Perform cutover	2 days	Thu 6/2/22	Fri 6/3/22
546	Confirm success	1 day	Mon 6/6/22	Mon 6/6/22
547	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Tue 6/7/22	Wed 6/8/22
548	**Perform flash network cutover**	**14 days**	**Tue 9/7/21**	**Fri 9/24/21**
549	Confirm fail-back plan in place	1 day	Tue 9/7/21	Tue 9/7/21
550	Turn-up core services	1 day	Wed 9/8/21	Wed 9/8/21

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
551	Activate interface between core services and legacy network	3 days	Thu 9/9/21	Mon 9/13/21
552	Migrate OSPs to i3 network	3 days	Thu 9/9/21	Mon 9/13/21
553	Onboard carriers into location database	3 days	Thu 9/9/21	Mon 9/13/21
554	Link core services to ESInet	1 day	Tue 9/14/21	Tue 9/14/21
555	Perform flash network cutover	1 day	Wed 9/15/21	Wed 9/15/21
556	Confirm carrier services	1 day	Thu 9/16/21	Thu 9/16/21
557	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Fri 9/17/21	Thu 9/23/21
558	Cutover confirmed to state	1 day	Fri 9/24/21	Fri 9/24/21
559	**Phase IV: Observation and Acceptance**	**39 days**	**Mon 9/27/21**	**Thu 11/18/21**
560	Execute ATP	5 days	Mon 9/27/21	Fri 10/1/21
561	Provisional acceptance accorded by state	1 day	Mon 10/4/21	Mon 10/4/21
562	Perform 30-day observation period	30 days	Tue 10/5/21	Mon 11/15/21
563	Close punch list	30 days	Tue 10/5/21	Mon 11/15/21
564	Final acceptance by state	2 days	Tue 11/16/21	Wed 11/17/21
565	Transition to operational environment	1 day	Thu 11/18/21	Thu 11/18/21
566	**North Eastern Region**	**197 days**	**Fri 11/19/21**	**Mon 8/22/22**
567	**OSP Connectivity Planning**	**77 days**	**Fri 11/19/21**	**Mon 3/7/22**
568	Distribute OSP survey forms and schedule individual OSP discussions	7 days	Fri 11/19/21	Mon 11/29/21
569	Conduct OSP discussions	60 days	Tue 11/30/21	Mon 2/21/22
570	Develop Draft OSP connectivity plan	10 days	Tue 2/22/22	Mon 3/7/22
571	Draft Aggregation plan and circulate for comment	10 days	Tue 2/22/22	Mon 3/7/22
572	**Survey (TBD) PSAPs and Dispatch Centers**	**96 days**	**Tue 11/30/21**	**Tue 4/12/22**
573	Publish survey form	1 day	Tue 11/30/21	Tue 11/30/21
574	schedule visits	5 days	Wed 12/1/21	Tue 12/7/21
575	Conduct visits, compile data and revise plans accordingly	90 days	Wed 12/8/21	Tue 4/12/22
576	Publish revised PM Plan	1 day	Wed 4/13/22	Wed 4/13/22
577	**Enhance datacenters as needed**	**7 days**	**Thu 4/14/22**	**Fri 4/22/22**
578	Confirm rack space and other DC needs satisfied	5 days	Thu 4/14/22	Wed 4/20/22
579	Plan for deploying ECRF, LVF and other GIS components	5 days	Thu 4/14/22	Wed 4/20/22

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

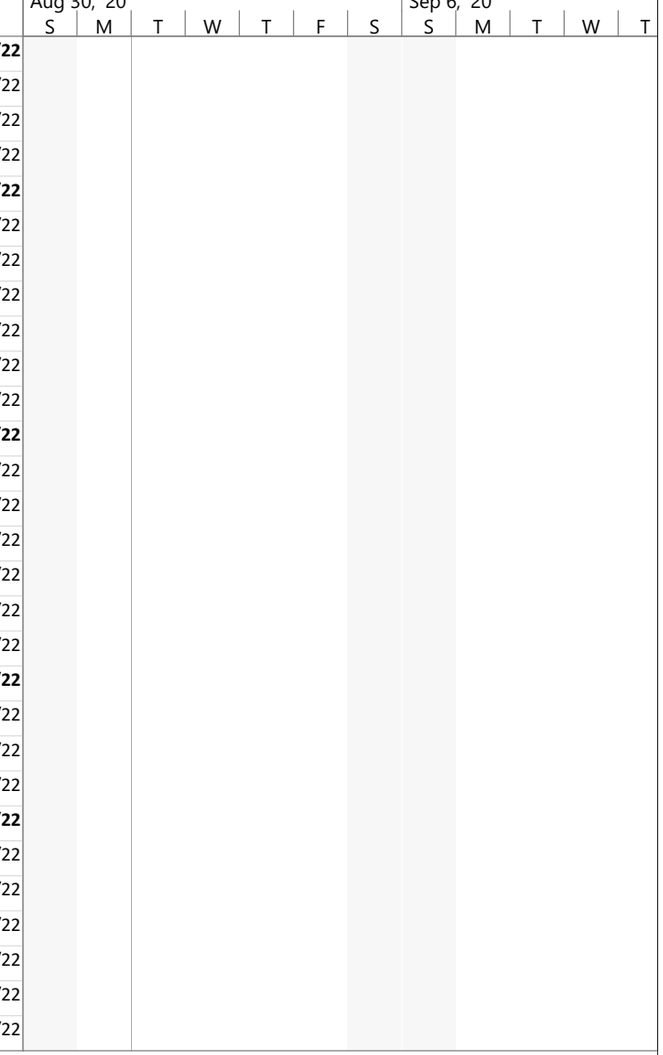
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
580	Identify enhancements needed in datacenters	5 days	Thu 4/14/22	Wed 4/20/22
581	Order new components and schedule labor	2 days	Thu 4/21/22	Fri 4/22/22
582	Identity and provision POIs	5 days	Thu 4/21/22	Wed 4/27/22
583	**Revise network design IAW tasks above**	**52 days**	**Thu 4/14/22**	**Fri 6/24/22**
584	Confirm network typology and provisioning plans	5 days	Thu 4/14/22	Wed 4/20/22
585	ID need for legacy gateways and provision	3 days	Thu 4/14/22	Mon 4/18/22
586	Complete NENA checklist 75-002	2 days	Thu 4/28/22	Fri 4/29/22
587	Confirm compliance with network security plan	2 days	Mon 5/2/22	Tue 5/3/22
588	Confirm transport independence and diversity	5 days	Wed 5/4/22	Tue 5/10/22
589	Prepare circuit plan and place orders	5 days	Wed 5/4/22	Tue 5/10/22
590	**ID changes to standard dashboard required for this project**	**30 days**	**Thu 4/14/22**	**Wed 5/25/22**
591	**ID PSAP needs and place orders**	**30 days**	**Thu 4/14/22**	**Wed 5/25/22**
592	Schedule installs and establish links to PSAP CPE vendors	30 days	Thu 4/14/22	Wed 5/25/22
593	Develop test plans with all vendors to ensure interface effectiveness	30 days	Thu 4/14/22	Wed 5/25/22
594	**Provision Monitoring**	**52 days**	**Thu 4/14/22**	**Fri 6/24/22**
595	Program OCOM	10 days	Thu 5/26/22	Wed 6/8/22
596	Program FortiSIEM	10 days	Thu 5/26/22	Wed 6/8/22
597	Plan E-Bonding capability	10 days	Thu 5/26/22	Wed 6/8/22
598	Adapt Call Data Record Management System / 9-1-1 Traffic Logging to satisfy state requirements	10 days	Thu 5/26/22	Wed 6/8/22
599	**Provision NGCS (Core Services) per NENA standards**	**47 days**	**Thu 4/21/22**	**Fri 6/24/22**
600	Provision two geographically diverse cores capable of 99.999% availability	30 days	Thu 4/28/22	Wed 6/8/22
601	Confirm active-active deployment negates any possible single-points-of-failure	1 day	Thu 6/9/22	Thu 6/9/22
602	**Design GIS solution**	**47 days**	**Thu 4/21/22**	**Fri 6/24/22**
603	Finalize plans for ECRF, LVF and other GIS components	45 days	Thu 4/21/22	Wed 6/22/22
604	Identify and provision GIS elements for use in datacenters	1 day	Thu 6/23/22	Thu 6/23/22
605	Confirm two instances of ECRF/PRF	1 day	Thu 6/23/22	Thu 6/23/22
606	Confirm data QA/QC manager is capable of meeting state and local needs	1 day	Fri 6/24/22	Fri 6/24/22
607	Publish training plan for stakeholder comment	50 days	Thu 4/14/22	Wed 6/22/22
608	**Phase II: Deployment**	**97 days**	**Tue 3/8/22**	**Wed 7/20/22**

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task	Inactive Task	Manual Summary Rollup	External Milestone
Split	Inactive Milestone	Manual Summary	Deadline
Milestone	Inactive Summary	Start-only	Progress
Summary	Manual Task	Finish-only	Manual Progress
Project Summary	Duration-only	External Tasks	

ID	Task Name	Duration	Start	Finish
609	**Complete OSP integration**	**50 days**	**Tue 3/8/22**	**Mon 5/16/22**
610	Execute interconnect agreements	10 days	Tue 3/8/22	Mon 3/21/22
611	Deploy i3-Interconnect where needed	30 days	Tue 3/22/22	Mon 5/2/22
612	Execute POI and datacenter interconnection	10 days	Tue 5/3/22	Mon 5/16/22
613	**Install datacenter links and enhancements**	**49 days**	**Thu 4/21/22**	**Tue 6/28/22**
614	Complete rack installs	7 days	Thu 4/21/22	Fri 4/29/22
615	Deploy core services and test diversity and compliance with call delivery standards.	30 days	Mon 5/2/22	Fri 6/10/22
616	Install GIS components	30 days	Mon 5/2/22	Fri 6/10/22
617	Install circuits, cross-connects and FOC	30 days	Tue 5/17/22	Mon 6/27/22
618	Confirm datacenter readiness	1 day	Tue 6/28/22	Tue 6/28/22
619	Install network connections and gateways	70 days	Tue 3/22/22	Mon 6/27/22
620	**Complete PSAP configurations**	**6 days**	**Tue 6/28/22**	**Tue 7/5/22**
621	Test CPE interfaces	5 days	Tue 6/28/22	Mon 7/4/22
622	Test circuits	5 days	Tue 6/28/22	Mon 7/4/22
623	Execute interface agreements if needed with CPE vendors	1 day	Tue 7/5/22	Tue 7/5/22
624	Confirm end-to-end connectivity and gateways to accommodate legacy systems	1 day	Wed 7/6/22	Wed 7/6/22
625	Standup POIs	1 day	Thu 7/7/22	Thu 7/7/22
626	Publish and review cutover plan with stakeholders	10 days	Thu 7/7/22	Wed 7/20/22
627	**Phase III: Cutover**	**197 days**	**Fri 11/19/21**	**Mon 8/22/22**
628	Execute training plan	3 days	Thu 7/21/22	Mon 7/25/22
629	confirm readiness for cutover	1 day	Tue 7/26/22	Tue 7/26/22
630	Obtain state and local concurrence to cutover PSAP 1	5 days	Wed 7/27/22	Tue 8/2/22
631	**Prepare PSAP 1 for cutover**	**12 days**	**Wed 8/3/22**	**Thu 8/18/22**
632	Confirm fail-back plan in place	1 day	Wed 8/3/22	Wed 8/3/22
633	Confirm CPE interfaces operational	5 days	Wed 8/3/22	Tue 8/9/22
634	Confirm OSP readiness	2 days	Wed 8/10/22	Thu 8/11/22
635	Confirm training completed	1 day	Fri 8/12/22	Fri 8/12/22
636	Confirm PSAP ready for flash network cutover	1 day	Mon 8/15/22	Mon 8/15/22
637	Notify state PSAP 1 ready for flash cutover	1 day	Mon 8/15/22	Mon 8/15/22



Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish
638	Perform cutover	2 days	Tue 8/16/22	Wed 8/17/22
639	Confirm success	1 day	Thu 8/18/22	Thu 8/18/22
640	Obtain state approval to proceed with cutovers of remaining PSAPS	2 days	Fri 8/19/22	Mon 8/22/22
641	**Perform flash network cutover**	**14 days**	**Fri 11/19/21**	**Wed 12/8/21**
642	Confirm fail-back plan in place	1 day	Fri 11/19/21	Fri 11/19/21
643	Turn-up core services	1 day	Mon 11/22/21	Mon 11/22/21
644	Activate interface between core services and legacy network	3 days	Tue 11/23/21	Thu 11/25/21
645	Migrate OSPs to i3 network	3 days	Tue 11/23/21	Thu 11/25/21
646	Onboard carriers into location database	3 days	Tue 11/23/21	Thu 11/25/21
647	Link core services to ESInet	1 day	Fri 11/26/21	Fri 11/26/21
648	Perform flash network cutover	1 day	Mon 11/29/21	Mon 11/29/21
649	Confirm carrier services	1 day	Tue 11/30/21	Tue 11/30/21
650	Confirm cutover of all PSAPs, datacenters and POIs	5 days	Wed 12/1/21	Tue 12/7/21
651	Cutover confirmed to state	1 day	Wed 12/8/21	Wed 12/8/21
652	**Phase IV: Observation and Acceptance**	**39 days**	**Thu 12/9/21**	**Tue 2/1/22**
653	Execute ATP	5 days	Thu 12/9/21	Wed 12/15/21
654	Provisional acceptance accorded by state	1 day	Thu 12/16/21	Thu 12/16/21
655	Perform 30-day observation period	30 days	Fri 12/17/21	Thu 1/27/22
656	Close punch list	30 days	Fri 12/17/21	Thu 1/27/22
657	Final acceptance by state	2 days	Fri 1/28/22	Mon 1/31/22
658	Transition to operational environment	1 day	Tue 2/1/22	Tue 2/1/22

Project: Nebraska NGCS Notional Pro
Date: Fri 5/22/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

CenturyLink®

CERTIFICATION REGARDING COMPLIANCE WITH E-VERIFY

CenturyLink, Inc. does hereby state the following facts to be true:

1. CenturyLink and its affiliates constitute a business entity that is an employer of employees in the United States or has subcontractors who employ employees in the United States.

2. CenturyLink is executing this affidavit to assure, confirm, and warrant that it has verified the work authorization of its employees at the time of hire through the E-Verify program operated by the United States Department of Homeland Security as defined in NCGS §64-25(5) since January 25, 2012. CenturyLink's subcontractors are contractually required to comply with all state and federal laws.

This the 13 day of February 2020

CenturyLink, Inc.

Signature: Abby McConnell
Name: Abby McConnell
Title: HR Shared Service Coordinator

State of

Louisiana
County of Ouachita
Parish

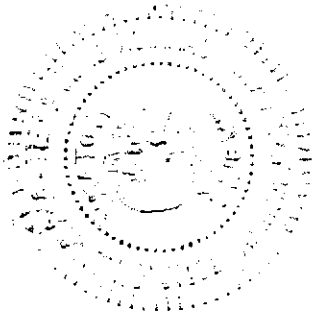
Carrick B. Inabnett, a Notary Public of the aforesaid
Parish
State and ~~County~~, do certify that Abby McConnell
personally, appeared before me this day, and being duly sworn and in my presence signed and acknowledged the execution of the foregoing CERTIFICATION.

Witness my hand and official seal, this the 13th day of February, 2020

Carrick B. Inabnett
Notary Public My commission expires: Death

Carrick B. Inabnett

100 CenturyLink Drive
Monroe, LA 71203
Tel: 318.388.9000
www.centurylink.com



CENTURYLINK MASTER SERVICE AGREEMENT
CENTURYLINK MPLS (IPVPN AND VPLS) VPN SERVICE
SERVICE SCHEDULE

1. Applicability. This Service Schedule forms part of the Master Service Agreement between CenturyLink and Customer ("Agreement") and is applicable only where Customer orders CenturyLink MPLS (IPVPN and VPLS) VPN Service (which may also be called IP VPN, IPVPN, IPVPN Port, Private Port, IQ Networking Private Port, MPLS/IP VPN Port, VPN, NBIPVPN (Network Based IP VPN), Virtual Private Network, or IP Solutions Private Port on ordering, pricing, invoicing, or other documentation). Capitalized terms used but not defined herein have the definitions given to them in the Agreement. Customer expressly agrees that CenturyLink may use affiliates or third party suppliers to provide MPLS VPN Service, provided that CenturyLink remains responsible to Customer hereunder.

2. Service Description. MPLS VPN Service includes two (2) virtual private network ("VPN") services, IPVPN and VPLS, providing private site-to-site communications over CenturyLink's MPLS network. IPVPN utilizes Internet Protocol; VPLS is provided using Ethernet. Customer must purchase at least 2 ports to set up private site-to-site connections. The Service is connected to each site, including additional sites designated by Customer (together "Customer Sites") through the Customer port at either a circuit location address or a CenturyLink Point of Presence (PoP) as specified in the Order. Customer Sites will be connected to a port at one or more CenturyLink MPLS Network PoPs at a fixed data transmission rate. Standard network management web tools are also provided in conjunction with the MPLS VPN Services. The VPLS offer of Enterprise Switched Native LAN ("SNLAN") allows multiple Customer locations to interconnect within a single CenturyLink-defined metro area network ("MAN"). The VPLS offer of Extended Native LAN ("ENLAN") allows Customer to connect multiple SNLAN networks between MANs.

3. Additional features and functionality may include:

a. Enhanced Reporting. CenturyLink offers enhanced reporting features including Performance Assurance, Enhanced Management, and End to End Statistics (collectively these are referred to herein as "Enhanced Reporting"). Customer may subscribe to Performance Assurance and End to End Statistics for an additional charge. If available at Customer's location, Enhanced Management will be included with Customer's MPLS VPN Service at no additional charge. Customer may request information regarding the availability of Enhanced Management at any particular location. Where available, these features provide end-to-end reporting and SLA's for the following statistics: data delivery, latency and jitter that can be accessed by Customer via the CenturyLink provided customer portal.

b. Class of Service (CoS). Customer may purchase CoS where available providing the ability to prioritize certain identifiable traffic flows between MPLS network ports. Customer is solely responsible for the selection of classes of service as stated in the Order. If a Service Order references Premium Plus/Premium CIR (or PIR), the stated bandwidth is included in, and not in addition to, the Committed Information Rate or Peak Information Rate.

c. Smart Demarcation. In certain locations, where available, for VPN and VPLS services with Ethernet access in the domestic U.S. and VPLS services with Ethernet access outside of the U.S., CenturyLink provides 'Smart Demarcation' which is the supply and installation of a Smart Demarcation device (also referred to as a Network Interface Device or "NID") used for Ethernet connectivity fault management for up to 1Gbps port speeds at Customer Sites.

4. Charges. Customer shall be billed non-recurring charges ("NRC") and monthly recurring charges ("MRC") for MPLS VPN Services as set forth in the Order or pricing attachment. NRC includes applicable installation charges for local-access circuit and each port. MRC includes local-access charges, port connection charges and bandwidth charges. Bandwidth may be identified on an Order or pricing attachment as Bandwidth, Commit, Committed Information Rate (or CIR), or Peak Information Rate (or PIR). Other charges, including but not limited to usage based charges, may apply as stated in the Order or pricing attachment. Where Customer orders MPLS VPN Services bundled with either CenturyLink Internet Services or Level 3 Enterprise Voice SIP Based Services (either combination is referred to herein as a "Converged Service") such charges will show on the invoice as Converged Services. For clarification, the Converged Service is treated as a single Service and if Customer wishes to unbundle or terminate a part of the Converged Service, early termination liability may apply and Customer will be required to execute new orders for the desired stand-alone Service.

5. The following services may be available at an additional charge to be set forth in an Order and pursuant to the separate Service Schedule for such services:

a. CenturyLink Internet Services. As part of a Converged Service, Customer may order Internet Services which are high speed symmetrical Internet services providing access to the CenturyLink IP Network and the global internet.

b. CenturyLink Enterprise Voice SIP Based Services. As part of a Converged Service, Customer may order SIP based enterprise voice for Public Switched Telephone Network connectivity, outbound (1+) access to U.S. (interstate and intrastate) and international locations, inbound (8XX) service, and international toll free calling.

c. Application Performance Management. As an optional service feature for IPVPN, where available Customer may subscribe to Application Performance Management ("APM") which provides near real-time information for live monitoring and historical data for analysis and reporting on all network traffic end-to-end, including advanced statistics on latency, jitter and packet loss, as well as general utilization by way of an inline Analysis Service Element ("ASE").

d. Managed Network Services. As an additional Service offering, where available Customer may order CenturyLink Managed Network Services ("MNS") in which Customer premises equipment ("CPE") is provided by either the Customer or CenturyLink, but in all cases is managed and maintained by CenturyLink. MNS may include, but is not limited to, Routers, IADs, SBCs, and firewalls.

e. Secure Access. As an additional Service offering, where available Customer may order Secure Access Site and Secure Access Cellular.

f. Managed Security Services. As an additional Service offering, if available Customer may order certain managed security services ("MSS") which may be available on a cloud-based (MSS-Cloud) solution. The MSS Cloud solution may also be referenced as a Secure Internet Access Firewall or SIA Firewall when ordered in conjunction with CenturyLink MPLS Service.

6. Customer Responsibilities. Customer is responsible for providing the network design specifications including pre-existing LAN/WAN IP addressing schemes, MAC addresses and circuit designs. Customer is solely responsible for all equipment and other facilities used in connection with the Service which are not provided by CenturyLink. All IP addresses, if any, assigned to Customer by CenturyLink shall revert to CenturyLink upon termination of Service, and Customer shall cease using such addresses as of the effective date of termination. For installation of the Smart Demarcation device (NID) at Customer's Site, Customer shall (i) provide access at each Site for installation, implementation and maintenance ("Work") at scheduled times, (ii) make appropriate contact personnel available on-site for such Work, (iii) provide all necessary power distribution boxes, conduits, telco backboard space for equipment mounting, grounding, surge and lightning protection and associated hardware and power outlets within 4 feet (1 meter) of the location at which a NID is to be installed, (iv) provide all required extended demarcation inside wiring, including any necessary building alterations to meet wiring and any other site requirements, (v) ensure that the NID can be installed within 6 feet (2 meters) of the Customer provided equipment and the Customer provided or third party provided extension of the local access circuit demarcation, or otherwise provide additional cabling at the Customer's expense, (vi) clearly marking each telecommunications extended local access circuit demarcation point to allow the installer to connect the correct circuit to the correct NID interface, and (vii) connection of the NID to the Customer Router or LAN.

7. On-Net and Off-net Access. Access services provided entirely on the CenturyLink owned and operated network ("Network") are "On-Net Access Services". Additionally, CenturyLink may use third parties to reach Customer's site from the CenturyLink Network ("Off-Net Access Services"). Local Access may be provisioned utilizing one of the following service technologies: special access, ethernet local access, or wavelength local access.

8. Service Levels and Service Credits. The following Service Levels (SLAs) apply as set forth below. When Converged Services are ordered the SLAs below apply in lieu of any SLAs identified in the applicable CenturyLink Internet Service Schedule and/or CenturyLink Enterprise Voice SIP Based Service Schedule as referenced above in Section 5. Depending on the type of Service ordered by Customer, the Class of Service levels of Premium Plus, Premium, Enhanced Plus, Enhanced, and Basic may be referenced on an Order as Real Time, Interactive, Mission Critical, Priority and Best Effort, respectively.

a. Availability Service Level. The Availability Service Level in the United States is 99.99%. Outside the United States, the Availability Service Level for Fully On-Net MPLS VPN Service is 99.99% and 99.9% for Off-Net Service. Fully On-Net MPLS VPN Service is provided entirely on CenturyLink's owned and operated network. Off-Net Service is a service that is partially or entirely provided using third party circuits not owned and operated by CenturyLink. For IPVPN and VPLS, Service Availability is calculated on a per site basis.

b. Packet Delivery, Latency and Jitter Service Levels - PoP to PoP. CenturyLink's service levels for packet delivery, latency, or jitter are set forth below in Tables A and B. These latency calculations are averaged monthly between all CenturyLink designated points of presence ("POPs") in a given region.

Table A: PoP to PoP

SLA Boundary	Measurement Parameter	Class of Service		
		Premium Plus/ Premium (e.g. Voice/ Video)	Enhanced Plus/Enhanced (e.g. Critical/ Preferred Data)	Basic Plus/ Basic (e.g. Default/ Internet / Bulk Data)
Intra Continental U.S.	Average Packet Delivery	99.99%	99.95%	N/A
	Average Two Way Latency	City Pair*	City Pair*	City Pair*
	Jitter (one way)	≤ 3 ms	N/A	N/A
Intra EU and EU - US	Average Packet Delivery	99.99%	99.95%	N/A
	Average Two Way Latency	City Pair	City Pair	City Pair
	Jitter (one way)	≤ 10 ms	N/A	N/A
Rest of World	Average Packet Delivery	99.9%	99.8%	N/A
	Average Two Way Latency	City Pair	City Pair	City Pair
	Jitter (one way)	Regional	N/A	N/A

*Appendix 1 sets forth the "City Pair" monthly average two way latency in the MPLS VPN PoP to PoP two way latency SLA matrix. Appendix 1 is available upon request. For city pairs that are not listed in Appendix 1, the following regional metrics apply per Table B. Regional metric calculations are averaged monthly between all CenturyLink POPs in a given region.

Table B: Regional Two Way Latency and Jitter

Description	Average Two Way Latency (milliseconds)	Average Jitter Roundtrip (milliseconds)
Trans-Atlantic (London/Amsterdam – New York)	≤ 95 ms	≤ 6 ms
Intra–United Kingdom	≤ 25 ms	≤ 6 ms
European network	≤ 45 ms	≤ 6 ms
North American Network *	≤ 65 ms	≤ 6 ms
Pacific (Tokyo – Sacramento, CA)	≤ 150 ms	≤ 6 ms
Sydney – US West (Sacramento, CA)	≤ 270 ms	≤ 6 ms
Sydney – Asia (Tokyo)	≤ 200 ms	≤ 6 ms
Intra–Asia **	≤ 140 ms	≤ 6 ms
South America (Buenos Aires, Sao Paolo, Panama City, Santiago, and Miami)	≤ 170 ms	≤ 6 ms
New York – South Africa	≤ 295 ms	≤ 40 ms
London – South Africa	≤ 230 ms	≤ 40 ms

* Add 90ms from/to the Mexico PoP

** 'Intra-Asia' is defined as: Japan, Australia, Hong Kong, Taiwan, Philippines, South Korea, Thailand, Malaysia, and Indonesia.

c. Packet Delivery, Latency and Jitter Service Levels – End to End (Optional). End to End Packet Delivery, jitter and two way latency SLAs apply only to sites where Customer has ordered Enhanced Reporting or APM for IPVPN. For sites with DSL, microwave or satellite access, End to End packet delivery, jitter, and latency SLAs do not apply. To calculate an end to end two way latency SLA, the loop factor table applies per Appendix 1.

Table C: End to End

SLA Boundary	Measurement Parameter	Class of Service		
		Premium Plus/ Premium (e.g. Voice/Video)	Enhanced Plus/Enhanced (e.g. Critical/Preferred Data)	Basic Plus/ Basic (e.g. Default/Bulk Data)
Intra Continental U.S.	Average Packet Delivery	99.9%	99.5%	N/A
	Average Two Way Latency	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*
	Jitter (Round Trip)	≤ 3 ms	N/A	N/A
Intra EU and EU -US	Average Packet Delivery	99.9%	99.5%	N/A
	Average Two Way Latency	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*
	Jitter (Round Trip)	≤ 10 ms	N/A	N/A
Rest of World	Average Packet Delivery	99.5%	99.0%	N/A
	Average Two Way Latency	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*	City Pair Plus Loop Factor Table*
	Jitter (Round Trip)	Regional	N/A	N/A

d. Credits for SLAs above. All SLA credits are calculated after deduction of all discounts and other special pricing arrangements, and are not applied to governmental fees, taxes, surcharges and similar additional charges. Credit percentages are applied to the MRC of the CIR/CDR rate, port charge, and local access circuits for applicable sites only. In no event will SLA credits in any calendar month exceed 100% of the total MRCs (excluding local access) for the affected Site(s). All approved SLA credits requested by Customer for a given month will be totaled and applied to Customer's next following invoice for the Service, or as promptly thereafter as is practical in the event of a dispute.

i. Availability Service Credit. Service is "Unavailable" (except in the case of an Excused Outage) if the Customer port at a Customer site is unable to pass traffic. Service Unavailability is calculated from the timestamp CenturyLink opens a trouble ticket following the report of a problem by the Customer until the time the ticket is closed. If credits are due under this SLA, no other SLAs apply to the same event. If Service is Unavailable for reasons other than an Excused Outage, Customer will be entitled to a service credit off of the MRC for the affected Service locations based on the cumulative Unavailability of the Service in a given calendar month as set forth in the tables below. For a Fully On-Net Service, the SLA and credits in Table D will apply. For Off-Net Service, the SLA and credits in Table E will apply.

Table D:
US Domestic Only or Fully On-Net MPLS VPN Service

Cumulative Unavailability (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:04:18 (99.99%)	No Credit
00:04:19– 00:43:00	5%
00:43:01 – 04:00:00	10%
04:00:01 – 8:00:00	20%
08:00:01 – 12:00:00	30%
12:00:01 – 16:00:00	40%
16:00:01 – 24:00:00	50%
24:00:01 or greater	100%

Table E:
Off-Net MPLS VPN Service and Service outside the Domestic US

Cumulative Unavailability (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:43:00 (99.9%)	No Credit
00:43:01 – 04:00:00	10%
04:00:01 – 8:00:00	20%
08:00:01 – 12:00:00	30%
12:00:01 – 16:00:00	40%
16:00:01 – 24:00:00	50%
24:00:01 or greater	100%

ii. Data Delivery, Latency, and Jitter Service Credits. The PoP to PoP SLAs are based on monthly average performance between nodes on CenturyLink's MPLS network. Where End to End SLAs apply, the monthly average performance is measured between the CenturyLink Equipment deployed for APM or Enhanced Reporting, as applicable. Customer will be entitled to a service credit off of the MRC for the affected Service locations as set forth below for the Service parameter(s) not met for reasons other than an Excused Outage. Customer will not be entitled to credits under the packet delivery, latency, or jitter SLA's for the affected Service where such failure is related to Unavailability under the Availability SLA.

Monthly Service Parameter	Service Level Credit
Data Delivery	10%
Latency	10%
Jitter	10%

e. Smart Demarcation Opt-Out. Where Smart Demarcation is required by CenturyLink and Customer wants the Service provisioned without Smart Demarcation, CenturyLink agrees upon Customer's request to meet with Customer to discuss alternative options (if available).

f. Chronic Outage. As its sole remedy, Customer may elect to terminate an affected MPLS VPN Service, or if applicable an affected Converged Service, prior to the end of the Service Term without termination liability if, for reasons other than an Excused Outage: such MPLS Service is Unavailable (as defined in Section 5(d)(i) above) in any calendar month for: (i) twice during a 30-day period, and becomes Unavailable a third time within 30 days following the second event, or (ii) more than 24 aggregate hours during a 30-day period.. Customer may only terminate such Service that is Unavailable as described above, and must exercise its right to terminate the affected Service under this Section, in writing, within 30 days after the event giving rise to a right of termination. For clarification, termination of a Converged Service will result in termination of all applicable Services bundled together as the Converged Service under the Order.

g. Installation Service Level. CenturyLink will exercise commercially reasonable efforts to install each MPLS VPN Service on or before the Customer Commit Date for the particular Service. This installation Service Level shall not apply to Orders that contain incorrect information supplied by Customer or Orders that are altered at Customer request after submission and acceptance by CenturyLink. In the event CenturyLink does not meet this Installation Service Level for a particular MPLS VPN Service for reasons other than an Excused Outage, Customer will be entitled to a service credit for each day of delay equal to the charges 1 day of the pro rata share of the MRC associated with the affected MPLS VPN service up to a monthly maximum credit of 10 days.

h. SLA Limitations. For circuits with Bandwidths of 15 Mbps or lower, the measurement of such Data Delivery, Latency and Jitter also excludes any time period that Customer's total bandwidth utilization or bandwidth utilization by CoS exceeds fifty percent (50%) of the applicable contracted bandwidth. For circuits with bandwidths over 15 Mbps, the measurement of such Data Delivery, Latency and Jitter also excludes any time period that Customer's total bandwidth utilization exceeds seventy percent (70%) of the applicable contracted bandwidth. The Enhanced Management SLA shall not apply to any site for any calendar month if CenturyLink's measurement of Data Delivery, Latency or Jitter does not include at least twenty five percent (25%) of the duration of any calendar month. Credits provided for the applicable metric are not cumulative and, in any calendar month, Customer shall only be entitled to one credit per metric per site. All measurements are based on the average of the metrics for that calendar month.

9. Resale Restriction. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Service provided pursuant to this Service Schedule except as expressly provided by CenturyLink, provided however, if Customer requests to resell any Converged Services such permission from CenturyLink must be in the form of an amendment signed by authorized representatives of both parties.

10. Latin American Services. With respect to Services provided in Latin America, Customer agrees that it (or its local Affiliate) will enter into a separate local country addendum/agreement (as approved by local authorities) ("LCA") with the respective CenturyLink Affiliate which provides the local Service(s) containing terms necessary to comply with local laws/regulations, and such CenturyLink Affiliate will invoice the Customer (or its local Affiliate) party to the LCA for the respective local Service(s).

11. Business Contact Information. Customer must provide to CenturyLink the names of and contact information ("Business Contact Information") for its employees ("Business Contacts") who have purchasing or other responsibilities relevant to CenturyLink's delivery of international Service under this Service Schedule. Customer consents to CenturyLink's and its affiliates or subcontractors' use and transfer to the United States of Business Contact Information for the purpose of: (a) fulfilling its obligations under this Service Schedule; and (b) providing information to Customer about CenturyLink's products and services via these Business Contacts. Customer represents that the Business Contact Information is accurate and that each Business Contact has consented to CenturyLink's processing of their Business Contact Information for the purposes set forth in this Service Schedule. The Business Contact Information provided by Customer has been collected, processed, and transferred in accordance with applicable laws, including, where applicable, any necessary notification to the relevant data protection authority in the territory in which Customer is established ("Authority"). Customer will notify CenturyLink promptly of staffing or other changes that affect CenturyLink's use of Business Contact Information. CenturyLink will have in place technical and organizational measures that ensure a level of security appropriate to the risk represented by the processing and the nature of the Business Contact Information and that protects such information against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access. CenturyLink will use the information only for the express purposes set forth in this Service Schedule. CenturyLink will identify a contact authorized to respond to inquiries concerning processing of Business Contact Information and will reasonably cooperate in good faith with Customer and the Authority concerning all such inquiries without excessive delays.

12. Withholding Taxes. All invoices will be issued to Customer and paid in the currency specified in the Order or pricing attachment. Customer will pay such invoices free of currency exchange costs or bank charges. Service charges are exclusive of taxes and presented without reduction for any Withholding Tax, all of which are the responsibility of the Customer. "Withholding Tax" means any amount or account of tax on sources of income which a payor is obliged to deduct from payments due to a recipient and account for or to any tax authority. In the event that any payment to be made to CenturyLink hereunder should be subject to reduction by reason of a Withholding Tax, Customer agrees to pay CenturyLink such amounts as would have been necessary so that the aggregate net amount received by CenturyLink after application of a Withholding Tax is the same amount as would have been received by CenturyLink if there had been no requirement to deduct or withhold such tax.

PRICING ATTACHMENT

For pricing, please refer to the RFP. This Pricing Attachment will be completed upon award.

CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK® LOCAL ACCESS SERVICE EXHIBIT

1. General. This Service Exhibit is applicable only where Customer orders CenturyLink Local Access Service (the "Service") and incorporates the terms of the Master Service Agreement or other service agreement and the RSS under which CenturyLink provides services to Customer (the "Agreement"). CenturyLink may subcontract any or all of the work to be performed under this Service Exhibit. All capitalized terms that are used but not defined in this Service Exhibit are defined in the Agreement or Order.

2. Service Description and Availability.

2.1 Description. Service provides the physical connection between the Service Address and the CenturyLink Domestic Network. If a generic demarcation point (such as a street address) is provided, the demarcation point for On-Net Access will be CenturyLink's Minimum Point of Entry (MPOE) at such location (as determined by CenturyLink). Off-Net Access demarcation points will be the off-net vendor's MPOE. If the Order identifies aspects of services that are procured by Customer directly from third parties, CenturyLink is not liable for such services. Customer may request additional wiring from the demarcation point to Customer's network interface equipment (where available). If Customer requests additional wiring, CenturyLink will notify Customer of the charge to be billed to Customer. Customer may either approve or disapprove CenturyLink providing the additional wiring. Additional wiring could entail electrical or optical cabling into 1) existing or new conduit or 2) bare placement in drop down ceilings, raised floors, or mounted to walls/ceilings. Once Service is accepted by Customer, the additional wiring then becomes property of and maintained by Customer. CenturyLink will maintain Service to the demarcation point only. Customer is responsible for any facility or equipment maintenance and repairs on Customer's side of the demarcation point. All equipment owned by CenturyLink remains property of CenturyLink. Customer disclaims any interest in any equipment, property or licenses used by CenturyLink to provide Service. CenturyLink will not provide Service to a residential location, even if business is conducted at that location. Service is not a standalone service and Customer must purchase the Service in connection with another CenturyLink service for which a local loop is required.

2.2 Types of Service Technologies. CenturyLink uses the following different technologies to provide Service. Some technologies or speeds may not be available in all areas or with certain types of Service.

(a) Special Access. "Special Access" means Service using digital signal bandwidths DS0, DS1 and DS3 or Optical Carrier signal bandwidths OC3, OC12, OC48 and OC192.

(b) Ethernet Local Access ("ELA"). ELA means Service under Ethernet technology and is available at bandwidths varying from 1 Mbps to 1,000 Mbps (1G) and 10G (Cross-Connect Access only).

(c) Wavelength Local Access. "Wavelength Local Access" means Service using wave division multiplexing technology. Wavelength Local Access is available at bandwidths of 1 GbE, 10 GbE LAN PHY, 2.5 G (OC48), 10 GbE WAN PHY (OC192), 40G, OTU1, OTU2, OTU3, 1G, 2G, 4G and 10G.

(d) DSL Local Access. "DSL Local Access" means access using digital subscriber line ("DSL") technology. DSL Local Access is available at bandwidths varying from 128 kbps/64 kbps to 15000 Mbps/1000 Mbps.

2.2.1 Use of IP Connection. In some locations, CenturyLink will enable the Service using "IP Connection" which is a Layer 3, symmetrical functionality that utilizes established IP and MPLS transport technologies. In such cases, Customer agrees that it will use IP Connection functionality only for the provision of either: (i) wireline broadband Internet access (as defined in applicable Federal Communications Commission orders and regulations), or (ii) wireline broadband Internet access plus additional information services, with wireline broadband Internet access constituting a principal use. CenturyLink can provision IP Connection functionality over multiple designs with MPLS transport supporting speeds up to 1G/1G.

2.3 Types of Service. CenturyLink offers the following three types of Service: CenturyLink Provided Access, Customer Provided Access or Cross-Connect Access.

2.3.1 CenturyLink Provided Access. "CenturyLink Provided Access" or "CLPA" means either On-Net Access or Off-Net Access. "On-Net Access" is provided on the CenturyLink owned and operated network. Any access not provided on the CenturyLink owned and operated network is "Off-Net Access." Customer may request a Preferred Provider for Off-Net Access from a list of available providers with whom CenturyLink has interconnect agreements. CenturyLink will attempt to use Customer's Preferred Provider, but both final routing and the provider actually used will be chosen by CenturyLink. If CenturyLink is unable to use Customer's Preferred Provider for a specific Service Address as designated in the pricing attachment or a quote, then the rate for Service at that Service Address may be subject to change. Where available for Special Access, ELA and Wavelength Local Access, Customer may request CenturyLink to provide a separate fiber facility path for a protection system between the local access provider's serving wire center and the Service Address ("Protect Route"). Protect Route uses backup electronics and two physically separate facility paths in the provisioning of Service. If the working facility or electronics fail, or the Service performance becomes impaired, the facility is designed to automatically switch to the Service protect path in order to maintain a near-continuous flow of information between locations. Special Access and ELA are also generally available as a central office meet point at a local access provider central office to which Customer has a dedicated connection. Unless otherwise covered by another SLA, On-Net Access is subject to the On-Net Local Access Service Level Agreement located at http://www.centurylink.com/legal/docs/Local-Access-SLA.pdf, which is subject to change.

2.3.2 Customer Provided Access. "Customer Provided Access" or "CPA" means a local loop that Customer orders from a local access provider to connect Customer's premises to the CenturyLink Domestic Network at a connection point specified by CenturyLink. CenturyLink will provide Customer with a limited letter of agency ("LOA"), which is incorporated by this reference, authorizing Customer

to act as CenturyLink's agent so that Customer's local access provider will connect Customer's premises to the CenturyLink Domestic Network. Customer will also need to execute a CPA-DAR Addendum for CPA POP with ELA or Wavelength Local Access. Customer will pay a CPA charge to CenturyLink when Customer uses the following: (a) Special Access CPA dedicated facilities or ELA CPA virtual local area network ("VLAN"), both of which are dedicated entrance facilities CenturyLink leases from a local access provider and that carry traffic only from CenturyLink; or (b) ELA CPA POP, which requires CenturyLink to provide space and power for the local access provider to install Ethernet equipment; or (c) Wavelength Local Access. Customer will pay a CPA charge to CenturyLink when Customer uses Special Access CPA non-dedicated facilities owned by local access providers and that carry traffic from multiple carriers, including CenturyLink, if the provider charges CenturyLink for those facilities. CPA ELA VLAN is an access type where CenturyLink will provision and assign an Ethernet virtual circuit from a CenturyLink POP to a Customer designated Ethernet facility leased from a common Ethernet service provider. This access will be used to connect to a CenturyLink VLAN assignment on a CenturyLink IQ® Networking Private Port or E-Line. CenturyLink will not bill customer a CPA charge for an IP layer 3 expansion site because Customer, not CenturyLink, is responsible for ordering a cross-connect from the IP layer 3 expansion site manager to meet CenturyLink in the IP layer 3 expansion site's meet-me-room. CPA is the responsibility of Customer and CenturyLink will not pay for or troubleshoot components of CPA.

2.3.3 Cross-Connect Access. "Cross-Connect Access" or "XCA" means: (a) an intra-POP connection between certain Customer facilities with direct access to the CenturyLink Domestic Network and the CenturyLink backbone access point (either (i) located within CenturyLink's transport area where CenturyLink allows Customer to bring its own fiber directly to the CenturyLink fiber under an executed Direct Connect Agreement ("Direct Connect") or (ii) in an area where Customer has leased space in a CPOP, a remote collocation site, or a collocation hotel under a Telecommunications Collocation License Agreement or (b) a connection between a CenturyLink-determined data center and a CenturyLink IQ Networking Port, Optical Wavelength Service ("OWS"), or E-Line ("Data Center Access") under an executed CenturyLink TS Service Exhibit with a CenturyLink IQ Networking, OWS or E-Line Service Exhibit. Data Center Access is available in bandwidths of 100 Mbps, 1G, and 10G (CenturyLink IQ Networking and OWS only). Direct Connect requires splicing of Customer and CenturyLink fibers and cross-connection of individual circuits.

2.4 RSS. Customer understands that Service is an interstate telecommunications service, as defined by Federal Communications Commission regulations and represents while using the Service, more than 10% of its usage will be interstate usage.

3. Ordering. Customer may submit requests for Service in a form designated by CenturyLink ("Order"). CenturyLink will notify Customer of acceptance of an Order for Service by delivering (in writing or electronically) the date by which CenturyLink will install Service (the "Customer Commit Date"), or by delivering the Service. Provision of Services is subject to availability of adequate capacity and CenturyLink's acceptance of an Order. In lieu of installation Service Level credits, if CenturyLink's installation of Service is delayed by more than 30 business days beyond the Customer Commit Date, Customer may terminate the affected Service without liability upon written notice to CenturyLink, provided such written notice is delivered prior to CenturyLink delivering a Connection Notice for the affected Service. This termination right will not apply where CenturyLink is constructing facilities to a new location not previously served by CenturyLink.

4. Charges. Customer will pay the rates set forth in the attached pricing attachment or a quote or Order if the rates for Service at a particular Service Address are not included in the pricing attachment, and all applicable ancillary Service charges. CenturyLink invoices MRCs in advance and NRCs in arrears. If the delivery of a Connection Notice for any Service falls on any day other than the first day of the month, the first invoice to Customer will consist of: (a) the pro-rata portion of the applicable MRC covering the period from the delivery of the Connection Notice to the first day of the subsequent month; and (b) the MRC for the following month. Charges for Service will not be used to calculate Contributory Charges. Customer will receive the rates for Service as shown on the pricing attachment regardless of whether an NPA/NXX split or overlay occurs. If CenturyLink cannot complete installation due to Customer delay or inaction, CenturyLink may begin charging Customer and Customer must pay such charges.

4.1 Ancillary Charges. Ancillary charges applicable to Service include but are not limited to those ancillary services set forth in this section. If an ancillary charge applies in connection with provisioning a particular Service, CenturyLink will notify Customer of the ancillary charge to be billed to Customer. Customer may either approve or disapprove CenturyLink providing the ancillary service.

(a) Expedite. A local loop expedite charge applies to Orders where Customer requests the delivery of Service one or more days before the Customer Commit Date. Customer may only request to expedite CenturyLink Provided Access of Special Access and ELA Orders (where underlying local access provider allows CenturyLink to order an expedited service.)

(b) Construction. Construction charges apply if; (i) special construction is required to extend Service to the demarcation point; or (ii) other activities not covered under the Building Extension Service Service Schedule are required beyond the demarcation point, that cause CenturyLink to incur additional expenses for provisioning the Service ("Construction"). If Customer does not approve of the Construction charges after CenturyLink notifies Customer of the charges, the Service ordered will be deemed cancelled.

(c) Multiplexing. Customer may request multiplexing for Special Access where available. CenturyLink will multiplex lower level local loop into a higher local loop, or vice-versa, for an additional charge. CenturyLink offers multiplexing at a CPOP, at an On-Net Access building or at an ILEC/CLEC facility providing the Off-Net Access. For multiplexing at a CenturyLink On-Net Access building, CenturyLink provides multiplexed circuit handoffs to Customer at the same On-Net Access Service Address. For multiplexing at ILEC/CLEC facility, CenturyLink facilitates the delivery of multiplexed circuit handoffs to Customer at a single Service Address or at multiple Service Addresses per Customer's request. Multiplexing is generally available at DS1 and OCn circuit levels. Pricing for multiplexing at an ILEC/CLEC facility is on an individual case basis.

(d) Changes. Ancillary change charge applies where Customer requests CenturyLink to change a local loop to a different Service Address that is within the same Customer serving wire center as the existing local loop, but a Cancellation Charge does not apply.

5. Term; Cancellation.

5.1 Term. The term of an individual Service continues for the number of months specified in the attached pricing attachment for a particular Service Address or a quote or Order for Service issued by CenturyLink if the rates for Service at a particular Service Address are not included in the pricing attachment ("Service Term"). Excluding voice loops and Data Center Access with a month-to-month Service Term, the Service Term will not be less than 12 months. Service will continue month-to-month at the expiration of the Service Term at the existing rates, subject to adjustment by CenturyLink on 30 days' written notice.

5.2 Cancellation and Termination Charges.

(a) Customer may cancel an Order (or portion thereof) prior to the delivery of a Connection Notice upon written notice to CenturyLink identifying the affected Order and Service. If Customer does so, Customer will pay CenturyLink a cancellation charge equal to the sum of: (1) for Off-Net Access, third party termination charges for the cancelled Service; (2) for On-Net Access one month's monthly recurring charges for the cancelled Service; (3) the non-recurring charges for the cancelled Service; and (4) CenturyLink's out-of-pocket costs (if any) incurred in constructing facilities necessary for Service delivery.

(b) Customer may terminate a specified Service after the delivery of a Connection Notice upon 30 days' written notice to CenturyLink. If Customer does so, or if Service is terminated by CenturyLink as the result of Customer's default, Customer will pay CenturyLink a termination charge equal to the sum of: (1) all unpaid amounts for Service actually provided; (2) 100% of the remaining monthly recurring charges for months 1-12 of the Service Term; (3) 50% of the remaining monthly recurring charges for month 13 through the end of the Service Term; and (4) if not recovered by the foregoing, any termination liability payable to third parties resulting from the termination and any out-of-pocket costs of construction to the extent such construction was undertaken to provide Service hereunder. The charges in this Section represent CenturyLink's reasonable liquidated damages and are not a penalty.

(c) Customer Provided Access—Cancellation of Connectivity after Delivery of a Connection Notice. To cancel CPA, Customer must provide CenturyLink with a written disconnect firm order confirmation ("DFOC") notice from Customer's CPA provider along with notice to cancel the CPA. If Customer fails to provide CenturyLink with the DFOC notice within 30 calendar days after CenturyLink's receipt of the notice to cancel the CPA, or if CenturyLink disconnects CPA for Cause, then CenturyLink may disconnect the CPA or require the CPA provider to do so. Customer will remain liable for charges for the connectivity to CPA (even if Customer cannot use the CPA) until: (i) Customer furnishes the required DFOC to CenturyLink; or (ii) either party cancels the associated CPA with the CPA provider.

6. Provisioning, Maintenance and Repair. CenturyLink may re-provision any local access circuits from one off-net provider to another or to On-Net Access and such changes will be treated as scheduled maintenance. Scheduled maintenance will not normally result in Service interruption. If scheduled maintenance requires Service interruption CenturyLink will: (1) provide Customer seven days' prior written notice, (2) work with Customer to minimize interruptions and (3) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time. Customer may request a technician dispatch for Service problems. Before dispatching a technician, CenturyLink will notify Customer of the dispatch fee. CenturyLink will assess a dispatch fee if it determines the problem is on Customer's side of the demarcation point or was not caused by CenturyLink's facilities or equipment on CenturyLink's side of the demarcation point. If third-party local access services are required for the Services, Customer will: (4) provide CenturyLink with circuit facility and firm order commitment information and design layout records to enable cross-connects to CenturyLink Service(s) (provided by CenturyLink subject to applicable charges), (5) cooperate with CenturyLink (including changing demarcation points and/or equipment and providing necessary LOAs) regarding circuit grooming or re-provisioning, and (6) where a related Service is disconnected, provide CenturyLink a written DFOC from the relevant third-party provider.

7. Other Terms.

7.1 General. Any references to a Revenue Commitment or Contributory Charges will not apply to this Service Exhibit.

7.2. Cancellation and Termination Charges. This Section replaces the Cancellation and Termination Charges Section in the Agreement:

> **Termination.** Either party may terminate a specified Service: (a) as set forth above with 60 days' prior written notice to the other party, or (b) for Cause. Customer may cancel an Order (or portion thereof) for Service prior to the delivery of a Connection Notice upon written notice to CenturyLink identifying the affected Order and Service. If Customer does so, Customer will pay Centurylink the termination charges set forth above, in addition to any and all charges that are accrued but unpaid as of the termination date. If the Agreement is terminated by Customer for any reason other than for Cause, or by CenturyLink for Cause prior to the conclusion of the Term, all Services are deemed terminated, and Customer will pay the termination charges set forth above, in addition to any and all charges that are accrued but unpaid as of the termination date. "Cause" means the failure of a party to perform a material obligation under the Agreement, which failure is not remedied: (a) for payment defaults by Customer, within five days of separate written notice from CenturyLink of such default; or (b) for any other material breach, within 30 days after written notice (unless a shorter notice period is identified in a Service Attachment).

7.3 Out-of-Service Credit. For Services without a Service Level or applicable out-of-service credit for service interruption in a Tariff, this Out-of-Service Credit is the Service Level provision for purposes of the Agreement. Customer must request the Out-of-Service Credit and open a trouble ticket to report to CenturyLink the interruption of Service to CenturyLink. If CenturyLink causes Downtime, CenturyLink will give Customer a credit; such credit will be paid as a percentage of the Customer's MRC based on the ratio of the number of minutes of Downtime relative to the total number of minutes in the month when the Downtime occurred. No credits will be given where the Downtime is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its End Users; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink or its international service providers; (c) Force Majeure Events; (d) scheduled service maintenance, alteration or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) CenturyLink's termination of Service for Cause or Customer's violation of the Use of Service provisions in this Appendix or in the applicable Service Exhibit; or (i) improper or inaccurate network specifications provided by Customer. "Downtime" is an interruption of Service confirmed by CenturyLink that is measured from the time Customer opens a trouble ticket with CenturyLink to the time Service has been restored. "Cause" means the failure of a party to perform a material obligation under the Agreement, which failure is not remedied: (a) for payment defaults by Customer, within five days of separate written notice from CenturyLink of such default; or (b) for any other material breach, within 30 days after written notice.

7.4 Service Notices. Notices for disconnection of Service must be submitted to CenturyLink via Email at: BusinessDisconnects@Centurylink.com. Notices of non-renewal for Services must be sent via e-mail to: CenturyLink, Attn.: CenturyLink NoRenew, e-mail: Norenew@centurylink.com. Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at https://www.centurylink.com/business/login/ or via Email at: Care.Inquiry@Centurylink.com. All other routine operational notices will be provided by Customer to its CenturyLink sales representative.

7.5 Acceptable Use Policy and Use of Service. CenturyLink may also terminate Service for Cause under this Section where Customer's use of the Service: (a) is contrary to the Acceptable Use Policy incorporated by this reference and posted at http://www.centurylink.com/legal/, (b) constitutes an impermissible traffic aggregation or Access Arbitrage, (c) avoids Customer's obligation to pay for communication services, and (d) violates the Use of Service terms or compliance terms. Customer may have obligations under 47 CFR 9.5 relating to 911 if Customer combines the Service with other products creating a VoIP or VoIP-like service that facilitates the transmission of voice services.

7.6 CPNI. CenturyLink is required by law to treat CPNI confidentially. Customer agrees that CenturyLink may share CPNI within its business operations (e.g., wireless, local, long distance, and broadband services divisions), and with businesses acting on CenturyLink's behalf, to determine if Customer could benefit from the wide variety of CenturyLink products and services, and in its marketing and sales activities. Customer may withdraw its authorization at any time by informing CenturyLink in writing. Customer's decision regarding CenturyLink's use of CPNI will not affect the quality of service CenturyLink provides Customer. "CPNI" means Customer Proprietary Network Information, which includes confidential account, usage, and billing-related information about the quantity, technical configuration, type, destination, location, and amount of use of a customer's telecommunications services. CPNI reflects the telecommunications products, services, and features that a customer subscribes to and the usage of such services, including call detail information appearing in a bill. CPNI does not include a customer's name, address, or telephone number.

7.7 Conflicts. If a conflict exists among the provisions of the Service Attachments, the order of priority will be as follows: the Service Exhibit and then the Agreement.

7.8 Fees. Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit http://www.centurylink.com/taxes. Additional rates, charges and fees for Service elements not identified in the Agreement are located in the applicable Tariff. "Tariff" includes as applicable: CenturyLink state tariffs, price lists, price schedules, administrative guidelines, catalogs, and rate and term schedules incorporated by this reference and posted at http://www.centurylink.com/tariffs.

8. Definitions.

"CenturyLink Domestic Network" means the CenturyLink network located within the contiguous U.S., Alaska and Hawaii, which is comprised only of physical media, including switches, circuits, and ports that are operated by CenturyLink.

"CPOP" means a CenturyLink-owned physical point of presence that lies directly on the CenturyLink Domestic Network where direct interconnection between the CenturyLink Domestic Network and a local access provider's network is possible.

"Service Address" means the building where Customer receives Service. Only a building that is classified by CenturyLink as a business address can be a Service address.

CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK® LOCAL ACCESS SERVICE EXHIBIT

PRICING ATTACHMENT

Except as set forth in this pricing attachment, capitalized terms will have the definitions assigned to them in the Agreement or the Local Access Service Exhibit.

1. Customer will pay the MRCs and NRCs for Service at the particular Service Address; or NPA/NXX or CLLI if no Service Address is provided, set forth in the pricing table below. In addition, Customer will pay all MRCs or NRCs for any ancillary services provided as described in the Local Access Service Exhibit, including without limitation Construction charges. The MRCs and NRCs set forth below apply to new Service only and do not apply to Service ordered prior to the effective date of this pricing attachment. All MRCs and NRCs set forth in the below table apply per circuit and not per Service Address. Any modifications to any attribute of the particular Service in the pricing table below (i.e., the NPA/NXX or CLLI, Service Address, Type of Local Access, Service Term or circuit speed) will render the pricing below void, and Customer will pay the revised rates agreed upon by the parties for the particular Service at the Service Address or NPA/NXX or CLLI, as applicable. If a DS1 is bonded with one or more DS1s to create a higher speed NxDS1 at the same Service Address, the MRC for the DS1 may be multiplied by the number of bonded DS1s to determine the MRC for the NxDS1.Any future Service ordered will be charged the current quoted MRC and NRC per Service as specified on a valid CenturyLink quote or Order, not the MRC and NRC per Service specified below. No other discounts or promotions apply. Certain types of Service have separate service or agreement requirements as defined in the Local Access Service Exhibit.

For pricing, please refer to the RFP. This Pricing Attachment will be completed upon award.

CENTURYLINK ON-NET LOCAL ACCESS
SERVICE LEVEL AGREEMENT
(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This Service Level Agreement ("SLA") only applies to On-Net Access circuits ("Service") ordered by CenturyLink's customer ("Customer") pursuant to a signed agreement ("Agreement") with CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). On April 1, 2014, Qwest Communications Company, LLC completed a name change to CenturyLink Communications, LLC. References in supporting agreements or other documents, to Qwest Communications Company, LLC or its predecessors are replaced with "CenturyLink Communications, LLC." Service terminates at CenturyLink's Minimum Point of Entry (MPOE) as determined by CenturyLink.

1. Definitions

"Calendar Month" refers to the period beginning at 12:00 midnight on the first day of a month and ending at 11:59 PM on the last day of that month.

2. Availability Objective

CenturyLink offers the following SLA for Service with a minimum one-year Service term. The SLA is effective as of the first day of the second month after initial installation and Customer acceptance of Service.

Customer will, subject to the terms, exclusions, and restrictions described in this SLA, be entitled to receive from CenturyLink a credit if the availability of a particular circuit ("Circuit Availability") for any Calendar Month falls below the percentage shown in the applicable credit schedule included in this section. CenturyLink guarantees the Circuit Availability only to the point to which CenturyLink can perform remote loop back testing, even if the demarcation point extends past such point. Service will for purposes of this document be deemed to be unavailable to Customer only if the circuit ("Affected Circuit") is subject to an interruption (other than as noted in this SLA) that results in the total disruption of the Service ("Outage").

The credit ("Outage Credit") to which Customer may be entitled under this section will be equal to the applicable credit percentage identified in the table below of Customer's monthly recurring charges ("MRCs") for the Affected Circuit after application of any credits or discounts ("Eligible Circuit Charges"). The Outage Credit will not include credits on any other MRCs charged to Customer for any other service.

Circuit Availability Percentage is calculated as follows:

$$\left[\frac{(\text{Applicable Days in Calendar Month} \times 24 \times 60) - (\text{Minutes of Outage on Affected Circuit in Calendar Month})}{(\text{Applicable Days in Calendar Month} \times 24 \times 60)}\right] \times 100$$

For purposes of measuring Customer's Circuit Availability, the CenturyLink Trouble Management System determines the number of minutes of an Outage. An Outage will be deemed to commence upon verifiable notification thereof by Customer to the CenturyLink Trouble Management System, and CenturyLink's issuance of a trouble ticket. An Outage will conclude upon the restoration of the Affected Circuit as evidenced by the appropriate network tests conducted by CenturyLink.

Credit Schedule for Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.999%	0%
< 99.999%	99.99%	5%
< 99.99%	99.9%	10%
< 99.9%	99.5%	25%
< 99.5%	0%	50%

Subject to the terms, exclusions and restrictions described in this SLA, in the event Customer experiences chronic Outages with respect to any circuit, Customer will be entitled to terminate the Affected Circuit. A circuit suffers from chronic Outages if such circuit, measured over any Calendar Month, experiences more than five Outages, or more than 48 aggregate hours of Outages. Customer may as its sole and exclusive remedy for chronic Outages, upon 30 days' prior written notice to CenturyLink, terminate the Affected Circuit without incurring any termination charges associated with that Affected Circuit except for all usage charges accrued to the date of termination. Customer must exercise any termination right available to it under this section within 30 days after Customer first becomes eligible to exercise the termination right. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will, with respect to the termination right, have waived its right to such termination right.

3. Terms and Conditions

CenturyLink is offering Service in accordance with the applicable CenturyLink agreement. In the event of a conflict between the terms of this document and the Rate and Services Schedule or applicable CenturyLink agreement, the terms of this document will control.

To be eligible for an Outage Credit under this SLA, Customer must, in addition to complying with the other terms included in this SLA, (i) be in good standing with CenturyLink and current in their obligations, other than those invoices that are recognized as being in dispute, and (ii) submit necessary supporting documentation and request reimbursement or credits hereunder within 30 days of the Outage resolution. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will, with respect to that remedy, have waived its right to such remedy.

CenturyLink will determine the Outage Credits provided to Customer by totaling the eligible Outage minutes throughout the Calendar Month on an Affected Circuit, subject to the restrictions and exclusions in this SLA. Outage Credits for any Calendar Month must exceed $25.00 to be processed. In no case will CenturyLink provide credit to Customer for an Affected Circuit that exceeds the monthly recurring charge or the stated applicable maximum credit percentage. Customer may receive Outage Credits for a particular Affected Circuit for a maximum of four months in any 12-month period.

CenturyLink will give notice to Customer of any scheduled maintenance as early as is practicable and a scheduled outage will under no circumstances be viewed as an Outage hereunder.

The remedies included in this SLA are Customer's sole and exclusive remedies for disruption of Service and will apply in lieu of any other Service interruption guarantee or credit, outage guarantee or credit or performance credit for which Customer might have otherwise been eligible. If Customer receives an Outage Credit, Customer is not entitled to receive any other credit that may be available under the local access service provided or ordered by CenturyLink on behalf of Customer for the Affected Circuit in that Calendar Month.

Except as provided in this SLA, the objectives and related remedies set forth herein will not apply to CenturyLink services other than the Service.

4. Restrictions and Exclusions

An Outage will not be deemed to have occurred if the Service is unavailable or impaired due to any of the following:

(a) Interruptions on a circuit that is not an "Accepted Circuit" where an Accepted Circuit is one that CenturyLink and Customer have tested and mutually agree is working as ordered following provisioning of an order or change order;

(b) Interruptions caused by the negligence, error or omission of Customer or others authorized by Customer to use or modify Service;

(c) Interruptions due to failure of power at Customer premises or failure or poor performance of Customer's premises equipment;

(d) Interruptions during any period in which CenturyLink or its agents are not afforded access to the premises where Service is terminated, provided such access is reasonably necessary to prevent a degradation or to restore Service;

(e) Interruptions during any period when CenturyLink has posted on the CenturyLink Web site or communicated to Customer in any other manner that Customer's Service will be unavailable for maintenance or rearrangement purposes, or Customer has released Service to CenturyLink for the installation of a customer service order;

(f) Interruptions during any period when Customer elects not to release the circuit for testing and/or repair and continues to use it on an impaired basis;

(g) Interruptions resulting from force majeure events beyond the reasonable control of CenturyLink including, but not limited to, acts of God, government regulation, labor strikes, national emergency or war (declared or undeclared);

(h) Interruptions resulting from Customer's use of Service in an unauthorized or unlawful manner;

(i) Interruptions resulting from a CenturyLink disconnect for Customer's breach of a term set forth in the Agreement pursuant to which CenturyLink is providing Service to Customer;

(j) Interruptions resulting from incorrect, incomplete or inaccurate orders from Customer;

(k) Interruptions due to improper or inaccurate network specifications provided by Customer;

(l) Interruptions resulting from a failure of a carrier other than CenturyLink providing local access circuits; or

(m) Special configurations of the Service that have been mutually agreed to by CenturyLink and Customer; provided, however, CenturyLink may provide a separate service level agreement to Customer for those special configurations.

CENTURYLINK® DOMESTIC NETWORK DIVERSITY®
SERVICE EXHIBIT

1. General; Definitions. This Service Exhibit is applicable only where Customer orders Domestic Network Diversity (the "Service" or "Diversity") for underlying services in the continental United States and incorporates the terms of the Master Service Agreement or other service agreement and RSS, under which CenturyLink provides services to Customer (the "Agreement"). CenturyLink may subcontract any or all of the work to be performed under this Service Schedule. All capitalized terms that are used but not defined in this Service Exhibit are defined in the Agreement or Order. Customer may submit requests for Service in a form designated by CenturyLink ("Order").

"Card Diversity" means the secondary or diverse circuit that originates and/or terminates onto a separate card on the same device within the same CenturyLink POP as the primary circuit.

"CenturyLink Domestic Network" means the CenturyLink network located within the contiguous U.S., Alaska and Hawaii, which is comprised only of physical media, switches, including switches, circuits, and ports that are operated by CenturyLink.

"Dedicated IP Access" means a special access local loop connection, from the Customer premises to an IP POP ("POP").

"Device Diversity" means the secondary or diverse circuit that originates and/or terminates in a separate aggregation device (such as routers, switches) within the same IP POP as the primary service.

"ELA" or "Ethernet Local Access" means CenturyLink Provided Access using Ethernet over SONET technology and is available at bandwidths varying from 1 Mbps to 1,000 Mbps (1Gbps).

"IP POP" is a CenturyLink POP where IP edge routers are located on the CenturyLink Domestic Network and IQ Networking Service is available.

"IP POP Diversity" means the diverse circuit that originates and/or terminates in a physically separate IP POP from the primary circuit.
"CenturyLink POP" means a point of presence ("POP") on the CenturyLink Domestic Network.

"Pricing Attachment" means a document containing rates specific to the Service and is incorporated by reference and made a part of this Service Exhibit.

"Single Circuit Diversity" unless otherwise stated in this Service Exhibit, means an individual circuit on the CenturyLink Domestic Network that either: (a) is routed to, or; (b) avoids a specified geographic location along the circuit's path between the originating and terminating CenturyLink transport POP buildings, subject to availability.

"SLA" means the service level agreement specific to the Service, located at http://www.centurylink.com/legal/, which is subject to change.

"Special Access" means CenturyLink Provided Access using Digital Signal speeds DS-0, DS-1, and DS-3 or Optical Carrier signal speeds OC-3, OC-12, OC-48, and OC-192.

"Switch Diversity" means the secondary or diverse circuit that originates and/or terminates in a separate CenturyLink switch from the primary circuit. Depending on available network facilities, the circuits may originate and/or terminate at the same or different CenturyLink POP.

"Transport Diversity" means two or more diversely related circuits that are independently routed on the CenturyLink Domestic Network transport systems between the originating and terminating CenturyLink POP buildings, subject to availability. At Customer's request and subject to availability, CenturyLink will provision diversely related Underlying Services from different CenturyLink POP buildings in the originating and/or terminating cities. In some instances, the diverse circuit may share common network facilities, infrastructure, and/or buildings with the primary circuit.

"Underlying Service" means an approved CenturyLink service offering on the CenturyLink Domestic Network that also supports Diversity.

"Wavelength Local Access" means CenturyLink Provided Access using wave division multiplexing technology at bandwidths of 1 GbE, 10 GbE LAN PHY, 2.5 G (OC48), 10 GbE WAN PHY (OC192), 40G, OTU1, OTU2, OTU3, 1G, 2G, 4G and 10G.

2. Service.

2.1 Description. Diversity is an enhanced routing option that routes an Underlying Service according to either: (a) a Customer-defined routing between two or more diversely related circuit(s); or (b) a predefined path that either routes to or avoids a specified geographic location on the circuit path ("Single Circuit Diversity") according to Customer's requirements, unless otherwise noted below; and (c) identifies and maintains the diversely routed circuit(s) in the CenturyLink provisioning systems, until the Service is cancelled. Diversity does not provide switching and/or routing of Customer's digital transmissions between primary and diversely routed circuits in the event of a failure on any one circuit or port. CenturyLink only offers protection switching, if any, inherent with the Underlying Services. The Diversity options described in this Service Exhibit are subject to availability and technical feasibility. The SLA is effective as of the first day of the second month after initial installation of Service. The SLA provides Customer's sole and exclusive remedy for service interruptions or service deficiencies of any kind whatsoever for the Service. CenturyLink's Underlying Services include: Domestic Private Line Service, EPL, Optical Wavelength, IQ Networking Service (including Internet Ports and Private Ports), ATM Service, Frame Relay Service, Dedicated Domestic Outbound/Inbound Long Distance Service ("Long Distance"), and related Local Access Service. The Underlying Services will, except to the extent modified in this Service Exhibit, be offered pursuant to the terms and conditions of the Agreement, Service Exhibits, and/or RSS applicable to the Underlying Services.

2.2 Diversity Configurations. Diversity configurations vary based on the Underlying Service. See below for options, subject to available network facilities.

(a) Domestic Private Line Diversity Service. Domestic Private Line Diversity Service is offered at circuit speeds of DS-1, DS-3, OC-3, OC-12, and OC-48. CenturyLink does not offer DS-0 and Fractional DS-1 Domestic Private Line Diversity Services. CenturyLink's routing of the diverse Domestic Private Line circuit(s) is based on the route of the designated working path of the circuit(s). Domestic Private Line Diversity Service is offered in the following configurations, but not in combination: Single Circuit Diversity or Transport Diversity. In some instances, the diverse circuit may share common network facilities, infrastructure, and/or buildings with the primary circuit.

(b) EPL Diversity Service. EPL Diversity Service is offered at circuit speeds of 50 Mbps, 100 Mbps, 150 Mbps, 500 Mbps, 600 Mbps, and 1000 Mbps. CenturyLink's routing of the diverse EPL circuit(s) is based on the route of the designated working path of the circuit(s). EPL Diversity Service is offered in the following configurations, but not in combination: Single Circuit Diversity or Transport Diversity.

(c) Optical Wavelength Diversity Service. Optical Wavelength Diversity Service is offered as an unprotected point-to-point transmission path between an originating and terminating CenturyLink POP at circuit speeds of 1 GbE, 2.5 Gbps and 10 Gbps. Optical Wavelength Diversity Service is offered in the following configurations, but not in combination: Single Circuit Diversity or Transport Diversity.

(d) IQ Networking Diversity Service. IQ Networking is offered at circuit speeds of DS-1, IMA (2xDS-1 up to 8xDS-1s), DS-3, OC-3, OC-12, and OC-48 transmission rates. DS-1s within an Nx bundle must all connect to the same POP. IQ Networking Diversity Service is offered in the following configurations but not in combination: IP POP Diversity, Device Diversity, Card Diversity, or Single Circuit Diversity. IQ Networking Single Circuit Diversity on the CenturyLink Domestic Network means a circuit that is routed to a specified IP POP. The secondary or diverse circuit cannot be used to load-balance Customer's traffic. The secondary or diverse circuit may share common network facilities, infrastructure, and/or buildings with the primary circuit.

(e) ATM/Frame Relay Diversity Service. ATM Diversity Service is offered at circuit speeds of DS-1, IMA (2xDS-1 up to 8xDS-1s), DS-3, OC-3, and OC-12 and Frame Relay Diversity Service is offered at circuit speeds of DS-1 and DS-3. DS-1s within an Nx bundle must all connect to the same POP. ATM/Frame Relay Diversity is offered in the following configurations, but not in combination: POP Diversity, Switch Diversity, Card Diversity, or Single Circuit Diversity. The diverse circuit may share common network facilities, infrastructure, and/or buildings with the primary circuit.

(f) Long Distance Diversity Service. Long Distance Diversity Service is offered at circuit speeds of DS-1, DS-3, OC-3, OC-12, and OC-48. The diverse circuit may share common network facilities, infrastructure, and/or buildings with the primary circuit. Long Distance Diversity Service is offered in the following configurations, but not in combination: Single Circuit Diversity, Switch Diversity, or Card Diversity. Long Distance Single Circuit Diversity on the CenturyLink Domestic Network means a circuit that is routed to a specified CenturyLink voice switch.

(g) Local Access Diversity Service. Local Access Diversity Service is an enhancement to Local Access that: (a) routes circuits based on Customer's reasonable routing requirements; and (b) identifies and maintains the Local Access circuits as diversely routed circuits in the CenturyLink provisioning systems. Local Access Diversity Service is offered with: (c) Special Access at circuit speeds of DS-1, 2xDS-1 up to 8xDS-1*, DS-3, OC-3, OC-12, and OC-48; (d) ELA at bandwidths varying from 1 Mbps to 1000 Mbps (1Gbps); or (e) Wavelength Local Access at 1 Gbps, 2.5 Gbps and 10 Gbps and may include CenturyLink ordering circuits utilizing alternate Central Offices or alternate Serving Wire Centers. DS-1s within an Nx bundle must all connect to the same POP. CenturyLink does not have direct control of the routing, installation, maintenance, performance, etc. of the third party local access facilities ordered on behalf of the Customer.

2.3 Ordering of Diversity Services. CenturyLink will notify Customer of acceptance of requested Service in the Order by delivering the date by which CenturyLink will install Service (the "Customer Commit Date"). CenturyLink will use commercially reasonable efforts to install each Service on or before the Customer Commit Date, but the inability of CenturyLink to deliver Service by that date will not be a default under the Agreement.

2.4 Service Conditions.

(a) CenturyLink will not provide special construction as part of the Service. Any requests for special construction are handled on an individual case basis.

(b) Customer understands and agrees that CenturyLink has no visibility into the location of fiber strands, conduits, and other network facilities of other carriers and that CenturyLink will not attempt to identify and/or manage other carrier's facilities as part of the Service. Furthermore, Customer understands and agrees that CenturyLink may rearrange (groom) Customer's circuits in accordance with standard CenturyLink network maintenance activities. If a CenturyLink-initiated network rearrangement removes the Customer's diversity, then CenturyLink will notify Customer to determine alternative Diversity solutions, if any.

(c) Customer may experience increased latency on diversely routed circuit(s) due to increased actual routing mileage.

(d) Single Diverse Circuit Additional Mileage Charges. If CenturyLink, in its sole discretion, determines that Customer's specified geographic routing criteria on a Single Circuit Diversity request results in excessive additional mileage, CenturyLink may charge Customer actual mileage charges on the Underlying Service.

(e) Customer acknowledges that diverse circuits must have traffic on them for CenturyLink to monitor connectivity.

3. Term. The term of this Service Exhibit will begin on the Effective Date of the Agreement (or, if applicable, an amendment to the Agreement if Customer adds this Service Exhibit after the Effective Date of the Agreement) and will continue until the termination of the last Service ordered under this Service Exhibit. Service will automatically terminate on the termination of the Underlying Service.

4. Charges. Customer will pay all Diversity charges set forth in a valid quote, Order Form or Pricing Attachment, in addition to the charges for the Underlying Services. If backhaul routing is required to complete Customer's Diversity order for IQ Networking (including Internet Ports and Private Ports), ATM Service, Frame Relay Service, or Long Distance, Customer will pay the backhaul charges for each diversely routed circuit. CenturyLink will deliver written or electronic notice (a "Connection Notice") to Customer when Service is installed, at which time billing will commence ("Service Commencement Date"). The Service is not entitled to the CTA Discount. Additional rates, charges and fees for Service elements not identified in the Agreement are located in the applicable Tariff. "Tariff" includes as applicable: CenturyLink state tariffs, price lists, price schedules, administrative guidelines, catalogs, and rate and term schedules incorporated by this reference and posted at http://www.centurylink.com/tariffs.

5. Other Terms.

5.1 General. Any references to a Revenue Commitment or Contributory Charges will not apply to this Service Exhibit.

5.2. Cancellation and Termination Charges. This Section replaces the Cancellation and Termination Charges Section in the Agreement:

(a) Cancellation. Customer may cancel an Order (or portion thereof) prior to the delivery of a Connection Notice upon written notice to CenturyLink identifying the affected Order and Service. Cancellation of an Order for Diversity will also cancel the Order for the Underlying Service and any cancellation charges for the Underlying Service will apply.

(b) Termination. Either party may terminate Diversity (i) after the delivery of a Connection Notice upon 60 days' prior written notice to the other party, or (ii) for Cause. If Customer terminates Diversity for any reason other than for Cause, or if Diversity is terminated by CenturyLink for Cause, Customer will also terminate the Underlying Service and Customer will pay CenturyLink the termination charge for the Underlying Service in addition to any charges for Diversity incurred but unpaid through the effective date of the termination. "Cause" means the failure of a party to perform a material obligation under the Agreement, which failure is not remedied: (a) for payment defaults by Customer, within five days of separate written notice from CenturyLink of such default; or (b) for any other material breach, within 30 days after written notice (unless a shorter notice period is identified in a Service Attachment). The charges in this Section represent CenturyLink's reasonable liquidated damages and are not a penalty.

(c) If the Agreement is terminated by Customer for any reason other than for Cause, or by CenturyLink for Cause prior to the conclusion of the Term, all Services are deemed terminated, and Customer will pay the applicable termination charges for all Services, in addition to any and all charges that are accrued but unpaid as of the termination date.

5.3 Installation, Maintenance and Repair. The following are supplemental terms to the Scheduled Maintenance and Local Access section of the Agreement: (a) Provision of Services is subject to availability of adequate capacity and CenturyLink's acceptance of a complete Order Form and (b) Customer is responsible for any facility or equipment repairs on Customer's side of the demarcation point. Customer may request a technician dispatch for Service problems. Before dispatching a technician, CenturyLink will notify Customer of the dispatch fee. CenturyLink will assess a dispatch fee if it determines the problem is on Customer's side of the demarcation point or was not caused by CenturyLink's facilities or equipment on CenturyLink's side of the demarcation point. "Order Form" includes both order request forms and quotes issued by CenturyLink. If a CenturyLink service requires a quote to validate the Order Form pricing, the quote will take precedence over the order request form, but not over the Service Exhibit.

5.4 Service Notices. Notices for disconnection of Service must be submitted to CenturyLink via Email at: BusinessDisconnects@Centurylink.com. Notices of non-renewal for Services must be sent via e-mail to: CenturyLink, Attn.: CenturyLink NoRenew, e-mail: Norenew@centurylink.com. Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at https://www.centurylink.com/business/login/ or via Email at: Care.Inquiry@Centurylink.com. All other routine operational notices will be provided by Customer to its CenturyLink sales representative.

5.5 Acceptable Use Policy and Use of Service. CenturyLink may also terminate Service for Cause under this Section where Customer's use of the Service: (a) is contrary to the Acceptable Use Policy incorporated by this reference and posted at http://www.centurylink.com/legal/, (b) constitutes an impermissible traffic aggregation or Access Arbitrage, (c) avoids Customer's obligation to pay for communication services, and (d) violates the Use of Service terms or compliance terms.

5.6 CPNI. CenturyLink is required by law to treat CPNI confidentially. Customer agrees that CenturyLink may share CPNI within its business operations (e.g., wireless, local, long distance, and broadband services divisions), and with businesses acting on CenturyLink's behalf, to determine if Customer could benefit from the wide variety of CenturyLink products and services, and in its marketing and sales activities. Customer may withdraw its authorization at any time by informing CenturyLink in writing. Customer's decision regarding CenturyLink's use of CPNI will not affect the quality of service CenturyLink provides Customer. "CPNI" means Customer Proprietary Network Information, which includes confidential account, usage, and billing-related information about the quantity, technical configuration, type, destination, location, and amount of use of a customer's telecommunications services. CPNI reflects the telecommunications products, services, and features that a customer subscribes to and the usage of such services,

including call detail information appearing in a bill. CPNI does not include a customer's name, address, or telephone number.

5.7 Conflicts. If a conflict exists among the provisions of the Service Attachments, the order of priority will be as follows: the Service Exhibit, the RSS or ISS, the general terms of the Agreement, SLA, SOW (if any) and Order Form, as applicable, and then any other documents attached or expressly incorporated into the Agreement. "ISS" means CenturyLink's Information Services Schedule incorporated by this reference and posted at: http://www.centurylink.com/tariffs/clc_info_services.pdf ."RSS" means as applicable: CenturyLink's Rates and Services Schedules incorporated by this reference and posted at http://www.centurylink.com/tariffs/fcc_clc_ixc_rss_no_2.pdf for CenturyLink's International RSS and at http://www.centurylink.com/tariffs/fcc_clc_ixc_rss_no_3.pdf for CenturyLink's Interstate RSS. "Tariff" includes as applicable: CenturyLink state tariffs, price lists, price schedules, administrative guidelines, catalogs, and rate and term schedules incorporated by this reference and posted at http://www.centurylink.com/tariffs.

5.8 Fees. Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate.

DOMESTIC NETWORK DIVERSITY SERVICES PRICING ATTACHMENT

This Domestic Network Diversity Service Pricing Attachment ("Pricing Attachment") is appended to, and subject in all respects to, the CenturyLink® Master Service Agreement between CenturyLink Communications, LLC and Customer ("Agreement") and the Domestic Network Diversity ("Diversity") Service Exhibit to which this is attached. Except as set forth in this Pricing Attachment, capitalized terms will have the definitions assigned to them in the Agreement or the Domestic Network Diversity Service Exhibit.

Pricing in this Pricing Attachment is for Diversity-related charges only. The Agreement, Service Exhibit, and/or Services Schedule contain the pricing and terms for the Underlying Service(s).

RATES AND CHARGES

1. Rates and Charges - The following rates and charges apply to Domestic Network Diversity Service based on the Underlying Service's circuit speed.

Diversity Enhancement Monthly Recurring Charges – Customer will pay only one Diversity Enhancement MRC per end to end circuit (that is with or without diversity on the CenturyLink ordered local access).

For pricing, please refer to the RFP. This Pricing Attachment (tables below) will be completed upon award.

1. CenturyLink IQ Networking Diversity Service Rates

Check the applicable elements of Diversity Service ordered.

☒ IP POP Diversity ☐ Device (Router) Diversity
☐ Card Diversity ☐ Single Circuit Diversity

Location: Address and NPA/NXX	Circuit Type	Circuit ID (if available)	Diversity Enhancement MRC	Backhaul MRC	Other Related Local Access Diversity Charges

2. Local Access Diversity Service Rates

A Location: Address and NPA/NXX	Z Location: Address and NPA/NXX	Circuit Type	Circuit ID (if available)	Diversity Enhancement MRC	A Location: Other Related Local Access Diversity Charges	Z Location: Other Related Local Access Diversity Charges

CENTURYLINK DOMESTIC NETWORK DIVERSITY
SERVICE LEVEL AGREEMENT
(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

1. Service Level Agreement. This Service Level Agreement ("SLA") applies to Domestic Network Diversity Service ("Diversity" or "Service") ordered by CenturyLink's customer ("Customer") pursuant to a signed agreement ("Agreement") with Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). Capitalized terms not defined in this SLA are defined in the Agreement.applies to the Diversity enhancement only. This SLA applies to the Diversity enhancement only. For purposes of this SLA, the CenturyLink Trouble Management System will be the sole source to determine the Customer's Diversity Availability. Unavailability will be deemed to commence upon verifiable notification thereof by Customer to the CenturyLink Trouble Management System, CenturyLink's issuance of a trouble ticket and verification by the CenturyLink Trouble Management System of Unavailability. Unavailability will conclude upon the restoration of the Service as evidenced by CenturyLink.

2 Service Availability. Customer will, subject to the terms, exclusions, and restrictions described herein, be entitled to receive from CenturyLink a credit if the Diversity for Domestic Private Line Service, Optical Wavelength Service Service, PRN Service, CenturyLink IQ™ Networking Service, ATM Service, Frame Relay Service, or Long Distance is unavailable as a result of CenturyLink's failure to maintain the desired Diversity routing on the CenturyLink Domestic Network, based upon the Diversity routing confirmed by CenturyLink at the time of ordering ("Unavailability"). The credit to which Customer may be entitled under this Section will be equal to 100% of the Diversity enhancement MRC for each of the affected circuits for the calendar month in which Diversity was Unavailable.

3 Network Rearrangements. In the event CenturyLink will perform a network rearrangement that materially affects Customer's Service such that the Diversity routing is terminated, then CenturyLink will provide prior notice in a commercially reasonable timeframe to Customer of an alternative Diverse routing of the affected circuit(s). Customer's existing charges of the Diversity enhancement and Underlying Service will not change as a result of Customer's acceptance of the alternative Diversity routing. Customer acceptance of alternative diverse routing will not be unreasonably withheld. Should Customer not accept the proposed alternative Diversity rerouting, Customer may as its sole and exclusive remedy, terminate the affected Service along with the affected Underlying Services without incurring cancellation charges for the Underlying Service, provided however, that Customer will be liable for any cancellation charges for circuits requiring special construction, third party cancellation charges, and Leased Local Access cancellation charges, if any, as more particularly set forth in the applicable Services Exhibit and/or Services Schedule for the Underlying Services.

4 Terms and Condition for the SLA.

4.1 To be eligible for a credit under this SLA, Customer must, in addition to complying with the other terms included herein: (a) be in good standing with CenturyLink and current in its obligations, other than those invoices that are recognized as being in dispute; and (b) submit necessary supporting documentation (if applicable) and request reimbursement or credit hereunder within 30 days of the conclusion of the service month in which the requisite Unavailability occurs. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will have waived such right.

4.2 Customer must exercise any termination right available to it under this SLA within 30 calendar days after Customer first becomes eligible to exercise the termination right. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will have waived such right.

4.3 The credit will not include credits on any other MRCs charged to Customer for any other Service including the Underlying Services. In no circumstance will Customer receive a credit that exceeds 100% of the Diversity enhancement MRC. Outages of the Underlying Services are governed by the service level agreement for such Underlying Service and CenturyLink will not provide a credit under this Service Level Agreement for failures of Diversity caused by outages.

CENTURYLINK® MASTER SERVICE AGREEMENT
CENTURYLINK® SELECT ADVANTAGE® SERVICE EXHIBIT

1. General; Definitions. This Service Exhibit for Products and Services (collectively "Solutions") is attached to and subject in all respects to the CenturyLink Master Service Agreement, CenturyLink Total Advantage, or CenturyLink Loyal Advantage Agreement between CenturyLink QCC and Customer. Capitalized terms not defined herein are defined in the Agreement. CenturyLink QCC will provide Solutions under the terms of the Agreement, the Service Exhibit, the Purchase Order and/or SOW. This Service Exhibit may not be used for the purchase of voice, data or IP services. In the event of a conflict in any term of any documents that govern the provision of Solutions hereunder, the following order of precedence will apply in descending order of control: any SOW, any Detailed Description(s), this Service Exhibit, the Agreement, and any PO. With respect to the Agreement, "Service" is replaced by "Solution" as defined herein, and "Order Form" is replaced with "Purchase Order" as defined herein.

"Change Order" means any change, submitted by Customer to CenturyLink or CenturyLink to Customer, to a SOW that was previously agreed upon by CenturyLink and Customer. Customer will be responsible for all charges related to such SOW Change Order.

"CPE" means either: (a) Customer Purchased Equipment, or (b) Customer Premises Equipment; and consists of hardware, software and materials used in the transport and/or termination/storage of data and voice transmission.

"Detailed Description(s)" means the terms and conditions of the Solution provided by CenturyLink which are posted at http://www.centurylinkselectadvantage.com/.

"Products" means CPE and Software offerings from CenturyLink.

"Purchase Order" or "PO" means either (a) a written document issued by Customer for the procurement of Solutions from CenturyLink; or (b) a CenturyLink quote or service order signed by Customer.

"Services" means offerings from CenturyLink that (a) install, maintain or manage CPE; (b) support Customer network management objectives, or (c) are consulting, professional, technical, development, and/or design services.

"Software" means software license offerings.

"SOW" means a statement of work that provides specific details, agreed to by CenturyLink and Customer, relating to the Solution purchased under a PO or the SOW. Agreement on the terms of the SOW will be satisfied by CenturyLink sending the final version of the SOW to Customer; and Customer's signature on the SOW.

2. CenturyLink Select Advantage Solutions.

2.1 Purchase. Customer may purchase Solutions by issuing a PO to CenturyLink, or executing an SOW. Customer's purchase of Solutions is subject to and controlled by Detailed Description(s) which are posted at http://www.centurylinkselectadvantage.com/ and are incorporated by this reference. Customer must register to create a username and password the first time the Web site is accessed to view these Detailed Descriptions. By issuing a PO or executing an SOW with CenturyLink, Customer warrants that Customer has read and agrees to the terms and conditions of the Detailed Description(s). CenturyLink reserves the right to amend the Detailed Description(s) effective upon posting to the Web site. Customer's continued use of the Solution constitutes acceptance of those changes. If a PO issued by Customer contains any preprinted terms, those terms will not amend, modify or supplement this Service Exhibit in any way whatsoever, notwithstanding any provisions in a PO to the contrary. Any PO or SOW must (a) reference and incorporate this Service Exhibit and its Effective Date, (b) contain the Customer's exact legal name, and (c) include any other requirements as may be further described in the Detailed Description(s).

2.2 Limitation of Liability. IN ADDITION TO THE LIMITATION OF LIABILITY UNDER THE AGREEMENT, CENTURYLINK'S TOTAL AGGREGATE LIABILITY ARISING FROM OR RELATED TO SOLUTIONS PURCHASED UNDER THIS SERVICE EXHIBIT, UNLESS OTHERWISE STATED IN THE DETAILED DESCRIPTIONS OR SOW, WILL IN NO EVENT EXCEED: (A) FOR CLAIMS ARISING OUT OF PRODUCTS, THE AMOUNT OF THE PRODUCT SET FORTH IN THE PO RELATING SOLELY TO THE AFFECTED PRODUCT; AND (B) FOR CLAIMS ARISING OUT OF NONRECURRING SERVICES, THE AMOUNT OF THE SERVICE SET FORTH IN THE PO OR SOW.

2.3 Additional Indemnification. CUSTOMER WILL DEFEND AND INDEMNIFY CENTURYLINK, ITS AFFILIATES, AGENTS AND CONTRACTORS FROM ALL THIRD PARTY CLAIMS, LIABILITIES, FINES, PENALTIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, ARISING FROM OR RELATED TO CUSTOMER'S, CUSTOMER'S END USER'S OR CUSTOMER'S THIRD PARTY PROVIDER'S ACTS, OMISSIONS (INCLUDING THE FAILURE TO PURCHASE OR IMPLEMENT FEATURES THAT ENABLE THE RECEIPT AND TRANSMISSION OF DIRECT-DIAL "911" CALLS OR MULTI-LINE TELEPHONE SYSTEM NOTIFICATIONS), OR FAILURES OF CONNECTIVITY THAT IMPEDE, PREVENT OR OTHERWISE MAKE INOPERABLE THE ABILITY OF CUSTOMER OR ITS END USERS TO DIRECTLY DIAL "911" OR TO RECEIVE OR TRANSMIT MULTI-LINE TELEPHONE SYSTEM NOTIFICATIONS, AS REQUIRED BY LAW, IN THE UNITED STATES.

3. Term; Termination. This Service Exhibit will commence on the Effective Date of the Agreement (or, if applicable, an amendment to the Agreement if this Service Exhibit is added to the Agreement after its Effective Date), and will remain in effect until canceled by either party upon 30 days prior written notice to the other party, or as otherwise stated in the SOW. If Service is terminated for any reason other than Cause, Service may be subject to Termination Charges as set forth in the Detailed Descriptions or SOW. Termination will not affect obligations under Purchase Orders accepted prior to the effective date of termination, and this Service Exhibit will remain in effect as to such obligations in the event it would otherwise have terminated.

4. Charges. Charges for Solutions will be specified in each PO or SOW and are due and payable upon Customer's receipt of the invoice or as otherwise stated in the PO or SOW. Any payment not received within 30 days after the invoice date may be subject to interest charges as permitted by applicable law. Customer will not be eligible for any discounts or promotional offers other than those specifically set forth in an executed PO.

OMR #R085547

CENTURYLINK MASTER SERVICE AGREEMENT
PUBLIC SAFETY VERSION
NEXT GENERATION 9-1-1 SERVICE SCHEDULE

CenturyLink Communications, LLC ("CenturyLink") will provide, and Customer will purchase, the CenturyLink Next Generation ("NG") 9-1-1 service ("Service" or "NG 9-1-1 Service") provided under this Service Schedule and the applicable Statement of Work ("SOW).

1. Services.

1.1 Service provided by CenturyLink, through its subcontractor Synergem, to Customer enables the routing of 9-1-1 dialed calls to a Customer–designated Public Safety Answering Point ("PSAP") over an Internet Protocol ("IP") network. Service is provided as described in this Service Schedule and in a Statement of Work ("SOW"), if applicable. The number "9-1-1" is intended as a universal emergency telephone number that provides the public direct access to a PSAP. A PSAP is an agency authorized to receive and respond to emergency calls. One or more PSAPs may be required for any given municipality or metropolitan area. PSAPs are designated by the Customer and specified in the SOW. Service includes components necessary for the answering, transferring, and forced disconnect of emergency 9-1-1 calls originated by persons within the servicing area(s). Service does not include Customer's telecommunications equipment. Customer will provide telecommunications equipment with a capacity adequate to handle the number of incoming 9-1-1 calls recommended by CenturyLink to be installed. It is Customer's responsibility to ensure that the telecommunications equipment is compatible with the Service furnished under this Service Schedule. CenturyLink does not answer and forward 9-1-1 calls, but furnishes the use of its facilities to enable the Customer's NG 9-1-1 and/or 9-1-1 personnel to respond to such calls. PSAP information, service locations, and addresses are set forth in the SOW. Customer may purchase additional Services by executing a subsequent SOW, which will be coterminous with the prior SOW.

1.2 Service provided under this Service Schedule does not include IP transport. Customer understands (a) that Service requires IP transport between certain points in Customer's 9-1-1 network to deliver the Automatic Location Identification ("ALI") or the Geographic Information Systems ("GIS") data to the PSAP, (b) that the IP transport provided by Customer must meet the requirements for this Service, (c) that Customer's access to this Service may be impacted by the terms and conditions imposed by Customer's provider of its IP transport, and (d) that IP transport may create access limitations to 9-1-1 emergency services differently than access limitations of traditional E9-1-1 transport and may limit Customerits access to the Service provided under this Service Schedule.

1.3 Service provided under this Service Schedule does not include Data Transport. Customer acknowledges and understands that any new or existing Data Transport used in conjunction with this Service is subject to the terms of a separate agreement. "Data Transport" means the circuits used to deliver the ALI or GIS data to the PSAP.

1.4 Service does not include facilities provided by Independent Providers. CenturyLink will provide Service up to the Standard Network Interface ("SNI") for each of the service locations at Customer's location(s). The SNI is that location where CenturyLink's facilities end and Customer's inside wire or network begins. "Independent Providers" means telephone companies, Incumbent Local Exchange Carriers ("ILECS"), Competitive Local Exchange Carriers ("CLECS"), or other communications service providers, (i.e., wireless carriers and/or interconnected VoIP providers).

1.5 Customer will use the NG 9-1-1 Service only for receiving and responding to requests for emergency assistance. Customer will be responsible for ensuring that each PSAP will also use the NG 9-1-1 Service in accordance with this Service Schedule and applicable SOW. Any other use of the database will result in immediate termination of Service.

1.6 CENTURYLINK ACCEPTS NO RESPONSIBILITY FOR OBTAINING OR FOR THE ACCURACY OF SUBSCRIBER, STATION, OR END-USER RECORD INFORMATION RECEIVED FROM INDEPENDENT PROVIDERS OR PRIVATE TELECOMMUNICATIONS SYSTEMS, SUCH AS PBX OR SHARED TENANT SERVICES.

1.7 Database. As applicable, the following will apply to Services:
(a) MSAG. Customer will provide an MSAG to CenturyLink for use in the database preparation. The MSAG must follow the NENA recommended United States Postal Service street name and directional addressing standard. Customer will ensure that each participating telephone service provider's records are sent electronically in the NENA format for database updates as specified by CenturyLink. CenturyLink will not deliver Service until each participating telephone service provider's records for Customer's service area match the applicable Master Street Address Guide with an accuracy rate of at least 98%. Customer is fully responsible for correcting all erroneous records and achieving such rate. "MSAG" means Master Street Address Guide. "NENA" means National Emergency Number Association.

(b) GIS Data. Customer will provide an the applicable PSAP boundaries to CenturyLink for use in the database preparation. The GIS provider will create and maintain all GIS data used by CenturyLink's routing and location functions and will provide the infrastructure or service necessary to ensure the GIS data remains current and timely resolve data errors. The GIS provider will also upload GIS data to CenturyLink's NENA compliant spatial interface ("SI"). CenturyLink's SI will validate and trigger a quality control process concerning the GIS updates. CenturyLink and the GIS data provider will establish the applicable quality control thresholds and such thresholds will satisfy NENA standards. CenturyLink's SI solution will block data updates published to CenturyLink's routing and location functions when quality control thresholds are exceeded. The GIS data provider will resolve all errors and any underlying discrepancy in the GIS data and thereafter submit the corrected GIS data to CenturyLink's SI. CenturyLink disclaims all responsibility and liability for incorrect routing of requests for emergency services due to incorrect or missing GIA data accompanying the request, due to incorrect GIS database entries provided by the underlying GIS data provider or authoritative service, as well as alternate routing needed due to PSAP conditions, network outages or other factors outside of CenturyLink's control.

1.8 Customer must promptly notify CenturyLink if the Service is not functioning properly. Some elements of the Service are inspected and/or monitored for performance as part of the routine maintenance of CenturyLink's network and on a routine basis, to discover errors, defects and malfunctions that might affect the Service. Such activities will not be interpreted, construed, or regarded, either expressly or impliedly as a warranty, service commitment or creating any CenturyLink obligation, nor do such activities relieve Customer of its responsibilities under this Service Schedule. Customer understands and acknowledges that such activities by CenturyLink may not detect all errors that may occur. Service related issues may arise that impact and delay or prevent call delivery. Service related issues may occur which the system will not recognize and will therefore not cause an automatic rerouting of calls to an alternate destination. Customer authorizes CenturyLink to manually implement an alternate call route as required.

2. Service Term. The term of this Service Schedule is 60 months (the Service Term"). Customer and CenturyLink agree to begin discussions regarding the renewal or discontinuation of Service 90 days before expiration of the Service Term. Renewals will require a new Service Term. If the parties do not reach agreement by the expiration of the Service Term, Service will continue on a month-to-month basis under the terms of this Service Schedule and applicable SOW and will convert to the then-current month-to-month rates as evidenced by CenturyLink's records). CenturyLink will inform Customer of its then-current rates for Service upon written request. If Service is continued on a month-to month basis, either party may terminate Service with 30 days' prior written notice to the other party.

3. Cancellation and Termination Charges. Either party may terminate Service and/or this Service Schedule with 30 days' written. Customer will remain liable for charges accrued but unpaid as of the termination date. Customer will also be liable for a termination charge calculated as follows: (i) an amount equal to the monthly recurring charge ("MRC") for terminated Services, multiplied by the number of months (complete or partial) remaining in the Service Term, (ii) the total amount of any and all waived installation or other non-recurring charges ("NRCs") associated with the Service, (iii) any NRC termination charges imposed CenturyLink by Independent Providers, and (iv) any credits for Services received by Customer.

4. Charges and Payment.

4.1 CenturyLink will notify Customer when Service is available for use or the date Service is available for use (the "Connection Notice"). Billing charges will commence within 30 business days from such date. Customer will pay the rates for the Service as set forth in the SOW. CenturyLink reserves the right to revise rates if a change in the statutes or administrative rules affects the cost of providing Service.

5. Other Terms.

5.1 Service Notices. Notices for disconnection of Service must be submitted to CenturyLink via Email at: BusinessDisconnects@Centurylink.com. Notices of non-renewal for Services must be sent via e-mail to: CenturyLink, Attn.: CenturyLink NoRenew, e-mail: Norenew@centurylink.com. Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at https://www.centurylink.com/business/login/ or via Email at: Care.Inquiry@Centurylink.com. All other routine operational notices will be provided by Customer to its CenturyLink sales representative.

5.2 Conflicts. If a conflict exists among the provisions of the Service Attachments, the order of priority will be as follows: this Service Schedule, the applicable SOW, the general terms of the Agreement, SLA, and Order(s), as applicable, and then any other documents attached or expressly incorporated into the Agreement.

CENTURYLINK MASTER SERVICE AGREEMENT
CENTURYLINK® SD-WAN SERVICE SCHEDULE

1. Applicability. This Service Schedule applies when Customer orders SD-WAN Service ("SD-WAN Service") which may be designated as "SD-WAN" or "Hybrid-WAN Connectivity" in the Customer Order, pricing attachment, Order acceptance, service delivery, billing and related documents, and the associated Access Services as described herein (collectively, the "Services"). This Service Schedule incorporates the terms of the Master Service Agreement or other service agreement pursuant to which CenturyLink provides services to Customer (the "Agreement"). Terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and the terms of this Service Schedule, this Service Schedule shall control with respect to the Service herein. Customer expressly agrees that CenturyLink may use third party suppliers to provide the Service, provided that CenturyLink remains responsible to Customer hereunder.

2.1 SD-WAN Service Description. SD-WAN Service is a management overlay that uses software, deployed on a CenturyLink-provided CPE appliance at Customer's location ("SD-WAN Device"), enabling Customer to build a homogeneous private network through different types of network connections. The CPE associated with SD-WAN is provided on a rental basis. The SD-WAN Device establishes logical connections with other Customer edge CPE appliances across a physical WAN. CenturyLink supports SD-WAN Service using diverse network controllers (collectively "Controller") and a password-protected management portal ("Management Portal"). The Controller provides an entry point for Customer's locations by authenticating the site and assisting to establish a secure channel between such Customer locations. The Management Portal provides centralized configuration and management. If changes in applicable law, regulation, rule, or order materially affect delivery of Service, the parties will negotiate appropriate changes to this Service Schedule. If the parties cannot reach agreement within 30 days after CenturyLink's notice requesting renegotiation, CenturyLink may, on a prospective basis after such 30-day period, pass any increased delivery cost on to Customer. If CenturyLink does so, Customer may terminate the affected Service on notice to CenturyLink delivered within 30 days of the cost increase taking effect.

SD-WAN Service supports private networking over the top of site to site networking and local internet breakout with firewall. SD-WAN Service includes a small CPE rental device that CenturyLink or its supplier configures and ships to the Customer site. In some cases, repackaged or substitute CPE may be used. The CPE device can be upgraded to a medium or large CPE rental device at additional charge. Customer may order Security Upgrade at an additional charge. Security Upgrade provides a set of firewall, web filtering, intrusion prevention, and localized DDOS features. Customer may order two SD-WAN Service packages at the same site to create a high-availability resilient network design. Subject to availability, On-Site Installation and On-Site Maintenance may be ordered at an additional charge for each location. The On-Site Installation option will provide a CenturyLink technician at the customer premises to support the SD-WAN Device activation. The On-Site Maintenance option will provide a CenturyLink technician at the customer premises to support the replacement of an SD-WAN Device in the event of a device failure.

2.2 CenturyLink Procured Third Party Provided Broadband and Cellular Back-Up Service Descriptions. In conjunction with SD-WAN, Customer may purchase CenturyLink procured broadband access service and/or cellular back-up access service ("Access Services", "Delta Port Internet Connection", or "Wireless Backup Service" as applicable) if available. Broadband access service is an unsecure local internet broadband connection. Cellular back-up access service leverages third party cellular network connectivity and is established utilizing CPE (internal modem or an external enterprise-class cellular-to-Ethernet bridge) in a back-up only or failover situation. If Customer purchases Access Services, those services are subject to the terms of this Service Schedule. If Customer purchases Delta Port Internet Connection for broadband service or Wireless Backup Service for cellular back-up access service, Customer must order and contract for those services separately.

3. Administration and Management. CenturyLink and the Customer will be able to perform ongoing management, monitoring, and reporting of the SD-WAN Service. Customer can submit up to 5 configuration changes per month per site. CenturyLink reserves the right to charge Customer $275 for each configuration request over that amount. CenturyLink or its supplier will maintain global administrative access to SD-WAN Service at all times and will maintain the root password for all functions. Customer may have the option to co-manage SD-WAN Service configuration via the Management Portal. However, CenturyLink is not responsible for outages or security incidents that occur due to Customer changes or configuration. CenturyLink is not responsible for any services, systems, software, or equipment Customer uses with SD-WAN Service which are not provided by CenturyLink. CenturyLink will not debug problems on, or configure, any internal or external hosts or networks (examples include, but are not limited to the following: routers, DNS servers, mail servers, WWW servers, and FTP servers).

4. Charges. Customer shall pay the monthly recurring charges ("MRCs"), non-recurring charges ("NRCs"), and usage charges (related to Access Services, if any) set forth in the Order, CenturyLink-issued quote, Order Form, or pricing attachment in accordance with the Agreement. The SD-WAN Service MRC includes the rental CPE MRC, which may be separately identified in invoices. Customer agrees to pay and/or reimburse CenturyLink for its additional time for fees, costs and expenses resulting from Customer's failure to comply with this Service Schedule and/or Customer's request for changes in services, unless such change is due to an act or omission of CenturyLink. In the event that Customer terminates the SD-WAN Service and/or Access Service prior to the end of the Service Term, Customer must provide CenturyLink with 60 days' advanced written notice and Customer shall pay early termination liability as set forth in the Agreement.

5. Service Levels.

(a) SD-WAN Service. If CenturyLink or its supplier causes Downtime which is not isolated to an issue with the SD-WAN Device, CenturyLink will provide Customer with a credit of one day's charges, prorated from the MRC for the affected SD-WAN Service, for each cumulative hour of Downtime in a calendar month. Total monthly credits will not exceed fifty percent (50%) of the charges for the affected SD-WAN Service for that month. If Downtime is caused by an issue with the SD-WAN Device, Customer will not be entitled to any monetary remedy. Instead, CenturyLink will use commercially reasonable efforts to ship a replacement CPE device to Customer within the following

time frames: (i) for locations within the continental U.S., next business day if Customer notifies CenturyLink by 2 pm mountain time the prior business day; and (ii) for locations outside the continental U.S., within five (5) business days from the time Customer notifies CenturyLink.

(b) Access Services. CenturyLink does not provide any service level credits for Service Unavailability for broadband access without cellular back-up service. The availability service level of broadband access is 99.99% when combined with cellular back-up service. In the event that CenturyLink fails to achieve the availability SLA, Customer shall be entitled to a credit as a percentage of its MRC for the affected broadband access service as follows:

Cumulative Unavailability (in hrs:mins:secs)	% of broadband access MRC
00:00:01 – 00:04:18 (99.99%)	No credit
00:04:19 – 00:43:00	10%
00:43:01 – 04:00:00	15%
04:00:01 – 12:00:00	30%
12:00:01 or greater	50%

(c) Definitions.

(i) "Downtime" is an interruption of SD-WAN Service (for reasons other than an Excused Outage or caused by an issue with Customer's underlying transport) which is confirmed by CenturyLink. Downtime is measured from the time Customer opens a trouble ticket with CenturyLink to the time the SD-WAN Service is restored.

(ii) "Excused Outage" is defined as any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents, or its end users; (b) the failure or malfunction of equipment, applications, or systems not owned or controlled by CenturyLink or its third party providers; (c) scheduled maintenance, alteration, or implementation; (d) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (e) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (f) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (g) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; (h) improper or inaccurate specifications provided by Customer; or (i) force majeure events.

(iii) "Service Unavailability" is defined as the complete inability (for reasons other than an Excused Outage) of Customer to deliver IP packets from an individual Customer site over both (a) the broadband access and (b) cellular back-up service.

6. Ownership. For the SD-WAN Service and rental CPE, no license is conveyed nor is any right, title, or interest in any intellectual property or other proprietary right transferred to Customer. CenturyLink's intellectual property and proprietary rights include any skills, know-how, modifications or other enhancements developed or acquired in the course of configuring, providing, or managing the Service. Each party agrees that it will not, directly or indirectly, reverse engineer, disassemble, decompile, reproduce, or otherwise attempt to derive source code, trade secrets, or other intellectual property from any information, material, software, or technology of the other party,its licensors, or suppliers. The software and all copyrights, patent rights, and all intellectual property rights related thereto are the sole and exclusive property of CenturyLink or its licensors. Customer is hereby provided a non-exclusive, limited, non-transferrable, personal, revocable (at CenturyLink's sole discretion), non-sublicenseable, non-assignable right to access and/or use the software solely in association with the Service hereunder; provided, however, Customer shall not remove any disclaimers, copyright attribution statements or the like from the software and any breach of the foregoing shall automatically result in termination of any license granted herein. Export restrictions must be followed for encryption technology. End user licenses cannot be transferred. Customer has the right to use the software until the expiration or termination of the applicable Service Term.

CPE is the personal property of CenturyLink or its supplier. Notwithstanding that, the CPE, or any part thereof, may be affixed or attached to Customer's real property or any improvements thereon. Customer has no right or interest to the CPE other than as provided herein and will hold the CPE subject and subordinate to the rights of CenturyLink or its supplier. Customer will: (a) at its own expense, keep the CPE free and clear of any claims, liens, and encumbrances of any kind; and (b) make no alterations or affix any additions or attachments to the CPE, except as approved by CenturyLink in writing. Customer will not remove, alter, or destroy any labels on the CPE and will allow CenturyLink or its supplier to inspect the CPE at any time. Customer must use not less than a reasonable standard of care to store and protect CPE and shall be responsible for providing a safe and secure environment for the equipment in accordance with CenturyLink's specifications. Customer agrees to: (i) not alter, move, or disconnect CPE and (ii) notify CenturyLink as soon as Customer is aware of any circumstances that may adversely affect the CPE or its operation. As between CenturyLink and Customer, Customer will bear the entire risk of loss, theft, casualty, destruction, or damage to the CPE following delivery from any cause whatsoever (collectively, "Loss"), until returned to CenturyLink. Customer will indemnify, defend, and hold harmless CenturyLink, its affiliates, and suppliers for any such Loss. Customer agrees to advise CenturyLink in writing within five business days of any such Loss. In no event will such Loss relieve Customer of the obligation to pay CenturyLink any amounts due hereunder. All CPE is subject to the terms and conditions set forth in the manufacturer's or publisher's warranty or end-user license.

7. Insurance. Without limiting the liabilities or indemnification obligations of Customer, Customer will, at its own cost and expense, maintain during the term of this Agreement, such insurance as required hereunder. The insurance coverage will be from a company, or companies, with an A.M. Best's rating of A-VII and authorized to do business in each state or country where CPE is located. Customer

may obtain all insurance limits through any combination of primary and excess or umbrella liability insurance. If local and/or regional laws stipulate higher values than those defined herein, then Customer must comply with the applicable higher value as required by law.

(a) Commercial General Liability with limits not less than $1,000,000 (USD) or local currency equivalent per occurrence and aggregate.

(b) "All-Risk" property insurance on a replacement cost basis in an amount sufficient to cover the CPE, including CenturyLink or a third party provider designated by CenturyLink, as loss payee as their interests may appear.

CenturyLink, its affiliates, subsidiaries, and parent, as well as the officers, directors, employees, and agents of all such entities will be included as additional insureds on the Commercial General Liability policy. Policies will be primary and not contributory to insurance which may be maintained by CenturyLink, subject to any and all indemnification provisions of this Agreement. Prior to commencement of work under this Agreement, Customer will make available to CenturyLink evidence of the insurance required herein.

8. Customer Responsibilities.

(a) Customer is responsible for providing design specifications, including authentication methods and user role information. Customer is solely responsible for all equipment and other facilities used with the Service which are not provided by CenturyLink. Customer will designate one primary and up to two additional Customer security contacts, and provide email and telephone contact details for each such contact (the "Customer Security Contacts"). Customer will ensure that CenturyLink is informed of any changes to the designation of, and contact details for, the Customer Security Contacts. Customer will ensure that at least one Customer Security Contact is available to be contacted by CenturyLink at any given time (24x7x365). Unless Customer purchases On-Site Installation, Customer is responsible for installation of service and integration into Customer's network. Customer shall ensure CenturyLink and its representatives have access to Customer sites for installation and maintenance (if purchased) and removal of equipment and Services as scheduled, including obtaining all landlord approvals or letters of agency. Customer will timely perform all inside wiring, outside plant, work, cabling, openings, connections, and/or building alterations and provide standard AC power to enable delivery of the Service and CPE. Customer may not resell the Services and may use the Services only within Customer's sites. CenturyLink may provide Customer with guidelines for Customer's network minimum system requirements, compatibility, and other information necessary to use the Access Service. Customer must notify CenturyLink of any move or relocation of SD-WAN Service.

(b) Use Restrictions. Customer will not use Services: (i) for fraudulent, abusive, or unlawful purposes or in any other unauthorized or attempted unauthorized manner, including unauthorized or attempted unauthorized access to, or alteration, or abuse of, information; (ii) in any manner that causes interference with CenturyLink's or another's use of the CenturyLink-provided network or infrastructure. Customer will cooperate promptly with CenturyLink to prevent third parties from gaining unauthorized access to the Services, including via Customer's facilities, if applicable; or (iii) in violation of CenturyLink's Acceptable Use Policy. Customer will ensure that all Customer data stored, transmitted, or processed via the Service complies with applicable law and reasonable information security practices, including those involving encryption.

If Customer orders Access Services, Customer shall not use the cellular access service other than in back-up capacity. Without limitation to CenturyLink's other remedies under the Agreement, CenturyLink reserves the right to charge, and Customer agrees to pay, for any misuse of cellular access services or its components, and/or for such usage in excess of CenturyLink's established data pool for Customer, separately at the rates then charged to CenturyLink by the third party cellular provider. Additionally, if CenturyLink provides Customer notice of such use of which CenturyLink becomes aware, CenturyLink may terminate the cellular access service within 10 days of such notice if such use does not cease. Any use of the cellular access service in a primary or non-back-up manner will give CenturyLink the right to immediately suspend such service and Customer shall be liable to CenturyLink for any overage fees that may be charged to CenturyLink for use of the cellular access service beyond a failover. CenturyLink is not responsible, however, for monitoring for such usage by Customer.

(c) CPE Return or Replacement. CenturyLink will provide Customer with instructions on return of CPE. Customer will deliver CPE to CenturyLink in the same condition it was on delivery to Customer, normal wear and tear excepted, and give CenturyLink written notice of such return. If CPE is not returned within 30 calendar days of termination, Customer will become owner of and bear all responsibility for the terminated or replaced CPE and CenturyLink may invoice Customer the then-current value of the applicable CPE model ("Replacement Cost"). Where CPE rented from CenturyLink is replaced due to loss or damage (for example, damage from accident, misuse, or abuse), Customer will pay: (i) the Replacement Cost for the damaged CPE, and (ii) a one-time charge to cover CenturyLink's cost to ship the new CPE. If On-Site Maintenance is not available and Customer requires on-site assistance from CenturyLink to install the replacement CPE, an additional dispatch charge will apply. CenturyLink will quote the charges in advance, obtain Customer's approval, and invoice the charges within 60 days. Customer is responsible for any claim for reimbursement from its insurance carrier. Replacement CPE may or may not be the same model, but will provide equivalent functionality in either case.

(d) To the extent required by law, Customer acknowledges and agrees that It is solely responsible for: (i) notifying its employees, vendors, contractors, or other users that network communications/transmissions on the Customer's network may be monitored, screened, and/or logged by Customer or CenturyLink on Customer's behalf and (ii) obtaining the consent of such employees, vendors, contractors, or other users to such monitoring and/or logging (which may include, where sufficient at law, implied consent).

9. Customer's Security Policies. Customer is responsible for Customer's own network security policy and security response procedures. Customer acknowledges that CenturyLink will implement security policies as reasonably directed by the Customer and,

accordingly, that Customer maintains overall responsibility for maintaining the security of Customer's network and computer systems. CenturyLink makes no guarantee that the Services hereunder will be invulnerable to malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third parties to create security exposures. CENTURYLINK MAKES NO WARRANTY, EXPRESS OR IMPLIED, THAT SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR THAT THE SERVICES WILL RENDER CUSTOMER'S NETWORK AND COMPUTER SYSTEMS SAFE FROM INTRUSIONS AND OTHER SECURITY BREACHES. CENTURYLINK MAKES NO WARRANTY THAT THE SERVICES WILL BE UNINTERRUPTED. If any equipment or software not provided by CenturyLink impairs Customer's use of any Service, Customer will nonetheless be liable for payment for all Services provided by CenturyLink. Furthermore, Customer understands and agrees that as a consequence of the operation of the service, CenturyLink makes no warranty, guarantee, or representation, express or implied, that all legitimate communications will be received by Customer. Customer will ensure that its systems and networks will have up-to-date security controls and patches and that its systems and networks that connect with those included with SD-WAN Service, or that use common network features, have appropriate security controls. Customer agrees to notify CenturyLink in advance of any network changes or activities that could impact Service or reasonably interfere with the monitoring of the Service, such as planned outages, configuration changes, maintenance, or systems changes.

10. Special Terms for Access Services.

(a) CenturyLink will use reasonable efforts to procure the Access Service type per Customer site as identified in the Order. However, CenturyLink does not commit that a certain access service type or technology will be available at a Customer site.

(b) If the specific Access Service type set forth in an Order is not available, CenturyLink will so notify Customer and the Order for Access Services at that Customer site (and only that Customer site) will be cancelled (other Customer sites under such Order will not be impacted). Additionally, if the MRC or NRC must be increased and/or additional construction costs may apply, CenturyLink will request Customer confirmation of such costs, which confirmation may be provided via e-mail and will be binding on Customer. If Customer fails to provide such confirmation within 10 business days, the Order for Access Services at that specific Customer site shall be deemed cancelled.

(c) CenturyLink reserves the right to commence billing Customer, and Customer shall pay for the Access Service MRCs, if and to the extent that (i) such access has been installed; (ii) CenturyLink is incurring charges from the supplier; and (iii) the remaining completion of service installation cannot occur due to Customer delay, inaction, or failure to perform the Customer obligations hereunder.

(d) To the extent that suppliers of Access Service have the right to change the terms and conditions upon which such access is provided, including but not limited to the right to terminate the service and/or to modify rates or charges, notwithstanding anything to the contrary in the Agreement, CenturyLink expressly reserves the right to make corresponding changes with Customer for such services. CenturyLink will provide Customer with as much advanced notice as is reasonable, given the notification provided to CenturyLink from such supplier. In the event of a termination, CenturyLink and Customer will work together in good faith to agree upon and expediently procure another type of Access Service at such Customer site.

(e) Stated speeds for access may not be achieved. Actual speeds may vary and are not guaranteed. Effective throughput may be affected by several factors including but not limited to: physical layer line issues, overhead from encryption of network traffic, congestion within the public Internet, congestion within the underlying supplier access network, TCP window fragmentation, application performance, server loads, or performance and latency from inefficient routing paths within the Internet.

11. Modification or Termination of Access Services by CenturyLink. CenturyLink reserves the right to modify any features or functionalities of the Access Services upon 90 days prior notice to Customer. In the event that such modification materially affects the features or functionality of these services, then Customer, as its sole remedy, may cancel the affected cellular and/or broadband access service without termination liability, as long as Customer notifies CenturyLink in writing of such termination within 60 days of such notice from CenturyLink. Additionally, CenturyLink may upon written notice terminate the cellular and/or broadband access service at a site (either before or after Service delivery) if CenturyLink determines that the bandwidth and/or coverage is insufficient to support the service at such site. In such case, CenturyLink will notify Customer via e-mail of termination of service at such site and Customer shall not be billed for service at that location.

12. Additional Limitations. Notwithstanding anything to the contrary in the Agreement, with respect to SD-WAN Service or any Access Services, no indemnification, security or data protection obligations, warranties, or representations apply.

13. Withholding Taxes. All invoices will be issued to Customer and paid in the currency specified in the Order, CenturyLink-issued quote, Order Form, or pricing attachment. Customer will pay such invoices free of currency exchange costs or bank charges. Service charges are exclusive of taxes and presented without reduction for any Withholding Tax, all of which are the responsibility of the Customer. "Withholding Tax" means any amount or account of tax on sources of income which a payor is obliged to deduct from payments due to a recipient and account for or to any tax authority. In the event that any payment to be made to CenturyLink hereunder should be subject to reduction by reason of a Withholding Tax, Customer agrees to pay CenturyLink such amounts as would have been necessary so that the aggregate net amount received by CenturyLink after application of a Withholding Tax is the same amount as would have been received by CenturyLink if there had been no requirement to deduct or withhold such tax.

14. Data and Information Notification to Authorized Users. Customer acknowledges that, by virtue of providing the Service, CenturyLink may need to process personal data of Customer's employees and users of the Service. Customer is the data controller of

such personal data and CenturyLink is the data processor. Customer is solely responsible for ensuring the lawful basis of such processing, and for notifying any employee or individual that it permits to use the Service on Customer's behalf (an "Authorized User"), that it has provided such Authorized User's personal data to CenturyLink for the purposes of allowing CenturyLink to provide the Service, and that the Authorized User's use of the Service may be monitored, screened, and/or logged by Customer or CenturyLink on Customer's behalf.

(a) In the event Customer and CenturyLink have entered into a data processing agreement whereby CenturyLink processes personal data on behalf of Customer, the Service shall be included within the scope of that data protection agreement and, if required, the parties shall amend such data processing agreement necessary to comply with applicable law. In the event Customer and CenturyLink have not entered into a data processing agreement applicable to the Services, the following terms shall apply:

(i) Cross-Border Transfers. Customer acknowledges and consents to CenturyLink's and its affiliates' or subcontractors' use and transfer to the United States, or other countries, data or information (including business contact information such as names, phone numbers, addresses, and/or email addresses) of the Customer for the sole purpose of: (A) providing and managing the Service; (B) fulfilling its obligations under the Agreement; and (C) complying with applicable laws. Customer represents and warrants that it will ensure that all information provided to CenturyLink is accurate at all times and will provide any required notifications to Authorized Users about the potential transfer of information to the United States and other countries. To the extent legally required, Customer and CenturyLink will enter into separate written agreements required to facilitate necessary cross-border transfers. Customer shall be responsible for notifying CenturyLink whether such written agreements are required.

(ii) Personal Data Processing. Customer acknowledges that, by virtue of providing the Service, CenturyLink, its affiliates, vendors, and/or agents may come into possession of, by way of example and not limitation, usage, billing, or other data containing personal and/or private information of Customer, its employees, and Authorized Users. Customer is the "data controller" and CenturyLink will be acting as a "data processor" (such terms defined under applicable law). Customer acknowledges that any processing of such information by CenturyLink, its affiliates, vendors, or contractors occurs exclusively at the direction and discretion of Customer, such direction and discretion exercised by acceptance of these terms. Customer further acknowledges and agrees that such possession is ancillary and not a primary purpose of the Service. Customer further represents and warrants that it has obtained, and will obtain, all legally required consents and permissions from relevant parties (including Authorized Users) for the use, processing, and transfer of the information described herein. To the extent legally required, Customer and CenturyLink will enter into separate written agreements required to comply with laws governing the relationship between a data controller and data processor with respect to the processing of personal data. Customer shall be responsible for notifying CenturyLink whether such written agreements are required.

15. Fees. Charges for certain Services are subject to (a) a property tax surcharge of 4.75% and (b) a cost recovery fee of 5.1% per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit https://www.centurylink.com/taxes.

PRICING ATTACHMENT FOR SERVICE LOCATIONS WITIHN THE CONTINENTAL UNITED STATES

1. Other Terms. The SD-WAN service specific terms apply when Customer orders SD-WAN Service ("CenturyLink SD-WAN Service Schedule" or "CenturyLink SD-WAN Service Exhibit" as applicable).

Despite anything to the contrary in the Agreement, the following terms apply:

1.1 Any references to a Revenue Commitment or Contributory Charges will not apply to SD-WAN. Any references to a Renewal Order will not apply to SD-WAN.

1.2 Scheduled maintenance will not normally result in Service interruption. If scheduled maintenance requires Service interruption, CenturyLink will use commercially reasonable efforts to minimize such interruptions and provide notice to Customer. Customer understands that Service is not eligible for any service level agreements.

1.3 Cancellation and Termination Charges. Either party may terminate an individual Service: (a) with 60 days' prior written notice to the other party, or (b) for Cause. "Cause" means the failure of a party to perform a material obligation under the Agreement, which failure is not remedied: (i) for payment defaults by Customer, within five days of separate written notice from CenturyLink of such default; or (ii) for any other material breach, within 30 days after written notice (unless a shorter notice period is identified in a Service Attachment). If an individual Service is terminated by Customer for any reason other than for Cause or by CenturyLink for Cause prior to conclusion of the applicable Service Term, then Customer will pay the Cancellation Charges set forth below, in addition to any and all charges that are accrued but unpaid as of the termination date. If the Agreement is terminated by Customer for any reason other than for Cause, or by CenturyLink for Cause prior to the conclusion of the Service Term, all Services are deemed terminated, and Customer will pay the Cancellation Charges set forth below, in addition to any and all charges that are accrued but unpaid as of the termination date.

1.4 Customer must purchase each Service for a specific term for the particular Service ordered (each, a "Service Term"). The Service Term for each new SD-WAN Service instance will begin and charges will commence five days after the date CenturyLink notifies Customer that Service is provisioned and ready for use ("Start of Service Date"). Upon expiration of the Service Term, Service will continue on a month-to month basis unless either party elects to cancel the Service by providing 60 days prior written notice of such cancellation to the other party. If the Agreement is terminated or Service is canceled prior to the expiration of the applicable Service Term for reasons other than by Customer for Cause, then Customer will pay to CenturyLink a "Cancellation Charge" equal to (a) 100% of the applicable SD-WAN MRCs, including those for purchased optional services, multiplied by the number of months remaining in the first 12 months of the Service Term, if any, plus; (b) 35% of the applicable SD-WAN MRCs, including those for purchased optional services, multiplied by the number of months remaining to complete 24 or 36 months of the remaining Service Term, if any; and (c) the amount of any NRCs/installation charges that CenturyLink discounted or waived. Customer remains responsible for all accrued and unpaid charges for the canceled Service provided through the effective date of such cancellation. Charges for Customer's failure to return CPE will also apply.

1.5 CenturyLink is required by law to treat CPNI confidentially. Customer agrees that CenturyLink may share CPNI within its business operations (e.g., wireless, local, long distance, and broadband services divisions), and with businesses acting on CenturyLink's behalf to determine if Customer could benefit from the wide variety of CenturyLink products and services and in its marketing and sales activities. Customer may withdraw its authorization at any time by informing CenturyLink in writing. Customer's decision regarding CenturyLink's use of CPNI will not affect the quality of service CenturyLink provides Customer. "CPNI" means Customer Proprietary Network Information, which includes confidential account, usage, and billing-related information about the quantity, technical configuration, type, destination, location, and amount of use of a customer's telecommunications services. CPNI reflects the telecommunications products, services, and features that a customer subscribes to and the usage of such services, including call detail information appearing in a bill. CPNI does not include a customer's name, address, or telephone number.

1.6 CenturyLink may use a CenturyLink affiliate or a third party to provide Service to Customer, but CenturyLink will remain responsible to Customer for Service delivery and performance.

2. Charges. A single MRC and NRC apply for each Service instance. Charges are presented in U.S. Dollars. Charges for Service are as follows.

2.1 SD-WAN Service.
60 Month Term

For pricing, please refer to the RFP. This Pricing Attachment will be completed upon award.

2.2 Rental CPE. The charges for Rental CPE are included in the SD-WAN Service MRC.

CENTURYLINK MASTER SERVICE AGREEMENT
RENTAL CPE SERVICE EXHIBIT

1. General; Definitions. CenturyLink will provide Customer with rental customer premises equipment and software license offerings (collectively, "CPE") and CPE installation and maintenance ("Service") under the terms set forth in the Agreement, this Service Exhibit and any Rental CPE Rate Attachment submitted hereunder. Capitalized terms not defined herein are defined in the Agreement. "Rental CPE Rate Attachment" means the CenturyLink order request form issued and executed by CenturyLink and Customer. CPE, as defined in this Service Exhibit, does not include CPE purchased by Customer. In order to qualify for CPE, Customer must also purchase either CenturyLink IQ® Networking, SIP Trunk, Analog VoIP, Hosted VoIP, Managed Office, Managed Enterprise, Integrated Access, Hosted Collaboration Solution, SD-WAN or any CenturyLink bundle, package or promotion that includes these services; or CenturyLink QC intrastate Metro Ethernet service under a separate agreement (collectively "Underlying Service").

2. Delivery and Return. CPE will be delivered to Customer's location as identified, in writing, by Customer. Delivery will be made either by F.O.B. origin, freight paid by Customer, or personal delivery by CenturyLink. CPE will be installed as designated herein, or as otherwise agreed upon by the parties. Except as otherwise provided in the Service Exhibit for the Underlying Service, upon termination of Service, or when Customer replaces CPE with upgraded models, Customer must return terminated or replaced CPE at its own expense within 15 calendar days of termination or replacement. CenturyLink will provide Customer with return instructions. Customer will deliver CPE to CenturyLink in the same condition it was on the Effective Date, normal wear and tear excepted, and give CenturyLink written notice of such return. If CPE is not returned within 15 calendar days of termination, Customer will become owner of and bear all responsibility for the terminated or replaced CPE and CenturyLink may invoice Customer the then-current value of the applicable CPE model ("Replacement Cost").

3. Ownership and Use. Except as provided in Paragraph 2, CPE is the personal property of CenturyLink, its designee or a third-party provider, notwithstanding that the CPE, or any part thereof, may be affixed or attached to Customer's real property or any improvements thereon. Customer has no right or interest to the CPE other than as provided herein and will hold the CPE subject and subordinate to the rights of CenturyLink. Customer will: (a) at its own expense, keep the CPE free and clear of any claims, liens, and encumbrances of any kind; and (b) make no alterations or affix any additions or attachments to the CPE, except as approved by CenturyLink in writing. Customer will not remove, alter or destroy any labels on the CPE and will allow CenturyLink the inspection of the CPE at any time. As between CenturyLink and Customer, Customer will bear the entire risk of loss, theft, casualty, destruction or damage to the CPE following delivery from any cause whatsoever (collectively, "Loss"), until returned to CenturyLink. Customer will indemnify, defend and hold harmless CenturyLink its affiliates, and contractors for any such Loss. Customer agrees to advise CenturyLink in writing within five business days of any such Loss. In no event will such Loss relieve Customer of the obligation to pay CenturyLink any amounts due hereunder.

4. Software. Software licensor has retained title to the software. To the extent possible, CenturyLink grants Customer a software license or sublicense in the software according to the licensing agreement accompanying such software, which extends only to Customer's own internal business use of such software and only on or with the designated CPE. Software must be held in confidence and may not be reproduced unless specifically authorized by the software licensor. Customer is prohibited from reverse engineering, decompiling or disassembling the CPE or otherwise attempting to derive the source code of the software. All CPE is subject to the terms and conditions set forth in the manufacturer's or publisher's warranty or end-user license.

5. Insurance. Without limiting the liabilities or indemnification obligations of Customer, Customer will, at its own cost and expense, maintain during the term of this Agreement, such insurance as required hereunder. The insurance coverage will be from a company, or companies, with an A.M. Best's rating of A-VII and authorized to do business in each state where CPE is located. Customer may obtain all insurance limits through any combination of primary and excess or umbrella liability insurance.

(a) Commercial General Liability with limits not less than $1,000,000 per occurrence and aggregate.

(b) "All-Risk" property insurance on a replacement cost basis in an amount sufficient to cover the CPE, including CenturyLink or a third-party provider designated by CenturyLink, as loss payee as their interests may appear.

CenturyLink, its affiliates, subsidiaries, and parent, as well as the officers, directors, employees and agents of all such entities will be included as additional insureds on the Commercial General Liability policy. Policies will be primary and not contributory to insurance which may be maintained by CenturyLink, subject to the Indemnification provisions of this Agreement. Prior to commencement of work under this Agreement, Customer will make available to CenturyLink evidence of the insurance required herein.

6. Charges. The charges for CPE and Service are set forth in the Rental CPE Rate Attachment, and will be used to calculate Contributory Charges. Charges will commence within five days of CenturyLink's notification to Customer that the Underlying Service is provisioned and ready for use ("Start of Service Date"). CenturyLink may cease providing Service and demand return of CPE if payment is not made when due.

7. CPE Replacement Recovery Charge. Where CPE rented from CenturyLink is replaced due to loss or damage not covered by maintenance under the applicable Detailed Description (for example, damage from accident, misuse or abuse), Customer will pay: (a) the Replacement Cost for the damaged CPE, and (b) a one-time charge to cover CenturyLink's cost to ship the new CPE. If Customer requires on-site assistance from CenturyLink to install the replacement CPE, an additional dispatch charge will apply. CenturyLink will quote the charges in advance, obtain Customer's approval, and invoice the charges within 60 days. Customer is responsible for any claim for reimbursement from its insurance carrier. The terms and conditions in this Service Exhibit will continue to apply. Replacement CPE may or may not be the same model.

8. Term. This Service Exhibit will commence on the Effective Date of the Agreement (or, if applicable, an amendment to the Agreement if this Service Exhibit is added to the Agreement after its Effective Date), and will remain in effect until terminated. Either party may terminate this Service Exhibit with at least 60 days prior written notice to the other party. Termination will not affect obligations under Rental CPE Rate Attachments accepted prior to the effective date of termination, and this Service Exhibit will remain in effect as to such obligations if it would otherwise have terminated. CPE and Service ordered during the Term will commence on the Start of Service Date and will continue for a number of months as set forth on the Rental CPE Rate Attachment ("CPE Term"). Upon expiration of the CPE Term, CPE and Service will automatically renew on a month to month basis at the then current rates, unless either party elects to terminate the CPE and Service by providing 60 days prior written notice of such termination to the other party. If the Agreement or any CPE and Service provided hereunder are terminated prior to the expiration of the applicable CPE Term for reasons other than by Customer for Cause, then Customer will pay to CenturyLink: (a) all charges for CPE and Service provided through the effective date of such cancellation; and (b) an early cancellation charge of 100% of the balance of MRCs that otherwise would have become due for the unexpired portion of the CPE Term.

9. Installation, Maintenance and Safety Compliance. Installation, maintenance or other labor provided to Customer pursuant to this Agreement is subject to, and controlled by, Detailed Description(s) which are posted under CPE at http://www.centurylink.com/legal/ and are incorporated by reference and made a part of this Service Exhibit. CenturyLink may change the Detailed Descriptions at any time and such change will be effective upon posting to the Web site. Customer is responsible for informing CenturyLink of the existence, location and condition of any Hazardous Substances that may be in or around the CenturyLink work area. "Hazardous Substance" means a substance regulated by any safety regulation and includes, without limitation, asbestos. Customer will indemnify and hold CenturyLink harmless from any fines or other liability of CenturyLink arising from Customer's failure to inform CenturyLink of hazardous substances.

10. Additional Limitation of Liabilities. If CPE contains a firewall or other security features, CenturyLink makes no warranty, guarantee, or representation, express or implied, that all security threats and vulnerabilities will be detected or that the performance of Service will render Customer's systems invulnerable to security breaches. Customer is responsible for Customer's own network security policy and security response procedures. If any equipment or software not provided by CenturyLink impairs Customer's use of CPE, Service or an Underlying Service: (a) Customer will nonetheless be liable for payment for all CPE, Service and Underlying Service provided by CenturyLink; and (b) any SLA generally applicable to the Service or Underlying Service will not apply.

11. Miscellaneous. With respect to the Agreement terms incorporated by reference, "Service" is replaced with "CPE" and "Service" as defined in this Service Exhibit.

12. Other Terms.

12.1 General. Any references to a Revenue Commitment or Contributory Charges will not apply to this Service Exhibit.

12.2 Cancellation and Termination Charges. This Section replaces Section 4.6, the Cancellation and Termination Charges set forth in the Agreement:

> **Termination.** Either party may terminate an individual Service: (a) as set forth above with 60 days' prior written notice to the other party, or (b) for Cause. If an individual Service is terminated by Customer for any reason other than for Cause or by CenturyLink for Cause prior to conclusion of the applicable CPE Term, then Customer will pay the termination charges set forth above, in addition to any and all charges that are accrued but unpaid as of the termination date. If the Agreement is terminated by Customer for any reason other than for Cause, or by CenturyLink for Cause prior to the conclusion of the Term, all Services are deemed terminated, and Customer will pay the termination charges set forth above, in addition to any and all charges that are accrued but unpaid as of the termination date. "Cause" means the failure of a party to perform a material obligation under the Agreement, which failure is not remedied: (a) for payment defaults by Customer, within five days of separate written notice from CenturyLink of such default; or (b) for any other material breach, within 30 days after written notice (unless a shorter notice period is identified in a Service Attachment).

12.3 Service Notices. Notices for disconnection of Service must be submitted to CenturyLink via Email at: BusinessDisconnects@Centurylink.com. Notices of non-renewal for Services must be sent via e-mail to: CenturyLink, Attn.: CenturyLink NoRenew, e-mail: Norenew@centurylink.com. Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at https://www.centurylink.com/business/login/ or via Email at: Care.Inquiry@Centurylink.com. All other routine operational notices will be provided by Customer to its CenturyLink sales representative.

12.4 CPNI. CenturyLink is required by law to treat CPNI confidentially. Customer agrees that CenturyLink may share CPNI within its business operations (e.g., wireless, local, long distance, and broadband services divisions), and with businesses acting on CenturyLink's behalf, to determine if Customer could benefit from the wide variety of CenturyLink products and services, and in its marketing and sales activities. Customer may withdraw its authorization at any time by informing CenturyLink in writing. Customer's decision regarding CenturyLink's use of CPNI will not affect the quality of service CenturyLink provides Customer. "CPNI" means Customer Proprietary Network Information, which includes confidential account, usage, and billing-related information about the quantity, technical configuration, type, destination, location, and amount of use of a customer's telecommunications services. CPNI reflects the telecommunications products, services, and features that a customer subscribes to and the usage of such services,

including call detail information appearing in a bill. CPNI does not include a customer's name, address, or telephone number.

12.5 Conflicts. If a conflict exists among the provisions of the Service Attachments, the order of priority will be as follows: the Service Exhibit, the general terms of the Agreement, SLA, SOW (if any) and Order Form, as applicable, and then any other documents attached or expressly incorporated into the Agreement.

CENTURYLINK® TOTAL ADVANTAGE® AGREEMENT
TELECOMMUNICATIONS SERVICE PRIORITY SERVICE EXHIBIT

1. General. CenturyLink QCC will provide Telecommunications Service Priority ("Service" or "TSP") for National Security/Emergency Preparedness ("NS/EP") pursuant to the terms and conditions of the Agreement and this Service Exhibit.

2. Service.

2.1 Description. Customer can assign a 12-digit alphanumeric code issued by the Office of Priority Telecommunications ("OPT") with the TSP control identifier ("TSP Authorization Code") to its interstate telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis as set forth in 47 CFR Part 64, Appendix A ("NS/EP Telecommunications Services"). The TSP Authorization Code provides TSP priority levels that identify the provisioning and restoration priority-level assignment for a particular circuit. Telecommunications Service Priority allows CenturyLink to provision and restore Customer's NS/EP Telecommunications Services with TSP Authorization Codes before services without such assignments as set forth in 47 CFR part 64, Appendix A. TSP Service is available on CenturyLink services that have a unique and identifiable circuit identification number. The Service is only provided per-circuit on an end-to-end basis where the entire circuit is provided by CenturyLink (whether on its network or through leased facilities) so that the entire circuit is included in the TSP designation. The underlying NS/EP Telecommunications Service is offered pursuant to the terms and conditions of the Agreement, Service Exhibit, and/or Services Schedule applicable to the service and separate rates. TSP service is only available to federal, state, and local government users and certain private sector organizations that have services that support an NS/EP function and is applied only to interstate telecommunications services, as defined by Federal Communications Commission regulations.

2.2 Ordering. CenturyLink will provide the Service in accordance with 47 CFR Part 64, Appendix A and if: (a) Customer provides CenturyLink with a valid TSP Authorization code issued by the OPT for each circuit, via an Order Form; and (b) the Order Form is accepted by CenturyLink. CenturyLink will not accept TSP assignments or orders without an assigned TSP Authorization Code. TSP restoration priorities must be requested and assigned via an Order Form before a service outage occurs in order to have priority restoration. .

3. Term; Cancellation. The Service will become effective upon CenturyLink's acceptance of an order form and will terminate upon Customer's written notice of termination to CenturyLink or OPT's revocation of the TSP Authorization Code. Service will automatically expire should Customer terminate the circuit. In the event Customer cancels Service, Customer will pay for the Service provided through the effective date of the cancellation.

4. Charges. "Pricing Attachment" means the attached document containing Service rates, which is incorporated by reference and made a part of this Service Exhibit. Customer will pay all applicable MRCs and NRCs as set forth in the Pricing Attachment or Order Form. The rates will be used to calculate Contributory Charges. CenturyLink reserves the right to modify rates with 30 days written notice to Customer.

PRICING ATTACHMENT

TSP Service	Charge Type	Amount
TSP Provisioning installation and/or Restoration priority (excludes coordination of Leased Access) per circuit	NRC	$400
TSP Provisioning installation and/or Restoration priority for Leased Access, per Local Access circuit	NRC	$128
TSP Priority Level Change	NRC	$50
TSP Administration and Maintenance	MRC	$20

DATA SECURITY ADDENDUM

This Data Security Addendum ("Addendum") forms part of the service agreement ("Agreement") between Customer and CenturyLink and is applicable to the services provided by CenturyLink pursuant to the Agreement ("Services"). In the event of a conflict between the Agreement and this Addendum, the terms of this Addendum shall control.

CenturyLink has implemented the data security measures described in this Addendum and shall maintain them, or an equally secure equivalent, during the applicable term of the Services. These measures generally apply to CenturyLink's standard services and certain measures may not apply or may be applied differently to customized services, configurations, or environments ordered or as deployed by Customer. These measures have been implemented by CenturyLink to protect, directly or indirectly, the confidentiality, integrity and availability of Customer Data. As used in this Addendum, "Customer Data" means any data, content or information of Customer or its end users that is stored, transmitted, or otherwise processed using the CenturyLink Services.

1. COMPLIANCE WITH LAW, AUDIT REPORT

CenturyLink has adopted and implemented a corporate information security program as described below, which program is subject to reasonable changes by CenturyLink from time to time. CenturyLink has completed an AICPA sanctioned Type II audit report (SSAE18/ISAE3402 SOC 1 or SOC 2) for certain facilities/services and will continue to conduct such audits pursuant to a currently sanctioned or successor standard. Customer will be entitled to receive a copy of the then-available report upon request, which report is CenturyLink Confidential Information. Customer may make such report available to its end users subject to confidentiality terms provided by CenturyLink. Customer will ensure that all Customer Data complies with all applicable laws and appropriate information security practices, and nothing herein shall relieve Customer from its responsibility to select and implement such practices.

2. INFORMATION SECURITY PROGRAM

CenturyLink has implemented an information security program (the "Program") that includes reasonable measures designed to: (1) secure the confidentiality and integrity of Customer Data; (2) to the extent related to the Services and CenturyLink infrastructure, protect against foreseeable threats to the security or integrity of Customer Data; (3) protect against unauthorized access to, disclosure of or unauthorized use of Customer Data; and (4) provide that CenturyLink employees are aware of the need to maintain the confidentiality, integrity and security of Customer Data. CenturyLink will limit access to Customer Data to only those employees, agents, contractors or service providers of CenturyLink who need the information to carry out the purposes for which Customer Data was disclosed to CenturyLink.

The CenturyLink Program is modelled on the ISO27001:2013-based Information Security Management System ("ISMS"), which establishes the guidelines and general principles used for establishing, implementing, operating, monitoring, reviewing, maintaining and improving protections for CenturyLink information and Customer Data. The CenturyLink Program, in alignment with the ISMS, is designed to select adequate and proportionate security controls to protect information and provides general guidance on the commonly accepted goals of information security management and standard practices for controls in the following areas of information security management:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Communications security
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance
- Cryptography
- Supplier relationships

CenturyLink has also implemented a formal information security policy and supporting methods and procedures, technical standards, and processes to reinforce the importance of information security throughout the organization ("Information Security Policy"). The Information Security Policy is in alignment with ISO 27002:2013 and is approved by the Chief Information Security Officer. The Information Security Policy outlines the requirements to maintain reasonable security for the Services. Employees and contractors with access to corporate information and Customer Data are

required to complete annual security training based on the Information Security Policy. The Information Security Policy includes the following:

- Physical Security Policy for data centers and Office Locations
- Electronic Use Policy including:
  - Email Usage
  - Wireless Networks
  - Internet Access
  - Anti-Virus control
- Password Management
- Remote and Home Working
- Computer Security Incident Response Plan
- Information Protection
- Third Party Connections Agreements
- Third Party Access
- Wireless Scanning
- Risk Management
- Vendor Management

3. SPECIFIC SECURITY CONTROLS

CenturyLink's security controls include:

- Logical access controls to manage access to Customer Data on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, strong (i.e. two-factor) authentication for remote access systems (and elsewhere as appropriate), and promptly revoking or changing access in response to terminations or changes in job functions.

- Password controls to manage and control password complexity and expiration. Any password controlling access to the CenturyLink infrastructure must be of a minimum length and complexity.

- Operational procedures and controls to provide that technology and information systems are configured and maintained according to prescribed internal standards.

- Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection/prevention systems to help protect systems from intrusion and/or limit the scope or success of any attack or attempt at unauthorized access.

- Vulnerability management procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

- Approved anti-malware software is installed on CenturyLink equipment capable of running it where the risk of infection is high. It is configured to prevent users disabling the software where possible or altering its configuration without authorization. Periodic evaluations are performed to confirm whether systems continue to require (or not) antivirus software.

- Change management procedures outlining that modifications to CenturyLink technology and information assets are tested, approved, recorded, and monitored.

- Organizational management designed to ensure the proper development and maintenance of information security and technology policies, procedures and standards.

- Dedicated organizations with global responsibility for all physical security operations, security systems, access administration, and security controls within all CenturyLink-owned facilities and data centers. Third-party data

centers are utilized for certain services and, in such cases, certain physical security and other controls are reviewed by CenturyLink.

- Security policies which reinforce the importance of physical security of all company facilities including procedures specific to data center physical security. Data center security personnel are responsible for controlling data center access, monitoring local security alarms and managing all reported physical security-related events.

- CCTV (Closed Circuit Television) commonly deployed as a physical security control in high value facilities to deter, detect and identify intruders. The Corporate Security Operations Center (CSOC) provides global, 24/7 support with remote monitoring, management, administration and maintenance of the CCTV video surveillance systems used throughout CenturyLink.

- The Central Access Control Center (CACC) supports the distribution of all CenturyLink access badges and administration of access permissions within the access control system.

- Disposal procedures for different types and classifications of information which are documented and communicated to personnel. Employees have access to secure shredders for hardcopy. Electronic media are disposed of through certified disposal vendors.

- Pre-employment screening and background checks are conducted on incoming personnel in accordance with CenturyLink human resource on-boarding practices and applicable local law. The checks are dependent on, amongst other things: the role, location, any custom requirements, and can include: identity, drug, criminal, academic and credit checks.

- Annual security awareness training for CenturyLink employees and contractors working on CenturyLink premises. The training reflects current threats and encourages basic security good practice, access to and knowledge of Information Security Policy and procedures such as how to report an incident. Employees in particular positions receive supplementary security training and if a training or testing issue arises (e.g., internal phishing exercises), further guidance is provided. CenturyLink conducts a continuous program of phishing tests on staff to reinforce the requirement for awareness and good email and browsing habits and to assess the effectiveness of security awareness training. The company intranet and email system are used to disseminate flash announcements on security matters as appropriate.

4. SECURITY AUDITS.

Customer may, no more than once per year and at its own expense, audit CenturyLink's performance with respect to its security obligations under this Addendum ("Audit"). In the event Customer retains a third party to perform an Audit, CenturyLink may require additional documentation be executed by the third party auditor prior to granting access to a CenturyLink facility where Services are provided, and CenturyLink may, at its sole and reasonable discretion, decline to allow a third party access to a data center. CenturyLink shall reasonably cooperate with Customer in its performance of the Audit and shall make available to Customer or its auditors documents and records reasonably required to complete the Audit. CenturyLink shall provide Customer with reasonable access to the relevant facility for the purpose of inspection of the equipment and facilities which are used to provide the Services to Customer. For purposes of clarification, access will not be granted to certain areas of certain facilities (such as data centers) to which CenturyLink does not generally allow access to its customers (e.g. areas which house equipment used to support services for multiple customers). Audit access is subject to CenturyLink's reasonable security requirements for its most sensitive security policies/materials. Audit access must be within CenturyLink's normal business hours and must be scheduled at least ten (10) business days in advance, and Customer or its auditor shall be escorted by CenturyLink personnel during the period of access. The Audit and any findings related thereto shall be treated as Confidential Information.

5. SECURITY INCIDENTS AND RESPONSE.

In the event CenturyLink determines that a Security Incident has impacted Customer Data, CenturyLink shall promptly take the following actions:

- Notify Customer of such Security Incident and provide periodic updates as appropriate given the nature of the Security Incident and as information becomes available;
- Take reasonable steps to remediate and mitigate the Security Incident, to the extent such steps are technically feasible and appropriate in the circumstances;
- Conduct a preliminary investigation into the Security Incident to determine, to the extent reasonably feasible, its root cause; and

- Reasonably cooperate with Customer in its efforts to remediate or mitigate the Security Incident and its efforts to comply with applicable law and legal authorities, as necessary.

For purposes hereof, “Security Incident” means any unlawful or unauthorized access, theft, or use of Customer Data while being stored, transmitted or otherwise processed using CenturyLink services.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
1	1	Senior Management Statement	4.1	Has Senior Management created a Senior Management Statement (SMS) of Policy?(Audit Guidance: this could take the shape of a security plan, executive level security policy, or other such documents. The auditor should use his/her discretion as to whether the document in question meets the requirements of this portion of the NG-SEC standard)	R	C	
2	1	Senior Management Statement	4.1	Does the SMS designate the person responsible for security (e.g. Security Administrator)?	R	C	
3	1	Senior Management Statement	4.1	Does the SMS clearly document the security goals and objectives of the organization?	R	C	
4	2	Acceptable Use Policy	4.2	Does the organization have an Acceptable Usage Policy?	R	C	Customers may access CenturyLink's AUP at: http://www.centurylink.com/aboutus/legal/acceptable-use-policy.html
5	2	Acceptable Use Policy	6.6	Are any and all actual, attempted, and/or suspected misuses of Public Safety assets reported and documented by appropriate organizations?	R	C	
6	3	Authentication / Password Policy	4.2	Does the organization have an Authentication / Password Policy?	R	C	
7	3	Authentication / Password Policy	7.1.1	Is each individual requiring access to the NG9-1-1 System provided a unique Identification and authentication?	R	CP	There is a shared Application User ID in use on some systems.
8	3	Authentication / Password Policy	7.1.1	Do individuals share their authentication information (including usernames and passwords) with other individuals or groups?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
9	3	Authentication / Password Policy	7.1.2	Are requests for new User Accounts, User IDs, and File and Resource authorization documented? (Audit	R	C	
10	3	Authentication / Password Policy	7.1.2	Do personnel performing entity or security administration ensure that only approved entities are granted access?	R	C	
11	3	Authentication / Password Policy	7.1.2.1	Does the organization have procedures for changing access authority?	R	C	
12	3	Authentication / Password Policy	7.1.2.1	Does the organization have procedures for removing access authority for terminated personnel?	R	C	
13	3	Authentication / Password Policy	7.1.3	When system to system access is implemented does the system mask individual accountability for transactions?(Audit Guidance: The system shall not mask individual accountability for transactions)	R	CP	For automated system to system access; individual user actions are logged at the application level through unique credentials and never masked. There is less detailed logging when changing through interactive sessions.
14	3	Authentication / Password Policy	7.1.3	When system to system access is implemented is the source system authenticated before each transfer session?	R	C	
15	3	Authentication / Password Policy	7.1.3	When system to system access is implemented and push technology is utilized, is the destination authenticated by the source?	R	N/A	The ESInet solution does not push system updates
16	3	Authentication / Password Policy	7.1.3	When system to system access is implemented and a continuous connection is utilized, was authentication performed at the initial connection?	R	C	
17	3	Authentication / Password Policy	7.1.3	When system to system access is implemented are individuals accessing any of the systems required to Authenticate when initially accessing each system?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
18	3	Authentication / Password Policy	7.1.5	Are Authentication Credentials displayed in an obscured format when entered on computer screens? (Auditor Guidance: Check to see if passwords can be seen on the screen when typed in. They should not be able to be seen so as to prevent “shoulder surfing.”)	R	C	
19	3	Authentication / Password Policy	7.1.4	Are users locked out after no more than 5 invalid sign on attempts?	R	C	
20	3	Authentication / Password Policy	7.1.5	Are Default and Null Passwords changed when installing new equipment or software?	R	C	
21	3	Authentication / Password Policy	7.1.5	Are Authentication Credentials encrypted when stored on a computer?	R	C	
22	3	Authentication / Password Policy	7.1.5	When two-factor authentication is used, (e.g. SecurID + Pin or Certificate + Passphrase) are two authentication factors stored in such fashion that one incident can compromise both? (Auditor Guidance: e.g. password or pin isn’t written down on the token, or stored with the token)	R	C	
23	3	Authentication / Password Policy	7.1.5.1	All user accounts shall require a password	R	C	
24	3	Authentication / Password Policy	7.1.5.1	Passwords are not based on the user’s account name.	R	C	
25	3	Authentication / Password Policy	7.1.5.1	Passwords must meet the following complexity requirements: Contains characters from three of the following four categories: Uppercase alphabet characters (A–Z)Lowercase alphabet characters (a–z)Arabic numerals (0–9)Non-alphanumeric characters (for example, !$#,%)	R	C	
26	3	Authentication / Password Policy	7.1.5.1	Minimum password length shall be 8 characters or greater	R	C	
27	3	Authentication / Password Policy	7.1.5.1	Minimum password age shall be 3 days or greater	R	C	
28	3	Authentication / Password Policy	7.1.5.1	Maximum password age requirement 60 days or less	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
29	3	Authentication / Password Policy	7.1.5.1	Maximum password age **recommendation** 30 days	BP	No	Maximum password age is 60 days.
30	3	Authentication / Password Policy	7.1.5.1	If feasible, authentication schemes shall provide for password exchange in a format that cannot be captured and reused/replayed by unauthorized users to gain authenticated access, e.g., random password generating tokens or one-way encryption (also known as hashing) algorithms.	R	C	
31	3	Authentication / Password Policy	7.1.5.1	When using temporary passwords they shall be required to be changed upon initial login	R	C	
32	3	Authentication / Password Policy	7.1.5.1	Passwords should not be hard coded into automatic login sequences, scripts, source code and batch files, etc., unless required by business need and then only if protected by security software and/or physical locks on the workstation, and passwords are encrypted.	BP	C	
33	3	Authentication / Password Policy	7.1.5.1	Password construction should be complex enough to avoid use of passwords that are easily guessed, or otherwise left vulnerable to cracking or attack. Names, dictionary words, or combinations of words shall not be used; nor shall they contain substitutions of numbers for letters, e.g., s3cur1ty. Repeating numbers or sequential numbers shall also not be used	BP	CP	While required by policy, this requirement is not enforceable on all ESInet systems.
34	3	Authentication / Password Policy	7.1.5.1	Passwords should not contain sequences of three (3) or more characters from the user's login ID or the system name.	BP	CP	While required by policy, this requirement is not enforceable on all ESInet systems.
35	3	Authentication / Password Policy	7.1.5.1.4	Passwords should not contain sequences of three (3) or more characters from previous chosen or given passwords.	BP	CP	While required by policy, this requirement is not enforceable on all ESInet systems.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
36	3	Authentication / Password Policy	7.1.5.1.5	Passwords should not contain a sequence of two (2) or more characters more than once, e.g., a12x12.	BP	CP	While required by policy, this requirement is not enforceable on all ESInet systems.
37	3	Authentication / Password Policy	7.1.5.1.5	Passwords used to access Public Safety systems and resources should not be used on any external systems, e.g., Home PC's, Internet sites, shared public systems.	BP	C	
38	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used do they have a required length of at least 15 characters? (Audit Guidance: Alpha, numeric and special characters may all be used.)	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
39	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used they shall not use repeating words, or sequential characters or numbers.	R	N/A	The CenturyLink ESInet systems require password. They do not use passphrases.
40	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used they shall be case sensitive	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
41	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used and where they are automatically set or set by administrator, the initial passphrase shall be randomly generated and securely distributed.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
42	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used first-time users may create their own passphrase after authenticating.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
43	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used Users shall have the capability of changing their own passphrase online. However, the old passphrase shall be correctly entered before a change is allowed	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
44	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used a lost or forgotten passphrase can be reset only after verifying the identity of the user (or process owner) requesting a reset.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
45	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used passphrases shall automatically expire every 180 days or less for General Users.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
46	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used systems shall notify users at expiration time and allow the user to update the passphrase.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
47	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used and when it is changed, the old passphrase shall not be reused until either: 1. at least four (4) other passphrases have been used, or 2. at least 4 months have passed.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
48	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used systems shall not display the passphrase in clear text as the user enters it.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
49	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used shall not be stored in script files or function keys.	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
50	3	Authentication / Password Policy	7.1.5.2	When Passphrases are used Passphrases shall always be encrypted for transmission	R	N/A	The CenturyLink ESInet systems require passwords. They do not use passphrases.
51	3	Authentication / Password Policy	7.1.5.3	If Digital Certificates are used is a revocation procedure in place if compromised?	R	C	
52	3	Authentication / Password Policy	7.1.5.3	Are Digital Certificates kept current and expired or invalid certificates not used?	R	C	
53	3	Authentication / Password Policy	7.1.5.3	Cryptographic implementations use standard implementations of security applications, protocols, and format?	R	C	
54	3	Authentication / Password Policy	7.1.5.3	Cryptographic implementations shall be purchased from reputable vendors?	R	C	
55	3	Authentication / Password Policy	7.1.5.3	If Cryptographic solutions are developed in-house staff should be properly trained in cryptology.	R	C	
56	3	Authentication / Password Policy	7.1.5.3	Do employees protect and safeguard any encryption keys for which they are responsible?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
57	3	Authentication / Password Policy	7.1.5.3	Employees do not share private encryption keys with others except when applicable or appropriate authorities demand the key be surrendered (Termination, Promotion, Investigation etc.)	R	C	
58	3	Authentication / Password Policy	7.1.5.3	A process exists by which current validity of a certificate can be checked and a certificate can be revoked Validity testing includes: Do key holders initiate key revocation when they believe access to their keys have been compromised Has the Certificate Authority signature on the certificate been validated Is the date the certificate is being used within the validity period for the certificate The Certificate Revocation List for the certificates of that type are checked to ensure they have not been revoked The identity represented by the certificate - the "distinguished name" is valid (distinguished name refers to the location in the x.500 database where the object in question exists)	R	C	
59	3	Authentication / Password Policy	7.2.6	In order to help assure segregation of duties, developers shall not be System Administrators for the Production Systems they have developed (small, stand-alone systems can be excepted from this requirement)	R	C	
60	4	Data Protection	4.2	Does the organization have a Data Protection Policy?	R	C	
61	4	Data Protection	6.2	Application, system, and network administrators perform a security self-review on systems for which they have operational responsibility at least once per year.	R	C	
62	4	Data Protection	6.2	The self-review assessments are in writing and retained by the Security Manager and the NG9-1-1 Entity	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
63	4	Data Protection	6.2	A copy of the current security self-review or security assessments/audit reports are retained until superseded by another security assessment or the system is retired	R	C	
64	4	Data Protection	6.3	Application, system, and network administrators have identified which security solutions have or require periodic review and the frequency by which they shall occur (Auditor Guidance: This finding refers to recurring security solutions, such as audit logs, or Intrusion Prevention Systems.)	R	C	
65	4	Data Protection	6.3	Application, system, and network administrators conduct the periodic reviews defined in audit number 64	R	C	
66	4	Data Protection	6.4.2	All networks have a clearly defined purpose or mission so appropriate security measures can be implemented. (Auditor Guidance: To verify if this has occurred request documentation such as drawings, mission statements, policies, etc., that clearly indicate that the network in question's mission is defined)	BP	C	
67	4	Data Protection	6.4.3	For systems on the network in question, an accurate and current inventory is maintained. (Auditor Guidance: Request copies of a current inventory. Acceptable inventories included automated systems, paper logs, or logbooks).	R	C	
68	4	Data Protection	6.4.3	Inventories are appropriately classified and in accordance with the implemented information classification and protection policy	R	CP	A uniform data classification scheme is in the process of being implemented.
69	4	Data Protection	6.4.4	All administrative access to the network is precisely controlled with appropriate identification, authentication, and logging capabilities	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
70	4	Data Protection	6.4.4	Uncontrolled points of entry are not allowed on the network	R	C	
71	4	Data Protection	6.4.4	All point of ingress and egress to a network are fully documented, approved, and protected	R	C	
72	4	Data Protection	6.4.5	Connecting multi-homed computers to networks that have different security postures is not allowed	R	C	
73	4	Data Protection	6.4.5	When multi-homed computers are implemented Host IPS shall be installed on the multi-homed computer	R	N/A	No computers are multi-homed across security domains.
74	4	Data Protection	6.4.5	When multi-homed computers are implemented, all other appropriate security countermeasures, including those	R	N/A	No computers are multi-homed across security domains.
75	4	Data Protection	6.4.5	When multi-homed computers are implemented Anti-virus is running on both/all networks and the multi-	R	N/A	No computers are multi-homed across security domains.
76	4	Data Protection	6.4.5	When multi-homed computers are implemented, IP-forwarding is explicitly disabled?	R	N/A	No computers are multi-homed across security domains.
77	4	Data Protection	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Operating Systems'	BP	N/A	No computers are multi-homed across security domains.
78	4	Data Protection	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Applications'	BP	N/A	No computers are multi-homed across security domains.
79	4	Data Protection	6.4.6.3	Firewalls are maintained at all 4.9GHz network boundaries	R	C	
80	4	Data Protection	7.1.2.2	Does the organization have procedures for reviewing access authority for inactive accounts?	R	C	
81	4	Data Protection	7.2.1	Accounts shall be created based on "Least Privilege"	R	C	
82	4	Data Protection	7.2.1	Are users given access to only the functions and data necessary to perform their assigned duties	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
83	4	Data Protection	7.2.1	All computer resource access is restricted to only the command, data, and systems necessary to perform authorized functions	R	C	
84	4	Data Protection	7.2.1.1	All data has appropriate minimum access privileges, e.g. read, write, modify, as defined by the data owner and is in compliance with local laws	R	C	
85	4	Data Protection	7.2.1.2	Access is restricted to only those individuals and groups with a business need, and subject to the data's classification.	R	C	
86	4	Data Protection	7.2.1.2	Unrestricted/global access should be avoided whenever possible and is only used where specifically appropriate and with the data owners approval	BP	C	
87	4	Data Protection	7.2.1.2.a	Is an annual review of all resources, (e.g., files or directories, to which access is not restricted, i.e., have universal or public access) shall be performed and the resource owners shall be notified of the results.	R	C	
88	4	Data Protection	7.2.1.2.b	Is group membership restricted only to persons performing the given function?	R	C	
89	4	Data Protection	7.2.1.3	All unnecessary services and network services are disabled.	R	C	
90	4	Data Protection	7.2.1.3	Any application service which lets the user escape to a shell, provide access to critical system files, or maps/promotes IDs to privileged user levels is disabled.	R	C	
91	4	Data Protection	7.2.1.3a	Is an annual review for compliance with Audit Area 90 completed and findings documented?	R	CP	This section will be added to internal audit schedules.
92	4	Data Protection	7.2.1.3a	Are findings from the audit conducted in Audit Area 91 closed or has the risk been managed?	R	CP	Any findings will be tracked through existing nonconformance corrective action systems.
93	4	Data Protection	7.2.1.4	Administrator shall ensure that system access controls (e.g. filters that restrict access from only authorized source systems), are used where they exist and only contain necessary system authorizations?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
94	4	Data Protection	7.2.1.4.a	Is an annual review for compliance with Audit Area 93 completed and findings documented?	R	CP	This section will be added to internal audit schedules.
95	4	Data Protection	7.2.1.4.a	Are findings from the audit conducted in Audit Area 94 closed or has the risk been managed?	R	CP	Any findings will be tracked through existing nonconformance corrective action systems.
96	4	Data Protection	7.2.1.5	Do Administrators use non-Administrative accounts when performing non-Administrative tasks?	R	C	
97	4	Data Protection	7.2.1.6	Do ALL System Administrators have a personal Administrator account rather than use a generic account? (Auditor Guidance: Administrators shall not use default, or built-in Administrator accounts except during disaster recovery or initial installations. Each Administrator must have his or her own unique Administrator account to provide traceability. Administrator accounts shall never be shared)	R	C	
98	4	Data Protection	7.2.1.6	Systems that do not support unique administrative accounts should not be used as they pose a significant threat. Entities are encouraged to prevent inclusion of such systems onto the NG9-1-1 networks. .	BP	N/A	Users have unique identifiers and there will be no guest, shared, or anonymous accounts.
99	4	Data Protection	7.2.2	The login "Warning Notice" is displayed during the boot up or logon sequence (either before or after the authentication, preferably before, but it is displayed before any substantive data	R	C	
100	4	Data Protection	7.2.2	The "Warning Notice" remains displayed until positive action by the user is taken to acknowledge the message	R	C	
101	4	Data Protection	7.2.3	Computer resources, systems, applications, and networks shall be restricted at all times to authorized personnel	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
102	4	Data Protection	7.2.3	Where possible access control is accomplished with "role bases" privileges that assign users to roles and grant access to members of a role rather than to individuals	R	C	
103	4	Data Protection	7.2.4	Non-privileged users do not have read/write access to system files or resources such as protected memory, critical devices, executable programs, network configuration data, application file systems, etc.	R	C	
104	4	Data Protection	7.2.4	Only administrative users are assigned passwords to access and modify sensitive files/resources	R	C	
105	4	Data Protection	7.2.5	Files/File Folders are restricted to only those requiring access	R	C	
106	4	Data Protection	7.2.5	Rights assigned only to those who actually need them and are documented as needing them	R	C	
107	4	Data Protection	7.2.5	Access Groups used whenever possible to simplify administration	R	C	
108	4	Data Protection	7.2.5	Has the organization renamed built-in Administrator accounts?	R	C	
109	4	Data Protection	7.2.5	Anonymous and/or guest accounts are disabled to prevent exploitation	R	C	
110	4	Data Protection	7.2.5	Are periodic audits of user account access conducted to ensure users have only the "effective rights" required to perform their functions?	R	C	
111	4	Data Protection	7.2.6	Are Production and Non-Production systems separated to protect integrity of the Production System?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
112	4	Data Protection	7.2.6	If the Non-Production System is intended to become a Production System is it governed by the requirements of a Production System. (Auditor Guidance: While it is unlikely a non-production system will be “in-scope” during an audit, if it is, this requirement refers to the need for that system to comply with all requirements herein)	R	C	
113	4	Data Protection	7.2.6	Production data is not copied off the system without the service owner's permission and is protected to an equivalent or greater degree	R	C	
114	4	Data Protection	7.2.6	Production systems do not contain any software development tools except where essential for the application	R	C	
115	4	Data Protection	7.2.6	While software development tools may be installed for software upgrades, or installation of new software packages, or for troubleshooting, but they must be removed immediately after use	R	CP	Some software development tools are required and installed on production systems.
116	4	Data Protection	7.2.6	When software development tools are essential for production operation, they must be inaccessible to users	R	CP	Some software development tools are required and installed on production systems.
117	4	Data Protection	7.2.7	All devices capable of enforcing a password protected screensaver or a keyboard lock do so with an inactivity timeout of 15 minutes or less exceptions will comply with Para 7.2.7.1, .2,and .3 The following are exceptions: When superseded by local public safety policy	R	C	
118	4	Data Protection	7.2.7	All devices not capable of enforcing a password protected screensaver or a keyboard lock will have controlled access in accordance with all applicable physical and logistical security or have session inactivity timeouts set for 15 minutes	R	C	
119	4	Data Protection	7.2.7	Consoles not capable of enforcing a password protected screensaver or a keyboard lock are configured to automatically log out after 15 minutes of inactivity	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
120	4	Data Protection	7.2.7	If automatic inactivity logout is not supported are users required to logout when console is left unattended	R	C	
121	4	Data Protection	7.2.8.4	Peer to Peer Networking is NOT allowed in the NG 9-1-1 environment	R	C	
122	4	Data Protection	7.3.1	NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	C	
123	4	Data Protection	7.3.1	Specific guidelines must be written and followed to document what data is released, when and to whom when releasing NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	C	
124	4	Data Protection	7.3.1	The guidelines identified in Audit Area 123 shall capture any specific release requirements for data such as video, names, call content, message text, or other personal content	R	C	
125	4	Data Protection	7.3.1	Where such data is intermingled with other data of differing classification, consideration shall be given to replicating the public domain data into a separate data store	BP	C	
126	4	Data Protection	7.3.2	Where email is used to send NG 9-1-1 Sensitive Information, is the message clearly marked with its classification, do the senders ensure recipients are aware of the safeguards required.	R	C	
127	4	Data Protection	7.3.2	Where email is used for emergency communications, senders must verify the recipient's email ID is correct prior to sending	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
128	4	Data Protection	7.3.2	Where email is used for emergency communications, the recipient shall understand the safeguards associated with the proprietary marking	R	C	
129	4	Data Protection	7.3.2	Where email is used for emergency communications and email with Sensitive Information is printed it shall be protected according to the rules associated with its	R	C	
130	4	Data Protection	7.3.2	Where email is used for emergency communications, Sensitive Information must be encrypted when sent by email	R	CP	Encryption of restricted data when being sent across public networks.
131	4	Data Protection	7.3.2	Does the NG9-1-1 entity control the domain used for email communication unless otherwise covered by a formal contractual document. (Auditor Guidance: The intent of this audit question is to ensure that entities register a legitimate DNS domain name for any NG9-1-1	R	C	
132	4	Data Protection	7.3.2	Internal NG9-1-1 Entity email should not be made available on a 9-1-1 call-taking position workstation, but rather on a separate system.	BP	CP	In rare cases the West SFS Emergency Call RelayCenter may support calls that personnel have email on the same machine used for receiving emergency calls, however this does not directly impact service provide through the ESInet.
133	4	Data Protection	7.3.2	In lieu of detailed security standards for email use in an NG9-1-1 environment, NG9-1-1 Entities are encouraged to follow best practices such as those offered by the National Institute for Standards and Technology (NIST)	BP	N/A	We have and use detailed corporate security standards.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
134	4	Data Protection	7.3.2.1	Individual messaging services have been evaluated to ensure they comply with NG9-1-1 Entity production and security requirements	R	C	
135	4	Data Protection	7.3.3.1	Do cryptographic installations use industry standard cryptographic algorithms and standard modes of operations and comply with the laws of the United States	R	C	Information Security defines security requirements for the configuration of key servers, Public Key Infrastructures and related equipment. Information Security will also set standards for encryption algorithms, hashes, key lengths, key lifetimes, and other factors relevant to encryption practices. The user of proprietary encryption algorithms, either in-house or from Suppliers/Contributors of freeware/shareware is not permitted.
136	4	Data Protection	7.3.3.1	The use of encryption algorithm or device complies with the laws of the United States and any country in which there are plans to use data encryption	R	C	The use of proprietary encryption algorithms, either in-house or from Suppliers/Contributors of freeware/shareware is not permitted.
137	4	Data Protection	7.3.3.1	It is recommended the algorithm certified by the NIST FIPS 140 certification, currently AES, be used	BP	C	
138	4	Data Protection	7.3.3.1	Where there are no US federal standards for specific encryption functions e.g. public key cryptography, message digests, commercial algorithms may be used.	BP	C	A list of acceptable encryption standards are included in Security Policy.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
139	4	Data Protection	7.3.3.1	Implementations of cryptography shall follow best commercial practices e.g. Public Key Cryptography Standards.	R	C	Information Security defines security requirements for the configuration of key servers, Public Key Infrastructures and related equipment. Information Security will also set standards for encryption algorithms, hashes, key lengths, key lifetimes, and other factors relevant to encryption practices. The user of proprietary encryption algorithms, either in-house or from Suppliers/Contributors of freeware/shareware is not permitted.
140	4	Data Protection	7.3.3.1	Implementations and modes shall use the strongest available product (encryption algorithms)	R	C	
141	4	Data Protection	7.3.3.2	If Public Key Cryptography is used does the NG9-1-1 entity have a Public Key Infrastructure to manage and distribute public keys?	R	C	
142	4	Data Protection	7.3.3.2	Does the PKI manage both Symmetric and Asymmetric Keys through the entire life cycle?	R	CP	Separate PKIs for management of symmetric and asymmetric.
143	4	Data Protection	7.3.3.2	Encryption Devices and any server used to store encryption keys are protected from unauthorized access	R	C	
144	4	Data Protection	7.3.3.2	Key generation is performed using a commercial tool that comply with x.509 standards and produce x.509 compliant keys.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
145	4	Data Protection	7.3.3.2	Keys are not generated using predictable function or values	R	C	
146	4	Data Protection	7.3.3.2	Symmetric keys must be at least 112 bits in length and Asymmetric keys at least 1024 bits in length	R	C	
147	4	Data Protection	7.3.3.2	Keys are distributed to appropriate recipients through secure channels	R	C	
148	4	Data Protection	7.3.3.2	Keys used to secure stored data are safeguarded so authorized persons can recover them at any time	R	C	
149	4	Data Protection	7.3.3.3	Does the Public Key Infrastructure (PKI) have a documented Certificate Practice Statement defining how security is provided for the infrastructure, registration process, relative strength of the system, and Legitimate uses?	R	C	
150	4	Data Protection	7.3.3.3	Does the PKI implement a registration process that identifies the requester by an acceptable form of identification before the Certificate Authority (CA) creates a Digital Certificate?	R	C	
151	4	Data Protection	7.3.3.3	Does the PKI have a review process for validity checks and revocation as required?	R	C	
152	4	Data Protection	7.3.3.3	Do key holders initiate key revocation if they believe access to their keys have been compromised?	R	C	
153	4	Data Protection	7.4.1	Are all files and software scanned for viruses and malicious code, and verified as free of logic bombs or other malicious code?	R	C	
154	4	Data Protection	7.4.3	Does the NG 9-1-1 entity use licensed industry standard antivirus (or anti-malware) software on all devices capable of running it?	R	CP	AV software is loaded on all Window devices and Linux servers that are publically accessibility.
155	4	Data Protection	7.4.3	Does the NG 9-1-1 entity, install and maintain the latest version (including engine) of their licensed anti-virus	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
156	4	Data Protection	7.4.3	Is the antivirus software installed and maintained on any personal equipment used for business functions?	R	N/A	Personal equipment is not used for business functions.
157	4	Data Protection	7.4.3	Is the software current with the latest available and applicable virus definitions?	R	C	
158	4	Data Protection	7.4.3	Does the software scan all files when opened and/or executed (including files on network shares)?	R	CP	Scans are performed on all files that do not impact call processing performance.
159	4	Data Protection	7.4.3	Does the software scan files on local drives at least once a week?	R	C	
160	4	Data Protection	7.4.3	Does the software scan all files, attachments, and software received via email and/or downloaded from websites before opening?	R	C	
161	4	Data Protection	7.4.3	Does the software scan all removable media and software (including new workstations equipped with pre-loaded software) before opening and/or executing?	R	CP	Removable media is not scanned when it is plugged in. A scan is performed if the user attempts to open a file or if a file attempts to auto-execute
162	4	Data Protection	7.4.3	Does the NG 9-1-1 Entity scan all removable media and software before opening and/or executing if it has not been kept secure within its control?	R	C	
163	4	Data Protection	7.4.3	Are all files made available as network shares scanned at least once per week?	R	CP	A scan is performed when a file is opened. Servers that are hosts on are scanned once per week.
164	4	Data Protection	7.5.4	Does the NG 9-1-1 Entity have a backup procedure?	R	C	
165	4	Data Protection	7.5.4	Is a copy of the routine full backup media described in Audit Area 164 sent to a secure offsite location?	R	C	
166	4	Data Protection	7.6	All systems, applications, and databases have internal controls for logging, tracking, and personnel accountability	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
167	4	Data Protection	7.6.1	All systems, including but not limited to applications and databases, have a security event record(log) capable for after-the-fact investigation of loss, impropriety, or other inappropriate activity	R	C	
168	4	Data Protection	7.6.2	A written Security Audit Log Review Plan has been developed	R	C	
169	4	Data Protection	7.6.3	A Security Alarm Plan has been developed and documented which sets criteria for generating alarms, who is notified, and what actions are to be taken.	R	C	
170	4	Data Protection	8.3	Sensitive data is printed only on attended printers or on printers in a secured area. Distribution is controlled and printouts of sensitive information are secured when not in use.	R	C	
171	4	Data Protection	8.3	Data stored on removable media that are external to the system hardware is safeguarded.	R	C	
172	4	Data Protection	8.3	Personal storage devices are not used within the NG9-1-1 entity location. (Auditor Guidance: Examples of personal storage devices include USB Thumbstick, etc.)	R	C	
173	4	Data Protection	8.3	When storage media and output is destroyed it is in a manner that contents cannot be recovered or recreated	R	C	
174	4	Data Protection	8.3	When producing copies containing classified, the originals and copies are not left unattended	R	C	
175	4	Data Protection	8.3	NG9-1-1 Entity personnel ensure re-used storage media is "clean" (i.e. does not contain any residual of information from previous uses)	R	C	
176	4	Data Protection	8.3	All media distributed outside NG9-1-1 Entity is either new or comes directly from a recognized pool of "Clean" media	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
177	4	Data Protection	8.4.2	If possible, information resources using a power supply are connected to electrical outlets and communications connections that utilize surge protection	BP	C	
178	4	Data Protection	8.6.2.10	Combustible materials are not stored in the computer center or server room	R	C	
179	4	Data Protection	8.6.2.11	Furniture, storage cabinets, and carpets are of nonflammable material.	R	C	
180	4	Data Protection	8.6.2.12	Carpets are anti-static.	R	C	
181	4	Data Protection	8.6.2.6	All critical information resources are on UPS	R	C	
182	4	Data Protection	8.6.2.7&.8	Food, drinks, or smoking is not allowed in the server room	R	C	
183	4	Data Protection	8.6.2.9	Storage under raised floors or suspended ceilings is prohibited.	R	C	
184	5	Exception Request / Risk Assessment	12	An Exception Approval / Risk Assessment process is in place.	R	C	
185	5	Exception Request / Risk Assessment	12	The exception approval and risk acceptance process includes Risk Justification, Risk Identification, Risk Assessment, Risk analysis, and Risk Acceptance and Approval.	R	C	
186	5	Exception Request / Risk Assessment	12	The exception approval and risk acceptance process is documented on each Exception Approval / Risk Acceptance Form (EA/RAF), including the names and contact information of the people who carried out the analysis.	R	C	
187	5	Exception Request / Risk Assessment	12.1	The EA/RAF process is followed for "ALL RISKS" (e.g., security vulnerabilities cannot be fixed or security patched, or cases of non-compliance with this Security Standard.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
188	5	Exception Request / Risk Assessment	12.1	The specific non-compliance or vulnerability documented in each EA/RAF was reviewed by NG9-1-1 Entity security organization and the legal department.	R	C	
189	5	Exception Request / Risk Assessment	12.1	The actual form is maintained and tracked by the NG9-1-1 Entity Security Risk Manager, the Security Point of Contact, and all involved parties.	R	C	
190	5	Exception Request / Risk Assessment	12.2.1	The NG9-1-1 Entity has assigned a Security Risk Manager to manage security risks and is responsible for completing the EA/RAF in a complete and accurate manner prior to submitting to the Security Point of Contact / Team for review.	R	C	
191	5	Exception Request / Risk Assessment	12.2.1	The Security Risk Manager collaborates with other members of the pertinent security team in completing the form and obtains the approval signature from the NG9-1-Entity Risk Acceptance Approver.	R	C	
192	5	Exception Request / Risk Assessment	12.2.1	The Security Risk Manager is an employee or an authorized agent acting on behalf of the NG9-1-1 Entity.	R	C	
193	5	Exception Request / Risk Assessment	12.2.1	The Security Risk Manager is the person identifying the need for the execution of the exception approval and risk acceptance process with technical and business knowledge of the asset(s) at risk or, meets 195	R	C	
194	5	Exception Request / Risk Assessment	12.2.1	The Security Risk Manager is a system administrator, systems engineer, project manager, or other key stakeholder with technical and business knowledge of the asset(s) at risk.	R	C	
195	5	Exception Request / Risk Assessment	12.2.1	The Security Risk Manager acts as Point of Contact for the organization owning the identified asset(s) at risk within the scope of the exception approval and risk assessment process for the duration of the EA/RAF	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
196	5	Exception Request / Risk Assessment	12.2.1	If the Security Risk Manager leaves the entity or is changes job during the active duration of the EA/RAF, a new Security Risk Manager is identified to fill the role	R	C	
197	5	Exception Request / Risk Assessment	12.2.2	A Security Point of Contact / Team is assigned to review for completeness, accuracy, and consistency and subject matter expertise.	R	C	
198	5	Exception Request / Risk Assessment	12.2.2	For high level risks, a team of Subject Matter Experts (SME) is assembled to review, document concurrence, and sign the EA /RAF prior to submission for final approval.	R	C	
199	5	Exception Request / Risk Assessment	12.2.3	Has the senior official of the NG9-1-1 Entity has signed forms accepting complete accountability for any identified risk?	R	C	
200	5	Exception Request / Risk Assessment	12.3	Risks to the NG9-1-1 Entity are acknowledged, assessed, and managed according to their severity.	R	C	
201	5	Exception Request / Risk Assessment	12.3	Responsibility is not delegated to subordinates or peers, and adheres to the management level or higher.	R	C	
202	5	Exception Request / Risk Assessment	12.3	The Risk Acceptance Approver is the senior manager with financial and legal responsibilities for the services and operation of the specific NG9-1-1 Entity.	R	C	
203	5	Exception Request / Risk Assessment	12.3.1	The NG9-1-1 entity manages the process flow as noted below: 1. The NG9-1-1 Entity's Security Risk Manager identifies, justifies, assesses, and analyzes the risk. If the identification and/or analysis of the risk prove to be difficult, then a security team shall be contacted for assistance.	R	C	
204	5	Exception Request / Risk Assessment	12.3.2	The entity tracks and documents risks in accordance with the chart provided in Appendix A.	R	N/A	Timelines allow for thorough regression and interoperability testing before applying a patch to the production network.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
205	5	Exception Request / Risk Assessment	12.4	Risk assessments are reviewed periodically in compliance with the following timeframes: Critical 0 Months High 3 Months	R	C	
206	5	Exception Request / Risk Assessment	12.5	Any change to the circumstances identified in the EA/RAF that affect the associated risk is immediately documented and submitted through the EA/RAF process.	R	C	
207	5	Exception Request / Risk Assessment	12.6.1-.3	When conducting risk assessments, vulnerability assessments, and impact assessments they should be conducted using the guidance provided in sections 12.6	BP	CP	The majority of the section and field content are included.
208	5	Exception Request / Risk Assessment	12.6.8	The EA/RAF should comply with the requirements of Para 12.6.8.	BP	CP	The majority of the section and field content are included.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
209	6	Hiring Practices	4.2	Does the organization have a Hiring Practice Policy?	R	C	
210	7	Incidence Response	13 & 4.2	Has a formal, written Incident Response Plan detailing how the organization will respond to a computer security incident been created?	R	C	
211	7	Incidence Response	7.2.6	Are software and/or data changes initiated due to outage/recovery process documented and retained until it is determined the production system and data were not corrupted?	R	C	
212	7	Incidence Response	7.5.5	Have Business Continuity/Disaster Recovery (BC/DR) procedures been developed and tested?	R	C	
213	7	Incidence Response	7.5.5	Do the plans allow for the 'Worst Case' event (i.e. Incident Recovery outside 50 miles from normal location)?	R	C	
214	7	Incidence Response	7.5.5	Are BC/DR drills conducted at least annually?	R	C	
215	8	Information Classification and Protection	5	Does the organization have an Information Classification and Protection Policy that encompasses both administrative and production systems?	BP	C	
216	8	Information Classification and Protection	5.10.1	Does the organization have disposal procedures for hard copy or printed sensitive data?	BP	C	
217	8	Information Classification and Protection	5.10.2	Does the organization have sanitation procedures for media/devices containing sensitive data?	BP	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
218	8	Information Classification and Protection	5.2.1	Have Data **Owner** responsibilities been defined?	BP	C	
219	8	Information Classification and Protection	5.2.2	Have Data **Custodian** responsibilities been defined?	BP	C	
220	8	Information Classification and Protection	5.2.3	Are Data Classifications defined and used?	BP	C	
221	8	Information Classification and Protection	5.4.6	Is sensitive data received from a third party treated as if it were internal sensitive data?	BP	C	
222	8	Information Classification and Protection	5.5	When receiving information where the classification of information is unknown, does the organization treat it as Sensitive (Internal Use Only) until the proper classification is determined or it is determined to be Public Information by the originator or other applicable laws and regulations?	BP	C	
223	8	Information Classification and Protection	5.6	Does the organization protect classified information from unauthorized access?	BP	CP	Classification is not currently used in making access decisions, however, access to specific datasets is restricted to vetted employees and/or contractors.
224	8	Information Classification and Protection	5.7	Does the organization encrypt stored or transmitted classified information using AES Encryption Algorithm?	BP	CP	Encryption is not used in protected trust zones in all cases.
225	8	Information Classification and Protection	5.7	Does the organization have a policy for removing Mobile Computing Devices with classified data from the NG9-1-1 Entity?	BP	C	
226	8	Information Classification and Protection	5.8	Does the entity utilize recorded/certified delivery for transporting sensitive data or media/devices containing sensitive data?	BP	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
227	9	Physical Security	4.2	Does the organization have a Physical Security Policy?	R	C	
228	9	Physical Security	6.5	Does the Public Safety entity require annual Security Awareness Training?	R	C	
229	9	Physical Security	6.5	Have all Public Safety employees completed the annual Security Awareness Training?	R	C	
230	9	Physical Security	6.6	Does the entity have procedures for reporting any suspicious or unusual activity which may indicate an attempt to breach the Public Safety networks and systems?	R	C	
231	9	Physical Security	8	Is the entity is physically secured and protected from theft, misappropriation, misuse, and unauthorized access, and damage?	R	C	
232	9	Physical Security	8.1	Doors with security mechanisms shall not be propped open.	R	C	
233	9	Physical Security	8.1	Employees, suppliers, contractors and agents authorized to enter a controlled physical access area shall not allow unidentified, unauthorized or unknown persons to follow them through a controlled access area entrance.	R	C	
234	9	Physical Security	8.1	Each person entering a controlled access facility shall follow the physical access control procedures in place for that facility.	R	C	
235	9	Physical Security	8.1	Personnel shall be vigilant while inside the building and challenge and/or report unidentified persons including persons not displaying identification badges who have gained access.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
236	9	Physical Security	8.1	When automated access control and logging devices are installed, personnel shall use them to record their entry and exit.	R	C	
237	9	Physical Security	8.2.1	Personnel authorized with reoccurring unescorted access do not loan or share physical access devices or codes with another person?	R	C	
238	9	Physical Security	8.2.1.1	Non-employees granted reoccurring access are sponsored by NG9-1-1 management personnel?	R	C	
239	9	Physical Security	8.2.1.1	Does the facility's Physical Security Policy comply with all federal, state, and local laws?	R	C	
240	9	Physical Security	8.2.1.2	Identification badges containing a picture of the holder shall be issued to all residents of buildings containing information resources.	R	C	
241	9	Physical Security	8.2.1.2	Are ID Badges with picture issued to all residents of buildings containing information resources	R	C	
242	9	Physical Security	8.2.1.2	If the facility is guarded, identification badge is displayed to the guard on entry?	R	C	
243	9	Physical Security	8.2.1.2	Are persons on NG9-1-1 Entity premises required to present identification badges for examination and/or validation upon request?	R	C	
244	9	Physical Security	8.2.1.2	Building residents and non-residents with reoccurring access who do not have a valid identification badge in their possession are signed in and vouched for by an authorized building resident who possesses and displays a valid picture identification badge?	R	C	
245	9	Physical Security	8.2.1.2	Are temporary identification badge issued to all persons who do not have a permanent identification badge when entering the facility?	R	C	
246	9	Physical Security	8.2.1.2	Are persons who do not have a permanent identification badge escorted while in the facility?	R	C	
247	9	Physical Security	8.4.1	All portable computing devices in work areas are kept physically secure?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
248	9	Physical Security	8.4.1	When equipped with locks, portable computing devices are kept locked to prevent theft.	R	C	
249	9	Physical Security	8.4.1	Keys are stored in a secure location	R	C	
250	9	Physical Security	8.4.1	Docking station style portable devices are stored in a secure location when not in use.	R	C	
251	9	Physical Security	8.4.1	Docking station style portable devices are not left unattended outside normal working hours even when in the docking station	R	C	
252	9	Physical Security	8.4.1	Other portable devices are stored in a locked cabinet, drawer, or office (not just the building) when not in use	R	C	
253	9	Physical Security	8.4.1	Extra security precautions are implemented in and around the receiving, staging, assembly, and storage areas used for large deployments of portable computing devices	R	C	
254	9	Physical Security	8.4.2	Vigilance is maintained in airport luggage inspection and transfer areas, hotel check in and checkout areas and other public areas	R	C	
255	9	Physical Security	8.4.2	Devices are not left unattended in conference rooms, etc.	R	C	
256	9	Physical Security	8.4.2	Devices are not exposed to extreme heat or cold.	R	C	
257	9	Physical Security	8.5	Information resources are protected by a UPS system and/or a 'mirrored site' second location not subject to the same power outage.	R	C	
258	9	Physical Security	8.5	All buildings and critical support facilities have protective physical measures in place.	R	C	
259	9	Physical Security	8.6.1	Server Rooms, Data Centers, Wire Closets, and any other critical locations have limited and controlled access 24/7/365.	R	C	
260	9	Physical Security	8.6.1	Raised floors or suspended ceilings do not allow physical access to limited access areas.	R	C	
261	9	Physical Security	8.6.2.1	The facility has a fire protection/detection system which meets code and is maintained and inspected at regular intervals.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
262	9	Physical Security	8.6.2.2	If sprinkler systems are provided, fire retardant polyethylene sheeting is readily available to protect media and equipment.	R	CP	The ESInet complies for media. In some locations there are dry pipe water-based sprinkler systems and the area is too large to cover with sheeting. The ESInet has multiple redundant sites that immediately support call processing when one physical location is compromised.
263	9	Physical Security	8.6.2.4	Cooling equipment is installed and in good working order.	R	C	
264	9	Physical Security	8.6.2.5	HVAC systems are used to maintain environmental conditions meeting manufacturer's requirements and are supported by backup power systems dedicated.	R	C	
265	9	Physical Security	8.7.1	Network equipment and access to cabling and physical wiring infrastructure are secured with appropriate physical access controls.	R	C	
266	9	Physical Security	8.7.2	Active network jacks and connections are located only in physically secured locations (i.e., entity owned or leased space, in locked cabinets, or protected by locked physical barriers).	R	C	
267	9	Physical Security	8.7.3	Unused network connections are disabled or removed in a timely manner.	R	C	
268	9	Physical Security	8.7.4	Network Media are selected and located so as to minimize the possibility of wiretapping, eavesdropping, or tampering.	R	C	
269	10	Compliance Audits and Reviews	11	Internal audits are, at minimum, conducted annually.	R	C	
270	10	Compliance Audits and Reviews	11	Findings from such assessments are subject to corrective actions and are applied to the satisfaction of the auditing entity.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
271	10	Compliance Audits and Reviews	11	External security audits are conducted at a minimum, once every 3 years	R	C	
272	10	Compliance Audits and Reviews	11	Security audits utilize various methods to assess the security of networks and processes, applications, services, and platforms. Suggested methods include automated tools, checklists, documentation review, penetration testing, and interviews	R	C	
273	11	Network / Firewall / Remote Access	7.2.8.1	Before deployment of new forms of communication, a risk assessment should be conducted in accordance with: The impact of resource availability	BP	C	
274	11	Network / Firewall / Remote Access	4.2	Does the organization have a Remote Access Policy?	R	C	
275	11	Network / Firewall / Remote Access	9	No remote access is permitted to any NG9-1-1 Entity unless addressed by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional?	R	C	
276	11	Network / Firewall / Remote Access	9.1	Networks are segmented by business and technical functions to allow appropriate levels of protection be created while not placing unneeded restrictions on lesser risk areas	R	C	
277	11	Network / Firewall / Remote Access	9.1	All boundaries and points of ingress and egress are clearly defined for each network?	R	C	
278	11	Network / Firewall / Remote Access	9.1.1	Firewalls have been established at all boundary points to control traffic in and out.	R	C	
279	11	Network / Firewall / Remote Access	9.1.1	Firewalls use "fail all" as default?	R	C	
280	11	Network / Firewall / Remote Access	9.1.1	Application Layer Firewalls are in use (recommended)	BP	C	
281	11	Network / Firewall / Remote Access	9.1.10	Firewall logs are retained in accordance with applicable information retention requirements?	R	C	
282	11	Network / Firewall / Remote Access	9.1.10	Logs are replicated off of the firewall?	BP	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
283	11	Network / Firewall / Remote Access	9.1.11	Identification, authentication, and access rights to log data are controlled to preserve the chain of custody for evidentiary purposes?	R	C	
284	11	Network / Firewall / Remote Access	9.1.2	Access through firewalls is governed by an established policy defining clear guidelines for what is or will be allowed?	R	C	
285	11	Network / Firewall / Remote Access	9.1.3	At a minimum, restriction of source and destination IP addresses are specific to individual addresses?	R	C	
286	11	Network / Firewall / Remote Access	9.1.3	The security risks for every host or platform within the network range or subnet are evaluated?	R	C	
287	11	Network / Firewall / Remote Access	9.1.4	The Firewall Administrator has minimized the number of ports exposed or permitted though the firewall? Clarifying note: the firewall administrator should be employing the least-access necessary privilege to ensure that only the necessary ports required for operation are permitted through the firewall.	R	C	
288	11	Network / Firewall / Remote Access	9.1.5	All Firewall Administrators are highly qualified and experienced and have an in depth knowledge and/or experience in firewall support and management, various operating systems including application and operating system protocols (ports and sockets), networking, routing, LAN/WAN technologies and associated security implications? (Auditor Guidance: Qualifications considered are, industry and or vendor certifications with various firewall products)	R	C	
289	11	Network / Firewall / Remote Access	9.1.6	Is the use of ports used by the operating system or infrastructure functions and features across network boundaries strictly controlled at the firewall?	R	C	
290	11	Network / Firewall / Remote Access	9.1.7	Firewall rules are reviewed at least once per year to verify continued need?	R	C	
291	11	Network / Firewall / Remote Access	9.1.8	Firewalls are accessed at least annually to address vulnerabilities identified since the last inspection?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
292	11	Network / Firewall / Remote Access	9.1.9	All firewalls must log traffic with at minimum, source and destination addresses and ports are captured along with relevant time stamps and actions by the firewall.	R	C	
293	11	Network / Firewall / Remote Access	9.2	No remote access is allowed to any NG9-1-1 Entity unless addresses by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional	R	C	
294	11	Network / Firewall / Remote Access	9.2.1	Client based VPNs and/or consolidated modem pools are operated by NG9-1-1 Entity security personnel or personnel contracted for the purpose.	R	C	
295	11	Network / Firewall / Remote Access	9.2.1	Strict control is maintained for the VPN and/or consolidated modem infrastructures as they enable access to the NG9-1-1 Entity from public networks such as the Internet or public switched telephone network	R	C	
296	11	Network / Firewall / Remote Access	9.2.1	All client based VPNs utilize industry standard technologies.	R	C	
297	11	Network / Firewall / Remote Access	9.2.1	All client based VPNs and/or consolidated modem pools access utilize strong authentication which includes single use passwords.	R	C	
298	11	Network / Firewall / Remote Access	9.2.1	All client based VPNs and/or consolidated modem pools access are controlled by a Firewall.	R	C	
299	11	Network / Firewall / Remote Access	9.2.1	All client based VPNs and/or consolidated modem pools access are logged.	R	C	
300	11	Network / Firewall / Remote Access	9.2.2	If directly attached modems are used, have they been approved using the exception methodology in Section 12?	R	N/A	Modems are not used with the ESInet service.
301	11	Network / Firewall / Remote Access	9.2.2	Directly attached modems utilize industry standard third party authentication schema.	R	N/A	Modems are not used with the ESInet service.
302	11	Network / Firewall / Remote Access	9.2.2	Use of only 'secured modems' is permitted. Uncontrolled use of modems can result in serious vulnerabilities and shall use risk mitigation measures	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
303	11	Network / Firewall / Remote Access	9.2.2	When such modems are utilized through approved exception, they meet all criteria established for client based VPN or consolidated modem pools. Including firewall access controls and single use passwords.	R	N/A	Modems are not used with the ESInet service.
304	11	Network / Firewall / Remote Access	9.2.2	An accurate inventory of directly attached modems is maintained.	R	C	
305	11	Network / Firewall / Remote Access	9.2.2	Other modem technologies which shall be considered include "dial/dial back", only when primary access means is down or attached only to devices which have strong authentication mechanisms.	R	C	
306	11	Network / Firewall / Remote Access	9.2.2	The use of modems which are directly attached to servers, routers, switches, or other such equipment is strongly discouraged and should be prohibited by default	BP	C	
307	11	Network / Firewall / Remote Access	9.3.1	When using private facility networks such as T1, DS-2, etc., whenever possible the network technologies should be always considered in lieu of communications over public transport	BP	C	
308	11	Network / Firewall / Remote Access	9.3.1	Organizations should evaluate the importance of the data traversing the network and determine if encryption is appropriate to meet the necessary privacy levels (note: Use of these network technologies does not necessarily preclude the need for end to end encryption)	BP	C	
309	11	Network / Firewall / Remote Access	9.3.2	Communications over the Internet must be encrypted using IPSEC or SSL.	R	C	
310	11	Network / Firewall / Remote Access	9.3.2	If using endpoint authentication it has been implemented using either certificates or similar credentials.	R	C	
311	11	Network / Firewall / Remote Access	9.3.2	When using Internet protocols, industry standard protocols are to be used with minimum key length of 128 bit.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
312	11	Network / Firewall / Remote Access	9.3.3	When external connections are clearly identified as un-trusted, a firewall must be utilized to control communication between the external endpoint or network and the NG9-1-1 environment.	R	C	
313	11	Network / Firewall / Remote Access	9.3.4	When applications require access from external, public transport (i.e. Internet) they have been placed on a DMZ or employ network based encryption and authentication.	R	C	
314	11	Network / Firewall / Remote Access	9.4	When using Intrusion Detection / Prevention technologies they shall be positioned on internal networks at strategic locations. Note: use of IPS/IDS is not mandatory.	R	C	
315	11	Network / Firewall / Remote Access	9.4	When using Intrusion Detection / Prevention technologies, their signatures must be routinely updated with processes that include well defined schedules for signature updates and emergency update protocols for high risk and zero day events.	R	C	
316	11	Network / Firewall / Remote Access	9.5	When used, technologies such as VLAN, VRF, or VPN are classified as required in section 9.3 and once classified they are treated as separate networks.	R	C	
317	11	Network / Firewall / Remote Access	9.5	All support equipment for virtual or logical networks shall have a management tunnel for support and monitoring.	R	C	
318	11	Network / Firewall / Remote Access	9.5	All support equipment for virtual or logical networks limits user group access to the particular virtual facilities when possible.	R	C	
319	11	Network / Firewall / Remote Access	9.5	Commands (like Telnet), which allow direct access between virtual facilities, are disabled or is only allowed under the highest administrative privilege supported by the device.	R	C	
320	11	Network / Firewall / Remote Access	9.5	Layer 3 interactions between networks of differing security classifications are only done using a firewall or similar device.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
321	11	Network / Firewall / Remote Access	9.5	User access to devices supporting multiple virtual networks should utilize an industry standard authentication and access control protocol such as TACACS or RADIUS.	BP	CP	Local authentication must be available as a fallback.
322	12	Security Enhancement Technical Upgrade	4.2	Does the organization have a Security Enhancement/Technology Upgrade Policy?	R	C	
323	12	Security Enhancement Technical Upgrade	6.7	Do the design, development, administration, and use of any computer resource, network, system, or application always enable compliance with security policies and requirements to its intended use?	R	C	
324	12	Security Enhancement Technical Upgrade	6.7	Is incorporating security into new products, services, systems, and networks before they are deployed a priority?	R	C	
325	12	Security Enhancement Technical Upgrade	6.7	Is a security assessment of controls and procedures conducted and documented before deployment to certify compliance with security policy and is this document retained as evidence for any future audit?	R	C	
326	12	Security Enhancement Technical Upgrade	7.2.8	Is a full business and security assessment conducted for any new form of communications prior to it being connected to the NG 9-1-1 environment?	R	C	
327	12	Security Enhancement Technical Upgrade	7.2.8.2	Are communication partners and the full scope of products subjected to full risk assessment?	BP	CP	A risk assessment is performed to the fullest extent possible.
328	12	Security Enhancement Technical Upgrade	7.2.8.3.1	Are Client Software Add-ons ("plug ins") assessed for security risks?	R	CP	A level of testing is performed, as practical. Ability of users to install software and plug-ins is limited due to local admin right restrictions.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
329	12	Security Enhancement Technical Upgrade	7.2.8.3.1	Is client software configured to disallow auto installation of software add-on or plug-ins?	R	C	
330	12	Security Enhancement Technical Upgrade	7.2.8.3.1	Are new add-ons or plug-ins tested prior to installation?	R	CP	A level of testing is performed, as practical. Ability of users to install software and plug-ins is limited due to local admin right restrictions.
331	12	Security Enhancement Technical Upgrade	7.2.8.5	If the NG 9-1-1 Entity uses a VoIP system it does not connect to another VoIP System without securing the connection?	R	C	
332	12	Security Enhancement Technical Upgrade	9.6.1	Network **redundancy** is considered and implemented where possible for On-Site / Local High Availability environments.	R	C	
333	12	Security Enhancement Technical Upgrade	9.6.2	Network **diversity** is considered and implemented where possible when implementing NG9-1-1 networks.	R	C	
334	12	Security Enhancement Technical Upgrade	9.6.2	Traffic failover between different cities and firewall sites can result in dropping sessions at the time of failure. When employing applications in a network diversity-type model, applications shall be designed to recover such events and users advised to proper "restart" procedures in case such a failover event happens	R	C	
335	13	Technical Solutions Standards	10	Formalized pre and post security reviews are conducted when changes to architecture, design, or engineering of NG9-1-1 networks.	R	C	
336	13	Technical Solutions Standards	10	Security reviews are conducted by the NG91-1 security representative and any 3rd party vendors.	R	C	
337	13	Technical Solutions Standards	10	When changes to architecture, design, or engineering of NG9-1-1 network are made, a formal change control process is followed and appropriate documentation is produced and retained.	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
338	13	Technical Solutions Standards	10	When architecture, design, or engineering are major, a team of Subject Matter Experts is assembled to review and approve the change.	R	C	
339	13	Technical Solutions Standards	4.2	Does the organization have a Technology Selection Policy?	R	C	
340	13	Technical Solutions Standards	7.4.2	Is time synchronization in accordance with the NENA 04-002 NG9-1-1 Entity Master Clock standard?	R	C	
341	13	Technical Solutions Standards	7.4.4	Do formal documented procedures exist for any changes to computer systems and operating systems software?	R	C	
342	13	Technical Solutions Standards	7.4.4	Are the procedures identified in the preceding finding followed?	R	C	
343	13	Technical Solutions Standards	7.4.4	Is the appropriate level of authorization required and obtained prior to change?	R	C	
344	13	Technical Solutions Standards	7.4.4	Does the System Administrator control software changes that affect the operation of an application, operating system, or utilities?	R	C	
345	13	Technical Solutions Standards	7.4.4	Does the System Administrator control updates and upgrades that could affect user response, machine performance or operations, security, or system availability?	R	C	
346	13	Technical Solutions Standards	7.4.4	Has a detailed audit trail of all modifications to network hardware and software been created, retained, and reviewed at least annually?	R	CP	Policies and processes are in place for ESInet systems. Changes are documented and retained in the service / change management system.
347	13	Technical Solutions Standards	7.4.4	Are records of all system/application changes kept at least one year or the last major upgrade whichever is longer?	R	C	
348	13	Technical Solutions Standards	7.4.4	Do System Controls identify accountability for all program changes to a specific programmer and approving manager?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
349	13	Technical Solutions Standards	7.4.4	Excepting reporting procedures are built into the system software to detect computer program, communications and operations failures. .	R	C	
350	13	Technical Solutions Standards	7.4.4	Are error checking and validation controls are present in software?	R	C	
351	13	Technical Solutions Standards	7.4.4	Current complete backups are ALWAYS present prior upgrades to provide recovery capability in the event of system problems due to the changes?	R	C	
352	13	Technical Solutions Standards	7.4.4	If System Administration or Maintenance is outsourced all records kept by such agencies are available to the NG 9-1-1 Entity?	R	C	
353	13	Technical Solutions Standards	7.4.5	Have procedures been instituted to verify and document that the business hardware and software are currently supported by the manufacturer or supplier that advisories	R	C	
354	13	Technical Solutions Standards	7.4.5	Are Temporary Fixes applied when Permanent Fixes are not yet available and are Permanent Fixes applied promptly when they become available?	R	C	
355	13	Technical Solutions Standards	7.4.5	A process is in place which ensures all applicable Permanent fixes are installed and Temporary Fixes cannot become disabled until Permanent Fixes have been installed?	R	C	
356	13	Technical Solutions Standards	7.4.5	Are all Permanent or Temporary fixes tested prior to using them in a production environment?	R	C	
357	13	Technical Solutions Standards	7.4.6	Servers, workstations, desktops, or laptops shall be hardened utilizing recognized 'Best Practices for Operating System Hardening' like the National Institute For Standards and Technology (NIST) Guidelines or ISO 2700*x* standards?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
358	13	Technical Solutions Standards	7.4.6	All unused services are disabled and end users do not have local administrator rights?	R	CP	Local administrator rights are restricted for some, but not all users in the organization. Justification related to employee role is required for end users who have local administrator rights.
359	13	Technical Solutions Standards	7.5.2	Has the entity identified all 'single point of failure' items for their system and have the alternate strategies been planned and documented?	R	C	
360	13	Technical Solutions Standards	7.5.2	Is a plan in place to distribute the 'downtime window' if possible?	R	C	
361	13	Technical Solutions Standards	7.5.2	Is equipment managed and monitored so if one element is down the entity and management are notified?	R	C	
362	13	Technical Solutions Standards	7.5.3	Is 'geographic redundancy' available. If so, are procedures in place for activation, use, and testing of the alternate site. Are the results of testing documented	R	C	
363	13	Technical Solutions Standards	7.5.3	Are the results of testing of failover procedures documented?	R	C	
364	14	Wireless Security	4.2	Does the organization have a Wireless Policy?(Auditor Guidance: if no wireless technologies are in place, then this finding, and all subsequent findings is not applicable. All requirements of this document also apply to communications in the 4.9G Hz band)	R	N/A	The ESInet does not implement any wireless technology.
365	14	Wireless Security	6.4.6.1	Default router management passwords have been changed and is treated as an Administrator level password for syntax, history, and periodically changed?	R	N/A	The ESInet does not implement any wireless technology.
366	14	Wireless Security	6.4.6.1	Router management over wireless link is disabled. Router management uses an encrypted protocol?	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
367	14	Wireless Security	6.4.6.1	The SSID has been changed from the Default value to an identifier not easily associated with the NG 9-1-1 or easily guessed	R	N/A	ESInet does not implement any wireless technology.
368	14	Wireless Security	6.4.6.1	SSID broadcast is disabled?	R	N/A	ESInet does not implement any wireless technology.
369	14	Wireless Security	6.4.6.1	Wireless encryption is enabled WPA or greater is used? (Auditor Guidance: WEP is not allowed)	R	N/A	ESInet does not implement any wireless technology.
370	14	Wireless Security	6.4.6.1	The TKIP passphrase is non-trivial and meets the requirements of this document?	R	N/A	ESInet does not implement any wireless technology.
371	14	Wireless Security	6.4.6.1	The rekey maximum is no greater than 3600 seconds?	R	N/A	ESInet does not implement any wireless technology.
372	14	Wireless Security	6.4.6.1	The WIFI LAN is dedicated to the NG 9-1-1 entity and not shared with any other entity?	R	N/A	ESInet does not implement any wireless technology.
373	14	Wireless Security	6.4.6.1	Media Access Control (MAC) address filters are enabled and MAC Filter List is reviewed at least monthly and immediately after a machine is retired from the network?	R	N/A	ESInet does not implement any wireless technology.
374	14	Wireless Security	6.4.6.1	Ad hoc modes are disabled?	R	N/A	ESInet does not implement any wireless technology.
375	14	Wireless Security	6.4.6.1	Users should be authenticated to the wireless LAN using a two factor mechanism or emerging authentication standards like 802.1x?	BP	N/A	ESInet does not implement any wireless technology.
376	14	Wireless Security	6.4.6.1	The WIFI LAN should be separated from other networks by a firewall which limits access to and from the wireless network on an exception only basis.	BP	N/A	ESInet does not implement any wireless technology.

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
377	14	Wireless Security	6.4.6.1	Use of Intrusion Detection Systems (IDS) is encouraged on WIFI LANs	BP	N/A	ESInet does not implement any wireless technology.
378	14	Wireless Security	6.4.6.1	Maximum encryption key lengths supported by the device should be utilized	BP	N/A	ESInet does not implement any wireless technology.
379	14	Wireless Security	6.4.6.1	The WIFI LAN hardware should utilize a third party authentication service for management(such as TACAS, Radius) when supported	BP	N/A	ESInet does not implement any wireless technology.
380	14	Wireless Security	6.4.6.1	The default SSID channel should be changed from its default value	BP	N/A	ESInet does not implement any wireless technology.
381	14	Wireless Security	6.4.6.1	If DHCP is used, automatic assignment of other services(e.g. DNS servers, WINS servers) is allowed and should be reviewed in concert with the overall security plan	BP	N/A	ESInet does not implement any wireless technology.
382	14	Wireless Security	6.4.6.1	DHCP should be disabled and require static IP Addresses for connected devices. If DHCP must be used the DHCP scope(range of addresses) should be kept to a minimum	BP	N/A	ESInet does not implement any wireless technology.
383	14	Wireless Security	6.4.6.1	The WIFI LAN should utilize a Network Access Control technology to ensure proper patching and malicious software screening is performed on all LAN assets. At minimum, use of a rogue machine device detection capability is strongly recommended.	BP	N/A	ESInet does not implement any wireless technology.
384	14	Wireless Security	6.4.6.2	Bluetooth shall not be used for backup of any medium or device which contains sensitive (internal data only) or greater data.	R	C	
385	14	Wireless Security	6.4.6.2	If Bluetooth is used is shall be configured to require device identifiers.	R	C	
386	14	Wireless Security	6.4.6.2	Presence of frequency hopping, phase shifting, device serialization, or other technologies alone shall not satisfy encryption or identification requirements	R	C	

Audit Item Number	Section	Section Title	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
387	14	Wireless Security	6.4.6.2	Bluetooth wireless networks should be avoided, where possible, including wireless headsets and other human interface devices such as mice and keyboards	BP	C	
388	14	Wireless Security	6.4.6.3	Does the entity use the 4.9 MHz band spectrum licensed by the FCC?	R	N/A	The ESInet does not implement any wireless technology.
389	14	Wireless Security	6.4.6.3	If the 4.9 MHz band is used are all communications encrypted and all authentication, authorization, and accountability policies complied with?	R	N/A	ESInet does not implement any wireless technology.
390	14	Wireless Security	6.4.6.3	If the 4.9 MHz band is used a Firewall is deployed at the network boundary	R	N/A	ESInet does not implement any wireless technology.
391	14	Wireless Security	6.4.6.3	All communications on the 4.9G Hz band should be encrypted?	BP	N/A	ESInet does not implement any wireless technology.
392	14	Wireless Security	6.4.6.3	Authentication, authorization, and accountability should be maintained.	BP	N/A	ESInet does not implement any wireless technology.
393	14	Wireless Security	6.4.6.4	Each of these technologies(i.e. 3G, EDGE, etc.) should be regarded as a "remote access" capability and all security standards relevant to remote access found in this document are applicable	R	C	
394	14	Wireless Security	6.5	Does the NG 9-1-1 entity require contracting agencies to hold specific or certain certifications to prove compliance with this requirement?	R	N/A	ESInet does not implement any wireless technology.
395	14	Wireless Security	6.5	Entities responsible for system and security administration (including those contracted to do such tasks) employ individuals who have received current security training on their assigned systems.	R	C	
396	14	Wireless Security	6.5	All Public Safety employees receive complete security awareness training as established by each Public Safety Organization on an annual basis?	R	C	

CenturyLink™

brixKv_oneflexProbes Lookup Information

brixInstance	probe.sla_usage_count	psap.customer_name	psap.intrado_id	psap.psap_id	verifier_id	verifier_name
oneflex-standalone	1		13326	CO/EVXR/326/MS-C	7443	CO326-DENVPD-NG911PRB-2009130100

PSAP Profile Data

verifierfive	i_id	PSAP_Name	probe5
CO326		C	CO326

Sip Test Data

Time	Event
2020-05-27T12:44:57-0500	1590601497,42891,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3433,4640,139556,102735,57334,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,134916,0,90,2,0,90. 909,9.09,0,,0,2268," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a6b4fb77,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T12:37:56-0500	1590601076,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3436,4653,135137,105943,58088,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,130484,0,90,2,0,90. 909,9.09,0,,0,1791," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bdf658c3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T12:30:56-0500	1590600656,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3451,4667,137478,102572,55463,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,132811,0,90,2,0,90. 909,9.09,0,,0,304," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= afedc82f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T12:23:56-0500	1590600236,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3474,4808,157723,102125,58084,100000,100000,100000,100000,0,100000, 100000,1298,0,0,85,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,152915,0,90,2,0,90. 909,9.09,0,,0,7005," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5dbbc953,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T12:16:56-0500	1590599816,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3467,4919,138364,102013,55459,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13752,,,,,4.34,0,0,0,0,0,133445,0,90,2,0,90. 909,9.09,0,,0,418," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 655d3271,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T12:09:56-0500	1590599396,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3469,4684,138520,105530,57732,100000,100000,100000,100000,0,100000, 100000,1298,0,0,36,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,133836,0,90,2,0,90. 909,9.09,0,,0,330," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 11e9bfd7,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T12:02:56-0500	1590598976,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3330,4656,125705,106531,55455,100000,100000,100000,100000,0,100000, 100000,1298,0,0,60,0,0,0,,,,,,0,,,0,,,64.58.61.20,13730,,,,,4.34,0,0,0,0,0,121049,0,90,2,0,90. 909,9.09,0,,0,2212," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 919d5e2d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:55:56-0500	1590598556,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3433,4652,141757,107031,59930,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13744,,,,,4.34,0,0,0,0,0,137105,0,90,2,0,90. 909,9.09,0,,0,325," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5dd38662,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:48:56-0500	1590598136,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3404,4716,137249,100734,55451,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13786,,,,,4.34,0,0,0,0,0,132533,0,90,2,0,90. 909,9.09,0,,0,846," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c4ca561c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:41:56-0500	1590597716,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3425,4638,139314,105526,57866,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,134676,0,90,2,0,90. 909,9.09,0,,0,364," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c1669135,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:34:56-0500	1590597296,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3433,4658,140894,106104,59924,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13760,,,,,4.34,0,0,0,0,0,136236,0,90,2,0,90. 909,9.09,0,,0,2297," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7f16cdcd,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:27:56-0500	1590596876,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3422,4634,140547,103398,57862,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13758,,,,,4.34,0,0,0,0,0,135913,0,90,2,0,90. 909,9.09,0,,0,275," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b66b5a8b,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:20:56-0500	1590596456,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3336,4652,139601,106375,56446,100000,100000,100000,100000,0,100000, 100000,1298,0,0,68,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,134949,0,90,2,0,90. 909,9.09,0,,0,2613," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 608b5d56,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T11:13:56-0500	1590596036,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3452,4662,137794,106986,57192,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13714,,,,,4.34,0,0,0,0,0,133132,0,90,2,0,90. 909,9.09,0,,0,1897," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 75f628b3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T11:06:56-0500	1590595616,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3427,4635,138767,102182,56442,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,134132,0,90,2,0,90. 909,9.09,0,,0,342," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8850d1d8,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:59:56-0500	1590595196,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3458,4671,136500,105450,57188,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,131829,0,90,2,0,90. 909,9.09,0,,0,4797," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5cfb9f54,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:52:56-0500	1590594776,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3465,4765,139052,105976,59912,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13788,,,,,4.34,0,0,0,0,0,134287,0,90,2,0,90. 909,9.09,0,,0,299," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2097099c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:45:56-0500	1590594356,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3393,4871,137327,106603,57664,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13796,,,,,4.34,0,0,0,0,0,132456,0,90,2,0,90. 909,9.09,0,,0,3999," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7778c734,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:38:56-0500	1590593936,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3410,4638,335019,106061,56434,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,330381,0,90,2,0,90. 909,9.09,0,,0,892," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4d22434d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:31:56-0500	1590593516,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3882,5214,137251,100692,58052,100000,100000,100000,100000,0,100000, 100000,1298,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13750,,,,,4.34,0,0,0,0,0,132037,0,90,2,0,90. 909,9.09,0,,0,1014," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a8104a0a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:24:56-0500	1590593096,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3456,4690,139712,105121,55427,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,135022,0,90,2,0,90. 909,9.09,0,,0,2147," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7f10ed09,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T10:17:56-0500	1590592676,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3412,4620,138407,105465,57176,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,133787,0,90,2,0,90. 909,9.09,0,,0,744," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 64f87e47,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:10:56-0500	1590592256,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3460,4679,142853,107142,57654,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,138174,0,90,2,0,90. 909,9.09,0,,0,754," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e2a95b4e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T10:03:56-0500	1590591836,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3369,4860,140097,106870,57172,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13728,,,,,4.34,0,0,0,0,0,135237,0,90,2,0,90. 909,9.09,0,,0,866," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b0d3a2c5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:56:56-0500	1590591416,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3413,4628,141443,103322,57650,100000,100000,100000,100000,0,100000, 100000,1298,0,0,57,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,136815,0,90,2,0,90. 909,9.09,0,,0,1365," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= f0bc7008,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:49:56-0500	1590590996,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3444,4663,139207,99965,56420,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13790,,,,,4.34,0,0,0,0,0,134544,0,90,2,0,90. 909,9.09,0,,0,279," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2abaa02a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:42:56-0500	1590590576,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3443,4655,139755,107286,57646,100000,100000,100000,100000,0,100000, 100000,1298,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13716,,,,,4.34,0,0,0,0,0,135100,0,90,2,0,90. 909,9.09,0,,0,280," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= fa283814,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:35:56-0500	1590590156,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3464,4673,136053,110105,54617,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,131380,0,90,2,0,90. 909,9.09,0,,0,2122," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= de7ec826,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:28:56-0500	1590589736,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3344,4677,134820,105843,56414,100000,100000,100000,100000,0,100000, 100000,1298,0,0,82,0,0,0,,,,,,0,,,0,,,64.58.61.20,13784,,,,,4.34,0,0,0,0,0,130143,0,90,2,0,90. 909,9.09,0,,0,4818," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 9f30c626,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T09:21:56-0500	1590589316,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3347,4704,120846,108025,56374,100000,100000,100000,100000,0,100000, 100000,1299,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,116142,0,90,2,0,90. 909,9.09,0,,0,1007," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c069eac2,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-27T09:14:56-0500	1590588896,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3447,4694,122666,107276,56410,100000,100000,100000,100000,0,100000, 100000,1299,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13798,,,,,4.34,0,0,0,0,0,117972,0,90,2,0,90. 909,9.09,0,,0,1486," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4d9eed6f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-27T09:07:56-0500	1590588476,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3443,4651,135423,104386,58464,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13736,,,,,4.34,0,0,0,0,0,130772,0,90,2,0,90. 909,9.09,0,,0,2853," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 01c87669,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T09:00:56-0500	1590588056,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3422,4637,142634,103841,57406,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,137997,0,90,2,0,90. 909,9.09,0,,0,1040," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6fe1d10e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T08:53:56-0500	1590587636,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3437,4634,145504,107364,56572,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13762,,,,,4.34,0,0,0,0,0,140870,0,90,2,0,90. 909,9.09,0,,0,1929," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 21fa852f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T08:46:56-0500	1590587216,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3439,4650,123714,106505,55555,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,119064,0,90,2,0,90. 909,9.09,0,,0,604," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= f867f8e6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T08:39:56-0500	1590586796,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3477,4684,135604,104442,56010,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13700,,,,,4.34,0,0,0,0,0,130920,0,90,2,0,90. 909,9.09,0,,0,635," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= abec28f5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T08:32:56-0500	1590586376,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3436,4645,142493,107460,56566,100000,100000,100000,100000,0,100000, 100000,1298,0,0,60,0,0,0,,,,,,0,,,0,,,64.58.61.20,13746,,,,,4.34,0,0,0,0,0,137848,0,90,2,0,90. 909,9.09,0,,0,793," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 29543a59,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T08:25:56-0500	1590585956,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3603,4835,139409,105597,55549,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13754,,,,,4.34,0,0,0,0,0,134574,0,90,2,0,90. 909,9.09,0,,0,5568," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3ad0cf5c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-27T08:18:56-0500	1590585536,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3408,4894,139017,102835,59344,100000,100000,100000,100000,0,100000, 100000,1298,0,0,38,0,0,0,,,,,,0,,,0,,,64.58.61.20,13768,,,,,4.34,0,0,0,0,0,134123,0,90,2,0,90. 909,9.09,0,,0,3672," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5a6f65c3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-27T08:11:56-0500	1590585116,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3488,4700,140718,107197,55853,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13742,,,,,4.34,0,0,0,0,0,136018,0,90,2,0,90. 909,9.09,0,,0,1389," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 423ae8d7,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-27T08:04:56-0500	1590584696,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3432,4646,142831,101168,56724,100000,100000,100000,100000,0,100000, 100000,1298,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13714,,,,,4.34,0,0,0,0,0,138185,0,90,2,0,90. 909,9.09,0,,0,2306," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4c9af784,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-27T07:57:56-0500	1590584276,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3335,4832,141549,102399,56100,100000,100000,100000,100000,0,100000, 100000,1298,0,0,39,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,136717,0,90,2,0,90. 909,9.09,0,,0,536," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a0c58634,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-27T07:50:56-0500	1590583856,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3417,4639,123867,105250,54799,100000,100000,100000,100000,0,100000, 100000,1299,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13726,,,,,4.34,0,0,0,0,0,119228,0,90,2,0,90. 909,9.09,0,,0,1166," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 45cb029f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,,fixed
2020-05-27T07:43:56-0500	1590583436,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3479,4703,125581,104653,55417,100000,100000,100000,100000,0,100000, 100000,1299,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13788,,,,,4.34,0,0,0,0,0,120878,0,90,2,0,90. 909,9.09,0,,0,3587," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= baa8296f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,,fixed
2020-05-27T07:36:56-0500	1590583016,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3405,4727,140688,102246,57610,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13774,,,,,4.34,0,0,0,0,0,135961,0,90,2,0,90. 909,9.09,0,,0,601," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 69396596,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed

Time	Event
2020-05-27T07:29:56-0500	1590582596,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3398,4612,142226,106768,56126,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13744,,,,,4.34,0,0,0,0,0,137614,0,90,2,0,90. 909,9.09,0,,0,807," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6d25125e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T07:22:56-0500	1590582176,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3453,4672,140113,108771,54579,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13740,,,,,4.34,0,0,0,0,0,135441,0,90,2,0,90. 909,9.09,0,,0,2590," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3a976dad,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T07:15:56-0500	1590581756,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3412,4637,133341,106647,58956,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13736,,,,,4.34,0,0,0,0,0,128704,0,90,2,0,90. 909,9.09,0,,0,2047," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 0d59feb5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T07:08:56-0500	1590581336,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3353,4677,145213,101675,59848,100000,100000,100000,100000,0,100000, 100000,1298,0,0,70,0,0,0,,,,,,0,,,0,,,64.58.61.20,13706,,,,,4.34,0,0,0,0,0,140536,0,90,2,0,90. 909,9.09,0,,0,1211," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7e35f033,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T07:01:56-0500	1590580916,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3429,4637,140313,107408,58952,100000,100000,100000,100000,0,100000, 100000,1298,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13704,,,,,4.34,0,0,0,0,0,135676,0,90,2,0,90. 909,9.09,0,,0,634," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 18dee807,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:54:56-0500	1590580496,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3371,4575,140087,105883,59844,100000,100000,100000,100000,0,100000, 100000,1298,0,0,69,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,135512,0,90,2,0,90. 909,9.09,0,,0,3264," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 47f24ad0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:47:56-0500	1590580076,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3433,4647,138759,106063,57056,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,134112,0,90,2,0,90. 909,9.09,0,,0,2346," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ea9142a4,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:40:56-0500	1590579656,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3359,4666,139824,103262,59840,100000,100000,100000,100000,0,100000, 100000,1298,0,0,57,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,135158,0,90,2,0,90. 909,9.09,0,,0,739," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2dad91d0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T06:33:56-0500	1590579236,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3476,4687,134277,106541,57112,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,129590,0,90,2,0,90. 909,9.09,0,,0,320," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7977925d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:26:56-0500	1590578816,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3472,4690,137792,108171,57590,100000,100000,100000,100000,0,100000, 100000,1298,0,0,64,0,0,0,,,,,,0,,,0,,,64.58.61.20,13738,,,,,4.34,0,0,0,0,0,133102,0,90,2,0,90. 909,9.09,0,,0,566," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e7bb3132,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:19:56-0500	1590578396,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3435,4644,141392,105665,59834,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13760,,,,,4.34,0,0,0,0,0,136748,0,90,2,0,90. 909,9.09,0,,0,589," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 64e9b3b9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:12:56-0500	1590577976,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3401,4696,124457,106598,57106,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13754,,,,,4.34,0,0,0,0,0,119761,0,90,2,0,90. 909,9.09,0,,0,352," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c86bc97c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T06:05:56-0500	1590577556,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3426,4633,124642,101521,59830,100000,100000,100000,100000,0,100000, 100000,1299,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13728,,,,,4.34,0,0,0,0,0,120009,0,90,2,0,90. 909,9.09,0,,0,995," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 50531099,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-27T05:58:56-0500	1590577136,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3438,4661,137062,105970,57974,100000,100000,100000,100000,0,100000, 100000,1298,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13716,,,,,4.34,0,0,0,0,0,132401,0,90,2,0,90. 909,9.09,0,,0,1088," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c55b30b6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:51:56-0500	1590576716,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3532,4745,141731,107298,56352,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,136986,0,90,2,0,90. 909,9.09,0,,0,1153," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 9591c515,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:44:56-0500	1590576296,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3620,4845,142990,107013,57050,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,138145,0,90,2,0,90. 909,9.09,0,,0,444," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= d9095a3a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T05:37:56-0500	1590575876,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3458,4659,135785,105053,57096,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13714,,,,,4.34,0,0,0,0,0,131126,0,90,2,0,90. 909,9.09,0,,0,1865," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1ae1c440,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:30:56-0500	1590575456,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3382,4591,138320,109807,56830,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,133729,0,90,2,0,90. 909,9.09,0,,0,1208," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7c2054b6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:23:56-0500	1590575036,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3488,4700,153402,107560,57964,100000,100000,100000,100000,0,100000, 100000,1298,0,0,37,0,0,0,,,,,,0,,,0,,,64.58.61.20,13770,,,,,4.34,0,0,0,0,0,148702,0,90,2,0,90. 909,9.09,0,,0,259," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 49eb35c6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:16:56-0500	1590574616,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3483,4695,139723,101494,55459,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,135028,0,90,2,0,90. 909,9.09,0,,0,369," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8b0ee631,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:09:56-0500	1590574196,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3449,4750,138395,104699,56052,100000,100000,100000,100000,0,100000, 100000,1298,0,0,67,0,0,0,,,,,,0,,,0,,,64.58.61.20,13788,,,,,4.34,0,0,0,0,0,133645,0,90,2,0,90. 909,9.09,0,,0,1112," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e96ec76e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T05:02:56-0500	1590573776,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3469,4684,141718,105218,57176,100000,100000,100000,100000,0,100000, 100000,1298,0,0,38,0,0,0,,,,,,0,,,0,,,64.58.61.20,13798,,,,,4.34,0,0,0,0,0,137034,0,90,2,0,90. 909,9.09,0,,0,2016," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= cd8917f1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:55:56-0500	1590573356,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3437,4739,141786,103239,58040,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13730,,,,,4.34,0,0,0,0,0,137047,0,90,2,0,90. 909,9.09,0,,0,1577," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ccc692e5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:48:56-0500	1590572936,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3443,4655,140971,106851,57562,100000,100000,100000,100000,0,100000, 100000,1298,0,0,190,0,0,0,,,,,,0,,,0,,,64.58.61.20,13796,,,,,4.34,0,0,0,0,0,136316,0,90,2,0,90 .909,9.09,0,,0,1297," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bf214826,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T04:41:56-0500	1590572516,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3411,4614,141783,106092,59778,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13736,,,,,4.34,0,0,0,0,0,137169,0,90,2,0,90. 909,9.09,0,,0,205," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 41899f97,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:34:56-0500	1590572096,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3488,4710,121586,104469,57558,100000,100000,100000,100000,0,100000, 100000,1298,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13712,,,,,4.34,0,0,0,0,0,116876,0,90,2,0,90. 909,9.09,0,,0,1153," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 9784ca75,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:27:56-0500	1590571676,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,6439,8141,138839,103158,58424,100000,100000,100000,100000,0,100000, 100000,1298,0,0,64,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,130698,0,90,2,0,90. 909,9.09,0,,0,607," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1950919e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:20:56-0500	1590571256,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3438,4644,129162,101524,58604,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,124518,0,90,2,0,90. 909,9.09,0,,0,357," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3bba869e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:13:56-0500	1590570836,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3445,4650,160061,104840,57552,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13762,,,,,4.34,0,0,0,0,0,155411,0,90,2,0,90. 909,9.09,0,,0,3140," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 15b0b29c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T04:06:56-0500	1590570416,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3326,4810,143096,109946,58138,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,138286,0,90,2,0,90. 909,9.09,0,,0,618," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 95bc2729,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T03:59:56-0500	1590569996,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3486,4689,142208,108601,57548,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13764,,,,,4.34,0,0,0,0,0,137519,0,90,2,0,90. 909,9.09,0,,0,1208," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 9d6d0bd2,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T03:52:56-0500	1590569576,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3480,4694,141427,107573,55667,100000,100000,100000,100000,0,100000, 100000,1298,0,0,37,0,0,0,,,,,,0,,,0,,,64.58.61.20,13738,,,,,4.34,0,0,0,0,0,136733,0,90,2,0,90. 909,9.09,0,,0,738," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 27c2646d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T03:45:56-0500	1590569156,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3356,4668,140899,108066,57002,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,136231,0,90,2,0,90. 909,9.09,0,,0,2433," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= f804cffa,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T03:38:56-0500	1590568736,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3416,4728,138464,106433,58130,100000,100000,100000,100000,0,100000, 100000,1298,0,0,69,0,0,0,,,,,,0,,,0,,,64.58.61.20,13790,,,,,4.34,0,0,0,0,0,133736,0,90,2,0,90. 909,9.09,0,,0,3148," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e2a1e8e6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T03:31:56-0500	1590568316,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3457,4698,139798,101260,58144,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13768,,,,,4.34,0,0,0,0,0,135100,0,90,2,0,90. 909,9.09,0,,0,3158," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 82021d1e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T03:24:56-0500	1590567896,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3403,4708,121711,101210,56568,100000,100000,100000,100000,0,100000, 100000,1299,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13742,,,,,4.34,0,0,0,0,0,117003,0,90,2,0,90. 909,9.09,0,,0,959," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 20d38ee0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-27T03:17:56-0500	1590567476,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3388,4694,124250,106973,57536,100000,100000,100000,100000,0,100000, 100000,1299,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,119556,0,90,2,0,90. 909,9.09,0,,0,1514," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a5c10cac,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-27T03:10:56-0500	1590567056,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3432,4648,139978,107018,56564,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13732,,,,,4.34,0,0,0,0,0,135330,0,90,2,0,90. 909,9.09,0,,0,1175," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6298b740,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T03:03:56-0500	1590566636,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3451,4671,138275,102611,54445,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13770,,,,,4.34,0,0,0,0,0,133604,0,90,2,0,90. 909,9.09,0,,0,911," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5b3dc4ca,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T02:56:56-0500	1590566216,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3442,4661,143308,104772,57530,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,138647,0,90,2,0,90. 909,9.09,0,,0,361," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 18505c0f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-27T02:49:56-0500	1590565796,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3444,4662,140791,104287,59930,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13730,,,,,4.34,0,0,0,0,0,136129,0,90,2,0,90. 909,9.09,0,,0,360," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3bfe0401,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T02:42:56-0500	1590565376,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3338,4655,138974,103002,58394,100000,100000,100000,100000,0,100000, 100000,1298,0,0,58,0,0,0,,,,,,0,,,0,,,64.58.61.20,13750,,,,,4.34,0,0,0,0,0,134319,0,90,2,0,90. 909,9.09,0,,0,522," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bbe4b3f0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T02:35:56-0500	1590564956,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3431,4648,123542,102103,59926,100000,100000,100000,100000,0,100000, 100000,1299,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13740,,,,,4.34,0,0,0,0,0,118894,0,90,2,0,90. 909,9.09,0,,0,5134," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6a9e4189,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-27T02:28:56-0500	1590564536,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3429,4639,138525,106597,56336,100000,100000,100000,100000,0,100000, 100000,1298,0,0,38,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,133886,0,90,2,0,90. 909,9.09,0,,0,368," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1653bd1b,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T02:21:56-0500	1590564116,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3341,4658,123734,107410,57520,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13762,,,,,4.34,0,0,0,0,0,119076,0,90,2,0,90. 909,9.09,0,,0,3041," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 252d956b,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T02:14:56-0500	1590563696,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3376,4731,122641,107774,56774,100000,100000,100000,100000,0,100000, 100000,1299,0,0,62,0,0,0,,,,,,0,,,0,,,64.58.61.20,13704,,,,,4.34,0,0,0,0,0,117910,0,90,2,0,90. 909,9.09,0,,0,503," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7fc0b891,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-27T02:07:56-0500	1590563276,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3429,4680,142269,106752,58588,100000,100000,100000,100000,0,100000, 100000,1298,0,0,39,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,137589,0,90,2,0,90. 909,9.09,0,,0,314," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ca56eadf,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T02:00:56-0500	1590562856,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3440,4733,139307,106715,57514,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13760,,,,,4.34,0,0,0,0,0,134574,0,90,2,0,90. 909,9.09,0,,0,3042," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4958425a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-27T01:53:56-0500	1590562436,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3449,4700,138162,104293,54425,100000,100000,100000,100000,0,100000, 100000,1298,0,0,60,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,133462,0,90,2,0,90. 909,9.09,0,,0,1597," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e4309ba1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T01:46:56-0500	1590562016,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3410,4722,123626,106020,56282,100000,100000,100000,100000,0,100000, 100000,1299,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13716,,,,,4.34,0,0,0,0,0,118904,0,90,2,0,90. 909,9.09,0,,0,1145," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= f83866c0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-27T01:39:56-0500	1590561596,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3445,4667,143211,102828,59298,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13742,,,,,4.34,0,0,0,0,0,138544,0,90,2,0,90. 909,9.09,0,,0,1650," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6b8f99f4,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T01:32:56-0500	1590561176,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3370,4693,134526,104356,57506,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,129833,0,90,2,0,90. 909,9.09,0,,0,2304," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ad968523,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T01:25:56-0500	1590560756,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3620,4861,134617,109411,57304,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,129756,0,90,2,0,90. 909,9.09,0,,0,513," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bda364f5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T01:18:56-0500	1590560336,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3397,4612,136598,429709,57022,100000,100000,100000,100000,0,100000, 100000,1298,0,0,88,0,0,0,,,,,,0,,,0,,,64.58.61.20,13748,,,,,4.34,0,0,0,0,0,131986,0,90,2,0,90. 909,9.09,0,,0,2181," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 65cfe70e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T01:11:56-0500	1590559916,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3424,4645,139116,106806,56742,100000,100000,100000,100000,0,100000, 100000,1298,0,0,121,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,134471,0,90,2,0,90 .909,9.09,0,,0,1627," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c8fc0b83,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T01:04:56-0500	1590559496,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3662,4887,139111,105864,58110,100000,100000,100000,100000,0,100000, 100000,1298,0,0,62,0,0,0,,,,,,0,,,0,,,64.58.61.20,13796,,,,,4.34,0,0,0,0,0,134224,0,90,2,0,90. 909,9.09,0,,0,2068," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c73f3b90,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-27T00:57:56-0500	1590559076,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3398,4870,141897,102010,56738,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13712,,,,,4.34,0,0,0,0,0,137027,0,90,2,0,90. 909,9.09,0,,0,2157," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 913ea58e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-27T00:50:56-0500	1590558656,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3459,4714,122180,106071,57494,100000,100000,100000,100000,0,100000, 100000,1299,0,0,35,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,117466,0,90,2,0,90. 909,9.09,0,,0,303," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ac033a5a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-27T00:43:56-0500	1590558236,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3425,4639,140528,106314,54405,100000,100000,100000,100000,0,100000, 100000,1298,0,0,64,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,135889,0,90,2,0,90. 909,9.09,0,,0,845," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2abd662e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T00:36:56-0500	1590557816,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3424,4641,123745,99452,57490,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13776,,,,,4.34,0,0,0,0,0,119104,0,90,2,0,90. 909,9.09,0,,0,5981," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6279fcac,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T00:29:56-0500	1590557396,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3748,5119,125449,107788,55806,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13764,,,,,4.34,0,0,0,0,0,120330,0,90,2,0,90. 909,9.09,0,,0,998," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8502c6ea,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T00:22:56-0500	1590556976,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3475,4707,142603,106136,57006,100000,100000,100000,100000,0,100000, 100000,1298,0,0,37,0,0,0,,,,,,0,,,0,,,64.58.61.20,13760,,,,,4.34,0,0,0,0,0,137896,0,90,2,0,90. 909,9.09,0,,0,575," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a9951d66,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T00:15:56-0500	1590556556,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3397,4705,137797,104180,57484,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,133092,0,90,2,0,90. 909,9.09,0,,0,1848," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6eeedd36,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-27T00:08:56-0500	1590556136,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3442,4657,152856,106025,56562,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13752,,,,,4.34,0,0,0,0,0,148199,0,90,2,0,90. 909,9.09,0,,0,1686," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bc068117,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-27T00:01:56-0500	1590555716,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3444,4742,138385,101981,57000,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13732,,,,,4.34,0,0,0,0,0,133643,0,90,2,0,90. 909,9.09,0,,0,672," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 42036771,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:54:56-0500	1590555296,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3379,4701,123509,100678,55703,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,118808,0,90,2,0,90. 909,9.09,0,,0,464," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 98134e2f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:47:56-0500	1590554876,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3454,4675,137809,106072,56248,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13730,,,,,4.34,0,0,0,0,0,133134,0,90,2,0,90. 909,9.09,0,,0,3055," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 90063825,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:40:56-0500	1590554456,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3444,4679,138945,106012,58336,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13744,,,,,4.34,0,0,0,0,0,134266,0,90,2,0,90. 909,9.09,0,,0,918," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3d1f53f1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:33:56-0500	1590554036,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3447,4670,141112,101648,59262,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13740,,,,,4.34,0,0,0,0,0,136442,0,90,2,0,90. 909,9.09,0,,0,613," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1d4f9bcb,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:26:56-0500	1590553616,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3434,4642,140250,107714,57470,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,135608,0,90,2,0,90. 909,9.09,0,,0,746," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3a854e86,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:19:56-0500	1590553196,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3524,4769,143554,102424,59258,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,138785,0,90,2,0,90. 909,9.09,0,,0,1012," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ddd363bf,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T23:12:56-0500	1590552776,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3401,4715,122877,102528,56986,100000,100000,100000,100000,0,100000, 100000,1299,0,0,77,0,0,0,,,,,,0,,,0,,,64.58.61.20,13738,,,,,4.34,0,0,0,0,0,118162,0,90,2,0,90. 909,9.09,0,,0,1857," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 488eec34,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed

Time	Event
2020-05-26T23:05:56-0500	1590552356,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3603,4933,139955,102376,55874,100000,100000,100000,100000,0,100000, 100000,1298,0,0,71,0,0,0,,,,,,0,,,0,,,64.58.61.20,13754,,,,,4.34,0,0,0,0,0,135022,0,90,2,0,90. 909,9.09,0,,0,632," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 45030bde,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:58:56-0500	1590551936,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3455,4707,140376,104542,57462,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,135669,0,90,2,0,90. 909,9.09,0,,0,1556," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b0bf8af7,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:51:56-0500	1590551516,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3402,4712,124361,108785,58072,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,119649,0,90,2,0,90. 909,9.09,0,,0,1148," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 173177d9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:44:56-0500	1590551096,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3456,4681,140080,103403,59704,100000,100000,100000,100000,0,100000, 100000,1298,0,0,59,0,0,0,,,,,,0,,,0,,,64.58.61.20,13730,,,,,4.34,0,0,0,0,0,135399,0,90,2,0,90. 909,9.09,0,,0,3746," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= adceb4a9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:37:56-0500	1590550676,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3478,4720,140270,103707,57456,100000,100000,100000,100000,0,100000, 100000,1298,0,0,61,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,135550,0,90,2,0,90. 909,9.09,0,,0,750," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 40ff9269,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:30:56-0500	1590550256,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3343,4647,140108,106888,56560,100000,100000,100000,100000,0,100000, 100000,1298,0,0,71,0,0,0,,,,,,0,,,0,,,64.58.61.20,13762,,,,,4.34,0,0,0,0,0,135461,0,90,2,0,90. 909,9.09,0,,0,1131," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 68a9be80,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:23:56-0500	1590549836,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3340,4657,345617,104579,57452,100000,100000,100000,100000,0,100000, 100000,1298,0,0,58,0,0,0,,,,,,0,,,0,,,64.58.61.20,13738,,,,,4.34,0,0,0,0,0,340960,0,90,2,0,90. 909,9.09,0,,0,1388," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8cbab5d1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:16:56-0500	1590549416,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3439,4655,123955,101226,59268,100000,100000,100000,100000,0,100000, 100000,1298,0,0,66,0,0,0,,,,,,0,,,0,,,64.58.61.20,13704,,,,,4.34,0,0,0,0,0,119300,0,90,2,0,90. 909,9.09,0,,0,1733," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 18a862ad,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-26T22:09:56-0500	1590548996,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3413,4720,138301,106704,58316,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,133581,0,90,2,0,90. 909,9.09,0,,0,497," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1e20bef9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T22:02:56-0500	1590548576,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3415,4645,140874,103036,59264,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13768,,,,,4.34,0,0,0,0,0,136229,0,90,2,0,90. 909,9.09,0,,0,1104," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 736af3ed,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T21:55:56-0500	1590548156,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3338,4646,124569,107581,55669,100000,100000,100000,100000,0,100000, 100000,1298,0,0,61,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,119923,0,90,2,0,90. 909,9.09,0,,0,850," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 079971eb,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T21:48:56-0500	1590547736,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3442,4658,156903,105911,55926,100000,100000,100000,100000,0,100000, 100000,1298,0,0,59,0,0,0,,,,,,0,,,0,,,64.58.61.20,13796,,,,,4.34,0,0,0,0,0,152245,0,90,2,0,90. 909,9.09,0,,0,518," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e48693f9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T21:41:56-0500	1590547316,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3560,4980,122278,110776,55665,100000,100000,100000,100000,0,100000, 100000,1299,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13734,,,,,4.34,0,0,0,0,0,117298,0,90,2,0,90. 909,9.09,0,,0,1413," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= de02865d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T21:34:56-0500	1590546896,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3352,4699,121574,105775,56210,100000,100000,100000,100000,0,100000, 100000,1299,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13710,,,,,4.34,0,0,0,0,0,116875,0,90,2,0,90. 909,9.09,0,,0,614," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 81335694,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T21:27:56-0500	1590546476,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3457,4700,123849,106165,59226,100000,100000,100000,100000,0,100000, 100000,1299,0,0,72,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,119149,0,90,2,0,90. 909,9.09,0,,0,1208," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ce8f106e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T21:20:56-0500	1590546056,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3440,4667,122675,100980,56206,100000,100000,100000,100000,0,100000, 100000,1299,0,0,121,0,0,0,,,,,,0,,,0,,,64.58.61.20,13764,,,,,4.34,0,0,0,0,0,118008,0,90,2,0,90 .909,9.09,0,,0,3660," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 92ecd19c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed

Time	Event
2020-05-26T21:13:56-0500	1590545636,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3398,4702,219144,102887,58482,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,214442,0,90,2,0,90. 909,9.09,0,,0,1258," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c2a5aba1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T21:06:56-0500	1590545216,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3436,4653,141855,108111,55655,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,137202,0,90,2,0,90. 909,9.09,0,,0,3245," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b63abae2,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T20:59:56-0500	1590544796,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3440,4668,135592,104394,58016,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13746,,,,,4.34,0,0,0,0,0,130924,0,90,2,0,90. 909,9.09,0,,0,1324," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= fec41ebc,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T20:52:56-0500	1590544376,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3348,4666,124726,106484,55651,100000,100000,100000,100000,0,100000, 100000,1299,0,0,83,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,120060,0,90,2,0,90. 909,9.09,0,,0,3760," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c1725e9b,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T20:45:56-0500	1590543956,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3454,4677,122636,106993,58012,100000,100000,100000,100000,0,100000, 100000,1299,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13796,,,,,4.34,0,0,0,0,0,117959,0,90,2,0,90. 909,9.09,0,,0,795," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3c180e02,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T20:38:56-0500	1590543536,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3468,4693,142008,103323,58000,100000,100000,100000,100000,0,100000, 100000,1298,0,0,91,0,0,0,,,,,,0,,,0,,,64.58.61.20,13734,,,,,4.34,0,0,0,0,0,137315,0,90,2,0,90. 909,9.09,0,,0,993," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 0c702b44,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T20:31:56-0500	1590543116,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3410,4612,139624,104421,58008,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13786,,,,,4.34,0,0,0,0,0,135012,0,90,2,0,90. 909,9.09,0,,0,819," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 140e0c6f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T20:24:56-0500	1590542696,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3408,4725,120615,103631,55643,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,115890,0,90,2,0,90. 909,9.09,0,,0,2607," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5d78c6d5,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-26T20:17:56-0500	1590542276,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3349,4651,137029,101587,56184,100000,100000,100000,100000,0,100000, 100000,1298,0,0,215,0,0,0,,,,,,0,,,0,,,64.58.61.20,13728,,,,,4.34,0,0,0,0,0,132378,0,90,2,0,90 .909,9.09,0,,0,1742," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ece6f5f1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T20:10:56-0500	1590541856,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3445,4653,141748,107077,59632,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,137095,0,90,2,0,90. 909,9.09,0,,0,632," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= bb1f7106,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T20:03:56-0500	1590541436,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3353,4658,140176,103753,57412,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13732,,,,,4.34,0,0,0,0,0,135518,0,90,2,0,90. 909,9.09,0,,0,1066," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5a12c0cd,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:56:56-0500	1590541016,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3490,4777,137570,101546,57802,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,132793,0,90,2,0,90. 909,9.09,0,,0,2685," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5fe4d47e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:49:56-0500	1590540596,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3419,4708,136835,104093,56880,100000,100000,100000,100000,0,100000, 100000,1298,0,0,58,0,0,0,,,,,,0,,,0,,,64.58.61.20,13712,,,,,4.34,0,0,0,0,0,132127,0,90,2,0,90. 909,9.09,0,,0,7090," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2f0df344,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:42:56-0500	1590540176,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3418,4632,137884,106948,55175,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13734,,,,,4.34,0,0,0,0,0,133252,0,90,2,0,90. 909,9.09,0,,0,1166," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8f1524dd,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:35:56-0500	1590539756,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3393,4701,135426,107622,55605,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,130725,0,90,2,0,90. 909,9.09,0,,0,303," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ab556630,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:28:56-0500	1590539336,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3417,4739,135431,104481,57174,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,130692,0,90,2,0,90. 909,9.09,0,,0,835," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c0ecc037,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-26T19:21:56-0500	1590538916,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3441,4662,135861,103180,57400,100000,100000,100000,100000,0,100000, 100000,1298,0,0,59,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,131199,0,90,2,0,90. 909,9.09,0,,0,927," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 0e88f1f2,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T19:14:56-0500	1590538496,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3442,4673,139318,109764,55167,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,134645,0,90,2,0,90. 909,9.09,0,,0,962," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 48bd87ed,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:07:56-0500	1590538076,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3328,4634,139865,103131,57396,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,135231,0,90,2,0,90. 909,9.09,0,,0,1355," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 943928b0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T19:00:56-0500	1590537656,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3340,4658,137732,106233,55163,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13760,,,,,4.34,0,0,0,0,0,133074,0,90,2,0,90. 909,9.09,0,,0,976," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= aebf5368,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:53:56-0500	1590537236,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3442,4654,132311,103946,54493,100000,100000,100000,100000,0,100000, 100000,1298,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,127657,0,90,2,0,90. 909,9.09,0,,0,1564," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 628ff66d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:46:56-0500	1590536816,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3404,4725,139299,105697,56420,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,134574,0,90,2,0,90. 909,9.09,0,,0,587," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 3dbbe4d3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:39:56-0500	1590536396,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3406,4720,136126,101441,59178,100000,100000,100000,100000,0,100000, 100000,1298,0,0,58,0,0,0,,,,,,0,,,0,,,64.58.61.20,13762,,,,,4.34,0,0,0,0,0,131406,0,90,2,0,90. 909,9.09,0,,0,4184," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 0cf845e1,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:32:56-0500	1590535976,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3437,4647,124618,103003,55704,100000,100000,100000,100000,0,100000, 100000,1299,0,0,83,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,119971,0,90,2,0,90. 909,9.09,0,,0,849," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4931ae5a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed

Time	Event
2020-05-26T18:25:56-0500	1590535556,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3439,4749,139492,105291,59174,100000,100000,100000,100000,0,100000, 100000,1298,0,0,63,0,0,0,,,,,,0,,,0,,,64.58.61.20,13714,,,,,4.34,0,0,0,0,0,134743,0,90,2,0,90. 909,9.09,0,,0,4660," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b20bd2d9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:18:56-0500	1590535136,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3345,4659,122625,106922,57382,100000,100000,100000,100000,0,100000, 100000,1299,0,0,81,0,0,0,,,,,,0,,,0,,,64.58.61.20,13746,,,,,4.34,0,0,0,0,0,117966,0,90,2,0,90. 909,9.09,0,,0,1454," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= d6085d62,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-26T18:11:56-0500	1590534716,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3616,4828,140223,105355,55149,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13726,,,,,4.34,0,0,0,0,0,135395,0,90,2,0,90. 909,9.09,0,,0,3510," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8644d208,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T18:04:56-0500	1590534296,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3346,4646,140273,109660,56664,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,135627,0,90,2,0,90. 909,9.09,0,,0,2816," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 96ffca16,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T17:57:56-0500	1590533876,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3317,4620,138625,107224,55145,100000,100000,100000,100000,0,100000, 100000,1298,0,0,57,0,0,0,,,,,,0,,,0,,,64.58.61.20,13798,,,,,4.34,0,0,0,0,0,134005,0,90,2,0,90. 909,9.09,0,,0,4346," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 643a16ab,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T17:50:56-0500	1590533456,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3410,4633,140717,105180,56894,100000,100000,100000,100000,0,100000, 100000,1298,0,0,95,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,136084,0,90,2,0,90. 909,9.09,0,,0,1078," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 35a0707c,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T17:43:56-0500	1590533036,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3454,4676,139460,105499,55141,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,134784,0,90,2,0,90. 909,9.09,0,,0,2402," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= edc5d3c6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T17:36:56-0500	1590532616,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3406,4694,143028,106992,56142,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,138334,0,90,2,0,90. 909,9.09,0,,0,759," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5cae3190,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-26T17:29:56-0500	1590532196,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3543,4752,123552,101775,59040,100000,100000,100000,100000,0,100000, 100000,1296,0,0,272,0,2,0,,,,,,2,,,.153,,,64.58.61.20,13714,,,,,4.28,2,1,1,1,0,118800,0,87,2, 40,83.333,9.727,6.939,,0,1673," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61 .21;tag=9308a536,4.34,90,1,,,,,,,,,,,,,,,,,,,,,,,,1298,1297,,,,,,,,,,,,fixed
2020-05-26T17:22:56-0500	1590531776,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3460,4671,124605,102813,56886,100000,100000,100000,100000,0,100000, 100000,1298,0,0,317,0,1,0,,,,,,1,,,.076,,,64.58.61.20,13716,,,,,4.3,1,1,1,1,0,119934,0,88,2,20 ,85.714,9.75,4.534,,0,4233," sip:wlssuser@64.58.61.21:5060",BYE;OK,1,sip:442009130999@64.58.61.21 ;tag=5f09a710,4.36,91,1,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-26T17:15:56-0500	1590531356,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3379,4752,142040,109309,58232,100000,100000,100000,100000,0,100000, 100000,1296,0,0,195,0,2,0,,,,,,2,,,.153,,,64.58.61.20,13722,,,,,4.28,2,1,1,1,0,137288,0,87,2, 40,83.333,9.727,6.939,,0,1146," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61 .21;tag=6c4b65ec,4.34,90,1,,,,,,,,,,,,,,,,,,,,,,,,1298,1297,,,,,,,,,,,,fixed
2020-05-26T17:08:56-0500	1590530936,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3412,4620,140454,105107,56882,100000,100000,100000,100000,0,100000, 100000,1298,0,0,57,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,135834,0,90,2,0,90. 909,9.09,0,,0,631," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 2a2c9ee4,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-26T17:01:56-0500	1590530516,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3403,4616,142810,104190,57360,100000,100000,100000,100000,0,100000, 100000,1298,0,0,48,0,0,0,,,,,,0,,,0,,,64.58.61.20,13706,,,,,4.34,0,0,0,0,0,138194,0,90,2,0,90. 909,9.09,0,,0,2638," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4ec32827,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed
2020-05-26T16:54:56-0500	1590530096,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3434,4645,121533,102687,57750,100000,100000,100000,100000,0,100000, 100000,1299,0,0,58,0,0,0,,,,,,0,,,0,,,64.58.61.20,13728,,,,,4.34,0,0,0,0,0,116888,0,90,2,0,90. 909,9.09,0,,0,5554," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 59898648,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,,fixed
2020-05-26T16:47:56-0500	1590529676,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3434,4642,122695,105197,56876,100000,100000,100000,100000,0,100000, 100000,1299,0,0,60,0,0,0,,,,,,0,,,0,,,64.58.61.20,13750,,,,,4.34,0,0,0,0,0,118053,0,90,2,0,90. 909,9.09,0,,0,1105," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 147cd507,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,,fixed
2020-05-26T16:40:56-0500	1590529256,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3341,4729,122856,105306,55838,100000,100000,100000,100000,0,100000, 100000,1298,0,0,67,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,118127,0,90,2,0,90. 909,9.09,0,,0,4275," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1d86845f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,,fixed

Time	Event
2020-05-26T16:33:56-0500	1590528836,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3640,5062,136700,103337,56872,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13732,,,,,4.34,0,0,0,0,0,131638,0,90,2,0,90. 909,9.09,0,,0,403," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c559ae47,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T16:26:56-0500	1590528416,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3568,5017,139770,105030,56122,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,134753,0,90,2,0,90. 909,9.09,0,,0,824," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= d5c319a7,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T16:19:56-0500	1590527996,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3463,4670,138088,102152,54497,100000,100000,100000,100000,0,100000, 100000,1298,0,0,64,0,0,0,,,,,,0,,,0,,,64.58.61.20,13774,,,,,4.34,0,0,0,0,0,133418,0,90,2,0,90. 909,9.09,0,,0,1834," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 29a84f45,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T16:12:56-0500	1590527576,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3424,4626,136112,102211,56118,100000,100000,100000,100000,0,100000, 100000,1298,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13706,,,,,4.34,0,0,0,0,0,131486,0,90,2,0,90. 909,9.09,0,,0,329," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 845838e0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T16:05:56-0500	1590527156,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3415,4623,140936,103877,54493,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13788,,,,,4.34,0,0,0,0,0,136313,0,90,2,0,90. 909,9.09,0,,0,393," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 295493bf,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:58:56-0500	1590526736,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3451,4698,140140,106780,56454,100000,100000,100000,100000,0,100000, 100000,1298,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13700,,,,,4.34,0,0,0,0,0,135442,0,90,2,0,90. 909,9.09,0,,0,3427," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 9e0286f3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:51:56-0500	1590526316,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3405,4706,122672,106483,57340,100000,100000,100000,100000,0,100000, 100000,1298,0,0,81,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,117966,0,90,2,0,90. 909,9.09,0,,0,4368," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7843d3e4,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:44:56-0500	1590525896,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3443,4670,123748,103332,56450,100000,100000,100000,100000,0,100000, 100000,1298,0,0,43,0,0,0,,,,,,0,,,0,,,64.58.61.20,13758,,,,,4.34,0,0,0,0,0,119078,0,90,2,0,90. 909,9.09,0,,0,670," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4fcb761d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-26T15:37:56-0500	1590525476,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3407,4711,135542,100461,56276,100000,100000,100000,100000,0,100000, 100000,1298,0,0,34,0,0,0,,,,,,0,,,0,,,64.58.61.20,13782,,,,,4.34,0,0,0,0,0,130831,0,90,2,0,90. 909,9.09,0,,0,661," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c0e46373,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:30:56-0500	1590525056,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3393,4705,138129,102873,56446,100000,100000,100000,100000,0,100000, 100000,1298,0,0,45,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,133424,0,90,2,0,90. 909,9.09,0,,0,1061," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ff571a0f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:23:56-0500	1590524636,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3414,4621,139999,100936,55768,100000,100000,100000,100000,0,100000, 100000,1298,0,0,120,0,0,0,,,,,,0,,,0,,,64.58.61.20,13774,,,,,4.34,0,0,0,0,0,135378,0,90,2,0,90 .909,9.09,0,,0,3147," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8ce3e524,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:16:56-0500	1590524216,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3390,4733,138418,106462,56850,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13706,,,,,4.34,0,0,0,0,0,133685,0,90,2,0,90. 909,9.09,0,,0,580," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 0dc3cba9,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:09:56-0500	1590523796,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3402,4616,140735,101150,58938,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13756,,,,,4.34,0,0,0,0,0,136119,0,90,2,0,90. 909,9.09,0,,0,1090," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ddd61899,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T15:02:56-0500	1590523376,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3335,4650,199026,105873,56846,100000,100000,100000,100000,0,100000, 100000,1298,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,194376,0,90,2,0,90. 909,9.09,0,,0,1301," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 03c56289,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T14:55:56-0500	1590522956,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3389,4601,140397,106298,55549,100000,100000,100000,100000,0,100000, 100000,1298,0,0,103,0,0,0,,,,,,0,,,0,,,64.58.61.20,13790,,,,,4.34,0,0,0,0,0,135796,0,90,2,0,90 .909,9.09,0,,0,2808," sip:wlssuser@64.58.61.21:5060",BYE;OK,1,sip:442009130999@64.58.61.21;tag= 3969dfbb,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T14:48:56-0500	1590522536,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3776,4984,141030,100663,56842,100000,100000,100000,100000,0,100000, 100000,1298,0,0,53,0,0,0,,,,,,0,,,0,,,64.58.61.20,13718,,,,,4.34,0,0,0,0,0,136046,0,90,2,0,90. 909,9.09,0,,0,507," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5660a314,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Time	Event
2020-05-26T14:41:56-0500	1590522116,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3457,4654,140876,104913,57320,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13726,,,,,4.34,0,0,0,0,0,136222,0,90,2,0,90. 909,9.09,0,,0,4543," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= daf106ae,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T14:34:56-0500	1590521696,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3403,4610,123606,100668,55543,100000,100000,100000,100000,0,100000, 100000,1299,0,0,51,0,0,0,,,,,,0,,,0,,,64.58.61.20,13788,,,,,4.34,0,0,0,0,0,118996,0,90,2,0,90. 909,9.09,0,,0,3113," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 6c780e4a,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,fixed
2020-05-26T14:27:56-0500	1590521276,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3423,4646,134159,99782,57316,100000,100000,100000,100000,0,100000, 100000,1298,0,0,82,0,0,0,,,,,,0,,,0,,,64.58.61.20,13728,,,,,4.34,0,0,0,0,0,129513,0,90,2,0,90. 909,9.09,0,,0,2282," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 814ab4ab,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T14:20:56-0500	1590520856,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,4469,5990,137066,100541,55547,100000,100000,100000,100000,0,100000, 100000,1298,0,0,62,0,0,0,,,,,,0,,,0,,,64.58.61.20,13714,,,,,4.34,0,0,0,0,0,131076,0,90,2,0,90. 909,9.09,0,,0,2348," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b6fae328,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T14:13:56-0500	1590520436,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3427,4638,141576,102052,57312,100000,100000,100000,100000,0,100000, 100000,1298,0,0,54,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,136938,0,90,2,0,90. 909,9.09,0,,0,1615," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= ec1440f6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T14:06:56-0500	1590520016,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3332,4700,140654,103266,55543,100000,100000,100000,100000,0,100000, 100000,1298,0,0,61,0,0,0,,,,,,0,,,0,,,64.58.61.20,13784,,,,,4.34,0,0,0,0,0,135954,0,90,2,0,90. 909,9.09,0,,0,640," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= b635faf2,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T13:59:56-0500	1590519596,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3350,4661,124386,106689,57132,100000,100000,100000,100000,0,100000, 100000,1298,0,0,39,0,0,0,,,,,,0,,,0,,,64.58.61.20,13708,,,,,4.34,0,0,0,0,0,119725,0,90,2,0,90. 909,9.09,0,,0,244," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 06ac8e71,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed
2020-05-26T13:52:56-0500	1590519176,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3473,4674,136188,104772,55531,100000,100000,100000,100000,0,100000, 100000,1298,0,0,50,0,0,0,,,,,,0,,,0,,,64.58.61.20,13794,,,,,4.34,0,0,0,0,0,131514,0,90,2,0,90. 909,9.09,0,,0,1614," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 7ffa9ab3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,fixed

Time	Event
2020-05-26T13:45:56-0500	1590518756,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3464,4662,122681,103424,56410,100000,100000,100000,100000,0,100000, 100000,1299,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13776,,,,,4.34,0,0,0,0,0,118019,0,90,2,0,90. 909,9.09,0,,0,980," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= e3a62c2d,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T13:38:56-0500	1590518336,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3346,4660,137721,107172,55527,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13792,,,,,4.34,0,0,0,0,0,133061,0,90,2,0,90. 909,9.09,0,,0,482," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 8d1d3bd6,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T13:31:56-0500	1590517916,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3436,4645,133538,105492,57300,100000,100000,100000,100000,0,100000, 100000,1298,0,0,44,0,0,0,,,,,,0,,,0,,,64.58.61.20,13798,,,,,4.34,0,0,0,0,0,128893,0,90,2,0,90. 909,9.09,0,,0,383," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 20a06916,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T13:24:56-0500	1590517496,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3391,4693,122649,105501,55782,100000,100000,100000,100000,0,100000, 100000,1298,0,0,52,0,0,0,,,,,,0,,,0,,,64.58.61.20,13722,,,,,4.34,0,0,0,0,0,117956,0,90,2,0,90. 909,9.09,0,,0,3370," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 83daf345,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T13:17:56-0500	1590517076,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3424,4634,143851,104182,57296,100000,100000,100000,100000,0,100000, 100000,1298,0,0,36,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,139217,0,90,2,0,90. 909,9.09,0,,0,523," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 46569812,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T13:10:56-0500	1590516656,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3452,4652,123744,106064,57244,100000,100000,100000,100000,0,100000, 100000,1299,0,0,40,0,0,0,,,,,,0,,,0,,,64.58.61.20,13712,,,,,4.34,0,0,0,0,0,119092,0,90,2,0,90. 909,9.09,0,,0,960," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 84745a02,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T13:03:56-0500	1590516236,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3415,4616,123675,102341,55517,100000,100000,100000,100000,0,100000, 100000,1298,0,0,55,0,0,0,,,,,,0,,,0,,,64.58.61.20,13702,,,,,4.34,0,0,0,0,0,119059,0,90,2,0,90. 909,9.09,0,,0,3397," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= a098d35f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:56:56-0500	1590515816,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3425,4630,122636,102485,56810,100000,100000,100000,100000,0,100000, 100000,1299,0,0,66,0,0,0,,,,,,0,,,0,,,64.58.61.20,13772,,,,,4.34,0,0,0,0,0,118006,0,90,2,0,90. 909,9.09,0,,0,2500," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 4c9a12d3,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed

Time	Event
2020-05-26T12:49:56-0500	1590515396,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3413,4627,134580,106533,59694,100000,100000,100000,100000,0,100000, 100000,1298,0,0,61,0,0,0,,,,,,0,,,0,,,64.58.61.20,13724,,,,,4.34,0,0,0,0,0,129953,0,90,2,0,90. 909,9.09,0,,0,593," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 36666c0e,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:42:56-0500	1590514976,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3600,4968,136854,103745,55511,100000,100000,100000,100000,0,100000, 100000,1298,0,0,36,0,0,0,,,,,,0,,,0,,,64.58.61.20,13704,,,,,4.34,0,0,0,0,0,131886,0,90,2,0,90. 909,9.09,0,,0,561," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 1e9b993f,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:35:56-0500	1590514556,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3403,4610,137663,102474,57284,100000,100000,100000,100000,0,100000, 100000,1298,0,0,47,0,0,0,,,,,,0,,,0,,,64.58.61.20,13798,,,,,4.34,0,0,0,0,0,133053,0,90,2,0,90. 909,9.09,0,,0,392," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 97b7af53,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:28:56-0500	1590514136,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3420,4639,137074,104831,56802,100000,100000,100000,100000,0,100000, 100000,1298,0,0,60,0,0,0,,,,,,0,,,0,,,64.58.61.20,13766,,,,,4.34,0,0,0,0,0,132435,0,90,2,0,90. 909,9.09,0,,0,798," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 09e5b969,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:21:56-0500	1590513716,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3467,4683,124643,105601,55505,100000,100000,100000,100000,0,100000, 100000,1299,0,0,46,0,0,0,,,,,,0,,,0,,,64.58.61.20,13720,,,,,4.34,0,0,0,0,0,119960,0,90,2,0,90. 909,9.09,0,,0,1413," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 00ac29e0,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1300,,,,,,,,,,,fixed
2020-05-26T12:14:56-0500	1590513296,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3450,4653,129515,101537,56798,100000,100000,100000,100000,0,100000, 100000,1298,0,0,42,0,0,0,,,,,,0,,,0,,,64.58.61.20,13716,,,,,4.34,0,0,0,0,0,124862,0,90,2,0,90. 909,9.09,0,,0,224," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= 5a0b21c8,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:07:56-0500	1590512876,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3420,4634,139001,104145,55501,100000,100000,100000,100000,0,100000, 100000,1298,0,0,41,0,0,0,,,,,,0,,,0,,,64.58.61.20,13768,,,,,4.34,0,0,0,0,0,134367,0,90,2,0,90. 909,9.09,0,,0,489," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c8762d14,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed
2020-05-26T12:00:56-0500	1590512456,42610,CO326-DENVPD-NG911PRB-2009130100,,,,"State of Colorado SIP Responders","SIP Responder NG911 Template","Denver City#RCL:511 Bldg ECMC:Denver",com.brixnet.swv.sipservicetest.4.9000,60,,addr, USEPORTRANGE,"G.711 at 20ms",RESPONDER,1,com.brixnet.defaultaudio.1.6071,"G.711 at 20ms",0,0,60,,1 ,100,0,DISABLED,0,0,1,0,0,50000,2,1,0,0,50000,,,16,0,0,0,5060,195@100.73.8.249,SOURCE,NONE, 25000,100000,0,0,10,AUDIOPRFL,,,,10000,,0,250,,75,25,,,60000,50000,,,3600,,,,1,30000,,,,,,500, CALL,CALL,20,0,UDP,,0,200,,,,,3476,4693,131032,106087,57274,100000,100000,100000,100000,0,100000, 100000,1298,0,0,49,0,0,0,,,,,,0,,,0,,,64.58.61.20,13780,,,,,4.34,0,0,0,0,0,126339,0,90,2,0,90. 909,9.09,0,,0,1745," sip:wlssuser@64.58.61.21:5060",BYE;OK,0,sip:442009130999@64.58.61.21;tag= c11f2822,4.4,92,0,,,,,,,,,,,,,,,,,,,,,,,,1298,1299,,,,,,,,,,,fixed

Verifier Health Data

Time	Event
2020-05-27T12:44:15-0500	1590601455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1257717,6,,,,,,,199,1,19999,3,1,900,21229,21643 ,2254415,882399,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C16_7443_a0116c71,C6_7443_1ac13cee,99,12140544, 41484288,973111296,0,0
2020-05-27T12:39:15-0500	1590601155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1257417,6,,,,,,,199,1,19999,3,1,900,21218,21626 ,2252969,878655,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41881600,973111296,0,0
2020-05-27T12:34:15-0500	1590600855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1257117,6,,,,,,,199,1,19999,3,1,900,21213,21621 ,2252329,878480,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41754624,973111296,0,0
2020-05-27T12:29:15-0500	1590600555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1256817,6,,,,,,,199,1,19999,3,1,900,21208,21616 ,2251689,878305,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41508864,973111296,0,0
2020-05-27T12:24:15-0500	1590600255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1256517,6,,,,,,,199,1,19999,3,1,900,21203,21611 ,2251424,878130,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41897984,973111296,0,0
2020-05-27T12:19:15-0500	1590599955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1256217,6,,,,,,,199,1,19999,3,1,900,21198,21606 ,2250784,877955,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41648128,973111296,0,0
2020-05-27T12:14:15-0500	1590599655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1255917,6,,,,,,,199,1,19999,3,1,900,21193,21601 ,2250144,877780,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41668608,973111296,0,0
2020-05-27T12:09:15-0500	1590599355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1255617,6,,,,,,,199,1,19999,3,1,900,21188,21596 ,2249504,877605,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41418752,973111296,0,0
2020-05-27T12:04:15-0500	1590599055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1255317,6,,,,,,,199,1,19999,3,1,900,21183,21591 ,2249239,877430,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41558016,973111296,0,0
2020-05-27T11:59:15-0500	1590598755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1255017,6,,,,,,,199,1,19999,3,1,900,21178,21586 ,2248599,877255,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41684992,973111296,0,0
2020-05-27T11:54:15-0500	1590598455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1254717,6,,,,,,,199,1,19999,3,1,900,21173,21581 ,2247959,877080,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41848832,973111296,0,0
2020-05-27T11:49:15-0500	1590598155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1254417,6,,,,,,,199,1,19999,3,1,900,21168,21576 ,2247694,876905,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41619456,973111296,0,0
2020-05-27T11:44:15-0500	1590597855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1254117,6,,,,,,,199,1,19999,3,1,900,21163,21571 ,2247054,876730,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41598976,973111296,0,0
2020-05-27T11:39:15-0500	1590597555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1253817,6,,,,,,,199,1,19999,3,1,900,21157,21564 ,2246238,876499,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41607168,973111296,0,0
2020-05-27T11:34:15-0500	1590597255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1253517,6,,,,,,,199,1,19999,3,1,900,21152,21559 ,2245598,876324,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41611264,973111296,0,0
2020-05-27T11:29:15-0500	1590596955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1253217,6,,,,,,,199,1,19999,3,1,900,21147,21554 ,2245333,876149,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41639936,973111296,0,0
2020-05-27T11:24:15-0500	1590596655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1252917,6,,,,,,,199,1,19999,3,1,900,21142,21549 ,2244693,875974,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41644032,973111296,0,0
2020-05-27T11:19:15-0500	1590596355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1252617,6,,,,,,,199,1,19999,3,1,900,21137,21544 ,2244053,875799,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41820160,973111296,0,0
2020-05-27T11:14:15-0500	1590596055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1252317,6,,,,,,,199,1,19999,3,1,900,21132,21539 ,2243788,875624,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 42008576,973111296,0,0
2020-05-27T11:09:15-0500	1590595755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1252017,6,,,,,,,199,1,19999,3,1,900,21127,21534 ,2243148,875449,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41545728,973111296,0,0
2020-05-27T11:04:15-0500	1590595455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1251717,6,,,,,,,199,1,19999,3,1,900,21122,21529 ,2242508,875274,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41435136,973111296,0,0

Time	Event
2020-05-27T10:59:15-0500	1590595155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1251417,6,,,,,,,199,1,19999,3,1,900,21117,21524 ,2241868,875099,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41787392,973111296,0,0
2020-05-27T10:54:15-0500	1590594855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1251117,6,,,,,,,199,1,19999,3,1,900,21112,21519 ,2241603,874924,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41537536,973111296,0,0
2020-05-27T10:49:15-0500	1590594555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1250817,6,,,,,,,199,1,19999,3,1,900,21107,21514 ,2240963,874749,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41299968,973111296,0,0
2020-05-27T10:44:15-0500	1590594255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1250517,6,,,,,,,199,1,19999,3,1,900,21102,21509 ,2240323,874574,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41701376,973111296,0,0
2020-05-27T10:39:15-0500	1590593955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1250217,6,,,,,,,199,1,19999,3,1,900,21097,21504 ,2240058,874399,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41332736,973111296,0,0
2020-05-27T10:34:15-0500	1590593655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1249917,6,,,,,,,199,1,19999,3,1,900,21092,21499 ,2239418,874224,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41467904,973111296,0,0
2020-05-27T10:29:15-0500	1590593355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1249617,6,,,,,,,199,1,19999,3,1,900,21087,21494 ,2238778,874049,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41635840,973111296,0,0
2020-05-27T10:24:15-0500	1590593055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1249317,6,,,,,,,199,1,19999,3,1,900,21082,21489 ,2238138,873874,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41877504,973111296,0,0
2020-05-27T10:19:15-0500	1590592755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1249017,6,,,,,,,199,1,19999,3,1,900,21077,21484 ,2237873,873699,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41644032,973111296,0,0
2020-05-27T10:14:15-0500	1590592455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1248717,6,,,,,,,199,1,19999,3,1,900,21072,21479 ,2237233,873524,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41582592,973111296,0,0
2020-05-27T10:09:15-0500	1590592155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1248417,6,,,,,,,199,1,19999,3,1,900,21067,21474 ,2236593,873349,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41873408,973111296,0,0
2020-05-27T10:04:15-0500	1590591855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1248117,6,,,,,,,199,1,19999,3,1,900,21062,21469 ,2236328,873174,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41746432,973111296,0,0
2020-05-27T09:59:15-0500	1590591555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1247817,6,,,,,,,199,1,19999,3,1,900,21057,21464 ,2235688,872999,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41631744,973111296,0,0
2020-05-27T09:54:15-0500	1590591255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1247517,6,,,,,,,199,1,19999,3,1,900,21052,21459 ,2235048,872824,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41893888,973111296,0,0
2020-05-27T09:49:15-0500	1590590955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1247217,6,,,,,,,199,1,19999,3,1,900,21047,21454 ,2234408,872649,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41562112,973111296,0,0
2020-05-27T09:44:15-0500	1590590655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1246917,6,,,,,,,199,1,19999,3,1,900,21042,21449 ,2234143,872474,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41455616,973111296,0,0
2020-05-27T09:39:15-0500	1590590355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1246617,6,,,,,,,199,1,19999,3,1,900,21037,21444 ,2233503,872299,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41676800,973111296,0,0
2020-05-27T09:34:15-0500	1590590055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1246317,6,,,,,,,199,1,19999,3,1,900,21032,21439 ,2232863,872124,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41803776,973111296,0,0
2020-05-27T09:29:15-0500	1590589755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1246017,6,,,,,,,199,1,19999,3,1,900,21027,21434 ,2232598,871949,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41549824,973111296,0,0
2020-05-27T09:24:15-0500	1590589455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1245717,6,,,,,,,199,1,19999,3,1,900,21022,21429 ,2231958,871774,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41680896,973111296,0,0
2020-05-27T09:19:15-0500	1590589155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1245417,6,,,,,,,199,1,19999,3,1,900,21017,21424 ,2231318,871599,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41558016,973111296,0,0
2020-05-27T09:14:15-0500	1590588855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1245117,6,,,,,,,199,1,19999,3,1,900,21012,21419 ,2230678,871424,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41574400,973111296,0,0

Time	Event
2020-05-27T09:09:15-0500	1590588555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1244817,6,,,,,,,199,1,19999,3,1,900,21007,21414 ,2230413,871249,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41422848,973111296,0,0
2020-05-27T09:04:15-0500	1590588255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1244517,6,,,,,,,199,1,19999,3,1,900,21002,21409 ,2229773,871074,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41693184,973111296,0,0
2020-05-27T08:59:15-0500	1590587955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1244217,6,,,,,,,199,1,19999,3,1,900,20997,21404 ,2229133,870899,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41570304,973111296,0,0
2020-05-27T08:54:15-0500	1590587655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1243917,6,,,,,,,199,1,19999,3,1,900,20992,21399 ,2228868,870724,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41697280,973111296,0,0
2020-05-27T08:49:15-0500	1590587355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1243617,6,,,,,,,199,1,19999,3,1,900,20987,21394 ,2228228,870549,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41832448,973111296,0,0
2020-05-27T08:44:15-0500	1590587055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1243317,6,,,,,,,199,1,19999,3,1,900,20982,21389 ,2227588,870374,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41996288,973111296,0,0
2020-05-27T08:39:15-0500	1590586755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1243017,6,,,,,,,199,1,19999,3,1,900,20977,21384 ,2226948,870199,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41750528,973111296,0,0
2020-05-27T08:34:15-0500	1590586455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1242717,6,,,,,,,199,1,19999,3,1,900,20972,21379 ,2226683,870024,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41500672,973111296,0,0
2020-05-27T08:29:15-0500	1590586155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1242417,6,,,,,,,199,1,19999,3,1,900,20967,21374 ,2226043,869849,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41885696,973111296,0,0
2020-05-27T08:24:15-0500	1590585855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1242117,6,,,,,,,199,1,19999,3,1,900,20962,21369 ,2225403,869674,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41639936,973111296,0,0
2020-05-27T08:19:15-0500	1590585555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1241817,6,,,,,,,199,1,19999,3,1,900,20957,21364 ,2225138,869499,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41771008,973111296,0,0
2020-05-27T08:14:15-0500	1590585255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1241517,6,,,,,,,199,1,19999,3,1,900,20952,21359 ,2224498,869324,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41771008,973111296,0,0
2020-05-27T08:09:15-0500	1590584955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1241217,6,,,,,,,199,1,19999,3,1,900,20947,21354 ,2223858,869149,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41922560,973111296,0,0
2020-05-27T08:04:15-0500	1590584655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1240917,6,,,,,,,199,1,19999,3,1,900,20942,21349 ,2223218,868974,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41705472,973111296,0,0
2020-05-27T07:59:15-0500	1590584355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1240617,6,,,,,,,199,1,19999,3,1,900,20937,21344 ,2222953,868799,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41832448,973111296,0,0
2020-05-27T07:54:15-0500	1590584055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1240317,6,,,,,,,199,1,19999,3,1,900,20932,21339 ,2222313,868624,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41963520,973111296,0,0
2020-05-27T07:49:15-0500	1590583755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1240017,6,,,,,,,199,1,19999,3,1,900,20927,21334 ,2221673,868449,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41435136,973111296,0,0
2020-05-27T07:44:15-0500	1590583455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1239717,6,,,,,,,199,1,19999,3,1,900,20923,21329 ,2221408,868274,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41947136,973111296,0,0
2020-05-27T07:39:15-0500	1590583155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1239417,6,,,,,,,199,1,19999,3,1,900,20913,21315 ,2220592,867881,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41594880,973111296,0,0
2020-05-27T07:34:15-0500	1590582855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1239117,6,,,,,,,199,1,19999,3,1,900,20908,21310 ,2219952,867706,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41721856,973111296,0,0
2020-05-27T07:29:15-0500	1590582555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1238817,6,,,,,,,199,1,19999,3,1,900,20903,21305 ,2219312,867531,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41725952,973111296,0,0
2020-05-27T07:24:15-0500	1590582255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1238517,6,,,,,,,199,1,19999,3,1,900,20898,21300 ,2219047,867356,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41607168,973111296,0,0

Time	Event
2020-05-27T07:19:15-0500	1590581955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1238217,6,,,,,,,199,1,19999,3,1,900,20893,21295 ,2218407,867181,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41988096,973111296,0,0
2020-05-27T07:14:15-0500	1590581655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1237917,6,,,,,,,199,1,19999,3,1,900,20888,21290 ,2217767,867006,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41705472,973111296,0,0
2020-05-27T07:09:15-0500	1590581355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1237617,6,,,,,,,199,1,19999,3,1,900,20883,21285 ,2217502,866831,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41582592,973111296,0,0
2020-05-27T07:04:15-0500	1590581055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1237317,6,,,,,,,199,1,19999,3,1,900,20878,21280 ,2216862,866656,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41844736,973111296,0,0
2020-05-27T06:59:15-0500	1590580755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1237017,6,,,,,,,199,1,19999,3,1,900,20873,21275 ,2216222,866481,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41480192,973111296,0,0
2020-05-27T06:54:15-0500	1590580455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1236717,6,,,,,,,199,1,19999,3,1,900,20868,21270 ,2215582,866306,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41504768,973111296,0,0
2020-05-27T06:49:15-0500	1590580155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1236417,6,,,,,,,199,1,19999,3,1,900,20863,21265 ,2215317,866131,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41766912,973111296,0,0
2020-05-27T06:44:15-0500	1590579855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1236117,6,,,,,,,199,1,19999,3,1,900,20858,21260 ,2214677,865956,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41533440,973111296,0,0
2020-05-27T06:39:15-0500	1590579555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1235817,6,,,,,,,199,1,19999,3,1,900,20853,21255 ,2214037,865781,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41639936,973111296,0,0
2020-05-27T06:34:15-0500	1590579255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1235517,6,,,,,,,199,1,19999,3,1,900,20848,21250 ,2213772,865606,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41771008,973111296,0,0
2020-05-27T06:29:15-0500	1590578955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1235217,6,,,,,,,199,1,19999,3,1,900,20843,21245 ,2213132,865431,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41906176,973111296,0,0
2020-05-27T06:24:15-0500	1590578655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1234917,6,,,,,,,199,1,19999,3,1,900,20838,21240 ,2212492,865256,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41783296,973111296,0,0
2020-05-27T06:19:15-0500	1590578355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1234617,6,,,,,,,199,1,19999,3,1,900,20833,21235 ,2211852,865081,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41656320,973111296,0,0
2020-05-27T06:14:15-0500	1590578055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1234317,6,,,,,,,199,1,19999,3,1,900,20828,21230 ,2211587,864906,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41783296,973111296,0,0
2020-05-27T06:09:15-0500	1590577755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1234017,6,,,,,,,199,1,19999,3,1,900,20823,21225 ,2210947,864731,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41414656,973111296,0,0
2020-05-27T06:04:15-0500	1590577455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1233717,6,,,,,,,199,1,19999,3,1,900,20818,21220 ,2210307,864556,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41418752,973111296,0,0
2020-05-27T05:59:15-0500	1590577155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1233417,6,,,,,,,199,1,19999,3,1,900,20813,21215 ,2210042,864381,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41807872,973111296,0,0
2020-05-27T05:54:15-0500	1590576855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1233117,6,,,,,,,199,1,19999,3,1,900,20808,21210 ,2209402,864206,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41525248,973111296,0,0
2020-05-27T05:49:15-0500	1590576555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1232817,6,,,,,,,199,1,19999,3,1,900,20803,21205 ,2208762,864031,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41328640,973111296,0,0
2020-05-27T05:44:15-0500	1590576255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1232517,6,,,,,,,199,1,19999,3,1,900,20798,21200 ,2208122,863856,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41873408,973111296,0,0
2020-05-27T05:39:15-0500	1590575955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1232217,6,,,,,,,199,1,19999,3,1,900,20793,21195 ,2207857,863681,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41750528,973111296,0,0
2020-05-27T05:34:15-0500	1590575655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1231917,6,,,,,,,199,1,19999,3,1,900,20788,21190 ,2207217,863506,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41652224,973111296,0,0

Time	Event
2020-05-27T05:29:15-0500	1590575355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1231617,6,,,,,,,199,1,19999,3,1,900,20783,21185 ,2206577,863331,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41787392,973111296,0,0
2020-05-27T05:24:15-0500	1590575055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1231317,6,,,,,,,199,1,19999,3,1,900,20778,21180 ,2206312,863156,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41664512,973111296,0,0
2020-05-27T05:19:15-0500	1590574755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1231017,6,,,,,,,199,1,19999,3,1,900,20773,21175 ,2205672,862981,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41771008,973111296,0,0
2020-05-27T05:14:15-0500	1590574455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1230717,6,,,,,,,199,1,19999,3,1,900,20768,21170 ,2205032,862806,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41422848,973111296,0,0
2020-05-27T05:09:15-0500	1590574155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1230417,6,,,,,,,199,1,19999,3,1,900,20763,21165 ,2204392,862631,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41820160,973111296,0,0
2020-05-27T05:04:15-0500	1590573855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1230117,6,,,,,,,199,1,19999,3,1,900,20758,21160 ,2204127,862456,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41574400,973111296,0,0
2020-05-27T04:59:15-0500	1590573555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1229817,6,,,,,,,199,1,19999,3,1,900,20753,21155 ,2203487,862281,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41709568,973111296,0,0
2020-05-27T04:54:15-0500	1590573255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1229517,6,,,,,,,199,1,19999,3,1,900,20748,21150 ,2202847,862106,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41459712,973111296,0,0
2020-05-27T04:49:15-0500	1590572955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1229217,6,,,,,,,199,1,19999,3,1,900,20743,21145 ,2202582,861931,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41713664,973111296,0,0
2020-05-27T04:44:15-0500	1590572655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1228917,6,,,,,,,199,1,19999,3,1,900,20738,21140 ,2201942,861756,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41570304,973111296,0,0
2020-05-27T04:39:15-0500	1590572355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1228617,6,,,,,,,199,1,19999,3,1,900,20733,21135 ,2201302,861581,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41705472,973111296,0,0
2020-05-27T04:34:15-0500	1590572055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1228317,6,,,,,,,199,1,19999,3,1,900,20728,21130 ,2200662,861406,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41717760,973111296,0,0
2020-05-27T04:29:15-0500	1590571755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1228017,6,,,,,,,199,1,19999,3,1,900,20723,21125 ,2200397,861231,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41398272,973111296,0,0
2020-05-27T04:24:15-0500	1590571455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1227717,6,,,,,,,199,1,19999,3,1,900,20718,21120 ,2199757,861056,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41615360,973111296,0,0
2020-05-27T04:19:15-0500	1590571155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1227417,6,,,,,,,199,1,19999,3,1,900,20713,21115 ,2199117,860881,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41492480,973111296,0,0
2020-05-27T04:14:15-0500	1590570855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1227117,6,,,,,,,199,1,19999,3,1,900,20708,21110 ,2198852,860706,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 42004480,973111296,0,0
2020-05-27T04:09:15-0500	1590570555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1226817,6,,,,,,,199,1,19999,3,1,900,20703,21105 ,2198212,860531,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41467904,973111296,0,0
2020-05-27T04:04:15-0500	1590570255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1226517,6,,,,,,,199,1,19999,3,1,900,20698,21100 ,2197572,860356,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41598976,973111296,0,0
2020-05-27T03:59:15-0500	1590569955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1226217,6,,,,,,,199,1,19999,3,1,900,20693,21095 ,2196932,860181,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41742336,973111296,0,0
2020-05-27T03:54:15-0500	1590569655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1225917,6,,,,,,,199,1,19999,3,1,900,20688,21090 ,2196667,860006,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41742336,973111296,0,0
2020-05-27T03:49:15-0500	1590569355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1225617,6,,,,,,,199,1,19999,3,1,900,20683,21085 ,2196027,859831,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41381888,973111296,0,0
2020-05-27T03:44:15-0500	1590569055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1225317,6,,,,,,,199,1,19999,3,1,900,20678,21080 ,2195387,859656,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41689088,973111296,0,0

Time	Event
2020-05-27T03:39:15-0500	1590568755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1225017,6,,,,,,,199,1,19999,3,1,900,20672,21073 ,2194946,859425,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41562112,973111296,0,0
2020-05-27T03:34:15-0500	1590568455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1224717,6,,,,,,,199,1,19999,3,1,900,20667,21068 ,2194306,859250,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41443328,973111296,0,0
2020-05-27T03:29:15-0500	1590568155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1224417,6,,,,,,,199,1,19999,3,1,900,20662,21063 ,2193666,859075,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41672704,973111296,0,0
2020-05-27T03:24:15-0500	1590567855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1224117,6,,,,,,,199,1,19999,3,1,900,20657,21058 ,2193026,858900,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41803776,973111296,0,0
2020-05-27T03:19:15-0500	1590567555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1223817,6,,,,,,,199,1,19999,3,1,900,20652,21053 ,2192761,858725,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41676800,973111296,0,0
2020-05-27T03:14:15-0500	1590567255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1223517,6,,,,,,,199,1,19999,3,1,900,20647,21048 ,2192121,858550,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41803776,973111296,0,0
2020-05-27T03:09:15-0500	1590566955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1223217,6,,,,,,,199,1,19999,3,1,900,20642,21043 ,2191481,858375,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41680896,973111296,0,0
2020-05-27T03:04:15-0500	1590566655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1222917,6,,,,,,,199,1,19999,3,1,900,20637,21038 ,2191216,858200,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41553920,973111296,0,0
2020-05-27T02:59:15-0500	1590566355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1222617,6,,,,,,,199,1,19999,3,1,900,20632,21033 ,2190576,858025,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41381888,973111296,0,0
2020-05-27T02:54:15-0500	1590566055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1222317,6,,,,,,,199,1,19999,3,1,900,20627,21028 ,2189936,857850,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41504768,973111296,0,0
2020-05-27T02:49:15-0500	1590565755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1222017,6,,,,,,,199,1,19999,3,1,900,20622,21023 ,2189296,857675,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 42033152,973111296,0,0
2020-05-27T02:44:15-0500	1590565455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1221717,6,,,,,,,199,1,19999,3,1,900,20617,21018 ,2189031,857500,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41635840,973111296,0,0
2020-05-27T02:39:15-0500	1590565155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1221417,6,,,,,,,199,1,19999,3,1,900,20612,21013 ,2188391,857325,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41660416,973111296,0,0
2020-05-27T02:34:15-0500	1590564855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1221117,6,,,,,,,199,1,19999,3,1,900,20607,21008 ,2187751,857150,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41807872,973111296,0,0
2020-05-27T02:29:15-0500	1590564555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1220817,6,,,,,,,199,1,19999,3,1,900,20602,21003 ,2187486,856975,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41422848,973111296,0,0
2020-05-27T02:24:15-0500	1590564255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1220517,6,,,,,,,199,1,19999,3,1,900,20597,20998 ,2186846,856800,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41811968,973111296,0,0
2020-05-27T02:19:15-0500	1590563955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1220217,6,,,,,,,199,1,19999,3,1,900,20592,20993 ,2186206,856625,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41656320,973111296,0,0
2020-05-27T02:14:15-0500	1590563655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1219917,6,,,,,,,199,1,19999,3,1,900,20587,20988 ,2185566,856450,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41541632,973111296,0,0
2020-05-27T02:09:15-0500	1590563355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1219617,6,,,,,,,199,1,19999,3,1,900,20582,20983 ,2185301,856275,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41672704,973111296,0,0
2020-05-27T02:04:15-0500	1590563055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1219317,6,,,,,,,199,1,19999,3,1,900,20577,20978 ,2184661,856100,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41799680,973111296,0,0
2020-05-27T01:59:15-0500	1590562755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1219017,6,,,,,,,199,1,19999,3,1,900,20572,20973 ,2184021,855925,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41684992,973111296,0,0
2020-05-27T01:54:15-0500	1590562455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1218717,6,,,,,,,199,1,19999,3,1,900,20567,20968 ,2183756,855750,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41553920,973111296,0,0

Time	Event
2020-05-27T01:49:15-0500	1590562155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1218417,6,,,,,,,199,1,19999,3,1,900,20562,20963 ,2183116,855575,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41308160,973111296,0,0
2020-05-27T01:44:15-0500	1590561855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1218117,6,,,,,,,199,1,19999,3,1,900,20557,20958 ,2182476,855400,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41566208,973111296,0,0
2020-05-27T01:39:15-0500	1590561555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1217817,6,,,,,,,199,1,19999,3,1,900,20552,20953 ,2181836,855225,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41660416,973111296,0,0
2020-05-27T01:34:15-0500	1590561255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1217517,6,,,,,,,199,1,19999,3,1,900,20547,20948 ,2181571,855050,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41418752,973111296,0,0
2020-05-27T01:29:15-0500	1590560955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1217217,6,,,,,,,199,1,19999,3,1,900,20542,20943 ,2180931,854875,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41672704,973111296,0,0
2020-05-27T01:24:15-0500	1590560655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1216917,6,,,,,,,199,1,19999,3,1,900,20537,20938 ,2180291,854700,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41578496,973111296,0,0
2020-05-27T01:19:15-0500	1590560355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1216617,6,,,,,,,199,1,19999,3,1,900,20532,20933 ,2180026,854525,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41676800,973111296,0,0
2020-05-27T01:14:15-0500	1590560055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1216317,6,,,,,,,199,1,19999,3,1,900,20527,20928 ,2179386,854350,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41680896,973111296,0,0
2020-05-27T01:09:15-0500	1590559755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1216017,6,,,,,,,199,1,19999,3,1,900,20522,20923 ,2178746,854175,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41807872,973111296,0,0
2020-05-27T01:04:15-0500	1590559455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1215717,6,,,,,,,199,1,19999,3,1,900,20517,20918 ,2178106,854000,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41656320,973111296,0,0
2020-05-27T00:59:15-0500	1590559155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1215417,6,,,,,,,199,1,19999,3,1,900,20512,20913 ,2177841,853825,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41689088,973111296,0,0
2020-05-27T00:54:15-0500	1590558855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1215117,6,,,,,,,199,1,19999,3,1,900,20507,20908 ,2177201,853650,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41664512,973111296,0,0
2020-05-27T00:49:15-0500	1590558555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1214817,6,,,,,,,199,1,19999,3,1,900,20502,20903 ,2176561,853475,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41668608,973111296,0,0
2020-05-27T00:44:15-0500	1590558255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1214517,6,,,,,,,199,1,19999,3,1,900,20497,20898 ,2176296,853300,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41558016,973111296,0,0
2020-05-27T00:39:15-0500	1590557955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1214217,6,,,,,,,199,1,19999,3,1,900,20492,20893 ,2175656,853125,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41717760,973111296,0,0
2020-05-27T00:34:15-0500	1590557655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1213917,6,,,,,,,199,1,19999,3,1,900,20487,20888 ,2175016,852950,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41594880,973111296,0,0
2020-05-27T00:29:15-0500	1590557355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1213617,6,,,,,,,199,1,19999,3,1,900,20482,20883 ,2174376,852775,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41472000,973111296,0,0
2020-05-27T00:24:15-0500	1590557055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1213317,6,,,,,,,199,1,19999,3,1,900,20477,20878 ,2174111,852600,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41725952,973111296,0,0
2020-05-27T00:19:15-0500	1590556755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1213017,6,,,,,,,199,1,19999,3,1,900,20472,20873 ,2173471,852425,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41762816,973111296,0,0
2020-05-27T00:14:15-0500	1590556455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1212717,6,,,,,,,199,1,19999,3,1,900,20467,20868 ,2172831,852250,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41381888,973111296,0,0
2020-05-27T00:09:15-0500	1590556155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1212417,6,,,,,,,199,1,19999,3,1,900,20462,20863 ,2172566,852075,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41275392,973111296,0,0
2020-05-27T00:04:15-0500	1590555855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1212117,6,,,,,,,199,1,19999,3,1,900,20457,20858 ,2171926,851900,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41664512,973111296,0,0

Time	Event
2020-05-26T23:59:15-0500	1590555555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1211817,6,,,,,,,199,1,19999,3,1,900,20452,20853 ,2171286,851725,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41541632,973111296,0,0
2020-05-26T23:54:15-0500	1590555255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1211517,6,,,,,,,199,1,19999,3,1,900,20447,20848 ,2170646,851550,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41680896,973111296,0,0
2020-05-26T23:49:15-0500	1590554955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1211217,6,,,,,,,199,1,19999,3,1,900,20442,20843 ,2170381,851375,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41807872,973111296,0,0
2020-05-26T23:44:15-0500	1590554655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1210917,6,,,,,,,199,1,19999,3,1,900,20437,20838 ,2169741,851200,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41861120,973111296,0,0
2020-05-26T23:39:15-0500	1590554355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1210617,6,,,,,,,199,1,19999,3,1,900,20427,20823 ,2168925,850772,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41406464,973111296,0,0
2020-05-26T23:34:15-0500	1590554055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1210317,6,,,,,,,199,1,19999,3,1,900,20422,20818 ,2168660,850597,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41664512,973111296,0,0
2020-05-26T23:29:15-0500	1590553755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1210017,6,,,,,,,199,1,19999,3,1,900,20417,20813 ,2168020,850422,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41803776,973111296,0,0
2020-05-26T23:24:15-0500	1590553455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1209717,6,,,,,,,199,1,19999,3,1,900,20412,20808 ,2167380,850247,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41361408,973111296,0,0
2020-05-26T23:19:15-0500	1590553155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1209417,6,,,,,,,199,1,19999,3,1,900,20407,20803 ,2166740,850072,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41488384,973111296,0,0
2020-05-26T23:14:15-0500	1590552855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1209117,6,,,,,,,199,1,19999,3,1,900,20402,20798 ,2166475,849897,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41639936,973111296,0,0
2020-05-26T23:09:15-0500	1590552555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1208817,6,,,,,,,199,1,19999,3,1,900,20397,20793 ,2165835,849722,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41607168,973111296,0,0
2020-05-26T23:04:15-0500	1590552255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1208517,6,,,,,,,199,1,19999,3,1,900,20392,20788 ,2165195,849547,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41619456,973111296,0,0
2020-05-26T22:59:15-0500	1590551955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1208217,6,,,,,,,199,1,19999,3,1,900,20387,20783 ,2164930,849372,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41365504,973111296,0,0
2020-05-26T22:54:15-0500	1590551655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1207917,6,,,,,,,199,1,19999,3,1,900,20382,20778 ,2164290,849197,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41873408,973111296,0,0
2020-05-26T22:49:15-0500	1590551355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1207617,6,,,,,,,199,1,19999,3,1,900,20377,20773 ,2163650,849022,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41627648,973111296,0,0
2020-05-26T22:44:15-0500	1590551055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1207317,6,,,,,,,199,1,19999,3,1,900,20372,20768 ,2163010,848847,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41631744,973111296,0,0
2020-05-26T22:39:15-0500	1590550755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1207017,6,,,,,,,199,1,19999,3,1,900,20367,20763 ,2162745,848672,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41771008,973111296,0,0
2020-05-26T22:34:15-0500	1590550455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1206717,6,,,,,,,199,1,19999,3,1,900,20362,20758 ,2162105,848497,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41615360,973111296,0,0
2020-05-26T22:29:15-0500	1590550155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1206417,6,,,,,,,199,1,19999,3,1,900,20357,20753 ,2161465,848322,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41529344,973111296,0,0
2020-05-26T22:24:15-0500	1590549855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1206117,6,,,,,,,199,1,19999,3,1,900,20352,20748 ,2161200,848147,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41406464,973111296,0,0
2020-05-26T22:19:15-0500	1590549555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1205817,6,,,,,,,199,1,19999,3,1,900,20347,20743 ,2160560,847972,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41455616,973111296,0,0
2020-05-26T22:14:15-0500	1590549255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1205517,6,,,,,,,199,1,19999,3,1,900,20342,20738 ,2159920,847797,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41750528,973111296,0,0

Time	Event
2020-05-26T22:09:15-0500	1590548955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1205217,6,,,,,,,199,1,19999,3,1,900,20337,20733 ,2159280,847622,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41848832,973111296,0,0
2020-05-26T22:04:15-0500	1590548655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1204917,6,,,,,,,199,1,19999,3,1,900,20332,20728 ,2159015,847447,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41861120,973111296,0,0
2020-05-26T21:59:15-0500	1590548355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1204617,6,,,,,,,199,1,19999,3,1,900,20327,20723 ,2158375,847272,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41738240,973111296,0,0
2020-05-26T21:54:15-0500	1590548055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1204317,6,,,,,,,199,1,19999,3,1,900,20322,20718 ,2157735,847097,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41451520,973111296,0,0
2020-05-26T21:49:15-0500	1590547755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1204017,6,,,,,,,199,1,19999,3,1,900,20317,20713 ,2157470,846922,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41852928,973111296,0,0
2020-05-26T21:44:15-0500	1590547455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1203717,6,,,,,,,199,1,19999,3,1,900,20312,20708 ,2156830,846747,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41730048,973111296,0,0
2020-05-26T21:39:15-0500	1590547155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1203417,6,,,,,,,199,1,19999,3,1,900,20307,20703 ,2156190,846572,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41742336,973111296,0,0
2020-05-26T21:34:15-0500	1590546855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1203117,6,,,,,,,199,1,19999,3,1,900,20302,20698 ,2155550,846397,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41742336,973111296,0,0
2020-05-26T21:29:15-0500	1590546555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1202817,6,,,,,,,199,1,19999,3,1,900,20297,20693 ,2155285,846222,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41746432,973111296,0,0
2020-05-26T21:24:15-0500	1590546255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1202517,6,,,,,,,199,1,19999,3,1,900,20292,20688 ,2154645,846047,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41631744,973111296,0,0
2020-05-26T21:19:15-0500	1590545955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1202217,6,,,,,,,199,1,19999,3,1,900,20287,20683 ,2154005,845872,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41758720,973111296,0,0
2020-05-26T21:14:15-0500	1590545655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1201917,6,,,,,,,199,1,19999,3,1,900,20282,20678 ,2153740,845697,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41607168,973111296,0,0
2020-05-26T21:09:15-0500	1590545355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1201617,6,,,,,,,199,1,19999,3,1,900,20277,20673 ,2153100,845522,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41480192,973111296,0,0
2020-05-26T21:04:15-0500	1590545055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1201317,6,,,,,,,199,1,19999,3,1,900,20272,20668 ,2152460,845347,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41484288,973111296,0,0
2020-05-26T20:59:15-0500	1590544755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1201017,6,,,,,,,199,1,19999,3,1,900,20267,20663 ,2151820,845172,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41832448,973111296,0,0
2020-05-26T20:54:15-0500	1590544455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1200717,6,,,,,,,199,1,19999,3,1,900,20262,20658 ,2151555,844997,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41488384,973111296,0,0
2020-05-26T20:49:15-0500	1590544155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1200417,6,,,,,,,199,1,19999,3,1,900,20257,20653 ,2150915,844822,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41746432,973111296,0,0
2020-05-26T20:44:15-0500	1590543855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1200117,6,,,,,,,199,1,19999,3,1,900,20252,20648 ,2150275,844647,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41713664,973111296,0,0
2020-05-26T20:39:15-0500	1590543555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1199817,6,,,,,,,199,1,19999,3,1,900,20247,20643 ,2150010,844472,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41844736,973111296,0,0
2020-05-26T20:34:15-0500	1590543255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1199517,6,,,,,,,199,1,19999,3,1,900,20242,20638 ,2149370,844297,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41598976,973111296,0,0
2020-05-26T20:29:15-0500	1590542955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1199217,6,,,,,,,199,1,19999,3,1,900,20237,20633 ,2148730,844122,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41603072,973111296,0,0
2020-05-26T20:24:15-0500	1590542655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1198917,6,,,,,,,199,1,19999,3,1,900,20232,20628 ,2148090,843947,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41750528,973111296,0,0

Time	Event
2020-05-26T20:19:15-0500	1590542355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1198617,6,,,,,,,199,1,19999,3,1,900,20227,20623 ,2147825,843772,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41504768,973111296,0,0
2020-05-26T20:14:15-0500	1590542055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1198317,6,,,,,,,199,1,19999,3,1,900,20222,20618 ,2147185,843597,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41140224,973111296,0,0
2020-05-26T20:09:15-0500	1590541755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1198017,6,,,,,,,199,1,19999,3,1,900,20217,20613 ,2146545,843422,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41553920,973111296,0,0
2020-05-26T20:04:15-0500	1590541455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1197717,6,,,,,,,199,1,19999,3,1,900,20212,20608 ,2146280,843247,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41549824,973111296,0,0
2020-05-26T19:59:15-0500	1590541155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1197417,6,,,,,,,199,1,19999,3,1,900,20207,20603 ,2145640,843072,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41533440,973111296,0,0
2020-05-26T19:54:15-0500	1590540855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1197117,6,,,,,,,199,1,19999,3,1,900,20202,20598 ,2145000,842897,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41693184,973111296,0,0
2020-05-26T19:49:15-0500	1590540555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1196817,6,,,,,,,199,1,19999,3,1,900,20197,20593 ,2144360,842722,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41955328,973111296,0,0
2020-05-26T19:44:15-0500	1590540255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1196517,6,,,,,,,199,1,19999,3,1,900,20192,20588 ,2144095,842547,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41705472,973111296,0,0
2020-05-26T19:39:15-0500	1590539955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1196217,6,,,,,,,199,1,19999,3,1,900,20186,20581 ,2143279,842316,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41607168,973111296,0,0
2020-05-26T19:34:15-0500	1590539655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1195917,6,,,,,,,199,1,19999,3,1,900,20181,20576 ,2142639,842141,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41738240,973111296,0,0
2020-05-26T19:29:15-0500	1590539355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1195617,6,,,,,,,199,1,19999,3,1,900,20176,20571 ,2142374,841966,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41607168,973111296,0,0
2020-05-26T19:24:15-0500	1590539055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1195317,6,,,,,,,199,1,19999,3,1,900,20171,20566 ,2141734,841791,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41488384,973111296,0,0
2020-05-26T19:19:15-0500	1590538755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1195017,6,,,,,,,199,1,19999,3,1,900,20166,20561 ,2141094,841616,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41742336,973111296,0,0
2020-05-26T19:14:15-0500	1590538455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1194717,6,,,,,,,199,1,19999,3,1,900,20161,20556 ,2140454,841441,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41639936,973111296,0,0
2020-05-26T19:09:15-0500	1590538155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1194417,6,,,,,,,199,1,19999,3,1,900,20156,20551 ,2140189,841266,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41644032,973111296,0,0
2020-05-26T19:04:15-0500	1590537855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1194117,6,,,,,,,199,1,19999,3,1,900,20151,20546 ,2139549,841091,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41406464,973111296,0,0
2020-05-26T18:59:15-0500	1590537555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1193817,6,,,,,,,199,1,19999,3,1,900,20146,20541 ,2138909,840916,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41549824,973111296,0,0
2020-05-26T18:54:15-0500	1590537255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1193517,6,,,,,,,199,1,19999,3,1,900,20141,20536 ,2138644,840741,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41545728,973111296,0,0
2020-05-26T18:49:15-0500	1590536955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1193217,6,,,,,,,199,1,19999,3,1,900,20136,20531 ,2138004,840566,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41525248,973111296,0,0
2020-05-26T18:44:15-0500	1590536655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1192917,6,,,,,,,199,1,19999,3,1,900,20131,20526 ,2137364,840391,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41451520,973111296,0,0
2020-05-26T18:39:15-0500	1590536355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1192617,6,,,,,,,199,1,19999,3,1,900,20126,20521 ,2136724,840216,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41332736,973111296,0,0
2020-05-26T18:34:15-0500	1590536055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1192317,6,,,,,,,199,1,19999,3,1,900,20121,20516 ,2136459,840041,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41717760,973111296,0,0

Time	Event
2020-05-26T18:29:15-0500	1590535755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1192017,6,,,,,,,199,1,19999,3,1,900,20116,20511 ,2135819,839866,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41590784,973111296,0,0
2020-05-26T18:24:15-0500	1590535455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1191717,6,,,,,,,199,1,19999,3,1,900,20111,20506 ,2135179,839691,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41594880,973111296,0,0
2020-05-26T18:19:15-0500	1590535155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1191417,6,,,,,,,199,1,19999,3,1,900,20106,20501 ,2134914,839516,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41590784,973111296,0,0
2020-05-26T18:14:15-0500	1590534855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1191117,6,,,,,,,199,1,19999,3,1,900,20101,20496 ,2134274,839341,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41607168,973111296,0,0
2020-05-26T18:09:15-0500	1590534555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1190817,6,,,,,,,199,1,19999,3,1,900,20096,20491 ,2133634,839166,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41832448,973111296,0,0
2020-05-26T18:04:15-0500	1590534255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1190517,6,,,,,,,199,1,19999,3,1,900,20091,20486 ,2132994,838991,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41578496,973111296,0,0
2020-05-26T17:59:15-0500	1590533955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1190217,6,,,,,,,199,1,19999,3,1,900,20086,20481 ,2132729,838816,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41209856,973111296,0,0
2020-05-26T17:54:15-0500	1590533655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1189917,6,,,,,,,199,1,19999,3,1,900,20081,20476 ,2132089,838641,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41598976,973111296,0,0
2020-05-26T17:49:15-0500	1590533355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1189617,6,,,,,,,199,1,19999,3,1,900,20076,20471 ,2131449,838466,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41332736,973111296,0,0
2020-05-26T17:44:15-0500	1590533055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1189317,6,,,,,,,199,1,19999,3,1,900,20071,20466 ,2131184,838291,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41496576,973111296,0,0
2020-05-26T17:39:15-0500	1590532755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1189017,6,,,,,,,199,1,19999,3,1,900,20066,20461 ,2130544,838116,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41250816,973111296,0,0
2020-05-26T17:34:15-0500	1590532455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1188717,6,,,,,,,199,1,19999,3,1,900,20061,20456 ,2129904,837941,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41603072,973111296,0,0
2020-05-26T17:29:15-0500	1590532155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1188417,6,,,,,,,199,1,19999,3,1,900,20056,20451 ,2129264,837766,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41607168,973111296,0,0
2020-05-26T17:24:15-0500	1590531855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1188117,6,,,,,,,199,1,19999,3,1,900,20051,20446 ,2128999,837591,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41611264,973111296,0,0
2020-05-26T17:19:15-0500	1590531555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1187817,6,,,,,,,199,1,19999,3,1,900,20046,20441 ,2128359,837416,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41742336,973111296,0,0
2020-05-26T17:14:15-0500	1590531255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1187517,6,,,,,,,199,1,19999,3,1,900,20041,20436 ,2127719,837241,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41496576,973111296,0,0
2020-05-26T17:09:15-0500	1590530955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1187217,6,,,,,,,199,1,19999,3,1,900,20036,20431 ,2127454,837066,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41512960,973111296,0,0
2020-05-26T17:04:15-0500	1590530655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1186917,6,,,,,,,199,1,19999,3,1,900,20031,20426 ,2126814,836891,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41517056,973111296,0,0
2020-05-26T16:59:15-0500	1590530355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1186617,6,,,,,,,199,1,19999,3,1,900,20026,20421 ,2126174,836716,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41377792,973111296,0,0
2020-05-26T16:54:15-0500	1590530055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1186317,6,,,,,,,199,1,19999,3,1,900,20021,20416 ,2125534,836541,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41631744,973111296,0,0
2020-05-26T16:49:15-0500	1590529755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1186017,6,,,,,,,199,1,19999,3,1,900,20016,20411 ,2125269,836366,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41521152,973111296,0,0
2020-05-26T16:44:15-0500	1590529455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1185717,6,,,,,,,199,1,19999,3,1,900,20011,20406 ,2124629,836191,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41529344,973111296,0,0

Time	Event
2020-05-26T16:39:15-0500	1590529155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1185417,6,,,,,,,199,1,19999,3,1,900,20006,20401 ,2123989,836016,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41312256,973111296,0,0
2020-05-26T16:34:15-0500	1590528855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1185117,6,,,,,,,199,1,19999,3,1,900,20001,20396 ,2123724,835841,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41574400,973111296,0,0
2020-05-26T16:29:15-0500	1590528555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1184817,6,,,,,,,199,1,19999,3,1,900,19996,20391 ,2123084,835666,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41701376,973111296,0,0
2020-05-26T16:24:15-0500	1590528255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1184517,6,,,,,,,199,1,19999,3,1,900,19991,20386 ,2122444,835491,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41324544,973111296,0,0
2020-05-26T16:19:15-0500	1590527955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1184217,6,,,,,,,199,1,19999,3,1,900,19986,20381 ,2121804,835316,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41291776,973111296,0,0
2020-05-26T16:14:15-0500	1590527655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1183917,6,,,,,,,199,1,19999,3,1,900,19981,20376 ,2121539,835141,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41422848,973111296,0,0
2020-05-26T16:09:15-0500	1590527355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1183617,6,,,,,,,199,1,19999,3,1,900,19976,20371 ,2120899,834966,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41459712,973111296,0,0
2020-05-26T16:04:15-0500	1590527055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1183317,6,,,,,,,199,1,19999,3,1,900,19971,20366 ,2120259,834791,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41492480,973111296,0,0
2020-05-26T15:59:15-0500	1590526755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1183017,6,,,,,,,199,1,19999,3,1,900,19966,20361 ,2119994,834616,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41369600,973111296,0,0
2020-05-26T15:54:15-0500	1590526455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1182717,6,,,,,,,199,1,19999,3,1,900,19961,20356 ,2119354,834441,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41754624,973111296,0,0
2020-05-26T15:49:15-0500	1590526155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1182417,6,,,,,,,199,1,19999,3,1,900,19956,20351 ,2118714,834266,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41406464,973111296,0,0
2020-05-26T15:44:15-0500	1590525855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1182117,6,,,,,,,199,1,19999,3,1,900,19951,20346 ,2118074,834091,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41512960,973111296,0,0
2020-05-26T15:39:15-0500	1590525555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1181817,6,,,,,,,199,1,19999,3,1,900,19941,20331 ,2117633,833663,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41660416,973111296,0,0
2020-05-26T15:34:15-0500	1590525255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1181517,6,,,,,,,199,1,19999,3,1,900,19936,20326 ,2116993,833488,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41541632,973111296,0,0
2020-05-26T15:29:15-0500	1590524955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1181217,6,,,,,,,199,1,19999,3,1,900,19931,20321 ,2116353,833313,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41291776,973111296,0,0
2020-05-26T15:24:15-0500	1590524655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1180917,6,,,,,,,199,1,19999,3,1,900,19926,20316 ,2116088,833138,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41545728,973111296,0,0
2020-05-26T15:19:15-0500	1590524355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1180617,6,,,,,,,199,1,19999,3,1,900,19921,20311 ,2115448,832963,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41840640,973111296,0,0
2020-05-26T15:14:15-0500	1590524055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1180317,6,,,,,,,199,1,19999,3,1,900,19916,20306 ,2114808,832788,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41562112,973111296,0,0
2020-05-26T15:09:15-0500	1590523755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1180017,6,,,,,,,199,1,19999,3,1,900,19911,20301 ,2114168,832613,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41275392,973111296,0,0
2020-05-26T15:04:15-0500	1590523455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1179717,6,,,,,,,199,1,19999,3,1,900,19906,20296 ,2113903,832438,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41664512,973111296,0,0
2020-05-26T14:59:15-0500	1590523155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1179417,6,,,,,,,199,1,19999,3,1,900,19901,20291 ,2113263,832263,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41414656,973111296,0,0
2020-05-26T14:54:15-0500	1590522855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1179117,6,,,,,,,199,1,19999,3,1,900,19896,20286 ,2112623,832088,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41558016,973111296,0,0

Time	Event
2020-05-26T14:49:15-0500	1590522555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1178817,6,,,,,,,199,1,19999,3,1,900,19891,20281 ,2112358,831913,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41562112,973111296,0,0
2020-05-26T14:44:15-0500	1590522255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1178517,6,,,,,,,199,1,19999,3,1,900,19886,20276 ,2111718,831738,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41439232,973111296,0,0
2020-05-26T14:39:15-0500	1590521955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1178217,6,,,,,,,199,1,19999,3,1,900,19881,20271 ,2111078,831563,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41443328,973111296,0,0
2020-05-26T14:34:15-0500	1590521655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1177917,6,,,,,,,199,1,19999,3,1,900,19876,20266 ,2110438,831388,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41443328,973111296,0,0
2020-05-26T14:29:15-0500	1590521355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1177617,6,,,,,,,199,1,19999,3,1,900,19871,20261 ,2110173,831213,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41472000,973111296,0,0
2020-05-26T14:24:15-0500	1590521055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1177317,6,,,,,,,199,1,19999,3,1,900,19866,20256 ,2109533,831038,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41414656,973111296,0,0
2020-05-26T14:19:15-0500	1590520755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1177017,6,,,,,,,199,1,19999,3,1,900,19861,20251 ,2108893,830863,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41431040,973111296,0,0
2020-05-26T14:14:15-0500	1590520455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1176717,6,,,,,,,199,1,19999,3,1,900,19856,20246 ,2108628,830688,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41689088,973111296,0,0
2020-05-26T14:09:15-0500	1590520155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1176417,6,,,,,,,199,1,19999,3,1,900,19851,20241 ,2107988,830513,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41451520,973111296,0,0
2020-05-26T14:04:15-0500	1590519855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1176117,6,,,,,,,199,1,19999,3,1,900,19847,20237 ,2107348,830373,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41312256,973111296,0,0
2020-05-26T13:59:15-0500	1590519555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1175817,6,,,,,,,199,1,19999,3,1,900,19842,20232 ,2106708,830198,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41439232,973111296,0,0
2020-05-26T13:54:15-0500	1590519255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1175517,6,,,,,,,199,1,19999,3,1,900,19837,20227 ,2106443,830023,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41189376,973111296,0,0
2020-05-26T13:49:15-0500	1590518955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1175217,6,,,,,,,199,1,19999,3,1,900,19832,20222 ,2105803,829848,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41304064,973111296,0,0
2020-05-26T13:44:15-0500	1590518655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1174917,6,,,,,,,199,1,19999,3,1,900,19827,20217 ,2105163,829673,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41553920,973111296,0,0
2020-05-26T13:39:15-0500	1590518355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1174617,6,,,,,,,199,1,19999,3,1,900,19822,20212 ,2104898,829498,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41684992,973111296,0,0
2020-05-26T13:34:15-0500	1590518055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1174317,6,,,,,,,199,1,19999,3,1,900,19817,20207 ,2104258,829323,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41558016,973111296,0,0
2020-05-26T13:29:15-0500	1590517755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1174017,6,,,,,,,199,1,19999,3,1,900,19812,20202 ,2103618,829148,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41218048,973111296,0,0
2020-05-26T13:24:15-0500	1590517455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1173717,6,,,,,,,199,1,19999,3,1,900,19807,20197 ,2102978,828973,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41598976,973111296,0,0
2020-05-26T13:19:15-0500	1590517155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1173417,6,,,,,,,199,1,19999,3,1,900,19802,20192 ,2102713,828798,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41476096,973111296,0,0
2020-05-26T13:14:15-0500	1590516855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1173117,6,,,,,,,199,1,19999,3,1,900,19797,20187 ,2102073,828623,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41324544,973111296,0,0
2020-05-26T13:09:15-0500	1590516555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1172817,6,,,,,,,199,1,19999,3,1,900,19792,20182 ,2101433,828448,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41488384,973111296,0,0
2020-05-26T13:04:15-0500	1590516255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1172517,6,,,,,,,199,1,19999,3,1,900,19787,20177 ,2101168,828273,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41242624,973111296,0,0

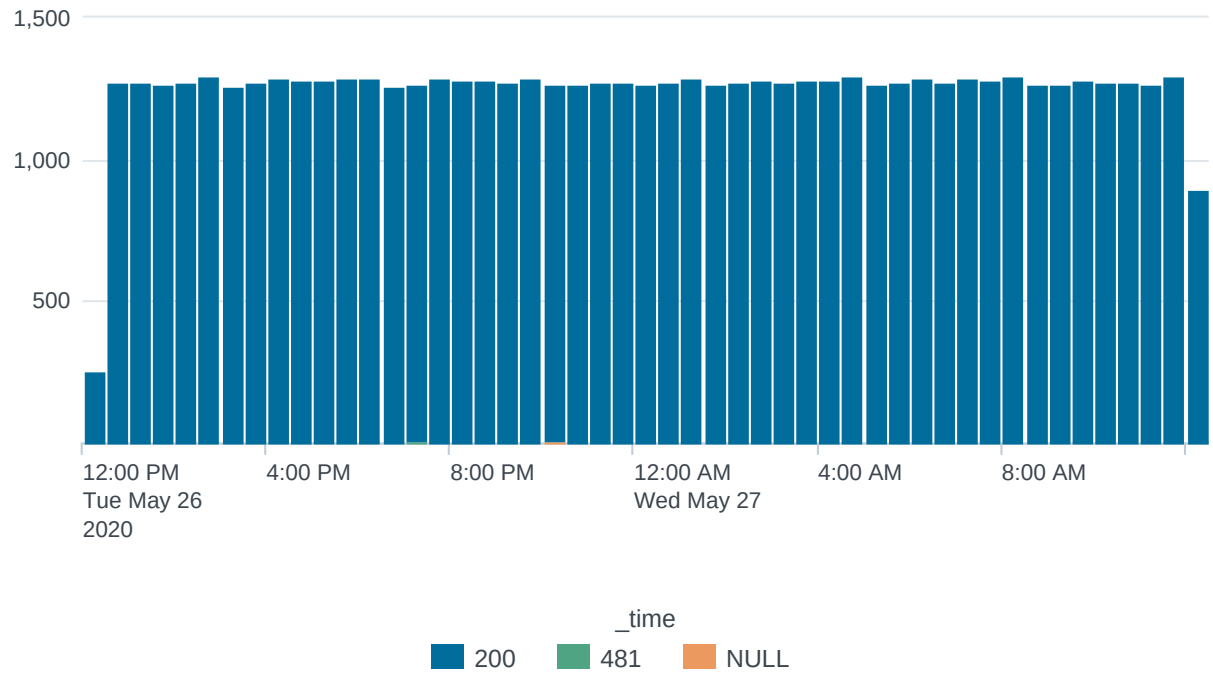
Time	Event
2020-05-26T12:59:15-0500	1590515955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1172217,6,,,,,,,199,1,19999,3,1,900,19782,20172 ,2100528,828098,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41406464,973111296,0,0
2020-05-26T12:54:15-0500	1590515655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1171917,6,,,,,,,199,1,19999,3,1,900,19777,20167 ,2099888,827923,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41410560,973111296,0,0
2020-05-26T12:49:15-0500	1590515355,42086,CO326-DENVPD-NG911PRB-2009130100,0,1171617,6,,,,,,,199,1,19999,3,1,900,19772,20162 ,2099248,827748,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41803776,973111296,0,0
2020-05-26T12:44:15-0500	1590515055,42086,CO326-DENVPD-NG911PRB-2009130100,0,1171317,6,,,,,,,199,1,19999,3,1,900,19767,20157 ,2098983,827573,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41299968,973111296,0,0
2020-05-26T12:39:15-0500	1590514755,42086,CO326-DENVPD-NG911PRB-2009130100,0,1171017,6,,,,,,,199,1,19999,3,1,900,19762,20152 ,2098343,827398,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41562112,973111296,0,0
2020-05-26T12:34:15-0500	1590514455,42086,CO326-DENVPD-NG911PRB-2009130100,0,1170717,6,,,,,,,199,1,19999,3,1,900,19757,20147 ,2097703,827223,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41664512,973111296,0,0
2020-05-26T12:29:15-0500	1590514155,42086,CO326-DENVPD-NG911PRB-2009130100,0,1170417,6,,,,,,,199,1,19999,3,1,900,19752,20142 ,2097438,827048,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41422848,973111296,0,0
2020-05-26T12:24:15-0500	1590513855,42086,CO326-DENVPD-NG911PRB-2009130100,0,1170117,6,,,,,,,199,1,19999,3,1,900,19747,20137 ,2096798,826873,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41590784,973111296,0,0
2020-05-26T12:19:15-0500	1590513555,42086,CO326-DENVPD-NG911PRB-2009130100,0,1169817,6,,,,,,,199,1,19999,3,1,900,19742,20132 ,2096158,826698,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41218048,973111296,0,0
2020-05-26T12:14:15-0500	1590513255,42086,CO326-DENVPD-NG911PRB-2009130100,0,1169517,6,,,,,,,199,1,19999,3,1,900,19737,20127 ,2095518,826523,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41730048,973111296,0,0
2020-05-26T12:09:15-0500	1590512955,42086,CO326-DENVPD-NG911PRB-2009130100,0,1169217,6,,,,,,,199,1,19999,3,1,900,19732,20122 ,2095253,826348,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,99,12140544, 41230336,973111296,0,0
2020-05-26T12:04:15-0500	1590512655,42086,CO326-DENVPD-NG911PRB-2009130100,0,1168917,6,,,,,,,199,1,19999,3,1,900,19727,20117 ,2094613,826173,0,eva-aarch64-monolith-12Dec2018.1.1530.eva,C15_7443_fd26f7ec,C6_7443_1ac13cee,98,12140544, 41488384,973111296,0,0

Initiate On Demand Active Test

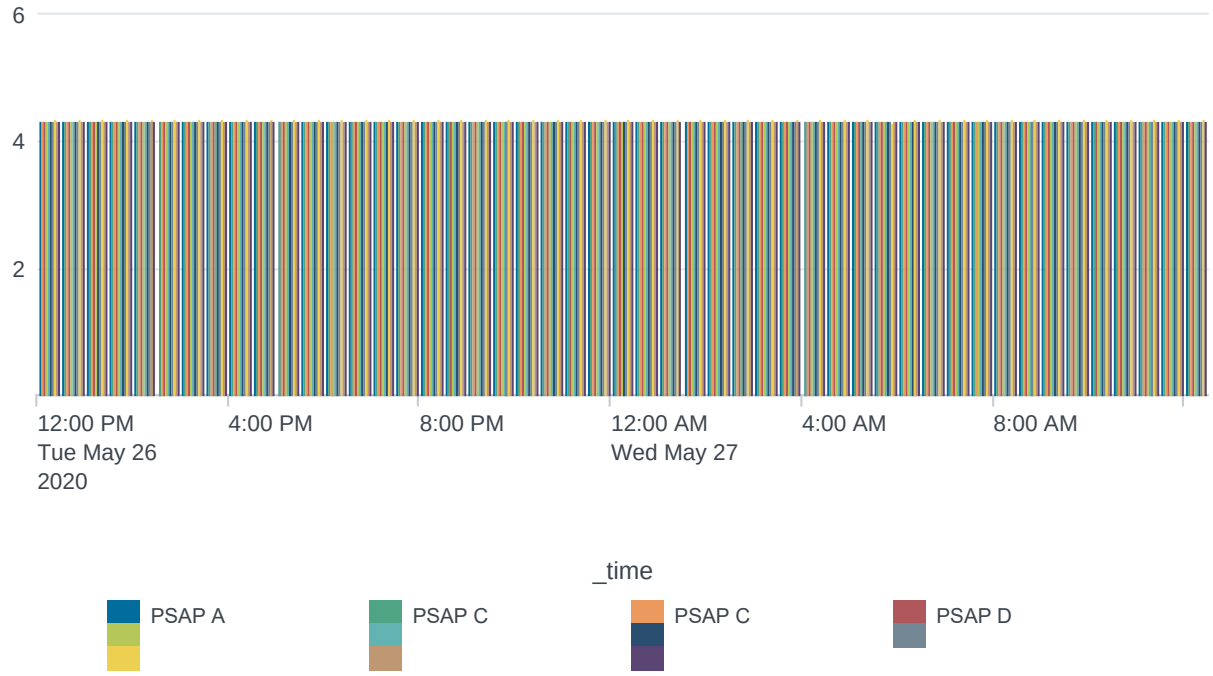
activetestlink

https://63.150.170.73/cgi-bin/all-mina-od.cgi

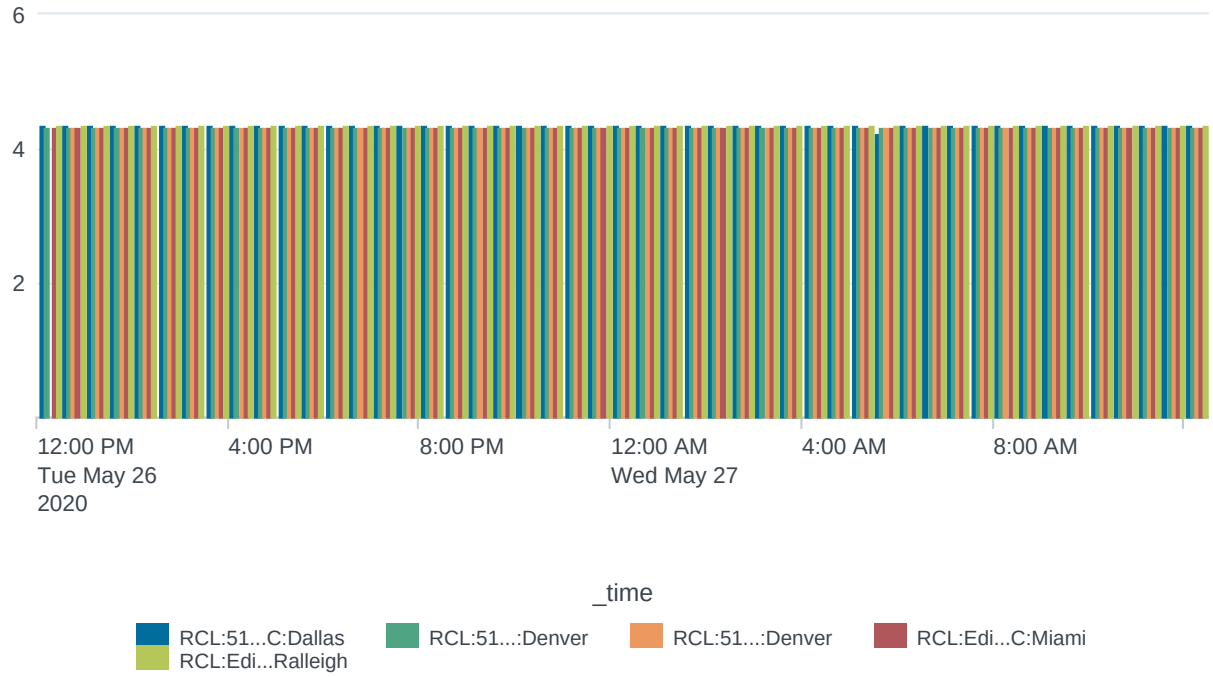
Test Completion Codes



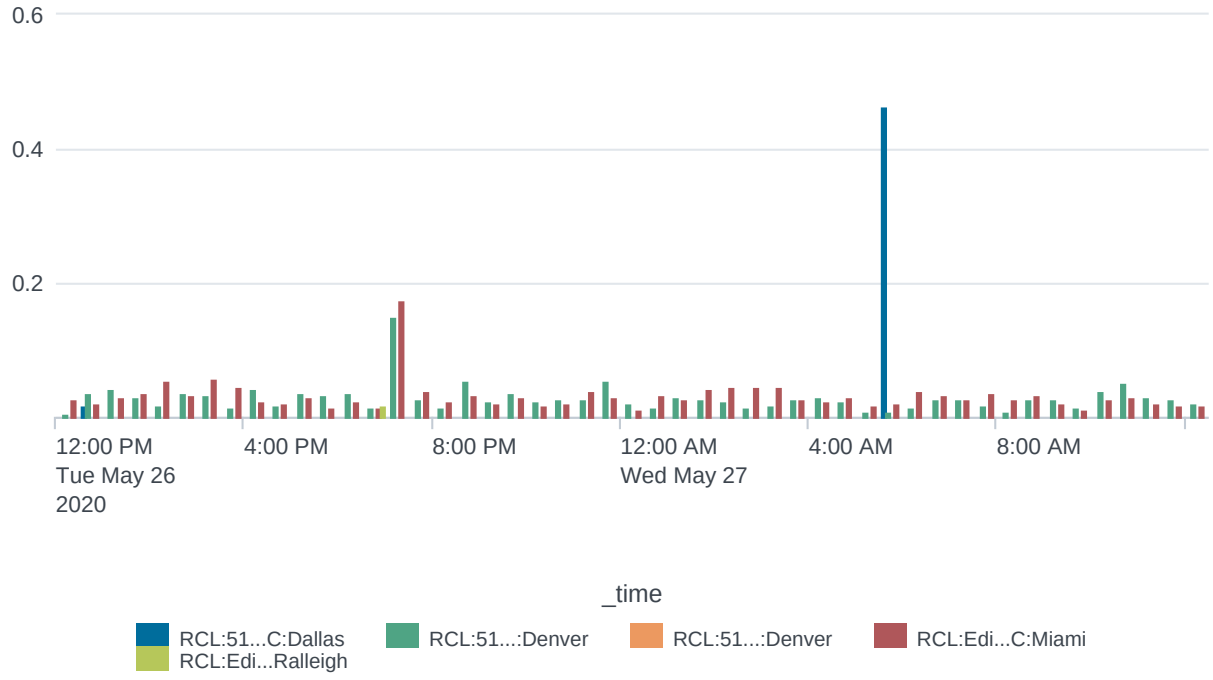
VQES MOS by PSAP



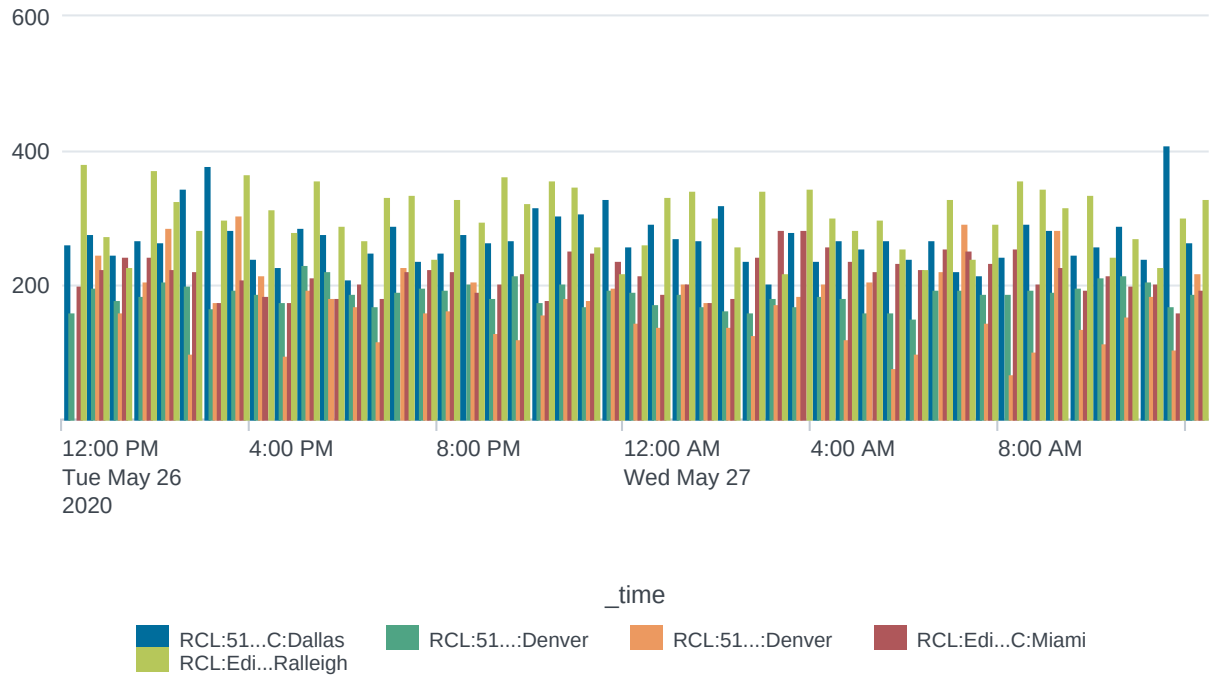
VQES MOS by ECMC Route



Packet Loss Percentage by ECMC Route



Delay Variation (Jitter) by ECMC Route



RTD by ECMC Route

No results found.

Speech Distortion by ECMC Route

No results found.

Signal/Noise by ECMC Route

No results found.

Speech Power by ECMC Route

No results found.

Agreement Document from CenturyLink

Final Audit Report 2020-06-03

Created:	2020-06-03
By:	Bjorn Johnson (bjorn.johnson@centurylink.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAN0q9pUKPMGEraq1zVgNI6fu46Bj-rD3m

"Agreement Document from CenturyLink" History

Document created by Bjorn Johnson (bjorn.johnson@centurylink.com)
2020-06-03 - 4:15:58 PM GMT- IP address: 13.108.254.8

Document emailed to Susan Baker (sue.baker@centurylink.com) for signature
2020-06-03 - 4:18:02 PM GMT

Email viewed by Susan Baker (sue.baker@centurylink.com)
2020-06-03 - 4:50:58 PM GMT- IP address: 155.70.104.122

Document e-signed by Susan Baker (sue.baker@centurylink.com)
Signature Date: 2020-06-03 - 4:51:11 PM GMT - Time Source: server- IP address: 155.70.104.122

Signed document emailed to all eligible parties.
2020-06-03 - 4:51:11 PM GMT

Instructions To Bidders

General

- All cells are locked except those allowing input (shaded green).
- **Do not attempt to edit formula cells**. Any attempt to edit a formula may cause bidder's entire response to be rejected.
- Tabs will contain cells for Non-Recurring Costs (NRC) and Monthly Recurring Charges (MRC).
- Follow the instructions for each Tab.
- Save as an Excel file and give it a unique name, using the following format: "**Company XYZ XXXX Z1 Cost Proposal Option C ESInet and NGCS**".
- Print the workbook (not just the worksheets) to verify content of each tab. Also, verify that all data can be seen in each cell.
- Include the saved Excel file when submitting the RFP response package to the Nebraska State Purchasing Bureau.
- If more rows are needed in each region, you can insert additional rows.
- Each sheet is divided into the 7 regions. Enter pricing information for each region based on bidders implementation plan.
- All PSAPs and regions may not be ready for geospatial routing on day one of operations and Bidder shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. Be sure the cost proposal response indicates the pricing difference between tabular and geospatial routing.
- Include pricing for Optional NGCS services on the Optional Svc tab.

NRC Milestones

- Milestone Payments - NRC payments will be made as structured on the NRC Milestones Tab.As each region is completed on each tab, it is calculated into the total milestone. **Bidders should prepare their cost proposal to reflect the timeline submitted with Bidder's Implementation Plan.**

Summary Tab

- As the name implies, this tab contains the totals from the ESInet, **Legacy Network Gateway (LNG)**, **Border Control Function (BCF)**, **Emergency Services Routing Proxy and Policy Routing Function (ESRP & PRF)**, **Emergency Call Routing Function and Location Validation Function (ECRF & LVF)**, **Spatial Interface (SI)**, **Location Database (LDB)** and **Miscellaneous (MISC) tabs.**
- Enter the Bidder name and date in the designated cells. This information automatically populates the other tabs.
- All other cells are locked.

ESInet Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services IP Network services (hardware, software, connectivity, training, maintenance, etc.) for each region. Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly per person amounts in cents**. The monthly amounts are automatically multiplied by the population of the region and by 12 months.

LNG Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Legacy Network Gateway services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the region's population.

BCF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Border Control Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ESRP & PRF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services Routing Proxy and Policy Routing Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ECRF & LVF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Call Routing Function and Location Validation Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

SI Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information for Spatial Interface services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

LDB Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Location Database services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

MISC Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Miscellaneous services that are not part of one of the above functional elements or that may not have been covered in the RFP but are required in order to complete the project. Add rows for each region as needed.

ESInet Milestones	
Milestone 1: **Region 1** regional host connection and testing acceptance	0.00
Milestone 2: **Region 2** regional host connection and testing acceptance	0.00
Milestone 3: **Region 3** regional host connection and testing acceptance	0.00
Milestone 4: **Region 4** regional host connection and testing acceptance	0.00
Milestone 5: **Region 5** regional host connection and testing acceptance	0.00
Milestone 6: **Region 6** regional host connection and testing acceptance	0.00
Milestone 7: **Region 7** regional host connection and testing acceptance	0.00
TOTAL	0.00

NGCS Milestones	
Milestone 1: **Region 1** deployments complete	60,748.04
Milestone 2: **Region 2** deployments complete	60,748.04
Milestone 3: **Region 3** deployments complete	60,748.04
Milestone 4: **Region 4** deployments complete	60,748.04
Milestone 5: **Region 5** deployments complete	60,748.04
Milestone 6: **Region 6** deployments complete	60,748.04
Milestone 7: **Region 7** deployments complete	60,748.04
TOTAL	425236.28

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
Next Generation Core Services	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**YEAR 6**	**YEAR 7**	**YEAR 8**	**YEAR 9**	**YEAR 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
ESInet	0.00	199,656.00	0.00	465,864.00	0.00	465,864.00	0.00	465,864.00	0.00	465,864.00	465,864.00	465,864.00	465,864.00	465,864.00	465,864.00
LNG	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BCF	23,342.04	43,199.99	31,122.72	100,799.96	0.00	100,799.96	0.00	100,799.96	0.00	100,799.96	100,799.96	100,799.96	100,799.96	100,799.96	100,799.96
ESRP & PRF	99,737.97	703,470.50	132,983.96	1,641,431.16	0.00	1,641,431.16	0.00	1,641,431.16	0.00	1,641,431.16	1,641,431.16	1,641,431.16	1,641,431.16	1,641,431.16	1,641,431.16
ECRF & LVF	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
LDB	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
MISC	59,164.11	0.00	78,885.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Total	182,244.12	946,326.48	242,992.16	2,208,095.11	0.00	2,208,095.11	0.00	2,208,095.11	0.00	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11

Project Totals	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
Yearly Totals (NRC+MRC)	1,128,570.60	2,451,087.27	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11	2,208,095.11
Initial Contract (5 Year NRC+MRC)	10,203,943.22									
+ Optional Year 6 (6 Year NRC+MRC)	12,412,038.33									
+ Optional Years 7 (7 Year NRC+MRC)	14,620,133.45									
+ Optional Years 8 (8 Year NRC+MRC)	16,828,228.56									
+ Optional Years 9 (9 Year NRC+MRC)	19,036,323.68									
+ Optional Years 10 (10 Year NRC+MRC)	21,244,418.79									

State Population	
	2019 Estimates
Region One - ~~SE~~ SC	259,183
Region Two - ~~SC~~ SE	512,126
Region Three - Metro	772,006
Region Four - NC	28,227
Region Five - EC	180,423
Region Six - NE	114,203
Region Seven - Metro West	63,100
Total Population	1,929,268

Bidder Name:	0
Date (MM/DD/YYYY):	1/0/1900

Emergency Services IP Network	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL - (4 Circuits /2 per host)	0.0000	0.0214	0.0000	0.0214	0.0000	0.0214	0.0000	0.0214	0.0000	0.0214	0.0214	0.0214	0.0214	0.0214	0.0214
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 1 TOTAL	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001
Region Two Milestone															
SOUTH EAST - (4 Circuits /2 per host)	0.0000	0.0108	0.0000	0.0108	0.0000	0.0108	0.0000	0.0108	0.0000	0.0108	0.0108	0.0108	0.0108	0.0108	0.0108
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 2 TOTAL	0.0000	66,551.9999	0.0000	66,551.9999	0.0000	66,551.9999	0.0000	66,551.9999	0.0000	66,551.9999	66,551.9999	66,551.9999	66,551.9999	66,551.9999	66,551.9999
Region Three Milestone															
METRO - (4 Circuits /2 per host)			0.0000	0.0072	0.0000	0.0072	0.0000	0.0072	0.0000	0.0072	0.0072	0.0072	0.0072	0.0072	0.0072
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 3 TOTAL	0.0000	0.0000	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001
Region Four Milestone															
NORTH CENTRAL - (4 Circuits /2 per host)			0.0000	0.1965	0.0000	0.1965	0.0000	0.1965	0.0000	0.1965	0.1965	0.1965	0.1965	0.1965	0.1965
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 4 TOTAL	0.0000	0.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000
Region Five Milestone															
EAST CENTRAL - (4 Circuits /2 per host)	0.0000	0.0307	0.0000	0.0307	0.0000	0.0307	0.0000	0.0307	0.0000	0.0307	0.0307	0.0307	0.0307	0.0307	0.0307
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 5 TOTAL	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	0.0000	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001	66,552.0001
Region Six Milestone															
NORTH EAST - (4 Circuits /2 per host)			0.0000	0.0486	0.0000	0.0486	0.0000	0.0486	0.0000	0.0486	0.0486	0.0486	0.0486	0.0486	0.0486
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 6 TOTAL	0.0000	0.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000
Region Seven Milestone															
METRO WEST - (4 Circuits /2 per host)			0.0000	0.0879	0.0000	0.0879	0.0000	0.0879	0.0000	0.0879	0.0879	0.0879	0.0879	0.0879	0.0879
IQ NETWORKING PRIVATE PORTS															
100 MB Bandwidth/1GB Port															
LOCAL ACCESS/100MB															
NETWORK DIVERSITY - IP POP															
NETWORK DIVERSITY - LOOP															
NRC/MRC REGION 7 TOTAL	0.0000	0.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	0.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000	66,552.0000
ESInet Total	0.0000	199,656.0002	0.0000	465,864.0002	0.0000	465,864.0002	0.0000	465,864.0002	0.0000	465,864.0002	465,864.0002	465,864.0002	465,864.0002	465,864.0002	465,864.0002

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
	INITIAL CONTRACT PERIOD														
Legacy Network Gateway	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
INCLUDED COST FOR LEGACY NETWORK GATEWAY IN ESRP & PRF TAB															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
LNG Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
	INITIAL CONTRACT PERIOD														
Border Control Function	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL															
SD-WAN PREMIUM		0.0046		0.0046		0.0046		0.0046		0.0046	0.0046	0.0046	0.0046	0.0046	0.0046
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)	7,780.6800														
NRC/MRC Region 1 Total	7,780.6800	14,399.9991	0.0000	14,399.9991	0.0000	14,399.9991	0.0000	14,399.9991	0.0000	14,399.9991	14,399.9991	14,399.9991	14,399.9991	14,399.9991	14,399.9991
Region Two Milestone															
SOUTH EAST															
SD-WAN PREMIUM		0.0023		0.0023		0.0023		0.0023		0.0023	0.0023	0.0023	0.0023	0.0023	0.0023
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)	7,780.6800														
NRC/MRC Region 2 Total	7,780.6800	14,399.9794	0.0000	14,399.9794	0.0000	14,399.9794	0.0000	14,399.9794	0.0000	14,399.9794	14,399.9794	14,399.9794	14,399.9794	14,399.9794	14,399.9794
Region Three Milestone															
METRO															
SD-WAN PREMIUM				0.0016		0.0016		0.0016		0.0016	0.0016	0.0016	0.0016	0.0016	0.0016
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)			7,780.6800												
NRC/MRC Region 3 Total	0.0000	0.0000	7,780.6800	14,399.9809	0.0000	14,399.9809	0.0000	14,399.9809	0.0000	14,399.9809	14,399.9809	14,399.9809	14,399.9809	14,399.9809	14,399.9809
Region Four Milestone															
NORTH CENTRAL															
SD-WAN PREMIUM				0.0425		0.0425		0.0425		0.0425	0.0425	0.0425	0.0425	0.0425	0.0425
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)			7,780.6800												
NRC/MRC Region 4 Total	0.0000	0.0000	7,780.6800	14,400.0000	0.0000	14,400.0000	0.0000	14,400.0000	0.0000	14,400.0000	14,400.0000	14,400.0000	14,400.0000	14,400.0000	14,400.0000
Region Five Milestone															
EAST CENTRAL															
SD-WAN PREMIUM		0.0067		0.0067		0.0067		0.0067		0.0067	0.0067	0.0067	0.0067	0.0067	0.0067
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)	7,780.6800														
NRC/MRC Region 5 Total	7,780.6800	14,400.0071	0.0000	14,400.0071	0.0000	14,400.0071	0.0000	14,400.0071	0.0000	14,400.0071	14,400.0071	14,400.0071	14,400.0071	14,400.0071	14,400.0071
Region Six Milestone															
NORTH EAST															
SD-WAN PREMIUM				0.0105		0.0105		0.0105		0.0105	0.0105	0.0105	0.0105	0.0105	0.0105
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)			7,780.6800												
NRC/MRC Region 6 Total	0.0000	0.0000	7,780.6800	14,399.9933	0.0000	14,399.9933	0.0000	14,399.9933	0.0000	14,399.9933	14,399.9933	14,399.9933	14,399.9933	14,399.9933	14,399.9933
Region Seven Milestone															
METRO WEST															
SD-WAN PREMIUM				0.0190		0.0190		0.0190		0.0190	0.0190	0.0190	0.0190	0.0190	0.0190
- Security Package - HA - (BCF)															
- HA – CPA Spare Premium (CTL) - (BCF)															
SBC (Routers)			7,780.6800												
NRC/MRC Region 7 Total	0.0000	0.0000	7,780.6800	14,399.9980	0.0000	14,399.9980	0.0000	14,399.9980	0.0000	14,399.9980	14,399.9980	14,399.9980	14,399.9980	14,399.9980	14,399.9980
BCF Total	**23,342.0400**	**43,199.9855**	**31,122.7200**	**100,799.9577**	**0.0000**	**100,799.9577**	**0.0000**	**100,799.9577**	**0.0000**	**100,799.9577**	**100,799.9577**	**100,799.9577**	**100,799.9577**	**100,799.9577**	**100,799.9577**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
Emergency Services Routing Proxy & Policy Routing Function	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL															
INCLUDES:	33,245.9900	0.0754		0.0754		0.0754		0.0754		0.0754	0.0754	0.0754	0.0754	0.0754	0.0754
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 1 Total	33,245.9900	234,490.1670	0.0000	234,490.1670	0.0000	234,490.1670	0.0000	234,490.1670	0.0000	234,490.1670	234,490.1670	234,490.1670	234,490.1670	234,490.1670	234,490.1670
Region Two Milestone															
SOUTH EAST															
INCLUDES:	33,245.9900	0.0382		0.0382		0.0382		0.0382		0.0382	0.0382	0.0382	0.0382	0.0382	0.0382
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 2 Total	33,245.9900	234,490.1655	0.0000	234,490.1655	0.0000	234,490.1655	0.0000	234,490.1655	0.0000	234,490.1655	234,490.1655	234,490.1655	234,490.1655	234,490.1655	234,490.1655
Region Three Milestone															
METRO															
INCLUDES:			33,245.9900	0.0253		0.0253		0.0253		0.0253	0.0253	0.0253	0.0253	0.0253	0.0253
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 3 Total	0.0000	0.0000	33,245.9900	234,490.1616	0.0000	234,490.1616	0.0000	234,490.1616	0.0000	234,490.1616	234,490.1616	234,490.1616	234,490.1616	234,490.1616	234,490.1616
Region Four Milestone															
NORTH CENTRAL															
INCLUDES:			33,245.9900	0.6923		0.6923		0.6923		0.6923	0.6923	0.6923	0.6923	0.6923	0.6923
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 4 Total	0.0000	0.0000	33,245.9900	234,490.1656	0.0000	234,490.1656	0.0000	234,490.1656	0.0000	234,490.1656	234,490.1656	234,490.1656	234,490.1656	234,490.1656	234,490.1656
Region Five Milestone															
EAST CENTRAL															
INCLUDES:	33,245.9900	0.1083		0.1083		0.1083		0.1083		0.1083	0.1083	0.1083	0.1083	0.1083	0.1083
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 5 Total	33,245.9900	234,490.1648	0.0000	234,490.1648	0.0000	234,490.1648	0.0000	234,490.1648	0.0000	234,490.1648	234,490.1648	234,490.1648	234,490.1648	234,490.1648	234,490.1648
Region Six Milestone															
NORTH EAST															
INCLUDES:			33,245.9900	0.1711		0.1711		0.1711		0.1711	0.1711	0.1711	0.1711	0.1711	0.1711
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 6 Total	0.0000	0.0000	33,245.9900	234,490.1662	0.0000	234,490.1662	0.0000	234,490.1662	0.0000	234,490.1662	234,490.1662	234,490.1662	234,490.1662	234,490.1662	234,490.1662
Region Seven Milestone															
METRO WEST															
INCLUDES:			33,245.9900	0.3097		0.3097		0.3097		0.3097	0.3097	0.3097	0.3097	0.3097	0.3097
ECRF & LFV															
SI															
LDB															
LNG															
NRC/MRC Region 7 Total	0.0000	0.0000	33,245.9900	234,490.1655	0.0000	234,490.1655	0.0000	234,490.1655	0.0000	234,490.1655	234,490.1655	234,490.1655	234,490.1655	234,490.1655	234,490.1655
ESRP & PRF Total	**99,737.9700**	**703,470.4973**	**132,983.9600**	**1,641,431.1561**	**0.0000**	**1,641,431.1561**	**0.0000**	**1,641,431.1561**	**0.0000**	**1,641,431.1561**	**1,641,431.1561**	**1,641,431.1561**	**1,641,431.1561**	**1,641,431.1561**	**1,641,431.1561**

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
Emergency Call Routing Function & Location Validation Function	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
ECRF & LVF Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
Spatial Interface	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
SOUTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
Si															
LDB															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
Si															
LDB															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
SI Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)
Date (MM/DD/YYYY):	6/3/2020

Location Database	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
SOUTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
INCLUDED IN : ESRP & PRF TAB															
Includes:															
ECRF & LFV															
SI															
LDB															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
LDB Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)														
Date (MM/DD/YYYY):	6/3/2020														
Miscellaneous	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
SOUTH CENTRAL															
CTL Labor (installation)	2,880.0000														
UPS	12,190.7700														
CTL Rack and related equipment	1,646.6100														
CTL Miscellaneous (patch cables/termination supplies)	3,003.9900														
NRC/MRC Region 1 Total	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
CTL Labor (installation)	2,880.0000														
UPS	12,190.7700														
CTL Rack and related equipment	1,646.6100														
CTL Miscellaneous (patch cables/termination supplies)	3,003.9900														
NRC/MRC Region 2 Total	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO			2,880.0000												
CTL Labor (installation)			12,190.7700												
UPS			1,646.6100												
CTL Rack and related equipment			3,003.9900												
CTL Miscellaneous (patch cables/termination supplies)															
NRC/MRC Region 3 Total	0.0000	0.0000	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
CTL Labor (installation)			2,880.0000												
UPS			12,190.7700												
CTL Rack and related equipment			1,646.6100												
CTL Miscellaneous (patch cables/termination supplies)			3,003.9900												
NRC/MRC Region 4 Total	0.0000	0.0000	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
CTL Labor (installation)	2,880.0000														
UPS	12,190.7700														
CTL Rack and related equipment	1,646.6100														
CTL Miscellaneous (patch cables/termination supplies)	3,003.9900														
NRC/MRC Region 5 Total	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
CTL Labor (installation)			2,880.0000												
UPS			12,190.7700												
CTL Rack and related equipment			1,646.6100												
CTL Miscellaneous (patch cables/termination supplies)			3,003.9900												
NRC/MRC Region 6 Total	0.0000	0.0000	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
CTL Labor (installation)			2,880.0000												
UPS			12,190.7700												
CTL Rack and related equipment			1,646.6100												
CTL Miscellaneous (patch cables/termination supplies)			3,003.9900												
NRC/MRC Region 7 Total	0.0000	0.0000	19,721.3700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
MISC Total	**59,164.1100**	**0.0000**	**78,885.4800**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

Bidder Name:	Centurylink (NGCS & ESINET Solution 1)
Date (MM/DD/YYYY):	6/3/2020

Optional Svc for NGCS	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
SOUTH CENTRAL															
TSP Provisioning installation and/or Restoration priority	578.0000														
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 1 Total	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
SOUTH EAST															
TSP Provisioning installation and/or Restoration priority	578.0000														
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 2 Total	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
METRO															
TSP Provisioning installation and/or Restoration priority			578.0000												
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 3 Total	0.0000	0.0000	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
NORTH CENTRAL															
TSP Provisioning installation and/or Restoration priority			578.0000												
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 4 Total	0.0000	0.0000	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
EAST CENTRAL															
TSP Provisioning installation and/or Restoration priority	578.0000														
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 5 Total	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
NORTH EAST															
TSP Provisioning installation and/or Restoration priority			578.0000												
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 6 Total	0.0000	0.0000	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
METRO WEST															
TSP Provisioning installation and/or Restoration priority			578.0000												
TSP Restoration priority for Leased Access, per Local Access circuit															
TSP Priority Level Change															
TSP Administration and Maintenance															
NRC/MRC Region 7 Total	0.0000	0.0000	578.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Opt. Svc NGCS Total	**1,734.0000**	**0.0000**	**2,312.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Bidders are instructed to complete a Matrix for Emergency Services Internet Protocol (IP) network (ESInet). Bidders are required to describe in detail how bidder's proposed solution meets the conformance specification outlined within each Requirement. The matrix is used to document and evaluate bidder's response to the requirements.

The matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. PSC will consider any such response to the requirements in this RFP to be non-responsive and the bid may be rejected. The narrative should provide The Public Service Commission (PSC) with sufficient information to differentiate the bidder's business solution from other bidders' solutions. Bidder shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details shall be provided in the same paragraph as the requirement. Bidder shall not include pricing information in the description and shall not refer the reader to pricing.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the matrix as provided by PSC. Failure to maintain these elements may render the bid non-responsive and result in for rejection of the bidder.

The bidder's response to each of the below requirements shall include an indication on the level of compliance that can be met. (Complies, Complies Partially, Complies with Future Capability, Does Not Comply) Bidder shall respond by placing an "X" in only **one** checkbox per requirement. Failure to complete this process properly will be treated the same as "Does Not Comply," and may result in the rejection of the response form.

1. Complies: Bidder's proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, generally available, and successfully deployed. Responding with "Complies" or "Complies with Future Capability" shall mean the bidder's solution meets or exceeds the requirement regardless of any comments included as additional information.

2. Complies Partially: Bidder's proposal addresses the RFP requirements through another method that currently is developed and available for implementation (i.e., shall be generally available), or the solution complies with some, but not all of the requirements. Bidder is responsible for clearly explaining how the proposed solution does not fully comply.

3. Complies with Future Capability: The RFP requirements will be met with a capability delivered at a future date. This response shall include a calendar quarter and year in which the requirement will be met with a generally available product or service at no additional cost.

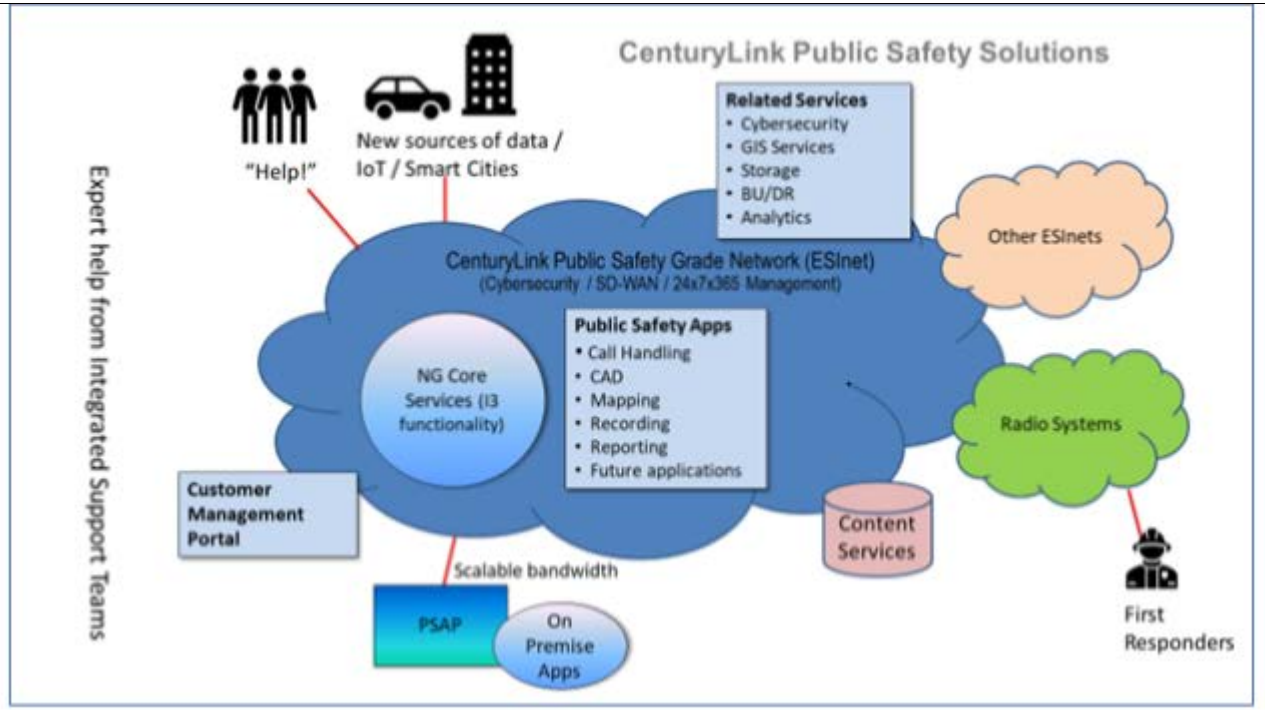
4. Does Not Comply: Bidder's proposal does not/cannot meet the specific RFP requirement.

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Req Identifier	Requirement Description				
GEN-1	**General Requirements** - **Bidder Vision of NG911** The Commission is issuing this RFP for the purpose of selecting a qualified bidder that understands and can clearly demonstrate alignment with the industry's evolution to NENA i3 -compliant ESInet and NGCS solutions. Describe bidder's vision of NG911 and how bidder's vision aligns with NENA's i3 standard, bidder's approach to monitoring and supporting evolving standards and the bidder's level of involvement in standards development and Industry Collaboration Events (ICE).	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink has a proud history of supporting 9-1-1 services throughout the United States for over 60 years and is fully committed to supporting The State of Nebraska in its journey of implementing a NENA i3 compliant Next Generation 9-1-1 (NG9-1-1) Core Services and ESInet platform. CenturyLink understand the methodology an implementation of a NG9-1-1 solution is a complex one. This complexity is reflected in the multiple, interrelated elements of NG9-1-1 (ESInets, NG core services, PSAP applications, GIS data, new data sources, etc.) Our vision for the Nebraska Public Safety community is to assist in this journey to ensure a smooth transition to a NG9-1-1 solution. Every year more elements are added to the mix and the complexity expands. New standards are released, new vendors enter the marketplace, methods of communication evolve and IoT promises to unleash new data types to be understood and leveraged to provide public safety. The evolution of NG9-1-1 will be complex, and the complexity will not end. At the beginning of the journey it is important to recognize that each city, county or state will design its own unique path to NG9-1-1, but all paths will be made up of common NG9-1-1 Building Blocks. The foundation for CenturyLink's NG9-1-1 solution is our award-winning network. As a leading network innovator, CenturyLink holds approximately 3,142 pending and issued patents worldwide. Our patent portfolio currently includes patents covering a wide range of telecom technologies: • Content delivery network and streaming media services (13%) • Voice and Softswitch services (25%) • Networking, infrastructure, and data services (47%) • Provisioning and systems design, including IT (1%) • Network security (1%) • Collaboration services, including Ready-Access (1%) • Other (12%) CenturyLink will continue to be a leader in network technologies, innovating and adapting industry standards as they evolve. CenturyLink is a long-term partner, contributor and supporter of the Metro Ethernet Forum (MEF) vision. We are an active participant in MEF initiatives, conferences, working group leadership, proof of concept show cases, certification processes and standards-making activities. The Metro Ethernet Form is an international industry association of about 200 companies dedicated to the adoption of assured services orchestrated across a global ecosystem of automated networks. In November 2019, our President and CEO, Jeff Story, was awarded the association's prestigious MEF-19 Industry Executive of the Year award for "leading bold investments in technology, advanced networking, and enterprise services." In addition, we also took home seven awards for				

	network services powered by Lifecycle Service Orchestration (LSO), Software Defined Networking (SDN), Network Functions Virtualization (NFV), Carrier Ethernet and SD-WAN technologies. In respect to Security, CenturyLink believes strong partnerships and collaboration among critical infrastructure providers and the public sector are vital to our nation's ability to combat and counteract cyber threats. As a designated critical infrastructure provider, CenturyLink plays a prominent role within the communications industry and with a wide range of public and private sector organizations to help keep us secure. This engagement includes Security Services we tailor to our customer needs such as the secure cloud connectivity and high speed Managed Trusted Internet Protocol Service (MTIPS) services provided to the U.S. Census Bureau to help them digitize the 2020 Census by moving it to an online platform, thus supporting the agency's IT modernization efforts. These services enable the detection and defense against aggressive network attacks while meeting the federal government's strict security standards and requirements. Additionally, CenturyLink's work as a critical infrastructure provider and leader in establishing sound cybersecurity policies and governance for the communications sector. We are a trusted partner for collaborative public-private relationships, including our recent cybersecurity work with the U.S. Department of Homeland Security (DHS) and ongoing support for the technical working groups of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC). CenturyLink also provided crucial input and leadership to the recent DHS Information and Communications Technology (ICT) criticality assessment that will support the development of additional strategies to protect our nation's critical communications infrastructure. In addition, CenturyLink has been providing considerable policy, security and legal expertise to the DHS ICT Supply Chain Risk Management Task Force working groups. We are providing leadership and support for four workstreams on current supply chain risks, including information exchange; threat-based evaluation of ICT supplies, products, and services; development of qualified bidder and manufacturer lists; and purchase of ICT from original manufacturers or authorized resellers. This public-private effort includes 20 federal agencies as well as 40 of the largest companies in the ICT sector. CenturyLink was also selected to help support a Government Accountability Office (GAO) report to Congress on the use and impacts of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework. Through our written response and comprehensive discussions with policymakers, we conveyed that NIST's Cybersecurity Framework has been a valuable tool for ensuring that security is integrated throughout an entire organization. This collaboration with NIST also includes CenturyLink's participation in The National Cybersecurity Center of Excellence (NCCoE) project on ensuring safe and secure internet traffic exchange - Secure Inter-Domain Routing Phase 1 - Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation. This project used commercially available technologies to develop a cybersecurity reference design that can be implemented to increase security and functionality in internet routing. CenturyLink actively participates on NENA working groups focused on ESInet and network security standards. We meet or exceed all NENA compliance requirements for ESInet. Our MPLS / IP VPN is the connectivity service based on IP MPLS technology that provides privacy and reliability in the transfer of information in a flexible, secure and scalable. It is a converging solution that allows you to stream multiple applications, voice and video by using a single network connection, ensuring the desired quality of each service. We see the ESInet as the foundation to support all critical applications utilized within the PSAP and Public Safety community. This would include CAD, Radio, Command & Control, or any other service or application requiring an adaptable, scalable, reliable, and secure IP enabled network. To support the applications that will ride the ESInet, will require new tools and highly skilled engineers to manage and monitor these critical and complex networks. Therefore, we are building a new, state of the art, NG911 NOC/SOC that will go online 4th quarter of 2020.

	Our NG9-1-1 vendor Synergem was the first to provision an end-to-end NENA i3 network and is currently the market share leader in terms of PSAPs contracted to support i3 NGCS. Because of this record, our staff members have been invited to sit on and sometimes chair the NENA committees charged with standards development. CenturyLink, along with our vendor Synergem have participated in NENA Industry Collaboration Events (ICE) held since 2011. Our vendor also served as members of the Event Planning Committee for ICE 5, 6 & 8. We've presented our suite of solutions for rigorous standards compliance and interoperability testing. ICE-6 focused on end-to-end NENA NG9-1-1 architecture functionality, interaction between vendor elements, and interoperability testing. Past ICE events leveraged elements which make up the end-to-end architecture. However, within each of those events participants focused on interfaces or facets of i3. This was the first time at ICE that an ESRP hierarchy was tested. Previous events used only one ESRP, but two were used at this event – a regional ESRP, and a county ESRP. This was done for each test run. This is a notable first for ICE, since it helped expose some issues in the i3 architecture, regarding call setup times and the possibility for loops that cannot be avoided. ICE 6 was also the first instance where complex geodetic shapes (like Circles, Ellipses, ArcBands, and Polygons) were used in conjunction with the kinds of calls enumerated. (Basic audio calls at ICE 3 and 4 also marked the testing of what were then, major innovations. This was the first time that new kinds of shapes were used with an ESRP hierarchy as well (the multilevel Regional and County ESRPs that were set up). This is the first time that the geodetic shape overlap onto ECRF coverage regions was tested. A partial list of the standards to which CenturyLink contributed includes: • 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

	 **Gen 1 - CenturyLink's NG9-1-1 Vision: An Integrated Solution Built on a Solid Foundation**

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

GEN-2	**Proprietary Solutions and Standards** 1. Describe any use of proprietary standards, interfaces, or protocols in bidder's proposed solution. 2. Describe any patented technology in the proposed solution, who owns the patent and describe any licensing arrangements. Disclose any technological limitations, in the response.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1. CenturyLink, along with vendor Synergem, does not employ proprietary standards, interfaces, or protocols in our subscription services. We own thousands of patents that contribute to the innovative, efficient, and reliable methods embedded in the design of our NGCS and ESInet solution. Licensing for applicable patented technologies and methods is included through services. CenturyLink employees a suite of hosted network solutions that is a non-proprietary NENA i3-compliant solution. CenturyLink has is a fully redundant/diverse network designed to offer services in compliance with the NENA NG9-1-1 standards defined in NENA-STA-010.2-2016 and future updates Our proposed solution is built on an open, standards-based platform. The system shall comply with SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), NENA 08-003, IETF ECRIT best practices, and ANSI standards. Our ESInet is designed on the basic principle of having no single point of failure. It provides open standards-based interfaces for interconnecting to today's existing legacy Time Division Multiplexed (TDM), point-to-point bearer channel trunking, as well as open, standards-based Session Initiation Protocol (SIP) interfaces for connecting to the most advanced carrier switches. CenturyLink is committed to supporting the NENA STA-010.2 standards for all external interfaces included in the CenturyLink ESINet offering that require interoperability with other vendors' systems. CenturyLink's NGCS solution network routing uses Standard protocols such as Open Shortest Path First ("OSPF") protocol, as defined in RFC 2328 and RFC 5340. External network routing, such as that to service providers and Egress ESInets, Border Gateway Protocol (BGP) peering is configured with Bidirectional Forwarding Detection (BFD) to enhance convergence times. The network architecture adheres to the guidelines and recommendations of the NENA ESIND (ESInet Network Design) CenturyLink meets the security criteria as defined in the NENA NG-SEC specifications for NG9-1-1 security. Our NGCS service adheres to the NENA i3 standards for NG9-1-1 models and offers customers transition strategies to an NG9-1-1 end state while maximizing investment and leveraging existing network assets. Our proposed CenturyLink solution supports interconnection with OSP's and Systems Service Providers (SSPs) in adjacent states as well as interconnection with regional networks. The CenturyLink solution supports interconnection to both legacy TDM emergency networks and next generation i3 ESInets. CenturyLink adheres to the various required interoperability non-proprietary protocols specified for use in the NENA i3 standards, such as HTTP-Enabled Location Delivery (HELD), LoST, Additional Data, MSRP, and others. 2. CenturyLink represents that it has all intellectual property rights to provide the offered solution. There are no technical limitations based on patents or other intellectual property rights.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	System and Network Architecture The Commission is seeking a Public Safety Grade Next Generation 911 System. System and network architecture, including the design and deployment of interface functions and security measures, shall comply with current NENA i3 requirements as established in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards for the NENA i3 Solution. Describe how the solution meets or exceeds the requirements in Section V.D.1.b. of the RFP.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-3	The Next Generation Core Services (NGCS) are provided as a "Software as a Solution" as part of our NGCS Solution design consistent with the NG9- 1-1 standards defined in NENA-STA-010.2-2016 as updated. Tour service is supported by a highly survivable network architecture designed from ingress to egress to have no single point of failure of critical elements. Each NGCS instance has been provisioned in an active-active configuration within each datacenter. The active-active design of each datacenter employs redundant, highly resilient, fault-tolerant components each simultaneously processing 100% of the load. Consequently, there is no fail-over. In our active-active design, if one component should fail, the redundant component within that datacenter *continues* to carry the entire load with no delay and no degradation of service. Our architecture is further supported by geographically diverse data centers that each operate in tandem. Each core service instance in each datacenter simultaneously processes calls. Consequently, if three of the four instances should fail, the remaining instance will continue to carry the entire load with no degradation of service. Characteristics of our NGCS solution that allows us to exceed requirements in Section V.D.1.b: • No single point of failure • 99.999% availability • Capable of dynamically bursting to support extreme call volumes • Each geo-redundant datacenter meets Tier III standards developed by the Telecommunications Industry Association (TIA) and the Uptime Institute (UI). Other measures include hardened defined external perimeters, hardened outer walls with no openings available for exploitation, access control lists, and at least two automated ID sensors. Visits by uncleared individuals must be approved in advance. All visitors are escorted. • We propose to install a suite of fully redundant, next generation core services designed in compliance with the NG9- 1-1 standards defined in NENA-STA-010.2-2016 as updated. These core services are provided as a "Software as a Solution". The ability to grow and integrate new capabilities is a built-in characteristic. This suite can be enhanced centrally with performance bounded only by the size and scope of local infrastructure. As it is proposed, this proposal is highly scalable capable of handling up to 4 million routes and up to 500,000 SIP-TLS sessions. It will: • Provide an **active-active** configuration for each of its Core Services for 99.999% availability. • Present no single points of failure. Our NGCS are designed to leverage multiple tiers of redundancy to eliminate any single point of failure. This Datacenter interconnectivity supported by an SD-WAN with dual-path, carrier diverse facilities delivered via separate building entrances. • All functional elements of the network architecture are N+1. • Supports calls from a variety of classes of service including Session Initiated Protocol (SIP), video, photos, text-to-9-1-1, and other modalities as carriers develop the capability to deliver them. • Capable of interconnecting with other NGCS providers per NENA's "Network of Networks" vision				

	• Each data center supported by emergency power consistent with SSAE 16 standards. Each data center is supported by redundant power grids and has up to three days of generator capacity. Each data center is considered a priority restoration site. • CenturyLink ESInet service is designed with complete Point of Present (POP) and local loop diversity utilizing autonomous System (AS) public safety grade diverse MPLS private IP networks. • Our MPLS networks terminate to each PSAP on separate edge Network Interface Devices (nids) and SBCBCF devices that will be connected to one of the pair of High Availability (HA) SDWAN appliances located at the PSAP. • PSAP demarcation will include SDWAN appliances that will be utilized for monitoring of all the networking edge devices for the ESInet. • The SDWAN platform will also create flows for the PSAP to ensure secure segmented delivery of Internet traffic and path diversity to the our NG9-1-1 solution.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

GEN-4	**General Requirements – Capacity- Initial Design and Deployment** The bidder's initial design and deployment of the ESInet and NGCS elements, including all components and physical network segments, shall provide capacity that will support current and planned ESInet traffic and usage that occurs as a result of data sharing in, and between, all participating PSAPs, the Commission, and designated support agencies. Additionally, the system and network design shall allow for 50 percent traffic and usage growth for the life of the contract. All current and potential core functions and applications shall be considered, e.g., call-handling systems, CAD, logging, GIS data, streaming media, real-time text (RTT), IP traffic, traffic management systems, communications systems, and incident management systems. Describe how bidder's solution will meet or exceed the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our ESInet is capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. CenturyLink can easily scale IP capacities through simple provisioning processes, eliminating the need for additional network buildouts, and enabling customers to increase capacities within a few weeks vs. months. CenturyLink will work with the State of Nebraska for capacity planning and to mutually agree on ordering timeframes. This methodology provides the State of Nebraska with a cost-effective solution in the near term and allows for growth based on coordinated agreements. The IP network transport used by CenturyLink's NGCS will initially be sized to comply with specified network bandwidth requirements. The CenturyLink MPLS IP network is monitored for capacity trends that indicate the need for proactive growth of the ESInet. As the needs of the State of Nebraska grow, local PSAP connectivity bandwidth will be scaled up or down by a change order process or through procedures as defined in the SLA and/or contract. Our solution provides a fully compliant, scalable environment in the existing LNG and ESInet core infrastructure. Currently the LNGs operate with redundancy at each location and the bandwidth is expandable in a short timeframe with no need for a forklift upgrade. The proposed network platform can handle up to 4 million routes and 500,000 SIP-TLS sessions. It features software code derived from the Ubiquity carrier-grade JSR 289 platform. It has been market tested to support over 3 Million Busy Hour Call Completions and it can support up to 25,000 locations and 250,000 SIP users. This allows us to size capacity of circuits in accordance with expected call volume and call handling capacity of the connected sites. Datacenter links are also provisioned and sized to handle the expected call volume. It is difficult to envision a capacity issue that would be beyond this system.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

GEN-5	**Capacity - Scalable Deployment** As the Commission migrates toward a fully compliant NG911 environment, additional PSAP functions will transition to the systems and network. The bidder's systems and network solution shall be designed and deployed in a way that is easily scalable, with the capability to grow in both capacity and coverage without disruption in service. Describe in detail how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

Our solution is specifically designed to accept new functions that comply with present and future NENA standards. Since such compatibility is a core feature of our business model, we ensure that our staff participates in most, if not all, of the NENA committees charged with developing the standards that impact our product suite. We are confident that we can accommodate changes in these standards within a calendar year of the change's introduction. New applications often require growth in network capacity; however, our NGCS is highly scalable and is capable of handling up to 4 million routes and up to 500,000 SIP-TLS sessions. This far exceeds any additional need that might be imposed by a new application.

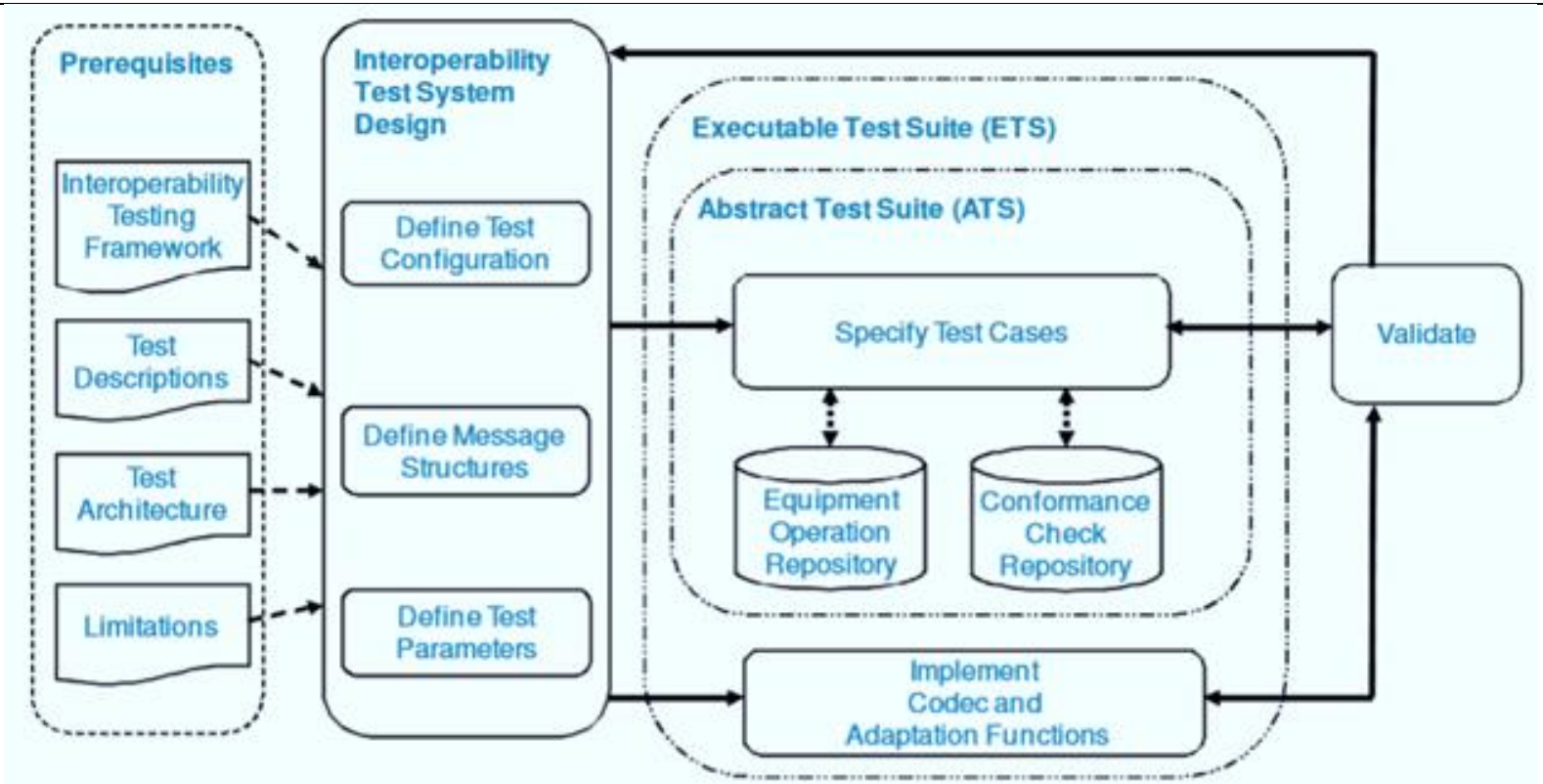
We have found that our aggressive attention to change management can impact the integration of new third-party applications Consequently, we have a comprehensive compatibility testing protocol in place to ensure these applications can be integrated so that no unintended consequences disrupt network operations. We test our software with any new solution in our lab and in that of the application developer. Our protocol requires us to establish interoperability and then to test the call and data delivery interfaces specified in STA010.xx. Before this, parties agree to specific test cases. These tests are done under increasingly stressful environments and conclude with tests under operational conditions. The specifics regarding demarc and handoffs vary from vendor test to vendor test., Our test procedures match the outline in relevant NENA doctrine in that we design our testing to discover:

- Loss of data
- Unreliable performance
- Unreliable operation
- Incorrect operation
- Low maintainability

In general, the test protocol involves

- Connect two or more devices or programs from different vendors
- Check connectivity between devices
- Check if a device can send/receives packets or frames from each other
- Check if data is handled correctly in the network and facility layers
- Check if implemented algorithms work correctly
- Result ok: check next result
- Result not ok: Use monitor tools to detect the source of error
- Report result in the Test reporting tool

The following chart depicts the interoperability test model upon which we base our tests. Please note, however, not all elements are tested each time.



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

There are two instances, each capable of the following:

- 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 11,000 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 250,000 SIP-TLS 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.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

<table>
<tr><td rowspan="2">SEC 1</td><td>Security - Cybersecurity
For the purposes of this RFP, cybersecurity (security) is considered to be the established systems and processes focused on protecting computers, networks, programs, and data from unintended or unauthorized access, modification, or destruction.

Security Requirements and Standards
The security requirements established in applicable standards listed in Section V.D.1. Table 1 of the RFP apply equally to all elements of the system requested in this RFP, including but not limited to components located in the following building types:
1. Data centers;
2. Network-housing structures ; and,
3. Regeneration sites and other buildings housing any element or device that is part of the overall system.

Describe how the solution meets or exceeds the above requirements.</td><td>Comply

X</td><td>Partially Comply</td><td>Complies with Future Capability</td><td>Does Not Comply</td></tr>
<tr><td colspan="5">Bidder Response:

We maintain a model cybersecurity plan that we adapt for every client. It is based on a frequently updated threat analysis that is used to modify a basic stance to meet the needs of each network and dataset we are charged to protect.

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.

Data Center Physical Security: All solution data is stored and backed up in CenturyLink data centers. Primary storage and backup devices are placed in CenturyLink secure cages. Access to these secure cages are limited to only authorized CenturyLink 911 support teams. All vendors must be escorted by CenturyLink technicians.

Host PSAP Physical Security: CenturyLink requires all Host PSAP locations to provide a secure location at the Host PSAP centers for all backroom NG9-1-1 network interfacing equipment (NID). The backroom is secured at all times and only authorized personnel should have access to these backrooms. For sites that don't have a secure backroom, CenturyLink has included as part our proposal a 7-foot locking cabinet.

NG9-1-1 ESInet: CenturyLink deploys its ESInets on our secure and private MPLS network. Our adaptive networking provides greater resiliency, control, and automation. With our Connected Security, we have built security into our network. Connected Security means the network acts as a threat sensor and a proactive defense platform. There are two basic concepts behind achieving Connected Security – the more you see, the more you can stop. With Connected Security, we are identifying threats sooner through global visibility and blocking threats to help protect our customers.

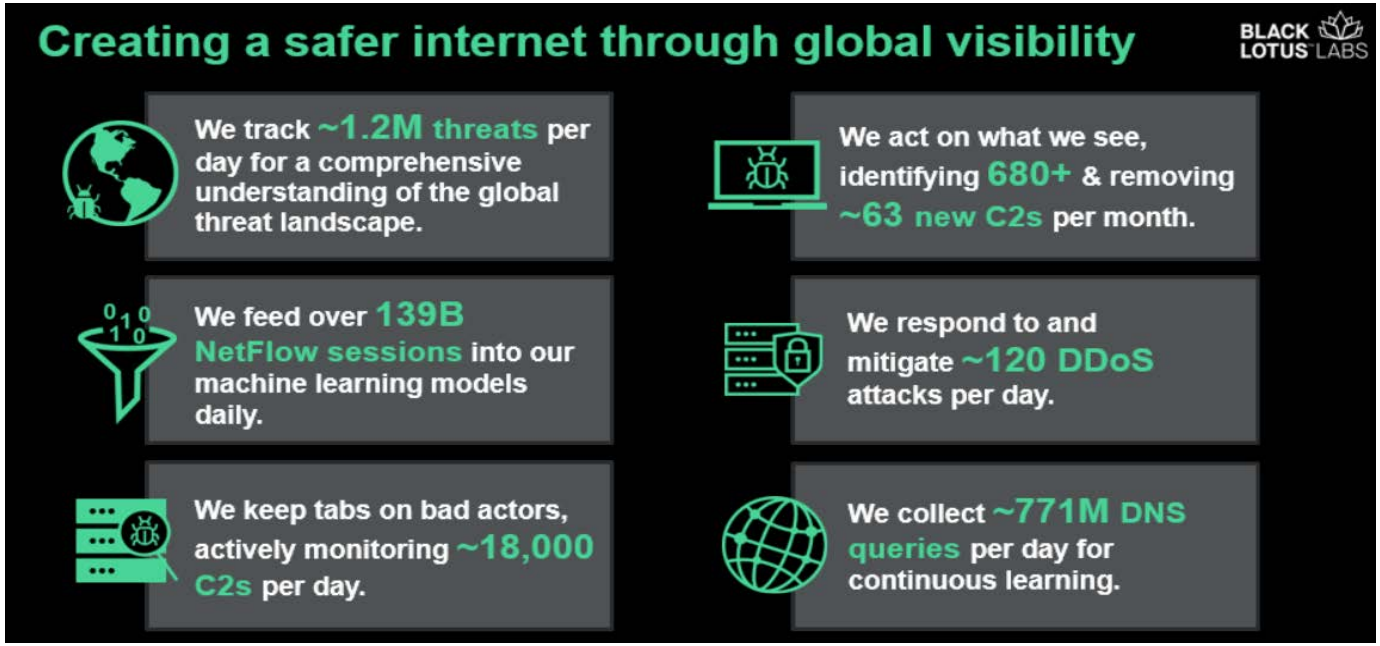
Connected Security from CenturyLink begins with our ability to See More and to sense threats. Unlike other IP Service Providers, CenturyLink has made major investments over the years to instrument our global backbone to perform as a threat sensor.

We have harnessed the power of our global visibility to take action against malicious activity through our continued investments to enhance our Visibility and our Expertise.</td></tr>
</table>

Visibility: Because of our expansive global backbone, Black Lotus Lab's, CenturyLink's threat research and operations arm, has access to the best raw data platforms for deriving our threat intelligence. This global data powers our ability to identify and monitor threats around the world.

The Black Lotus Labs team baselines the behavior of the CenturyLink global backbone by ingesting and analyzing billions of data records daily and uses this baseline to detect anomalies.

Sophisticated machine learning algorithms and big data analytics are applied to classify the anomalies that have been detected on our backbone. Through advanced automation, classified threats are validated in near real-time to help reduce noise, false positives and prioritize event response for our customers.



SEC 1 Cybersecurity – Visibility Drawing 1

Every day the Black Lotus Labs team of threat researchers and experts tackles the complexity of protecting one of the world's largest IP backbones 24/7. The original threat discovery and validation done by the Black Lotus Labs threat intel team drives the fidelity of our network-based intelligence. Proof Point: They discover over 680 new C2 networks per month and actively track 18,000 known C2s daily.

Black Lotus Labs leverages an extensive network of Honeypots known as a "HoneyNet". Each honeypot within the honeynet broadcasts a variety of seemingly valuable, but innocuous resources for threat actors to attack. Black Lotus Labs then logs attacker tactics, techniques and procedures (TTP) for analysis and uses advanced machine learning models to validate and produce trusted and actionable threat intelligence.

Stop More Because of our highly distributed network edge and deep peering, our backbone can sense and then block attacks closer to the source. By shifting the first line of defense upstream, our network acts a defense platform, detecting and blocking malicious activity before it impacts the customer environment

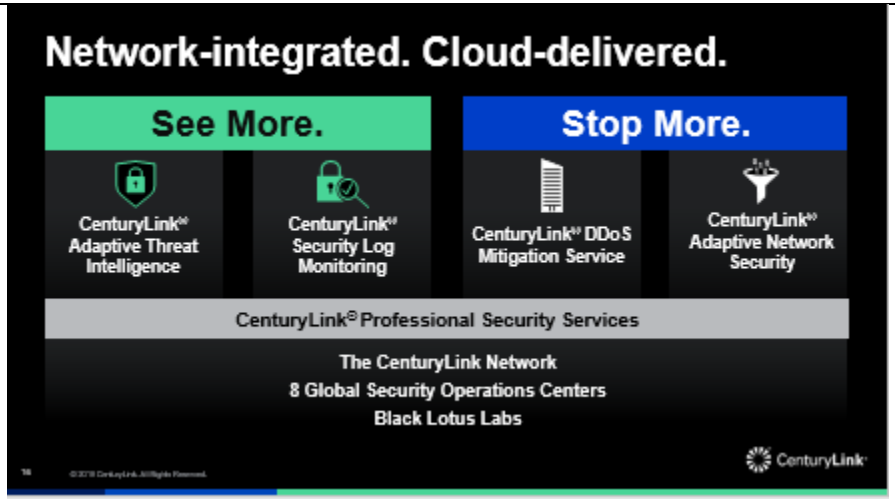
SEC 1 Cybersecurity – Visibility Drawing 2

And CenturyLink is in a unique position to defend against bandwidth-intensive volumetric DDoS attacks, as we can have the network capacity to absorb and/or drop bad traffic entering our global network at the edge and direct it to scrubbing centers only when needed, reducing latency and improving performance during attack mitigation for our customers.

Through a robust portfolio of network-integrated, cloud-delivered security solutions, we help deliver Connected Security for our customers.

See More: On the See More side, we have ATI and SLM to sense both internal and external threats. Stop More: On the Stop More side, we have DDoS Mitigation and ANS to turn the network into a proactive defense platform.

All can be supported by market-leading, managed security services if you don't want to manage your security environment on your own. Our portfolio of solutions is informed by what we see on the CenturyLink backbone, our 8 global Security Operations Centers, as well as original threat discovery from our Black Lotus Labs threat research and operations team.

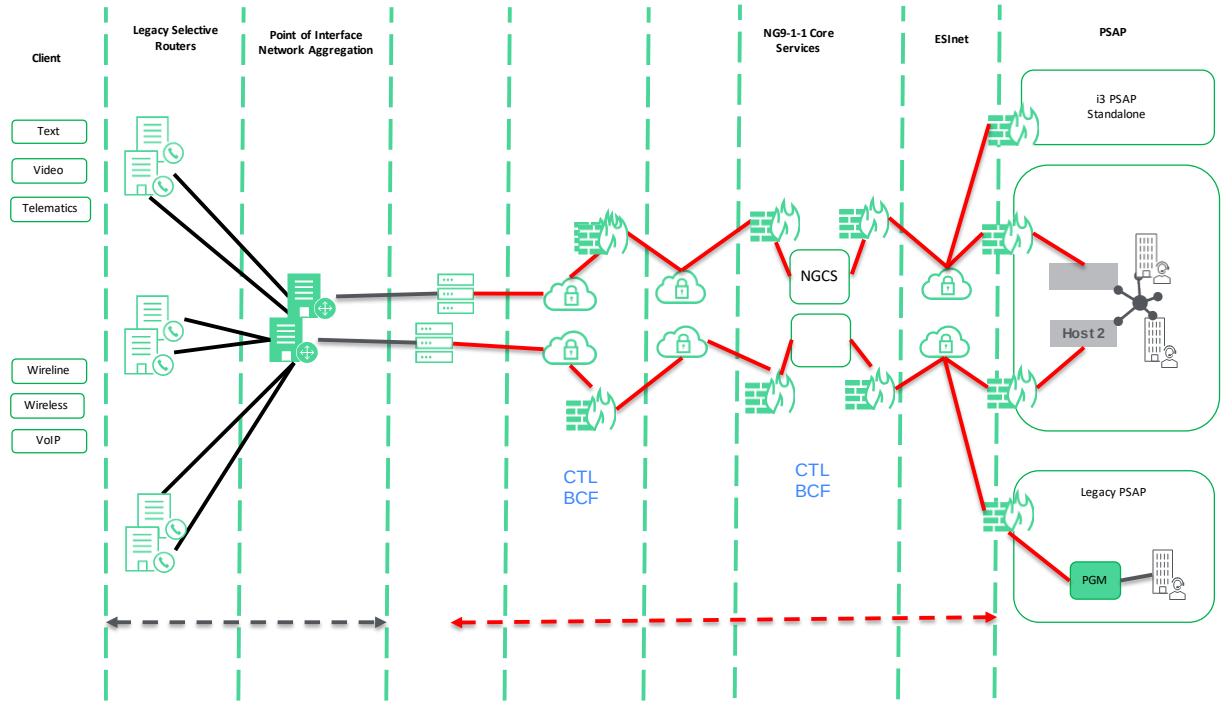


SEC 1 Cybersecurity – Visibility Drawing 3

This approach to security has made CenturyLink a leader in cybersecurity. CenturyLink provides cybersecurity services to over 40 federal government agencies and 1,500 Enterprises. We are:

1. We are one of only two service providers for the Defense Information System Agency (DISA) national transport backbone network
2. CenturyLink carries 100% of DoD Internet traffic
3. We are the advisors to the Department of Homeland Security, DOD, DOI, Cybersecurity Council and other multiple federal agencies
4. 1,500 Enterprise Security Clients, 250 Researchers, Testers, GIAC
5. 30 – Certified Intrusion Analysts and 30+ Security Consultants possessing 750+ combined experience
6. Over 5,000 security installations under management
7. 8 Global Cybersecurity Centers

Trusted Cybersecurity Vendor of DoD, DHS, and multiple federal agencies: If the DoD, DHS, multiple federal agencies, and over 1,500 global enterprise customers trust CenturyLink for their critical network transport and cybersecurity, The State can be assured we will apply the same practices to protect all critical data that rides the State NG9-1-1 ESInet. Security is built into the CenturyLink ESInet. CenturyLink's private MPLS network, which carries 9-1-1 traffic is isolated from CenturyLink's Internet networks. A general view of the CenturyLink 9-1-1 architecture looks like this:



SEC 1 – Cybersecurity – NG9-1-1 Architecture

Security must be a part of every domain of this network. Physical security and application level security is imperative:

Our approach is to create isolated security domains across our solution. Each domain has built-in and evolving security, including across the NGCS and ESINets, at the Central Offices, fiber huts, data centers and up to and including the PSAPs and Host Centers.

Our CenturyLink Public Safety and Security Operations implementation team uses industry standards for our NG9-1-1, i3 and security best practices documents to warrant consistency and transparency between OSPs, Call Handling Equipment (CHE) providers and other 9-1-1 integrators. We also work with our vendor vendors to ensure global interoperability all the way to the PSAP. CenturyLink follows both the Physical Security and logical security Guidelines as outlined in the Nena" Security Document NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) NENA 75-001" which includes:

- ESInet security. Our ESInet maintains an information security policy derived from the ISO 27000 suite of standards and observes practices and standards accordingly. CenturyLink has implemented controls that address the policy concerns of the NENA 75-001 NG-SEC security

	standard. CenturyLink separates physically and logically ESInet functions into separate security domains. This methodology provides a clear demarcation of NGCS functions and security requirements from Managed CPE functions and security requirements. • CenturyLink's NGCS Solution, access control is provided through the Border Control Function/Session Border Controller (BCF/SBC) at the NGCS datacenters, this secures and segments the core functions to the transport network for the PSAP and external data sources which all remain in separate security domains. All messaging transiting the network uses SIP. If not delivered in SIP natively, it must be interworked to SIP using the Protocol Interwork Function (PIF) of the Legacy Network Gateway (LNG). PSAP BCF/SBC are included part of this service as well that will terminate secure traffic to the PSAP and expect to hand off to the endpoint PSAP via customer provided call handling equipment firewall/BCF or SBC. • The CenturyLink's NGCS Solution and ESInet are provided with an array of BCFs/firewalls that inspects all traffic transiting the network edge. This device will employ both application and network layer protection and scanning capability as well as mitigates lower layer protocol attacks. The BCF provides Denial of Service (DoS) and Distributed Denial of Service (DDoS) detection and protection. Our network supports standard 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 datacenters and secure delivery of SIP traffic to the PSAP BCF. • Our network infrastructure is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. We employ high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/Application availability is safeguarded with clustering and load balancing techniques. Furthermore, our security architecture employs defenses that include, but are not limited to, Stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress. • Building and Physical Access Control • Hardened defined external perimeters, hardened outer walls with no openings available for exploitation, access control lists and at least two automated ID sensors such as palm-print readers, etc. Visits by uncleared individuals must be approved in advance. All visitors are escorted. • Entity identification badges, building access cards, building keys, and/or any other form of recurring access that does not require approval at the time of access shall be sponsored by a NG9-1-1 Entity management person. Appropriate local, state and federal laws and guidelines shall be followed for allowing nonemployee access (i.e. CJIS Background Checks, etc.). • Identification Badges • Mobile Security and Security in and outside the Work Area or PSAP • Physical Access • CenturyLink network Interconnect equipment (NID) which will include routers, firewalls, audio codes, HA-SD-WAN, network probes, UPS and other similar equipment shall be installed and contained in a secure locked cabinet located at each PSAP with appropriate physical access controls. If equipment is in equipment rooms shared with non-NG9-1-1 Entity entities or in unsecured space, it shall be contained in locked cabinets • All NG9-1-1 services within our ESInet that require authentication implement a Single Sign On paradigm. The mechanism used is OASIS SAML (Security Assertion Markup Language). There are two entities: An Identity Provider (IDP) which authenticates users and supplies services with a "token" that can be used in subsequent operations to refer to an authorized user and a Relying party which uses the token. SAML is used by a Relying Party to ask if an operation should be permitted by the user.

- Refer to section SEC 7 "Physical Security" for addition "Physical access security" that CenturyLink follows.
- With software developed in collaboration between our vendor Synergem; logical security, QoS, and interoperability are "baked in" to the functional element of NGCS solution.
- Rather than supporting signaling or voice encryption, we rely on the MPLS security and secured IP tunnels to provide confidentiality for signaling and voice.
- CenturyLink's NGCS solution facilities meet Tier III standards stipulated in the two main datacenter tier classifications developed by the Telecommunications Industry Association (TIA) and the Uptime Institute (UI). Physical security features include redundant commercial power (supplied from separate grids if possible), redundant backup generators, redundant uninterruptible power supplies ("UPS"), redundant heating, ventilation, and air conditioning ("HVAC") systems, fire suppression systems physical access security with separate communication service provider entry points.
- We employ the NENA 75-502.1 Audit Checklist to build our security program to include all system components and to test project compliance. We employ independent access control and auditing at the rack level for core services facilities.

Fault-zone design methodology

Configurations are automatically backed up and archived on every commit.

The CenturyLink Next Gen Core Services (NGCS) operates in an active-active configuration in each datacenter with redundant, highly available fault-tolerant critical components operating continuously in tandem. If one should fail, the redundant components continue to carry the entire load with no interruption of service. No failover time is required. All applications are deployed on virtual servers and data is shared among and within each data center. These applications leverage HA functionality within the vSphere hypervisor and associated Snapshots. vMotion, DRS and HA features are utilized to ensure backup and recovery. 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.

CenturyLink's SBC Core - Session Border Controllers (SBC) are engineered in a dual-pair, active-standby configuration for maximum call volume. High availability pairs of SBCs are deployed in an active-hot standby configuration. SBCs handle SIP/RTP network-to-network interfaces. Every SIP/RTP ingress/egress with has a path through a pair of SBCs.

A robust strategy for identity management, and user access to web-based applications is protected through an identity management system and prevents unauthorized individuals from accessing network resources or data.

Sensitive data is housed in our data centers with logical and physical access controls. Development environments are separate from production and production data is not used in DEV or SQA. Data transits untrusted networks through applications or communication channels with encryption to safeguard confidentiality and integrity.

The ESInet employs a defense-in-depth security strategy to protect sensitive information. Such controls include, but are not limited to, stateful packet inspection firewalls (host and network based), IDS/IPS, ACLs, Role-based Access control, two-factor authentication, encryption, and AV (email and host). Furthermore, systems are protected with build standards, patch management, and regular vulnerability scans.

Multi-factor authentication and role-based access control are used to restrict user access to trusted resources. User access via the public Internet requires two-factor authentication, where one factor is provided through username and password and the second factor is provided through a

	dynamic, randomly changing secure access code from a security token. Users are configured in the identity management system and linked to a specific security token and configured for access to a defined list of applications and data.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Security Plan A comprehensive security plan is a critical component of the Nebraska's NG911 network solution. Describe the security plan, including the 1. mitigation; 2. monitoring; 3. alerting and incident-response processes; and 4. provide information on specific hardware components and software systems incorporated in the proposed security plan. The proposed solution's security plan is required to utilize the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) and Task Force on Optimal PSAP Architecture (TFOPA) best practices.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 2	Bidder Response: The physical aspects of our security plan are described in section "SEC 1" above. We rely on standards produced by NENA, SSAE-16 accreditation and Tier identification sources. However, since ours is a highly centralized, Infrastructure As A Service (IAAS) solution; our emphasis is on cybersecurity. Our plan addresses each of these elements listed above, but in a slightly different format. Here is an executive summary of our plan: NG9-1-1 Cybersecurity must employ proactive measures to recognize, alert, log and report all security issues. This effort must be based on a comprehensive plan that establishes an Intrusion Prevention System (IPS) and strategies to deal with issues such as Distributed Denial of Service (DDoS), to avoid, limit and minimize disruptions to the network due to security incidents. CenturyLink maintains a cybersecurity posture satisfying federal, state and industry best practices, standards and regulations. Our approach stresses four security areas of emphasis: 1. Preparation 2. Detection and analysis 3. Containment, stabilization and return to a steady state. 4. Post incident activities that include a root cause analysis and corrective action. These phases are interrelated and represent a continuous loop of preparation, analysis and improvement that continues whether an actual emergency occurs or not. Further, this approach ensures our compliance with best practices advocated by the US Department of Homeland Security, numerous other advocacy groups and the organizations cited above.				

SEC 2 – Security Plan Preparation

A. CenturyLink Cybersecurity Objectives

8. Configure the ESInet in accordance with NENA 75-001and protect it with an array of firewalls.
9. Provide both application and network layer protection and scanning using the BCF/SBC. It will also mitigate lower layer protocol attacks and provide denial of service (DoS) and distributed denial of service (DDoS) detection and protection. The firewall component of the Oracle/Acme Packet BCF/SBC will inspect all traffic transiting the network edge.
10. In accordance with NENA-STA-010.2 (Section 6), locate call origination sources, gateways, and similar elements outside the ESInet, and ensure any connection will be through the BCF/SBC.
11. Pre-certify agents seeking access to the system through a Credentialing Agency. Once inside the system, agent privileges will be limited by policy.
12. Protect workstations and servers with access to the company network with dynamic malware applications that employ whitelisting and blacklisting with advanced static prevention in the form of deep packet inspection to block threats before endpoints are impacted.
13. Employ passwords that are complex employing a random selection of lower-case letters, capitals, symbols and numbers. Passwords will include least nine characters in length and will be routinely changed semi-annually or immediately if the account or the network is compromised.
14. Lock an account after a third unsuccessful login attempt.
15. Protect all critical networks and facilities with Multifactor authentication (MFA) and refrain from using public networks without linking them to their own VPN.
16. Meet Tier II-III standards in any company datacenters or those owned or operated as co-lo facilities.

B. Strategy Phase I Planning
Objective: Conduct a systematic process to develop and execute a strategy to meet defined objectives.

Tasks:

B.1. Identify the critical elements in the network that require protection.

B.2. Perform a threat analysis that identifies the danger posed to these elements.

B.3. Use checklists contained in NENA 75-001, to establish current state of network physical and information security. This assessment should include cyber risk evaluations of each critical element to include vulnerability and consequence analyses that identify capability gaps, and dependence on outside agencies that may not be under CenturyLink control.

B.4. The network security manager will create a baseline that will allow anomalies to be quickly identified. That manager will then establish procedures and protocols that detect and deter a wide array of threats to include:

a. Unusual outbound network traffic.
b. Anomalies in privileged user account activity.
c. Geographical irregularities.
d. Login red flags.
e. Increases in database read volume.
f. HTML response sizes.
g. Large numbers of requests for the same file.
h. Mismatched port-application traffic.
i. Suspicious registry or system file changes.
j. DNS request anomalies.
k. Unexpected patching of systems.
l. Mobile device profile changes.
m. Data bundles in the wrong places
n. Web traffic outside the norm of human behavior.
o. Signs of DDoS activity.

B.5. Conduct an interdependency analysis to identify the impact of cascading infiltration or attack.

B.6. Identify business/service impacts that would result from the failure of one or more specific elements. See Appendix B to this plan for template.

B.7. Using a FortiSIEM platform, design a robust end-to-end network monitoring program.

B.8. Develop incident reaction plans that; (1) Identify critical recovery objectives; (2) Provide a complete and integrated picture ofthe escalation and (3) Outline de-escalation sequences and the timeframe in which actions must be completed.

B.9. Identify outside sources of assistance.

B.10. Formalize vendorships in memorandums of understanding or pre-negotiated contractswith sector cyber incident or emergency response individuals/agencies to assist in the triage, and collaboratively response to incidents as required.

B.11. Identify reporting requirements.

C. Strategy Phase II Detection and Analysis

Objective:

Deploy a system and establish procedures that will assure the security, reliability, confidentiality, integrity, and availability of the CenturyLink networks, communications system and protect data from damage, unauthorized use, and exploitation.

Tasks (Supervised by the Customer of Excellence (CoE) or his/her designate):

Using results produced in Phase I, deploy physical and virtual safeguards that include limited access to critical locations and systems to authorized individuals carrying out legitimate activities.

1. Log all events throughout the network. A powerful logging pipeline gives a security team the core functionalities it needs to keep an eye on the infrastructure.
2. Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems.
3. Properly protect workstations with access to the company network with dynamic malware applications that employ whitelisting and blacklisting with advanced static prevention in the form of deep file inspection to block threats before they have a chance to impact endpoints. When this software detects an attack, it disables it without any need for human intervention and quickly returns the network to its last known safe status
4. Implement a password discipline that requires a change every six months with no repeat of used passwords for two years. Install an application that reminds end-users 30 days before their password expires.
5. Implement an automatic triggering mechanism that locks an account after three unsuccessful attempts to login within 60 minutes.
6. Develop a deep packet inspection protocol.
7. Institute log events and organize and implement agent credentialing to verify identity and to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited are harmed.
8. Implement a dark web scanning program to identify any compromised passwords or critical information.
9. Protect data using the following procedures:
    a. Dropbox will be the principal CenturyLink repository for critical business documents. Only the System administrator will be empowered to remove documents from Dropbox.
    b. Store Technical documents including source codes using the Microsoft Team Foundation Server (TFS) service. TFS provides source code management (either with Team Foundation Version Control or Git), reporting, requirements management, project management (for both agile software development and waterfall teams), automated builds, lab management, testing and release management.
    c. Human Resource documents will be stored on the TriNet platform which is accessible through multiple Internet pathways.
    d. Employees work exclusively within their Dropbox and/or TFS accounts. No work will be stored on personal computers more than 24 hours without moving it to either Dropbox or TFS.
    e. No document may be removed from any company database except by the network administrators.
10. Implement the FortiSIEM network monitoring and the Oracle Enterprise Operations Monitor.
11. Perform audit activities to verify and validate security mechanisms are performing asintended.
12. Conduct training to ensure staff-wide adherence to access control authorizations. This training will be accomplished initially upon hiring as part of the HR process and then annually. The manager of this plan will produce a Cybersecurity handbook that will be posted on the company website. The Center of Excellence (CoE) or his/her designate (Usually the network administrator) will monitor all password, login and access privilege programs for compliance with this plan. Annual training will be conducted by division managers or other designates using a syllabus prepared by the plan manager.
13. Using these tools and procedures, quickly identify any deviation from routine and then implement containment actions. Employ automatic triggers whenever possible.

D. Strategy Phase III: Containment
Objective:

Ensure CenturyLink is prepared to react to a range of threats and attacks with a toolbox that includes response efforts automatically triggered by threatening events and others that can be tailored to fit the incident profile. In order to ensure containment can be quickly imposed, CenturyLink must establish a baseline secure status, identify threats to that status and prepare containment.

TASKS

D.1. Verify that the network architecture is routinely functioning in N+1 mode.
D.2. Employ enhanced data backup with all applications deployed on virtual servers with data shared among and within each datacenter.
D.3. Leverage H/A functionality within the vSphere hypervisor and associated Snapshots. vMotion, Utilize DRS and H/A features to ensure backup and recovery.
D.4. Activate credentialing to verify identity to authorize, grant, or deny access to the networks, its applications, and any other systems that could be exploited to do harm; and employ NENA-defined Security Posture and logged events to help detect threats or attacks.
D.5. Verify password protocols are in use and that users are notified when passwords must be changed.
D.6. Activate deep packet inspection (DPI) and dark Internet ID efforts.
D.7. Ensure the BCF supports an automated interface that allows a downstream element to mark the source of a call as a "bad actor". This would normally occur when a call is received that appears to be part of a deliberate attack on the system.
D.8. Ensure the BCF installs a "NENA-source" parameter in the Via header that in the outgoing INVITE message associated with every call. Calls are marked by the SBC in a way that allows a recipient to identify the BCF that processed the call.
D.9. When a downstream element identifies a source as a "bad actor", ensure the responsible sender is notified by sending a "BadActorRequest" containing the source ID from the NENA-source parameter. This helps ensure that cascading impacts are minimized so as not to affect timing or invoke DoS for throughput of legitimate emergency calls.
D.10. Activate a network monitoring protocol that logs, measures and evaluates all network traffic.

Recovery Tasks:

1. Identify the incident (s): Unless event is clearly level 3 or higher, begin response with triage based on SIEM or active directory logs, apparent source of problem, severity and reporting requirements.
2. Isolate the affected device (s) or system if automatic triggers have not already done so. This may involve disconnecting or isolating network segments, creating additional firewall rules, employing active IDS/ IPS rules or simply disconnecting the infected network from the company and / or public networks.
3. Eradicate the cause. This process must include measures to not only remove the infection from the primary device, but various methods to scan every device on the affected network segment to ensure the relevant risk is addressed.
4. Recover the device, service or data. Ensure system is returned to last known safe status using software installed on every computer or server

E. Strategy Phase IV: Post Incident Activity

Objectives:

Ensure that the company learns any lessons that are available after an incident is contained. Report those lessons-learned and modify procedures to affect the improvements these findings suggest.

Tasks:

1. Analyze the incident. Review:
   a. Exactly what happened, at what times?
   b. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
   c. What information was needed sooner?

d. Were any steps or actions taken that might have inhibited the recovery?
e. What would staff and management do differently the next time a similar incident occurs?
f. How could information sharing with other organizations have been improved?
g. What corrective actions can prevent similar incidents in the future?
h. What precursors or indicators should be watched for in the future to detect similar incidents?
i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents

2. Report. An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
   a. Creating a formal event chronology (including time-stamped information from systems);
   b. Compiling a monetary estimate of the amount of damage the incident caused
   c. Retaining follow-up reports as specified in retention policies.
3. Perform Root Cause analysis. Focus on relevant objective assessment activities including:
   a. Review of logs, forms, reports, on other incident documentation
   b. Identify recorded precursors and indicators
   c. Determine if the incident caused damage before it was detected
   d. Determine if the actual cause of the incident was identified
   e. Determine if the incident is a recurrence of a previous incident
   f. Calculate the estimated monetary damage from the incident
   g. Measure the difference between initial impact assessment and the final impact assessment
   h. Identify measures, if any, that could have prevented the incident.

Satisfy local, state and federal reporting requirements. This includes SLA reporting requirements. Certain types of breaches also carry legal notification responsibilities.

CenturyLink Monitoring and Response of our NG9-1-1 ESInet Ingress and Egress Network and hardware components:

4. CenturyLink provides a complete end-to-end monitoring solution of all network transport services, network equipment, and security from call ingress to the call endpoint that will notify the PSAP/PSAP's of an outage with the prescribe time limit spelled out by the FCC.
5. The CenturyLink solution employs state-of-the-art and standards-based security measures for traffic in the ESInet and in connection to external IP networks. The proposed solution provides highly integrated security in a fully managed system. The solution includes monitoring of traffic and prevention of access to network infrastructure using session border controllers, firewalls, and other continuously monitored intrusion prevention systems

6. All ingress access points are protected with security devices, such as SBCs and firewalls, and traffic is managed and monitored 24x7x365. Unauthorized external access is prevented, allowing only authorized traffic to enter the ESInet. Virtual Private Networks (VPNs) are utilized to manage bandwidth and provide additional security. Border Gateway Protocol (BGP), IPSLA, and GRE tunnels are utilized to uphold service levels and provide oversight of the network. Active monitoring and proactive testing increase the solution's ability to react to abnormal situations.
7. Our SD-WAN appliances provides advanced security at each endpoint in our network.

i. Application Level Policies with UTM – We can support 3000+ pre-defined and customer defined application level policies
ii. URL Filtering – White List / Blacklist
iii. IP Filtering
iv. IPS / IDS

8. In our NGCS data centers, we use Oracle Enterprise Operations Monitor and the FortiSIEM security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP.
9. The CenturyLink Security Information and Event Management (SIEM) system is integrated into our ESInet network monitoring program.
10. As the cyber threat landscape continues to expand, Public Safety operational entities cannot have a false sense of security. CenturyLink provides a thorough approach to network security, one that is tied to our overall Public Safety networking strategy, enabling a comprehensive view of the overall networking architecture and threat environment. We see more, so we can stop more.
11. CenturyLink follows the NENA approach to Security for our NGCS and ESInet Solution for Nebraska. Including the NENA standards and documentation found in the following NENA standards:

    - NENA 75-001, Security for Next Generation 9-1-1 Standard (NG-SEC)
    - NENA – INF 15.1-2016, NENA NG9-1-1 Security Information Document
    - NENA 04-503, Network/System Access Security
    - NENA 75-502, Next Generation Security Audit Checklist

12. As a trusted advisor to the Department of Homeland Security (DHS), CenturyLink adheres to the TFOPA framework and helps DHS formulate best practices for securing NG9-1-1 ESInets.
13. CenturyLink's NG9-1-1 ESInet solution includes a Vulnerability Assessment Services (CVAS) Which identifies, prioritizes, and mitigates vulnerabilities across an ESInet networks, applications and systems in our NG9-1-1 ESInet solutions.
14. CenturyLink products and services are secure by proactively identifying and mitigating vulnerability risks that protect families, friends, communities, and our public safety customers.
15. Our Functional Priorities Includes:

    - Critical Vulnerability Response - Analyze new, publicly disclosed vulnerabilities for critical severity threat potential to CenturyLink systems and coordinate a plan of action with the business units to mitigate the threat.
    - Regulatory Compliance Support - Provide vulnerability scanning, penetration testing, and remediation oversight of findings as required to meet Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Service Organization Controls (SOC) 2 compliance standards.
    - Vulnerability Scanning- Determine the scope of vulnerability scanning, perform vulnerability scanning on designated systems in scope, notify the appropriate business units of vulnerability findings, and verify remediation actions were successful.
    - Penetration Testing - In collaboration with the our Public Safety team we, define the need, scope, and Rules of Engagement (ROE) for penetration testing, perform the penetration testing, notify the business unit of vulnerability findings, consult with the State of Nebraska on risks and mitigation strategies, and verify remediation actions were successful.

- Adversarial Cybersecurity Emulation (ACE) - Coordinate and execute targeted attacks using advanced malicious actor methods (ACE exercises) to determine defensive capabilities of CenturyLink and identify improvement areas. This capability is under development.
- Secure Code Guidance - In collaboration with developers within the public safety 9-1-1, we acquire access to developer code repositories, perform security analysis on the application source code, notify our vendors and public safety team including the state of Nebraska of vulnerability findings, and verify remediation actions were successful.

14. Our Security Best Practices:

- The CenturyLink ESInet network meets and exceeds the security criteria as defined in the NENA NG-SEC specifications for NG9-1-1 security. We develop security policies according to industry requirements and best practices including CSRIC, NIST, and the security policies, standards, and guidelines of the International Organization for Standardization and Control Objectives for Information and Related Technology.
- CenturyLink's NGCS solution utilizes the follow appliance/devices in it service delivery for NG9-1-1:
- SBC gateways for endpoint termination, stateful firewall and IPS Services.
- Oracle Packet Session Border Controller (SBC) for secure SIP TLS\Authentication and anchoring.
- AudioCodes for secure SIP termination if required for LPG termination converting SIP TLS traffic back to CAMA or CAS trunking at the PSAP/Host sites.
- Private Port MPLS where core routers support MPLS tunnels and implement Fast ReRoute (FRR). These technologies enable CenturyLink to reliably transport private VPN traffic in service specific overlay networks, referred to "Security Domains". FRR increase backbone resiliency with rapid recovery from network failures.

Any additional documentation can be inserted here:

SEC 3	**Security Compliance Matrix** Describe how the proposed solution addresses compliance in each of the following categories in NENA 75-502, NENA NG-SEC Audit Checklist.

Category
1. Senior Management Statement
2. Acceptable Use Policy
3. Authentication/Password Policy
4. Data Protection
5. Exception Request/Risk Assessment
6. Hiring Practices
7. Incident Response
8. Information Classification and Protection
9. Physical Security
10. Compliance Audits & Reviews
11. Network/Firewall/Remote Access
12. Security Enhancement Technical Upgrade

		13. Technical Solutions Standards 14. Wireless Security	
Bidder Detailed Response: Refer to the Security Compliance Matrix Below			

Any additional documentation can be inserted here: . (See Copies of embedded attachments in Proposal 1 option C file 1 of 4 Attachments)

SEC 3 Security Compliance Matrix.x

	Predictive Analysis and Monitoring Describe solution's capabilities to provide predictive analysis and modeling to combat security threats.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SEC 4	Bidder Response CenturyLink provides a complete end-to-end monitoring solution of all network transport services, network equipment, and security from call ingress to the call endpoint that will notify the PSAP/PSAP's of an outage with the prescribe time limit spelled out by the FCC. The CenturyLink solution employs state-of-the-art and standards-based security measures for traffic in the ESInet and in connection to external IP networks. The proposed solution provides highly integrated security in a fully managed system. The solution includes monitoring of traffic and prevention of access to network infrastructure using session border controllers, firewalls, and other continuously monitored intrusion prevention systems All ingress access points are protected with security devices, such as SBCs and firewalls, and traffic is managed and monitored 24x7x365. Unauthorized external access is prevented, allowing only authorized traffic to enter the ESInet. Virtual Private Networks (VPNs) are utilized to manage bandwidth and provide additional security. Border Gateway Protocol (BGP), IPSLA, and GRE tunnels are utilized to uphold service levels and provide oversight of the network. Active monitoring and proactive testing increase the solution's ability to react to abnormal situations. In our NGCS data centers, we use Oracle Enterprise Operations Monitor and the FortiSIEM security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP. Our Security Information and Event Management (SIEM) analysis is a daily task of our Security Operations Center. Network hosts, including all call processing elements and security infrastructure, provide logging through a centralized SIEM solution, providing real-time event correlation, predictive analysis and alerts across the NGCS environment. Information Security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. We deploy heuristic analysis, a method employed to detect previously unknown computer viruses, as well as new variants of viruses. Heuristic analysis is an expert-based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. In addition to performing continuous network traffic monitoring, we perform annual external and internal penetration testing of our critical systems and infrastructure. We maintain in-house tools and expertise to conduct penetration testing and work with nationally recognized penetration test providers to achieve third party assurance. The CenturyLink Security Information and Event Management (SIEM) system is integrated into our ESInet network monitoring program.				

	As the cyber threat landscape continues to expand, Public Safety operational entities cannot have a false sense of security. CenturyLink provides a thorough approach to network security, one that is tied to our overall Public Safety networking strategy, enabling a comprehensive view of the overall networking architecture and threat environment. We see more, so we can stop more. CenturyLink follows the NENA approach to Security for our NGCS and ESInet Solution for Nebraska. Including the NENA standards and documentation found in the following NENA standards: • NENA 75-001, Security for Next Generation 9-1-1 Standard (NG-SEC) • NENA – INF 15.1-2016, NENA NG9-1-1 Security Information Document • NENA 04-503, Network/System Access Security • NENA 75-502, Next Generation Security Audit Checklist CenturyLink's NG9-1-1 ESInet solution includes a Vulnerability Assessment Services (CVAS) Which identifies, prioritizes, and mitigates vulnerabilities across an ESInet networks, applications and systems in our NG9-1-1 ESInet solutions. CenturyLink products and services are secure by proactively identifying and mitigating vulnerability risks that protect families, friends, communities, and our public safety customers. Our Functional Priorities Includes: • Critical Vulnerability Response - Analyze new, publicly disclosed vulnerabilities for critical severity threat potential to CenturyLink systems and coordinate a plan of action with the business units to mitigate the threat. • Regulatory Compliance Support - Provide vulnerability scanning, penetration testing, and remediation oversight of findings as required to meet Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Service Organization Controls (SOC) 2 compliance standards. • Vulnerability Scanning- Determine the scope of vulnerability scanning, perform vulnerability scanning on designated systems in scope, notify the appropriate business units of vulnerability findings, and verify remediation actions were successful. • Penetration Testing - In collaboration with the our Public Safety team we, define the need, scope, and Rules of Engagement (ROE) for penetration testing, perform the penetration testing, notify the business unit of vulnerability findings, consult with the State of Nebraska on risks and mitigation strategies, and verify remediation actions were successful. • Adversarial Cybersecurity Emulation (ACE) - Coordinate and execute targeted attacks using advanced malicious actor methods (ACE exercises) to determine defensive capabilities of CenturyLink and identify improvement areas. This capability is under development. • Secure Code Guidance - In collaboration with developers within the public safety 9-1-1, we acquire access to developer code repositories, perform security analysis on the application source code, notify our vendors and public safety team including the state of Nebraska of vulnerability findings, and verify remediation actions were successful.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SEC 5	**Credentialing Process** Solution shall provide a process so that devices and carriers outside the IP network shall not have credentials, per NENA-STA-010.2-2016. Provide details regarding how the solution ensures that devices and carriers outside the IP network are not provided credentials.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

CenturyLink ESInet adheres to NENA 75-001 (NENA Security for Next-Generation 9-1-1 Standard [NG-SEC])

Following are devices and/or protocols used to restrict access.

- Our NGCS uses a security border API gateway for I3 data traffic. This device controls access to its services by using client trusted certificates.
- Session Border Controllers (SBC) are used for all SIP and SIP related communications.

CenturyLink verifies credentialed devices or that carriers are authorized access in the following manner:

- Client certificates issued by a trusted Certificate Authority (CA) are required in order to access I3 services such as LIS, ADR and ECRF.
- The trusted CA is currently provided by CenturyLink, that will use the authorized NENA PCA vendor once they roll out their program
- The IP address of any far end SIP endpoint must be provisioned in the SBC.
  - The endpoint is also required to send all traffic to a uniquely assigned IP: port combination on the SBC.
  - All SIP signaling is done over direct connections or VPNs.
  - IP connections to the ESInet are only allowed by vetted OSP's and/or data sources.
  - Connectivity to the ESInet is only by signed and approved agreement with data encapsulated by IPSEC MPLS VPN.
  - For PSAPs and 9-1-1 Authorities, the root Certificate Authority (CA) for agent and agency certificates is the PSAP Credentialing Agency (CA).
  - In accordance with NENA guidance, we require a CA to create and strictly adhere to a Certificate Policy and Practice Statement (CP/CPS) CP/CPS that include strict specifications for vetting who gets a certificate, under what conditions they get a certificate, and what proof of identity is needed before a certificate can be issued.
  - We require that an agency that cannot reasonably control its certificate issuing mechanisms or chooses not to do so, to contract to an entity that can provide strong controls and strict adherence to a suitable CP/CPS. Only those entities or devices able to present valid credentials can gain access to services and data in the ESInet.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SEC 6	**Third-Party Security Audits** Bidder shall allow for annual third-party security audits at the request and cost of the Commission. Describe bidder's current process for third party security audits.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: In compliance with security 3rd party internal and external security audits will be completed annually. 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. NG9-1-1 Entities performing internal audits or 'self-checks" may use external, 3rd party resources if necessary Presently, we use 3d parties to perform SSAE16 audits of all our datacenters. CenturyLink uses our Adaptive Network Security (ANS) and Network Based Security (NBS) Platform along with our IP Security SWAT and Operations teams to ensure our NG911 security compliance. CenturyLink also uses 3rd party vendors such as InteProIQ or Cybersecurity awareness training. Cyber Security Awareness Training and Phishing Platform – CenturyLink provides both Cyber Security Awareness Training and an employee Phishing Platform to help reduce exposure to the "human" element of a customer's cyber security risk. CenturyLink leverages nonbiased 3rd party audits annually including audits from other 3rd party agencies such as Black Lotus Labs, 3rd party partners etc. to ensure security compliance Findings resulting from our security assessments shall be subject to corrective actions.	X			

Any additional documentation can be inserted here:

SEC 7

Physical Security All structures outside the Commission's control that will house components of the ESInet and NGCS shall have security and access-control systems that ensure that only duly authorized individuals can access the areas housing the Commission's systems and network equipment. Any workstations or other equipment connected to, or capable of accessing, the ESInet and NGCS systems shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the Commission's systems similarly shall be protected. Identify any elements that are not under the direct control of the bidder, and a description of the building's security and access-control systems shall be provided.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			

Bidder Response:

Our geographically diverse datacenters monitor all critical systems automatically 24x7. Electronic logs are created and maintained in the system dashboard. This includes a historical record of availability and outage. We will employ datacenters in Chicago IL, and LA, CA, that meet the Tier III standards stipulated in the two main datacenter national tier classification protocols (Telecommunications Industry Association (TIA) and the Uptime Institute (UI)). Both are certified under the provisions of SSAE 16. Physical security features include defined external perimeters, hardened outer walls with no exploitable openings, access control lists and at least two automated ID sensors. Uncleared visitors are approved in advance and are escorted. The following chart depicts the basic security configuration:

Component	Type	Purpose
Badge card access system (EntraPass)	Kantech	The badge card system is utilized in conjunction with a biometric recognition access system to control entry into the greater datacenter and separately to the raised-floor production zone.
Biometric Recognition Access System (EntraPass)	Kantech	With badge control system, controls entry into the greater datacenter and separately to the raised-floor production zone.
Firewalls	Forigate Fort/OS	Corporate firewalls restrict traffic into the management network. Service delivery firewalls filter and route traffic for customer-specific environments that have borders that cannot be breached.
Management services backup servers	CommVault	Automated system software and network of servers provide backup and recovery for subscribing customers.
Routers and switches	Cisco NXOS	Route network traffic
Virtual Hypervisor	VMware vCenter	Authenticates and restricts access to customer virtual environments.
VMware hosts	VMware (ESXi 6.0)	Provide secure operation of client virtual machines

Web portal	Embotics vCommander	Customer portal system through which they manage their virtual machines which are isolated from all others.

CenturyLink will provide locking cabinets if required to the PSAP endpoints to protect the physical security on the customer side. Physical security at the data centers is assumed that would follow the appropriate standards for physical security including access control.

In addition to our basic configuration we use various procedures to help **ensure physical security** in our data centers, including controlling, monitoring, and recording physical access to facilities where client servers and other equipment reside. We provide complete physical security for our locations, with a special emphasis on security of the data centers and other sensitive areas.

Our physical security controls include:

- Access policies and procedures
- Access control system
- Employee access procedures
- Visitor procedures
- Contractor access procedures
- Building security
- Data center security
- Global Client Support Center (GCSC) security
- Onsite 24x7 guards
- Additional controls include:
- Multi-factor authentication for physical data center access
- Closed circuit TV monitoring
- Access logs
- Quarterly review of access list

Our automated access control system uses electronic badge readers, biometric hand scanners, and PIN keypads to control and monitor access to CenturyLink buildings and data centers. Security guards monitor the facilities and maintain a 24X7 physical presence at each data center, and the system logs access and sends alerts if entrances are left ajar.

We limit access to the data centers to only those employees who require access to perform their job functions. We lock the data center server racks and allow access only to persons who have proper authorization.

Access to other buildings, including lobby entrances, also requires an electronic access badge. As an additional measure, we use strategically located video cameras to record and monitor activity, both within and outside buildings and workspaces, in addition to having uniformed security personnel conducting regular rounds throughout facilities.

Local and remote monitored Power and Environmental controls (built at least to an N+1 methodology) include:

- HVAC

- Fire detection and suppression systems
- Diverse commercial power feeds
- Standby generator systems
- Dual Uninterruptible Power Supply (UPS)
- Grounding architecture
- Commercial power contingency arrangements

We limit access to the data centers and Customer Support Centers to only those personnel who require access to perform their job functions. We lock the data center server racks and allow access only to personnel who have proper authorization.

In addition, CenturyLink:

- Ensures all Information Resources intended for use by multiple users are located in secure physical facilities with access restricted to authorized individuals only.
- Monitors and records access to the physical facilities containing Information Resources intended for use by multiple users in connection with Supplier's performance of In-Scope Work.
- Physically secures any area where In-Scope Information is accessible to prevent access by unauthorized persons.

CenturyLink will perform physical security functions (e.g., identification badge controls, alarm responses) at all facilities under our vendors and CenturyLink controlled environments.

CenturyLink will prepare an Information Security Controls Document upon award of contract. This document is the security document that is used to capture the security policies and technical controls that the State of Nebraska requires, as requested by the State, on our managed systems, supported servers and the LAN within the scope of this contract. CenturyLink will submit a draft Information Security Controls document to the State review and approval during the transition period.

In addition to physical security CenturyLink will:

- Develop, maintain and update the Security Policies, including applicable State information risk policies, standards and procedures.
- Provide contact information for security and program personnel for incident reporting purposes.
- Provide the state a Single Point of Contact with responsibility for account security audits.
- Support intrusion detection and prevention and vulnerability scanning pursuant for Security Policies.
- Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.
- Provide security audit findings material for the Services based upon the security policies, standards and practices in effect as of the date of the audit.

Effective Date and any subsequent updates.

- Assist in performing a baseline inventory of access IDs for the systems for which we have security responsibility.
- Authorize User IDs and passwords personnel for the Systems software, software tools and network infrastructure systems and devices under our solution.

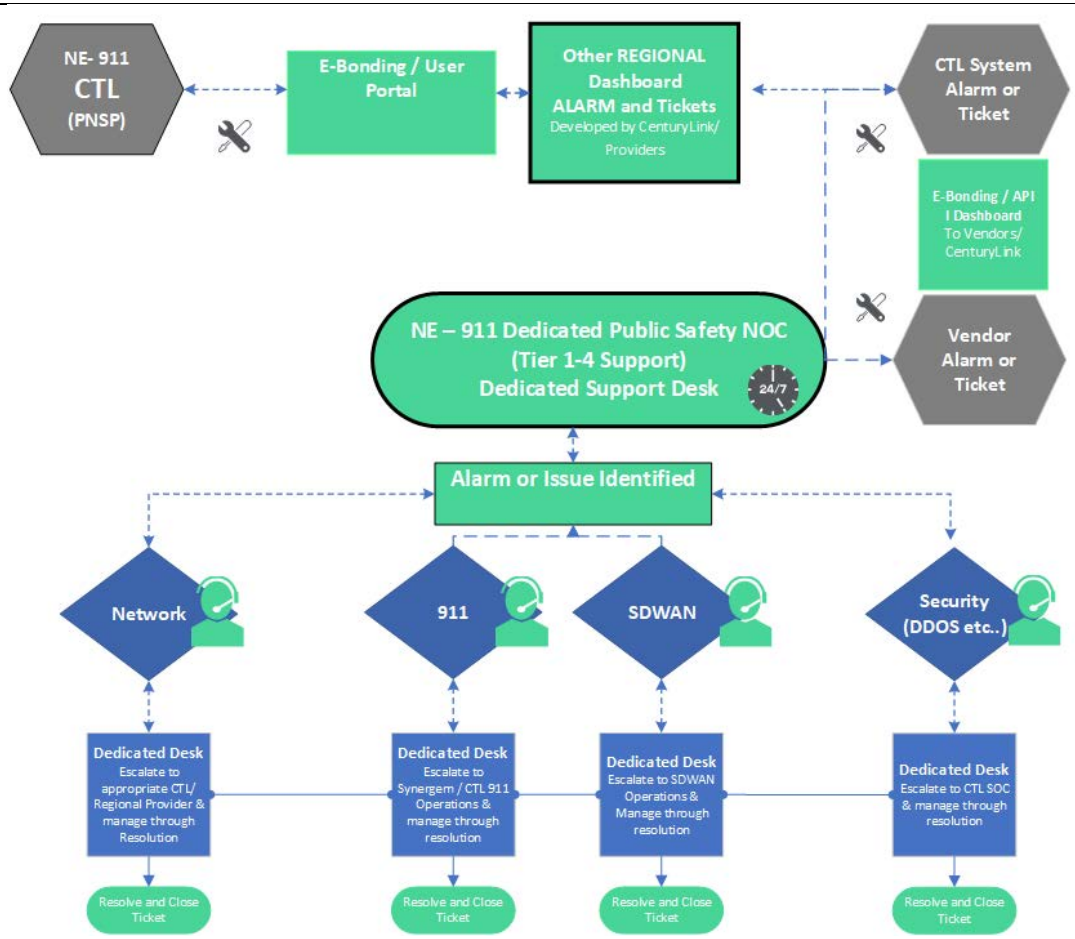
Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 1	**General Requirements – Network Operations Center (NOC)/Security Operations Center (SOC)**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Centralized NOC/SOC All services and components deployed and interconnected as part of the solution shall be monitored 24 hours a day, 7 days a week, 365 days a year (24 x 7 x 365) by a centralized Network Operations Center (NOC) and Security Operations Center (SOC). These functions may be in separate buildings or combined in a single building located in the continental United States.	X			
	NOC/SOC Interoperability Contractor shall have the ability to communicate, troubleshoot and connect with other vendors NOCs should there be a different ESInet and NGCS provider. In addition, the Contractor shall interface with the NOCs that support the regions throughout the state. This shall include ebonding of the ticket systems to support transparency throughout the troubleshooting process.	X			
	NOC/SOC Operations Model Provide documentation including organizational structure and procedures that describe bidder's 1. NOC/SOC operations model, 2. Continuity Of Operations Plan (COOP), 3. problem and change management systems, 4. reporting systems, 5. escalation plan, and 6. conformance with best practices (Information Technology Infrastructure Library (ITIL) or equivalent methodology)) for service-delivery management. The Contractor shall confirm the requirement compliance of any interconnected network utilized by the Contractor not previously identified to the Commission.	X			
	Bidder Response: Centralized U.S. NOC/SOC The CenturyLink Network Operations Center (NOC/SOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage CenturyLink's NGCS Solution associated services and connectivity. When a potential or actual customer-affecting event or outage is defined and determined to be an incident, the NOC/SOC will engage all responsible parties to ensure swift resolution. This includes resolution, documentation of any incident, communications, and post-event review and root cause analysis. We manage incidents and provide customers with notifications and status of ongoing service affecting issues that may impact the CenturyLink NGCS Solution. Our NOC/SOC and vendor locations are strategically located within the continental US. NOC/SOC Interoperability: CenturyLink's NGCS Solution is designed to be interoperable with any NENA-compliant solution regardless of its manufacturer. We work jointly with other vendors to plan interfaces and willingly joint teaming agreements to meet customer needs. We test all interfaces in our own lab and then use a battery of testing and failover scenarios onsite for testing that occurs before going live. This is accomplished according to plans developed with the end-user to ensure no loss of operational integrity during testing or installation. CenturyLink's solution will meet the NOC/SOC 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. Leveraging an SD-WAN overlay, services such as encryption, traffic prioritization, BGP routing, and creation of closed user groups are implemented via targeted software at the PSAP edge. CenturyLink uses a proactive monitoring and notification process. The process uses platform-specific alarm thresholds to identify potential service impairments. CenturyLink network alarms are customer specific and generate trouble tickets that automatically notify customers via e-mail and telephone. Proactive Customer Notification (PCN) also gives customers with flexibility to specify certain notification parameters on a service-by-service basis. To ensure rapid resolution of network issues, CenturyLink adheres to strict escalation procedures and measurable timeframes. If active progress and meaningful status updates are not being made, CenturyLink technicians are empowered to escalate issues internally and externally as required. The State may also request escalations. CenturyLink customer service is chartered to provide world-class customer support that attempts to resolve issues on a first contact basis. With geographically diverse NOC, CenturyLink ensures high availability of technical support personnel who provide rapid problem resolution and efficient work management in the event of natural or manmade disaster. CenturyLink also maintains records (log) of all trouble tickets. Our records allow our managers to review trouble tickets on a customer-by-customer, day-by-day, and criticality basis. When an incident impacts a CenturyLink customer our response is not complete until a CenturyLink representative contacts the customer with an explanation of the problem and a discussion of the actions that CenturyLink took to resolve issues and a discussion of how CenturyLink plans to keep the problem from occurring again. Communication - Communication will be supplied to all parties provided to CenturyLink by the Customer and its entities. We provide notification by various means. In the event of an outage CenturyLink applies immediate and sustained effort, 7x24, until a final resolution is in place. We use all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. If a temporary workaround solution is provided, we provide an action plan to be mutually agreed upon for the final resolution. We continue resolution activity until full service is restored. The primary objective of an incident is to mitigate impact. The Incident Commander and Incident Administrator can call upon whatever resources are required to identify and restore functionality. Disaster Recovery CenturyLink has established defined and reasonable business continuity and restoration plans including complex disaster and evacuation contingencies and conducts annual reviews to confirm adequacy of the plans. Adequate hardware spares are on hand to enable attainment of reliability and mean time between failure objectives. Geographically diverse engineering and redundancy provide ability to survive disaster scenarios. Power infrastructure and environmental systems are deployed so that a commercial power failure does not result in an interruption of service. The CenturyLink solution's essential processes, systems, and networks supporting 9-1-1 traffic are designed and deployed to accommodate possible disruptions and disasters to any given element or data center and support 24x7x365 continuous operation. In the event of unplanned system or network outages, this diversity allows CenturyLink systems to continue operating while Incident Management processes are engaged to identify and resolve issues. In case of a service interruption and/or outage during the 30-day period and beyond, we have instituted Event Management processes and procedures for dealing with various severity levels during an event. CenturyLink has in place a robust business and service continuity program designed to prevent or mitigate service disruptions and support rapid response to loss or impairment of crucial business functions or infrastructure. CenturyLink Program Manager (CPgmM) along with other project team resource provides a comprehensive Project Development Plan (PDP) which includes Continuity OF Operations Plan (COOP), problem and change management processes reporting systems and an escalation plan. Please refer to attachment 2.d "CenturyLink Sample Program Management Plan for Nebraska".



NOC/SOC 1 Diagram

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 2	**NOC/SOC - Remote Connectivity Required** Contractor shall provide any network connectivity required to support Contractor's NOC/SOC services. Describe any remote connectivity required by the solution including, but not limited to, Virtual Private Network (VPN), phone-home connection, and tech support remote access.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Remote access to secure NGCS is limited to qualified CenturyLink personnel. We pre-certify agents seeking access to the system through a Credentialing Agency. Once inside the system, agent privileges will be limited by policy. We protect workstations and servers with access to the company network with dynamic malware applications that employ whitelisting and blacklisting with advanced static prevention in the form of deep packet inspection to block threats before endpoints are impacted. We employ passwords that are complex employing a random selection of lower-case letters, capitals, symbols and numbers. Passwords include at least nine characters in length and are routinely changed semi-annually or immediately if the account or the network is compromised. We lock any account after a third unsuccessful login attempt. Our NG9-1-1 systems utilize the highest capabilities of protection and authentication available, including IPsec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification: This includes following the "best polices" pertaining to remote access and connectivity: • Operating system and application protections are configured for segregation of duties, and strong password policies are enforced to ensure that password length and minimum change restrictions are followed. • Strict auditing controls are enforced across the enterprise. • Remote access to the CenturyLink NG9-1-1 ESInet network is permitted providing that authorized users are authenticated, and privileges are restricted. Remote access is only permitted via equipment which utilizes an approved firewall, anti-virus protection, and strong authentication. • Any connections over the Internet employ an authorized VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH). • Firewalls, IDS, token-based authentication, encrypted remote access for network and service management systems/work centers. • We protect workstations and servers with access to the company network with dynamic malware applications that employ whitelisting and blacklisting with advanced static prevention in the form of deep packet inspection to block threats before endpoints are impacted. • We employ passwords that are complex employing a random selection of lower-case letters, capitals, symbols and numbers. Passwords include at least nine characters in length and are routinely changed semi-annually or immediately if the account or the network is compromised. • We lock any account after a third unsuccessful login attempt. • CenturyLink administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform the work. • Once inside the system, agent privileges will be limited by policy. CenturyLink incorporates a robust strategy for identity management, and user access to CenturyLink web-based applications is protected through an identity management system. New users must complete a rigorous online registration process. Multi-factor authentication and role-based access				

	control are used to restrict user access to CenturyLink's trusted resources. User access via the public Internet requires two factor authentications, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from a CenturyLink-provided security token. Users are configured in the identity management system and linked to a specific security token and configured for access to a defined list of applications. Our Network based and adaptive security NOC/SOC personnel provides all support for VPN, phone-home connections, and support for any remote tech support changes or issues. Our CenturyLink portal/Dashboard is used to request new or make changes to any remote support requests.

Any additional documentation can be inserted here:

NOC/ SOC 3	**NOC/SOC - Network Security Monitoring and Management** **Security Management Solution** The bidder's security management solution shall control access to network resources in accordance with public safety network security best practices such as NIST, NENA and the FCC to prevent sabotage, service interruption (intentional or unintentional) and the compromise of sensitive information. Security management shall comply with security- and data-integrity standards listed in Section V.D.1. Table 1 in the RFP, to monitor users logging into network resources and to refuse access to those who enter inappropriate access codes. The proposed IP network and systems shall support standard security policies that may include the use of firewall rules, Access -Control Lists (ACLs), Virtual Local-Area Networks (VLANs), VPNs, and Transport Layer Security (TLS) protocols to control network traffic and access. The systems shall support the use of software to detect and mitigate viruses, malware, and other attack vectors. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink NG9-1-1 adheres to NENA 75-001 (NENA Security for Next-Generation 9-1-1 Standard [NG-SEC]) and NENA 04-503 (PSAP Security), as applicable, and we track alignment to the NIST Cybersecurity Framework in addition to the applicable areas of the FBI CJIS Security Policy. The CenturyLink NG9-1-1 solution provides for the centralized management of user permissions, rights, and security settings by designated administrators. The system administrators can use the application to manage user roles and privileges, including granular authentication, user profiles, and other security rights. The system can be configured so that wherever an authenticated user logs in, without regard to which workstation or which PSAP, all the user's rights, permissions and configurations follow that user. The proposed system is password-protected, so only properly credentialed, authorized users can use it. Security options can be configured according to user group. Administrators can create groups of user assigned roles with associated user settings to be automatically applied when users are authenticated during log-in. All systems utilize the highest capabilities of protection and authentication available, including • 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 datacenters and secure delivery of SIP traffic to the PSAP BCF • ("TLS") over TCP • Session Border Controller's (SBC) for secure SIP TLS\Authentication and anchoring. • IPsec and Secure Sockets Layer SSL, virtual private networks VPN technology for remote access from un-trusted networks • SSH for encrypted management capability • Two-factor authentication for remote access to sensitive applications along with digital certificate verification. • Stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress				

	Operating system and application protections are configured for segregation of duties, and strong password policies are enforced to ensure that password length and minimum change restrictions are followed. Strict auditing controls are enforced across the enterprise. Remote access to the CenturyLink NG9-1-1 network is permitted providing that authorized users are authenticated, and privileges are restricted. Remote access is only permitted via equipment which utilizes an approved firewall, anti-virus protection, and strong authentication. Any connections over the Internet employ an authorized VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH). CenturyLink administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform the work. CenturyLink incorporates a robust strategy for identity management, and user access to CenturyLink web-based applications is protected through an identity management system. New users must complete a rigorous online registration process. Multi-factor authentication and role-based access control are used to restrict user access to CenturyLink's trusted resources. User access via the public Internet requires two-factor authentication, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from a CenturyLink-provided security token. Users are configured in the identity management system, and linked to a specific security token and configured for access to a defined list of applications While NENA 75-502.1 is our principal guide for security, we do meet applicable US DHS, FBI and state directives where we operate. All encryption mechanisms are supported in accordance with NENA STA010 and AES256. This extends to the following protocols: Transmission Control Protocol ("TCP"), User Datagram Protocol ("UDP"), Transport Layer Security ("TLS") over TCP, and Stream Control Transmission Protocol ("SCTP"). Protocols supported are selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems. **Access**: All NG9-1-1 services within the ESInet that require authentication implement a Single Sign On paradigm. The mechanism used is OASIS SAML (Security Assertion Markup Language). There are two entities: An Identity Provider (IDP) which authenticates users and supplies services with a "token" that can be used in subsequent operations to refer to an authorized user and a Relying party which uses the token. SAML is used by a Relying Party to ask if an operation should be permitted by the user. Authorization and Data Rights Management in NG9-1-1 is based on XACML 1.0 [87]. Each XACML policy defines: a "target", which describes what the policy applies to (by referring to attributes of users, roles, operations, objects, dates, and more), and one or more "rules" to permit or deny access. Access is defined to mean some combination of: • Read – the ability to retrieve a data object • Update – the ability to modify an existing data object • Create – the ability to create a new data object • Delete – the ability to remove an existing data object • Execute – the ability to execute one or more functions from a service. • Rules may "permit" or "deny" access.

Any additional documentation can be inserted here:

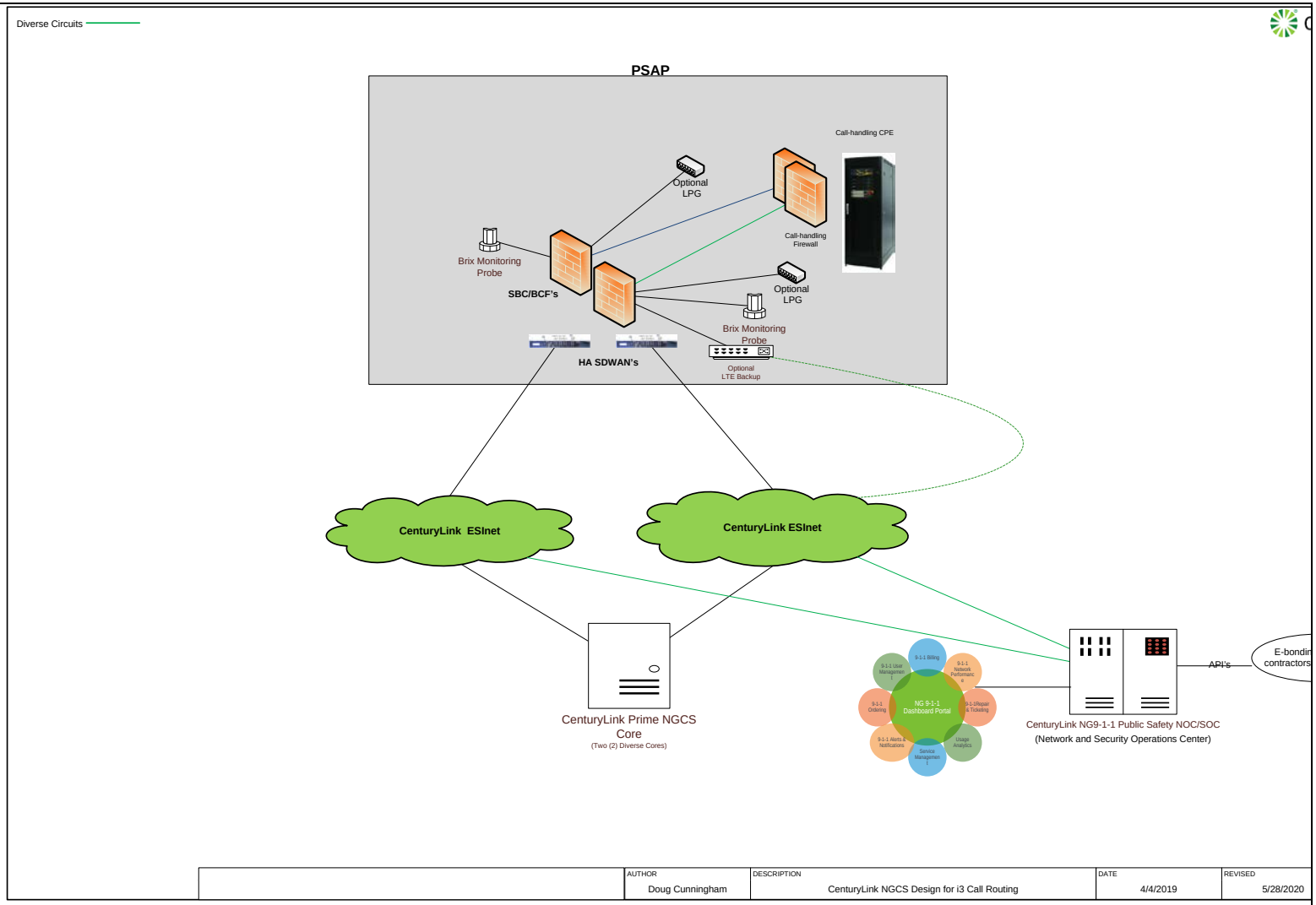
NOC/ SOC 4	**NOC/SOC - Connected Systems Compliance** Any system that connects to an IP network shall be required to comply with listed standards in Table 1, including security standards, and demonstrate compliance through an initial and recurring audit. **Security Reports and Recommendations** Contractor shall provide, within 30 days of the end of each calendar month, security summary reports and recommended improvements on a monthly basis (at a minimum), including incidents and incident response; building, facility, and network access reports, including failed attempts; and updates or changes to security systems and software. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Describe how the solution meets or exceeds the above requirement.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Security reports will be provided per requirement. The assigned Program Manager will accommodate the required frequency for report generation. Our Network Security Dashboard—displays the landing page of the reporting application that combines important metrics from all features in distinct panels. • Traffic—displays a report of traffic allowed and denied by firewall policy. (Requires that the All Traffic option under Policy Logging be selected during service setup.) Reports show how traffic was managed in response to such policies. • CenturyLink Security Solutions Portal for Dashboards and Reports including: • Rapid Threat Defense • Threat Visualization • DDoS/TDoS • Network Security reports CenturyLink program manager will collaborate with the Nebraska Commission in the preparation of the customization of the monthly security reports. All data reports can be viewed electronically via our dashboard portal and will be retained for the duration of the contract.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 5	**NOC/SOC – Connected Systems Compliance Support for Similar Solutions** Provide details concerning how bidder provides security monitoring and management for similarly deployed production solution. Provide details, including drawings, which explain how the proposed solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's NG9-1-1 NOC/SOC management system monitors and manages PSAP's in over 32 states of the US. Our NG9-1-1 NOC/SOC monitoring includes similar deployments in states like Arizona, California, North Dakota, Minnesota and other city and county PSAP agencies throughout the US. Over 500 NG9-1-1 PSAP's are monitored across the US in these states. CenturyLink Network Operations Team is made up of three (3) sub-teams, 911 Network & Security Operations, 911 Support Services and the Network Event Management Center. CenturyLink NOC/SOC currently provides responsible for the day-to-day management, operation and maintenance of CenturyLink's E9-1-1 and NG91-1 networks.				

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



NOC/SOC 5 CenturyLink NG911 Public Safety NOC/SOC Monitoring and Management System

	Our NG9-1-1 Public Safety NOC/SOC security and event management services include: **CenturyLink Adaptive Network Security (ANS)** – Our ANS is reliable managed and monitored security providing a layer of protection against an increasingly complicated threat landscape in Public Safety. It forms the basis of a network solution that brings multiple customer sites and users (with various access technologies) into one holistic platform for Unified Threat Management (UTM) for an increasingly diverse and mobile workforce. It has many features such as firewall, IPS and content filtering options with enhanced reporting portals **CenturyLink Network Based Security Service (NBS)** provides additional layers of security using Firewalls and Unified Threat Management (UTM) functionality for CenturyLink public safety MPLS networks. An integral part of NBS is the ability for CenturyLink to dynamically announce a default route (0.0.0.0/0.0.0.0) into the MPLS VPN. Site to Site VPN's will be provided for new or future applications entering our ESInet solution. The use of eBGP by NBS at the routing level provides for both scale and resiliency. Additionally, using BGP attributes, such as Local Preference and AS Prepend, the values of default routes can be changed based on customer topology requests. **Network Monitoring & Response** Circuit Tagging – All of our 9-1-1 circuits are physically, and system tagged as critical 9-1-1 Services. Our CenturyLink dashboard will provide a consolidated view of the network from several contributing platforms. Chief among these is our SD-WAN security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms. Also, our CenturyLink Network Operations Team is made up of three (3) sub-teams, 911 Network & Security Operations, 911 Support Services and the Network Event Management Center. Between them they are responsible for the day-to-day management, operation and maintenance of CenturyLink's E9-1-1 and NG91-1 networks A notification of the upcoming event will be sent to the customer as applicable. Planned events are fully staffed and managed with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. We maintain a model cybersecurity plan that we adapt for every client. It is based on a frequently updated threat analysis that is used to modify a basic stance to meet the needs of each network and dataset we are charged to protect. Our plan stresses four phases: 1. Preparation 2. Detection and analysis 3. Containment, stabilization and return to a steady state. 4. Post incident activities that include a root cause analysis and corrective action. These phases are interrelated and represent a continuous loop of preparation, analysis and improvement that continues whether an actual emergency occurs or not.

Any additional documentation can be inserted here:

	NOC/SOC - Physical Access Monitoring and Management Contractor shall track and log all physical access to structures housing IP network components serving the Commission or have the capability to obtain access logs for structures not under immediate control of the bidder. Reports may be requested and shall be made available for review upon request. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Provide a detailed explanation of bidder's processes and procedures for logging physical access to ESInet /NGCS components, and how the bidder's solution generates the required reports.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

NOC/SOC 6

Bidder Response:

CenturyLink uses multi-tiered security measures for logging and restricting Physical access our NGCS and ESInet components. This includes our Data Centers and any structure maintaining ESInet and NGCS components. We allow access only to authorized people and we track and log physical access. Security measures include continuous closed-circuit video monitoring, 24-hour on-premises live security, electronic key card access, individual, personal access codes, and biometric hand scans. CenturyLink actively maintains an access list. All additions to this list must be submitted in advance and in writing. Access is limited to areas designated in the access list. Only individuals identified on this list will have access. We further protect our operations and equipment by using controlled entrance and exit doors, security breach alarms, secured cage and cabinet environment, mantraps, and discrete buildings (no signage). We align with the applicable areas of the FBI CJIS Security Policy.

CenturyLink's datacenters meet Tier III standards stipulated in the two main datacenter tier classifications developed by the Telecommunications Industry Association (TIA) and the Uptime Institute (UI). Physical security includes hardened defined external perimeters, hardened outer walls with no openings available for exploitation, redundant commercial power (supplied from separate grids if possible), redundant backup generators, redundant uninterruptible power supplies ("UPS"), redundant heating, ventilation, and air conditioning ("HVAC") systems, fire suppression systems physical access security with separate communication service provider entry points. Access control lists and at least two automated ID sensors such as proximity cards and biometrics, etc. Visits by uncleared individuals must be approved in advance. All visitors are escorted. While the exact infrastructure varies slightly from one center to the next, the following chart depicts the basic layout:

Component	Type	Purpose
Badge card access system (EntraPass)	Kantech	The badge card system is utilized in conjunction with a biometric recognition access system to control entry into the greater datacenter and separately to the raised-floor production zone.
Biometric Recognition Access System (EntraPass)	Kantech	With badge control system, controls entry into the greater datacenter and separately to the raised-floor production zone.
Firewalls	Forigate Fort/OS	Corporate firewalls restrict traffic into the management network. Service delivery firewalls filter and route traffic for customer-specific environments that have borders that cannot be breached.
Management services backup servers	CommVault	Automated system software and network of servers provide backup and recovery for subscribing customers.
Routers and switches	Cisco NXOS	Route network traffic
Virtual Hypervisor	VMware vCenter	Authenticates and restricts access to customer virtual environments.

VMware hosts	VMware (ESXi 6.0)	Provide secure operation of client virtual machines
Web portal	Embotics vCommander	Customer portal system through which they manage their virtual machines which are isolated from all others.

The CenturyLink NGCS and ESInet solution provides for the centralized management of user permissions, rights, and security settings by designated administrators. The system administrators can use the application to manage user roles and privileges, including granular authentication, user profiles, and other security rights.

The system can be configured so that wherever an authenticated user logs in, without regard to which workstation or which PSAP, all the user's rights, permissions and configurations follow that user.

The proposed system is password-protected, so only properly credentialed, authorized users can use it. Security options can be configured according to user group. Administrators can create groups of user assigned roles with associated user settings to be automatically applied when users are authenticated during log-in. All systems utilize the highest capabilities of protection and authentication available, including IPsec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification.

Operating system and application protections are configured for segregation of duties, and strong password policies are enforced to ensure that password length and minimum change restrictions are followed. Strict auditing controls are enforced across the enterprise.

Remote access to the CenturyLink ESInet network is permitted providing that authorized users are authenticated, and privileges are restricted. Remote access is only permitted via equipment which utilizes an approved firewall, anti-virus protection, and strong authentication. Any connections over the Internet employ an authorized VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH).

CenturyLink administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform the work. CenturyLink incorporates a robust strategy for identity management, and user access to CenturyLink web-based applications is protected through an identity management system. New users must complete a rigorous online registration process. Multi-factor authentication and role-based access control are used to restrict user access to CenturyLink's trusted resources.

User access via the public Internet requires two factor authentications, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from a CenturyLink-provided security token. Users are configured in the identity management system and linked to a specific security token and configured for access to a defined list of applications.

CenturyLink ESInet cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology.

CenturyLink ESInet infrastructure is designed to withstand sophisticated cyber-attacks. CenturyLink ESInet is a secured and private IP managed network providing services for 9-1-1 call delivery. All inbound and outbound traffic interactions are with pre-vetted entities, utilize well defined protocols and traverse controlled access points. Call processing and real-time data delivery are implemented through specialized subnets.

Sensitive data is housed in data centers with logical and physical access controls. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough vulnerability scan testing. Corporate, development, and test environments are separate from production, and live production data is not used for development or testing purposes. Inter-zone traffic is

	restricted to only authorized personnel and the necessary protocols destinations used to support the management and applications of CenturyLink ESInet with all other traffic implicitly denied by way of redundant and diverse session border controllers and firewalls. CenturyLink ESInet infrastructure is built to withstand sophisticated attacks by means of a defense-in-depth strategy. Traffic between core processing and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) are route-secure and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of CenturyLink ESInet CenturyLink ESInet also employs a regularly scheduled patching process to protect against security vulnerabilities and the effects of malware. Computing devices are subjected to thorough security scans for malware elements. Physical, network, and application access to production components is restricted to personnel that have a direct operational responsibility, with all activity audited and monitored. The Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage CenturyLink ESInet associated services and connectivity to the network. When a potential or actual customer-affecting issue is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established processes that are ISO 9001:2015-compliant for immediate escalation, notification, resolution, and reporting. All buildings, NOC and Data Center access are monitored by 24x7 security and access control systems. Security Information and Event Management (SIEM) analysis is a daily task of our Security Operations Center. We have deployed a SIEM tool for log aggregation and consolidation from multiple machines and for log correlation and analysis. Info security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. We deploy heuristic analysis, a method employed to detect previously unknown computer viruses, as well as new variants of viruses. Heuristic analysis is an expert-based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. We perform annual external and internal penetration testing of our critical systems and infrastructure. We maintain in-house tools and expertise in order to conduct penetration testing and work with nationally recognized penetration test providers to achieve third party assurance CenturyLink uses multi-tiered security measures to restrict access to our Data Centers and any structure maintaining ESInet and NGCS components. We allow access only to authorized people and we track and log physical access. Security measures include continuous closed-circuit video monitoring, 24-hour on-premises live security, electronic key card access, individual, personal access codes, and biometric hand scans. CenturyLink actively maintains an access list. All additions to this list must be submitted in advance and in writing. Access is limited to areas designated in the access list. Only individuals identified on this list will have access. We further protect our operations and equipment by using controlled entrance and exit doors, security breach alarms, secured cage and cabinet environment, mantraps, and discrete buildings (no signage). We align with the applicable areas of the FBI CJIS Security Policy. CenturyLink follows both the Physical Security and logical security Guidelines as outlined in the Nena" Security Document NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) NENA 75-001" which includes: • CenturyLink separates physically and logically ESInet functions into separate security domains. This methodology provides a clear demarcation of NGCS functions and security requirements from Managed CPE functions and security requirements.

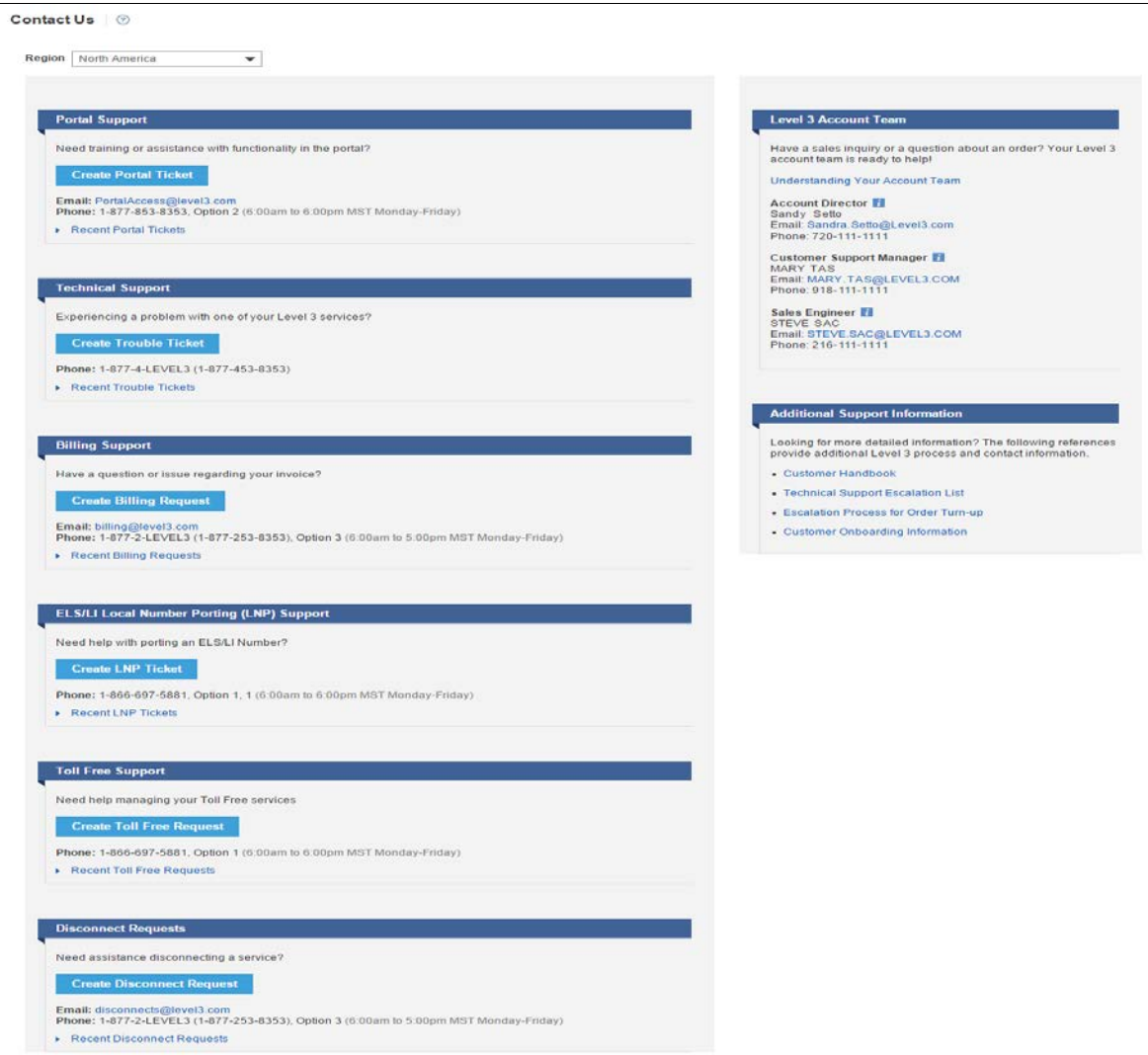
	• CenturyLink's NGCS Solution, access control is provided through the Border Control Function/Session Border Controller (BCF/SBC) at the NGCS datacenters, this secures and segments the core functions to the transport network for the PSAP and external data sources which all remain in separate security domains. • All messaging transiting the network uses SIP. If not delivered in SIP natively, it must be interworked to SIP using the Protocol Interwork Function (PIF) of the Legacy Network Gateway (LNG). PSAP BCF/SBC are included part of this service as well that will terminate secure traffic to the PSAP and expect to hand off to the endpoint PSAP via customer provided call handling equipment firewall/BCF or SBC. • The CenturyLink's NGCS Solution and ESInet are provided with an array of BCFs/firewalls that inspects all traffic transiting the network edge. This device will employ both application and network layer protection and scanning capability as well as mitigates lower layer protocol attacks. The BCF provides Denial of Service (DoS) and Distributed Denial of Service (DDoS) detection and protection. Our network supports standard 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 datacenters and secure delivery of SIP traffic to the PSAP BCF. • Our network infrastructure is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. We employ high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/Application availability is safeguarded with clustering and load balancing techniques. Furthermore, our security architecture employs defenses that include, but are not limited to, Stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress. • Building and Physical Access Control • Hardened defined external perimeters, hardened outer walls with no openings available for exploitation, access control lists and at least two automated ID sensors such as palm-print readers, etc. Visits by uncleared individuals must be approved in advance. All visitors are escorted. • Entity identification badges, building access cards, building keys, and/or any other form of recurring access that does not require approval at the time of access shall be sponsored by a NG9-1-1 Entity management person. Appropriate local, state and federal laws and guidelines shall be followed for allowing nonemployee access (i.e. CJIS Background Checks, etc.). • Identification Badges • Mobile Security and Security in and outside the Work Area or PSAP • Physical Access • CenturyLink network Interconnect equipment which will include routers, firewalls, Audio Codes and other similar equipment shall be installed and contained in a secure locked cabinet located at each PSAP with appropriate physical access controls. If equipment is in equipment rooms shared with non-NG9-1-1 Entity entities or in unsecured space, it shall be contained in locked cabinets • All NG9-1-1 services within our ESInet that require authentication implement a Single Sign On paradigm. The mechanism used is OASIS SAML (Security Assertion Markup Language). There are two entities: An Identity Provider (IDP) which authenticates users and supplies services with a "token" that can be used in subsequent operations to refer to an authorized user and a Relying party which uses the token. SAML is used by a Relying Party to ask if an operation should be permitted by the user. • Rather than supporting signaling or voice encryption, we rely on the MPLS security and secured IP tunnels to provide confidentiality for signaling and voice.

	• We employ the NENA 75-502.1 Audit Checklist to build our security program to include all system components and to test project compliance. We employ independent access control and auditing at the rack level for core services facilities.

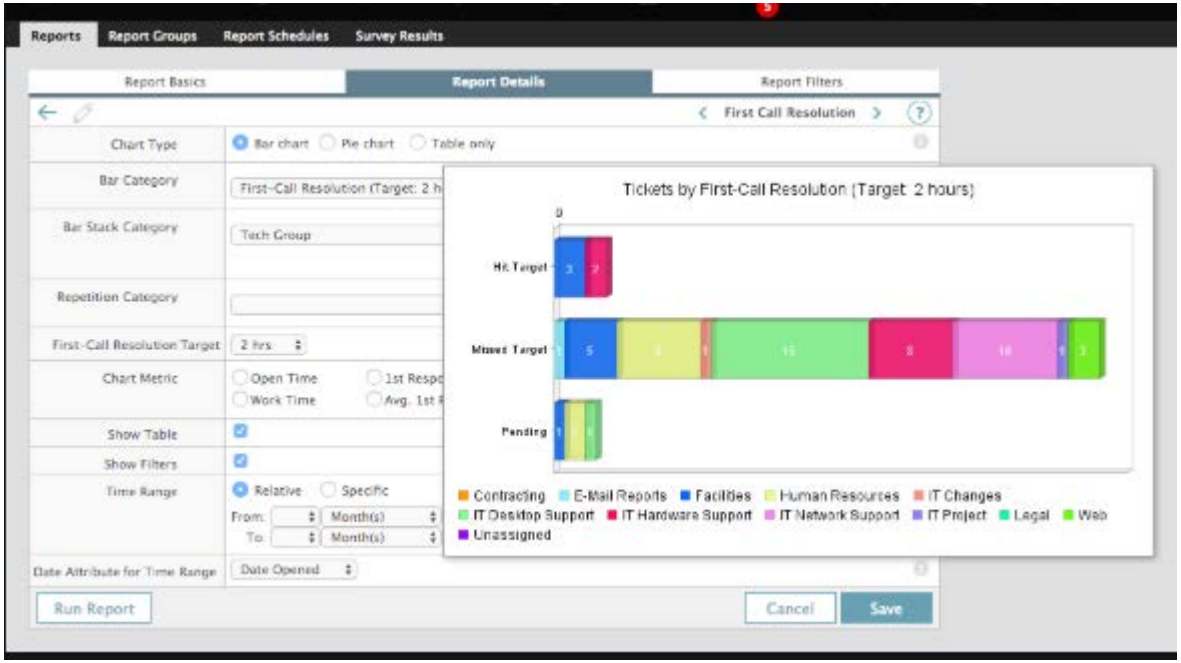
Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	NOC/SOC - Incident Management System The bidder's incident management system shall log all support requests, both from users and those automatically generated. 1. Provide examples of monthly reports detailing tickets opened, pending, resolved, and closed. 2. Provide a matrix outlining Service Impact Levels in a detailed response, to include notification times and response times.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 7	Bidder Response: 1. CenturyLink PSAPs and the State of Nebraska stakeholders have access to an online ticketing system to open, update, view status and request ticket closure for maintenance issues. This includes Monthly reports, showing pending online Web portal. We provide a ticketing system for the NG9-1-1 network from several contributing platforms. Chief among these is the FortiSIEM event management platform. This tool gathers a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. This tool has a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP. For the manager, this dashboard provides an unprecedented level of network visibility in a variety of networks and devices. This depth of real-time visibility includes signaling messages – as they traverse through individual devices – media quality, message parameters, etc.				



Samples of Dashboard Portal View



Sample of Monthly Ticket Reports

In case of a service interruption and/or outage, our team has instituted Incident Management processes and procedures for dealing with various severity levels during the course of an incident. Our incident response tools include use of the Incident Command System (ICS), which is housed within our Ticketing System. The ICS is modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute for major incidents. The ICS processes include resolution, documentation of any incident, communications, and post- event analysis. Incidents overall, regardless of level of severity, are tracked within our ticketing system, which also provides broadcast messaging available for real-time updates and status of ongoing service affecting issues that may impact the NG9-1-1 solution.

Incident Management personnel are trained in incident command with courses provided by the Emergency Management Institute, a FEMA-sponsored Emergency Management Course as well as the ITIL framework. Incident Management is available 24 hours a day, 7 days a week.

CenturyLink utilizes the Incident and Problem Management modules of Remedy, which allows for tracking of break/fix issues as well as any resulting Problem Management requests. All support requests from users and those automatically generated are logged.

2.A table outlining Service Impact Levels, to including notification times and response times is below

The table below equates incident and reporting levels.

Severity[1]	Description[2]	Response
Level 5: Emergency	NGCS is no longer able to provide some critical services to any user. Prime assuming responsibilities for region. Debilitating denial of services, large amounts of data exfiltrated, inappropriate disclosure, ransomware attacks, unauthorized privilege escalation.	Immediate. Notifications made within one hour. Response partners placed in full emergency response mode. State immediately notified.
Level 4: Severe	Poses a threat to essential services or causes some subset failures that can be compensated for through active-active. May impact systems outside the CenturyLink region. Includes significant denial of services, abnormal ad-hoc requests, unauthorized access or attempted access, inappropriate disclosure, inappropriate destruction of sensitive data, etc.	Within two-hours of notification. Response partners placed on standby for immediate dispatch if needed. State immediately notified if outage occurs.
Level 3: High	Impacts ESInet reducing optimum performance but does not impact essential services nor impact SLA status significantly. Includes web defacements, denial of services, hacking activities, modification of software or systems, suspicious activities.	Within four hours. Response partners alerted. State notified per SLA
Level 2: Medium	Internal system impact that slows company work processes and may interrupt some non-essential tasks. Includes power outages, physical damage, sabotage, physical loss or theft of information.	With two workdays.
Level 1: Low	Unsubstantiated or inconsequential event including social engineering, Trojan or virus infections, harassment, elevated data disclosure, improper disposal of documents.	Within five workdays of notification that event has occurred.
Level 0	Steady state. System monitoring operating and protection in place.	Standby

This chart is modeled on USDHS threat ID levels.

Examples drawn from California Joint Cyber Incident Guide.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/SOC 8	NOC/SOC - Change Management System Change Management Review System Describe bidder's change management system and the ability to provide the Commission's program manager and designated PSAP representatives with the ability to review proposed change requests and the client approval process. The Contractor shall provide monthly reports detailing change tickets opened, pending, resolved, and closed.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well as best-in-class tools for Change Management for managing changes to the service. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management. The result of each change is tracked and available for future reference in our Change Management Module whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the NGCS Core Team. If the change was successful with deviation, this is also tracked with the deviations documented. The process proceeds through several defined steps: 1. The change must be proposed by an authorized individual usually within the agency impacted by the change. 2. A thorough technical review is conducted to identify feasibility, direct and indirect impacts, potential compatibility issues and effect on network availability. 3. A security impact review is conducted, and plans are amended as needed. 4. A final approval is obtained from the appropriate level of management. 7. A project plan is prepared. 8. Users are notified if an outage is expected. 9. The project is completed and accepted. 10. A formal change report is submitted with a complete analysis of lessons learned. CenturyLink also utilizes Incident and Problem Management modules, which allows for tracking of break/fix issues as well as any resulting Problem Management requests. Our Change Management team shall provide all required monthly reports to the State of Nebraska detailing change tickets opened, pending, resolved, and closed of each event. Refer to below NOC/SOC 11 for additional details.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 9	**NOC/SOC - Change Management System** **Change Management Tools** Provide detailed descriptions of any other tools bidder intends to use to provide access to the change management system, such as web portals and client software.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Access to the change management system will be available and viewed through our customized CenturyLink NG9-1-1 Public Safety web dashboard and portal. Our NG9-1-1 Public Safety NOC in conjunction with the CenturyLink change management team coordinates planned and unplanned maintenance to reduce the impact to customer service. Our change management team will provide notice of the change via emails, distribution mailboxes and or Web portal. Each change is tracked and available for future reference in our Change Management Module of portal whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the NGCS Core Team. If the change was successful with deviation, this is also tracked with the deviations documented in our Web portal and email processes.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 10	**NOC/SOC – Change Management System** **Change Testing and Training Environment** A non-production ESInet replica / NGCS replica, test lab, or similar system shall be established to test, and exercise proposed upgrades, third-party interfaces, and applications prior to release in live production. This system also could be leveraged for training purposes. Provide detailed descriptions of how the solution satisfies this function in the change management process.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: We employ rigorous steps to technically and operationally review all new hardware, software, network and patch releases end-to-end. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. The testing program includes the following elements. • Test plans developed in conjunction with equipment and software vendors. • Labs that mirror the production architecture and operating environment. • Coordination with vendors to address any problems related to new product or software releases. • Oversight of the First Office Application (FOA) of all newly introduced hardware or software releases We employ rigorous steps to technically and operationally review all new hardware, software and patch releases end-to-end. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. The testing program includes the following elements. • Test plans developed in conjunction with equipment and software vendors. • Labs that mirror the production architecture and operating environment. • Coordination with vendors to address any problems related to new product or software releases. • Oversight of the Approved for Field Use (AFU) of all newly introduced hardware or software releases. • Provides Approval for Use and certifies new hardware or software release upon successful completion of FOA soak period. • CenturyLink offers an NG9-1-1 ESInet i3 test lab program. As part of this program, NG911 vendors can test with CenturyLink's NG9-1-1 lab to validate network, i3 interactions and Call Handling Equipment (CHE) before going into production.				

Any additional documentation can be inserted here:

NOC/ SOC 11	**NOC/SOC – Change Management System** **Change Management Process** 1. Outline bidder's proposed change management process. The ITIL change management standard methods and procedures are preferred. 2. Include a description of the process for notifying the Commission and affected PSAPs. Notification shall be made no less than ten (10) business days in advance of the change, except in emergency situations, in which case notification shall be provided immediately. 3. Include explanation of solution's Fault, Configuration, Accounting, Performance, and Security (FCAPS) procedures. 4. Provide a detailed explanation describing how the proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

CenturyLink will conduct major and minor planned and critical un-planned changes for all CenturyLink's NG9-1-1 ESInet system maintenance and or upgrades that may impact customers. CenturyLink will manage and complete events with a trained ESInet change management team facilitating the change implementation, monitoring, and communication through the length of the event. CenturyLink adheres to stringent internal event plan processes and procedures which include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. CenturyLink will include the required back-out time within the scheduled maintenance timeframe.

Our 24x7x365 NOC dedicated to 9-1-1 call delivery services supports the CenturyLink's NGCS Solution network, core services, and equipment. CenturyLink utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well as best-in-class tools for Change Management.

We will rigorously enforce a formal change management program that satisfies the guidelines published by the Project Management Institute (PMI).

Change Requests vary widely in terms of scope and complexity, dependent upon the type of change. Change Requests with largest potential impact are submitted to a NGCS Core Team for approval. The NGCS Core Team is a committee that makes decisions regarding whether a change should be implemented. CenturyLink manages all aspects of Change Management through the Change Management Process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management. Our team coordinates planned and unplanned maintenance to reduce and or eliminate the impact to customer. The intent is to work within the PSAPs current Standard Operating Procedures (SOPs) or provide guidance on creating them on how to manage the planned or unplanned maintenance.

There are five categories of changes.

Table 1: Change Management Categories

Change Category	Description
STANDARD	This change indicates a low risk and repeatable change that occurs frequently. Once it is deemed appropriate (3 successful) Change plans / MOPs are in place, a template will be built so the change can be entered as a Standard Change for future usage negating the need for a normal change. This change type does not require Program Management Team approval.

NORMAL	Normal changes are often categorized according to risk and impact to the organization. A normal change will proceed through all steps of the change management process, including the Program Management team for approval.
LATENT	This change should be utilized for unplanned work, resulting from a critical incident ticket &/or Major Incident.
EXPEDITED	An expedited change will proceed through all steps of the change management process and will be reviewed by the our NG9-1-1 Program Management team. There is a valid business reason to bypass the 48-hour advance submittal time frame.
EMERGENCY	Utilized for a change that resolves a problem deemed critical to business continuity and for which a workaround is not enough. Examples are a router that could put voice delivery at risk and has a potential for an immediate threat to the production environment and /or to be a major impact to Business or Customer. Emergency changes are approved by our NG9-1-1 Program Management Team

NOCSOC 11 - Change Management Change Categories

CenturyLink will provide a notice in writing within five business days to the State on all Planned changes.

For Normal, Emergency, and Expedited changes, a change request is submitted to the NGCS Team. The request must include a step-by-step explanation of the purposed changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment.

The result of each change is tracked and available for future reference in our Change Management Module whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the NGCS Core Team. If the change was successful with deviation, this is also tracked with the deviations documented.

The process proceeds through several defined steps:

1. The change must be proposed by an authorized individual usually within the agency impacted by the change.
2. A thorough technical review is conducted to identify feasibility, direct and indirect impacts, potential compatibility issues and effect on network availability.
3. A security impact review is conducted, and plans are amended as needed.
4. A final approval is obtained from the appropriate level of management.
7. A project plan is prepared.
8. Users are notified if an outage is expected.
9. The project is completed and accepted.
10. A formal change report is submitted with a complete analysis of lessons learned.

	CenturyLink also utilizes Incident and Problem Management modules, which allows for tracking of break/fix issues as well as any resulting Problem Management requests.

Any additional documentation can be inserted here:

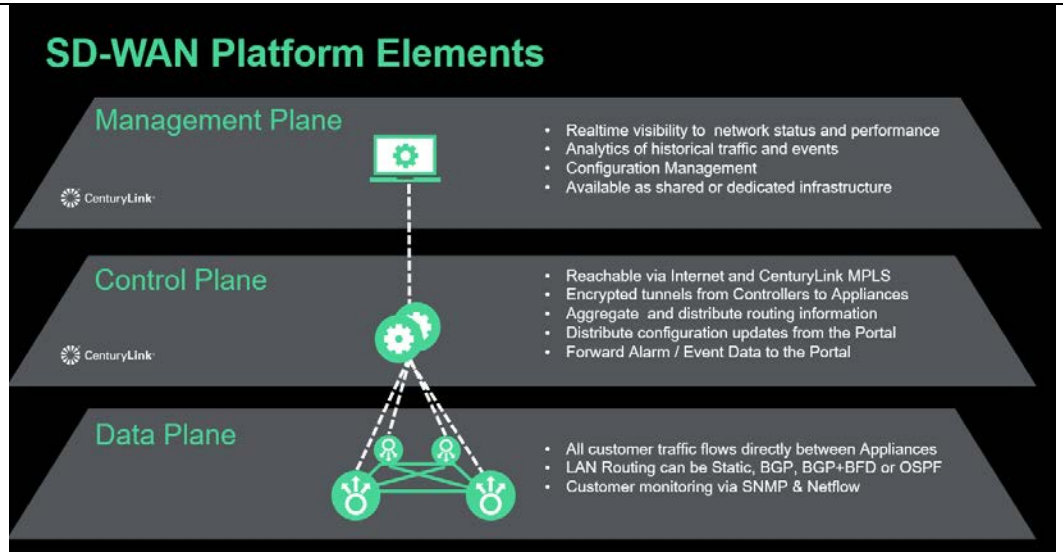
NOC/ SOC 12	**NOC/SOC - Network Management System** **System and Network Management Software** Software packages are widely available for capturing, analyzing, and reporting the network's health based on the Simple Network Management Protocol (SNMP) traffic it receives. Provide the name and description of the management software that will be implemented including all functional modules associated with it (e.g., reporting, backup, and IP address management).	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

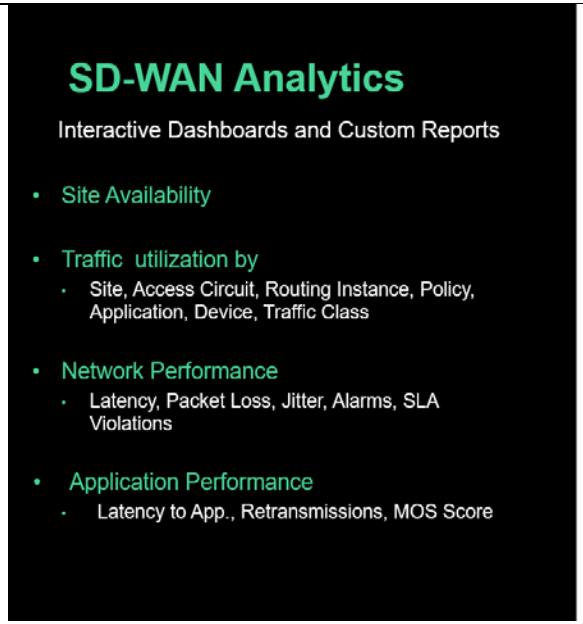
CenturyLink will provide 24x7x365 monitoring of the NG9-1-1 network and equipment. CenturyLink will provide real-time reporting capabilities as well as access to the NOC for real-time updates on network and equipment health.

CenturyLink integrates a comprehensive set of tools for constant monitoring and management of the network. Multiple network management components will monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components will generate alarms to appropriate systems. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Delivery of monitoring reports, including bandwidth utilization and connectivity are provided as mutually agreed upon during contract negotiations. Traditional network management tools are complimented by active application monitoring and alerting. Application elements, BRIX probes and well as SDWAN deployment will also report network failures as detected by their monitoring activity, some of which is specific to managing the availability and integrity of the network.

Our SD-WAN provides Realtime visibility to our network with analytics of historical traffic and events. The SD-WAN platform consists of the core elements: Management Plane, Control Plane, and Data Plane.



Our SD-WAN Analytics can generate customer reports and will integrate into our NG9-1-1 Dashboards. This includes Site Availability, Traffic Utilization, Network Performance, and Application Performance.



SolarWinds will capture and analyze the end to end health of the NG9-1-1 network, includes an IP manager,monitors all network elements and E-Bonding to the dashboard to provide "Near" Real-Time data for alarming, notification, SLA reporting, etc Some of our reporting and monitoring tools that will be used such SolarWinds Network Atlas, Utility Tools (Ping, Tracroute, NSlookup, Power Tools, Commercial Scanners and Open Source type Tools .

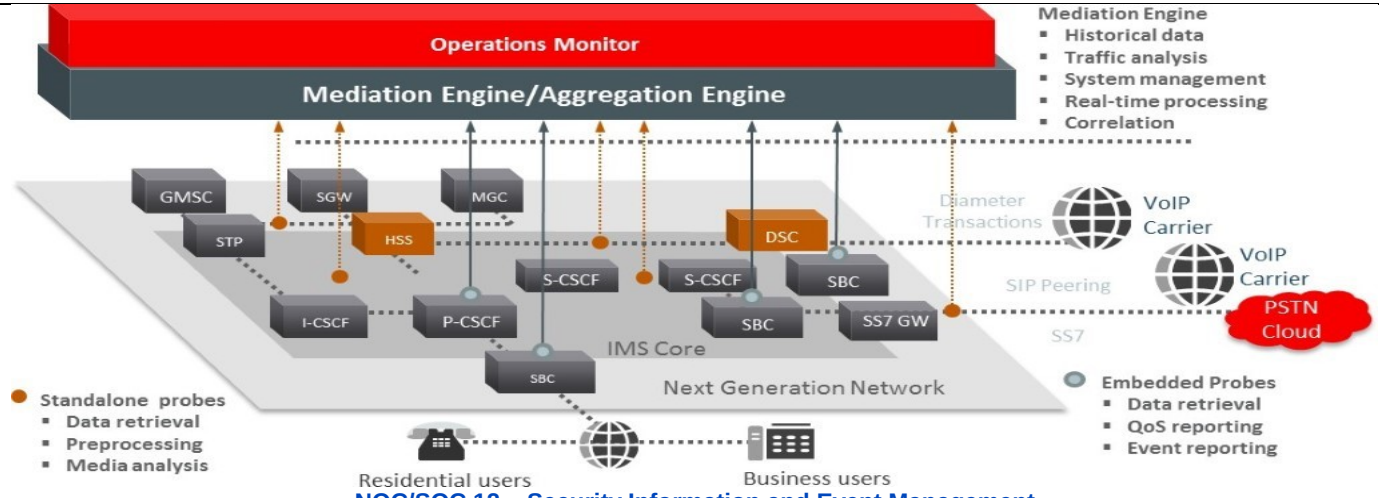
The combined tools provide extremely detailed reporting and visibility to network functionality across the PSAPs and the regional cores.

CenturyLink's solution supports all version of SNMP but only uses SNMPv3 due to the security risk with using earlier versions. MIBS for network components are included in our monitoring solution and will be implemented for that function of the proposed solution

Our NGCS includes additional monitoring through Oracle Enterprise Operations Monitor and the FortiSIEM security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP.

Oracle Communications Operations Monitor **(**OCOM) is a proactive call monitoring solution. It captures and analyzes all required signaling messages and media from the network, providing full correlation and quality metrics in real time. It also enables easy-to-use, drill-down troubleshooting for root-cause analysis of any reported problem related to a user, user group, trunk, network device, or Internet Protocol (IP) address. Key features include:

	• End-to-end call correlation and analytics in real time • Segmentation of the network path for fast and accurate problem localization • On-demand troubleshooting down to the individual subscriber, customer, or employee • Media quality analysis, including R- Factor and MOS scores • Unparalleled insight into and analysis of signaling messages • Embedded software to eliminate need for additional monitoring equipment in the network • Intuitive and simple GUI The breadth of OCOM is depicted below. FortSIEM enables unified and cross-correlated analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the threat data available in the organization. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for handling real-time searches, rules, dashboards and ad-hoc queries. Key features include: • Unified, Real-Time, Network Analytics • Single IT Pane of Glass • Multi-tenancy • MSP/MSSP Ready • Cross Correlation of SOC & NOC Analytics • Self-Learning Asset Inventory • Cloud Scale Architecture • Security and Compliance out-of-the-box The FortiSIEM model is also depicted below.



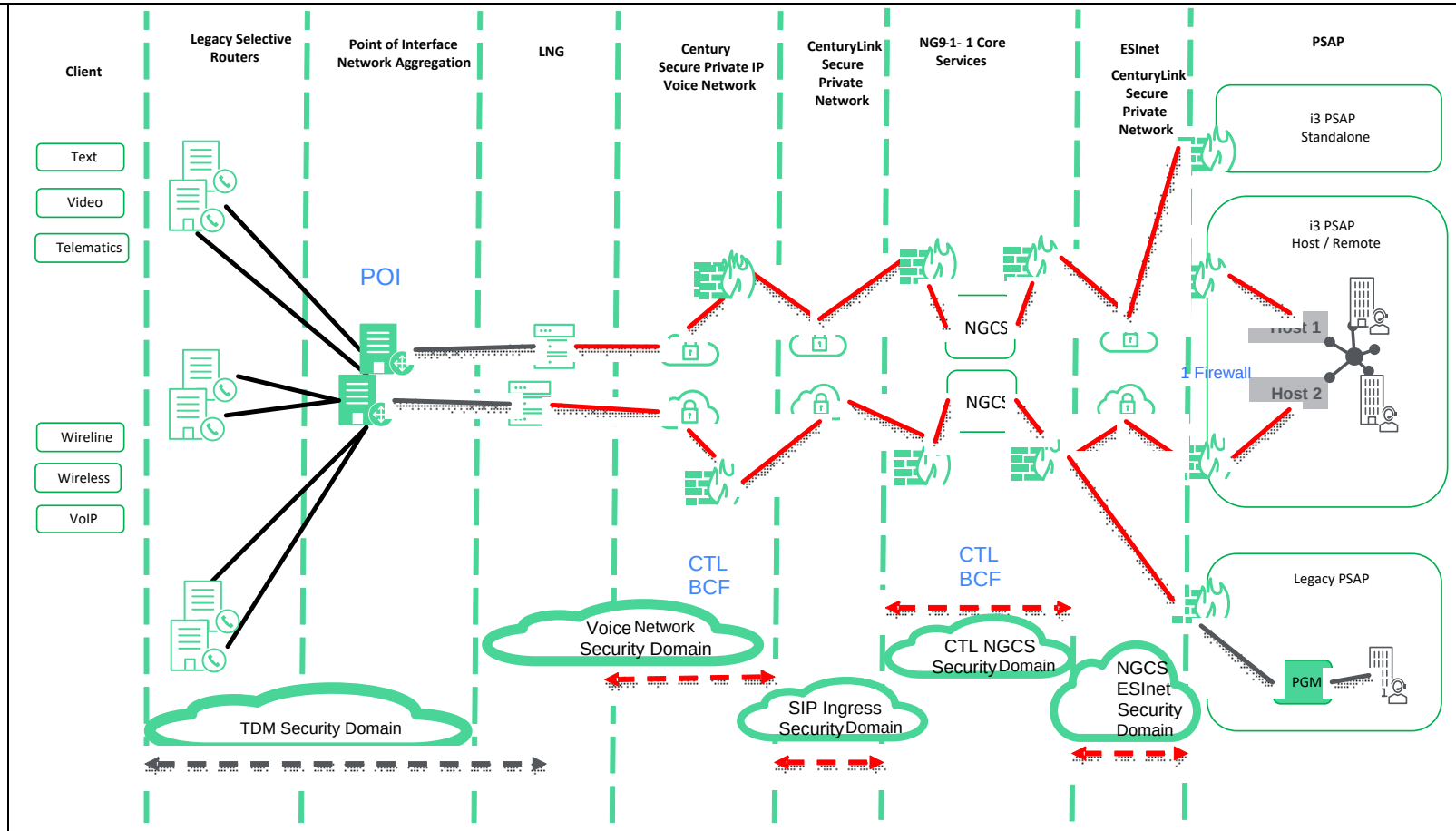
NOC/SOC 12 – Security Information and Event Management

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 13	**NOC/SOC – Network Management System** **NMIS Interworking with Elements and Services** Provide a detailed explanation and associated drawings explaining how the proposed solution interworks with all of the various elements and services of the proposed systems and network elements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage NG Routing services and connectivity. Our NOC/SOC team uses established processes that are ISO 9001:2015-compliant for immediate escalation, notification, resolution, and reporting. Multiple network management components monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Active application monitoring and alerting complement traditional network management. The NG Routing application elements also report network failures as detected by their application messaging activity, some of which is specific to managing the availability and integrity of the solution. All application and network elements are monitored at the NOC. This includes the LNGs, ESRPs, ECRFs, BCFs, functional elements, and PSAP site network interface equipment (NID). CenturyLink HA SDWAN appliance configured provides an additional layer of network management across the network to the PSAP Endpoint's including. • Network management and monitoring of all the networking edge devices for the ESInet. • Create flows for the PSAP to ensure secure segmented delivery of Internet traffic and path diversity to the our NG9-1-1 solution.				

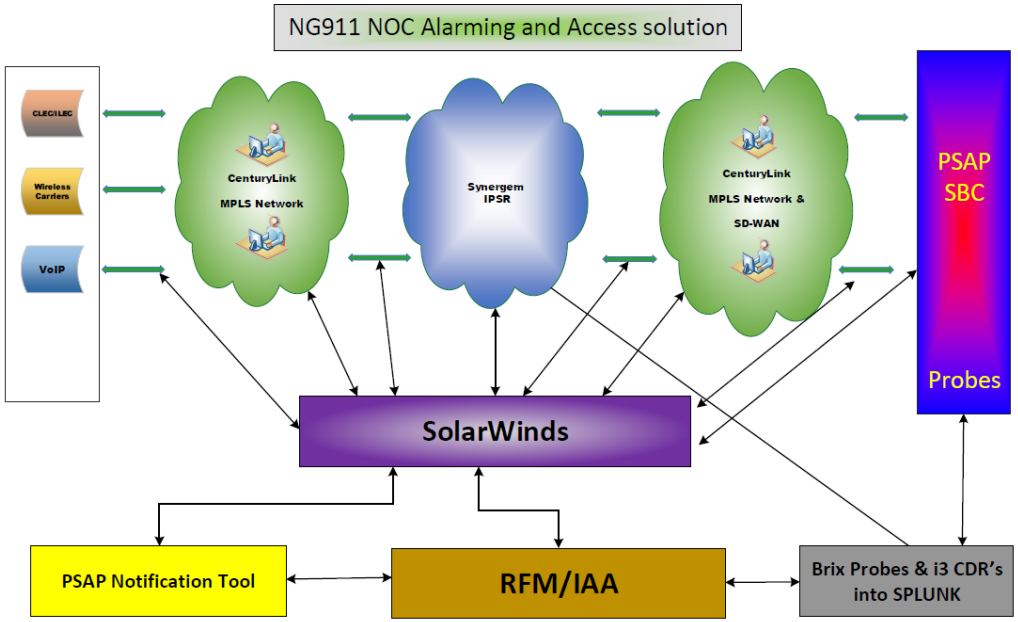
Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



The NOC monitors and tracks net flow statistics and performs packet level capture and forensics at the core sites. There are currently two varieties of interfa systems in use at the NOC. One provides a "single pane of glass" for network and system status. This provides SNMP trap and syslog receiver capabilities. These systems also provide ICMP and SNMP trending and threshold alarming. The second type of system provides packet capture, display, and troubleshooting capabilities.

CenturyLink uses multiple real time monitoring tools to track performance and fault management activities. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to our Oracle Enterprise Operations Monitor (OCOM) system and the FortiSIEM security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network,

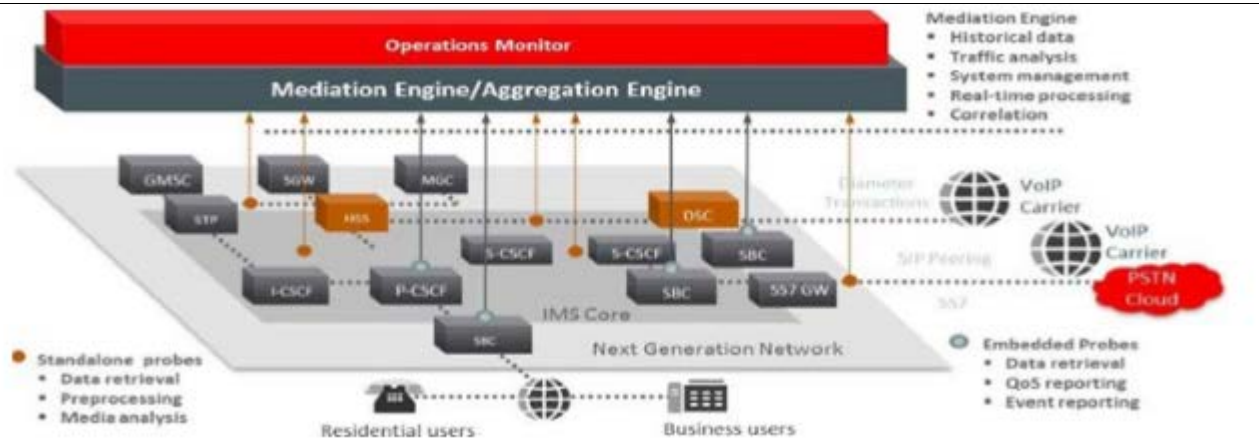
including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP. Then, these and other data sources such as E-Bonding ticket information are consolidated into a single viewing portal for access by the state.



This provides critical path hop-by-hop analysis and visualization all along the delivery track. We can quickly see maps of network connections, dependency relationships, and topology information, and know who and what's connected to the network, and when and where they're connected. This application ensures devices are configured and operating in compliance with regulatory standards and that network managers are prepared to recover quickly from hardware faults and human errors using automatic backups.

Our other monitoring tools will also allow end-users to gain visibility into signaling and media interactions, and leverage key indicators to identify, troubleshoot, and resolve issues that can reduce the efficiency of enhanced IP network service. Our monitoring tools captures all messages transiting the network using network probes linked to an unrivaled correlation engine. Results are viewable through a web-architected GUI. This Monitor runs on commercial-off-the-shelf hardware and software components that are integrated into our session border controller (SBC) service delivery platforms

Following diagram illustrates the breadth of OCOM:



CenturyLink's NG9-1-1 ESInet network utilizes many mechanisms for event tracking and alerting. Systems leverage syslog and SNMP traps for event / fault notifications. Application hosts also utilize embedded agents which communicate directly with our monitoring platforms. Systems are monitored by use of SNMP polling and application health-checks. All systems are provisioned for fault, performance, and configuration monitoring / management.

CenturyLink Real Time Monitoring via SolarWinds modular and scalable network management tools will obtain end-to-end visibility into the health and performance of the ESInet. Also Detects, diagnose, & resolves network performance issues.

Additional interworking management tools that will be used Network Atlas, NetBrain, BRIX probes, SD WAN , Utility Tools (Ping, Tracroute, NSlookup, Power Tools, Commercial Scanners and Open Source type Tools.

CenturyLink will work with authorized State and PSAP personnel to allow secure access to this monitoring for network health/status of the Nebraska NG9-1-1 network.

Any additional documentation can be inserted here:

NOC/ SOC 14	**NOC/SOC - Network Event Logging** **System and Network Event Logging and Reporting** The network management system shall capture real-time and historical tracking of network and system events, as well as event resolution of the IP network and attached systems. This is for logging errors and statistical information related to the health of the network and attached systems. Events shall include, but are not limited to, hardware (power, processor, interface cards, ports), software (operating system errors, database errors, application errors and failures), network (Quality of Service (QoS), Mean Opinion Score (MOS), jitter, latency, and packet loss)). The events recorded in this section are not related to the event logging of 911 requests for service as part of NGCS Option B requirement NGCS 13 Event Logging. Describe how the solution meets or exceeds the above requirement.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink Real Time Monitoring via SolarWinds modular, scalable network management tools will obtain end-to-end visibility into the health and performance of the ESInet. This provides critical path hop-by-hop analysis and visualization all along the delivery track. We can quickly see maps of network connections, dependency relationships, and topology information, and know who and what's connected to the network, and when and where they're connected. This application ensures devices are configured and operating in compliance with regulatory standards and that network managers are prepared to recover quickly from hardware faults and human errors using automatic backups. CenturyLink's NG9-1-1 Solution utilizes software developed in collaboration with Oracle; security, Quality of Service (QoS), and interoperability are "baked in" to our critical services. QoS monitoring and reporting measures each media flow through the system, calculating quality scores (such as Mean Opinion Score) and aggregating the information into data for transmission to external reporting systems At each ESInet Site location, CenturyLink will provide redundant routers for each physical circuit and a Network Probe for network monitoring. Network performance event monitoring provides constant monitoring of Customer's contracted devices and associated network elements using a suite of monitoring tools which collect various types of performance related data. This data is delivered to the CenturyLink NOC monitoring center via intelligent probes, data collectors, or VPN polling as required. The data is then analyzed by NOC personnel to identify fault occurrences and to determine the overall health of the managed portions of the Customer's network. Our other monitoring tools will also allow end-users to gain visibility into signaling and media interactions, and leverage key indicators to identify, troubleshoot, and resolve issues that can reduce the efficiency of enhanced IP network service. Our monitoring tools captures all messages transiting the network using network probes linked to an unrivaled correlation engine. Results are viewable through a web-architected GUI. This Monitor runs on commercial-off-the-shelf hardware and software components that are integrated into our session border controller (SBC) service delivery platforms. CenturyLink's network performance monitoring includes but is not limited to bandwidth utilization, delay(latency), jitter, MOS, and packet loss to name the most used items for monitoring. Custom elements can be configured if required by the State. With our NG9-1-1 solution, problems that might be a request for service in a CPE situation are often recognized by our network event logging management tools before a customer realizes there is an issue and submits a ticket.				

1. To track and report the performance of the NGCS core, we employ the Oracle Enterprise Operations Monitor (OCOM) and the FortiSIEM security and event management platform and other Network and CPE monitoring and alarm systems. A software and hardware health check against each instance is automatically performed once per second and will immediately pull an unhealthy element from our active-active pool and raise a system alert.

   Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP. Then, these and other data sources such as E-Bonding ticket information are consolidated into a single viewing portal for access by the state.

   Oracle Communications Operations (OCOM) is a proactive call monitoring solution. It captures and analyzes all required signaling messages and media from the network, providing full correlation and quality metrics in real time. It also enables easy to-use, drill-down troubleshooting for root-cause analysis of any reported problem related to a user, user group, trunk, network device, or Internet Protocol (IP) address. Key features include:

   - End-to-end call correlation and analytics in real time
   - Segmentation of the network path for fast and accurate problem localization
   - On-demand troubleshooting down to the individual subscriber, customer, or employee
   - Media quality analysis, including R- Factor and MOS scores
   - Unparalleled insight into and analysis of signaling messages
   - Embedded software to eliminate need for additional monitoring equipment in the network
   - Intuitive and simple GUI

   FortSIEM enables unified and cross-correlated analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the threat data available in the organization. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for handling real-time searches, rules, dashboards and ad-hoc queries. Key features include:

   - Unified, Real-Time, Network Analytics
   - Single IT Pane of Glass
   - Multi-tenancy
   - MSP/MSSP Ready
   - Cross Correlation of SOC & NOC Analytics
   - Self-Learning Asset Inventory
   - Cloud Scale Architecture

Security and Compliance out-of-the-box Data collected from these platforms and other sources is then reviewed in our multi-level audit program.

This program has three audit levels.

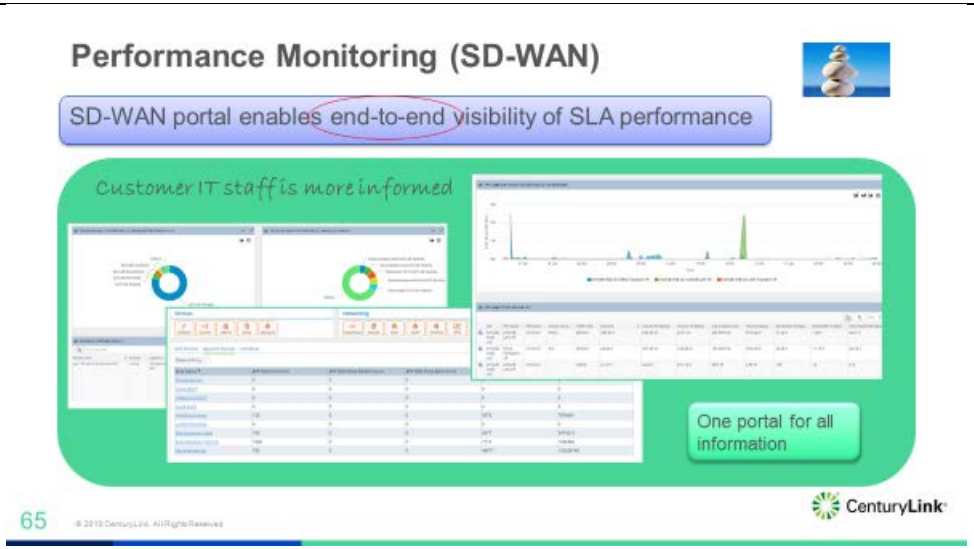
- The first (Management) includes control self-assessments (CSAs), attack/break penetration testing, functional/technical testing, social/behavioral testing and regular management reviews. Level activities typically are reviewed annually.
- The second (Risk Management) includes assessments of threats, vulnerabilities and risk followed by a formal risk evaluation. This level also produces a business impact analysis (BIA) and draws conclusions about emerging risk. Level two activities are accomplished at least quarterly and more often if the threat so dictates.
- The third level (Internal Audit) involves internal controls testing, cyber security compliance, a Formal risk acceptance protocol and appropriate investigation/forensics. These are usually unannounced and scheduled by the Network Security Officer. Some sort of level three audit occurs monthly.

Our change management protocol requires an environmental impact assessment and risk management review prior to the implementation of any change in the operational environment.

2. To track report and log statistics and the performance of the **NG9-1-1 MPLS and TDM ESInet network**, we employ SDWAN, Network Probes and Solar Winds

   Solarwinds event logs events including:

   - Pcap files to determine issues with packet or frame level networking failures
   - Bandwidth utilization,
   - Tracks IP and switch ports of the network.
   - Monitors and provides event logs on each edge device in the network including SBC's edge routers etc.
   - Our SDWAN appliance in an HA configuration event logs, overlaid on the MPLS delivery logs including:
   - Secure flows, IDS and IPS to ensure segmentation of traffic for 9-1-1 call delivery to the PSAP end points delivery to the PSAP interface and endpoints. Monitors and logs traffic for signature and anomaly-based attacks.
   - QOS including prioritization, policing and marking. QOS Policies can identify traffic based on Layer 3 attributes such as source/destination IP/Port as well as DSCP markings along with Layer 7 capabilities such as Application and URL category to provide fine grained QOS Control.
   - BGP and OSPF Routing – Provides flexibility in routing integration



NOC/SOC 14 SD WAN Event Sample

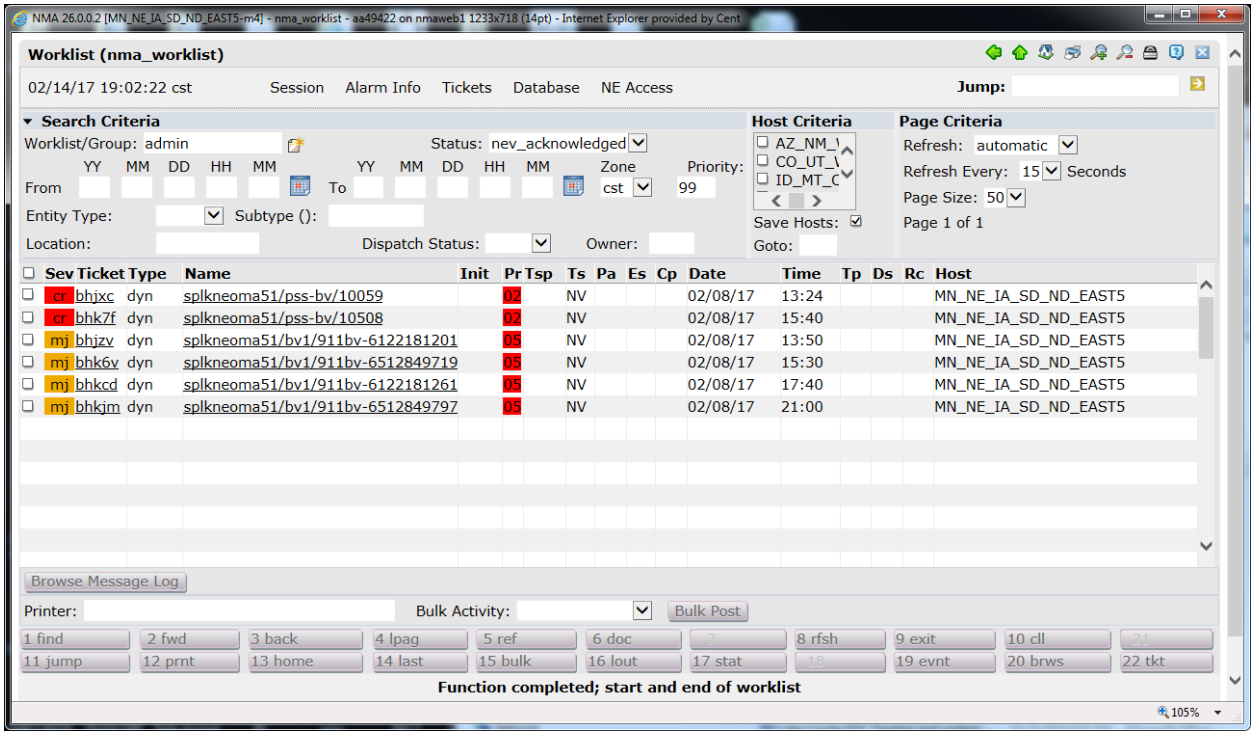
3. CenturyLink will deploy a Brix network probe solution for End-to-End MOS scoring from Ingress to PSAP edge to track, report and log events including:

   Capture of all messages transiting the network using network probes linked to a correlation engine

   CenturyLink's solution will use network probes at each PSAP per circuit for MOS scoring and event logging including:

   - This will test end to end call quality metrics (MOS Scoring)
   - This system will also do automatic call testing to insure network availability and functionality.
   - Capture of all messages transiting the network using network probes linked to a correlation engine
   - Brix verifier solution for End-to-End MOS scoring from Ingress to PSAP edge
   - Our Brix solution uses Perceptual Objective Listening Quality Analysis (POLQA). Our Brix places a short call every minute to every PSAP probe and a long call every 4 to 7 minutes specifically to test MOS.
   - Probes will generate alarms/tickets on the impacted service If specific criteria are met
   - CDR Streaming for call by call reporting
   - Provides events on:
     - No Heartbeat (HB)

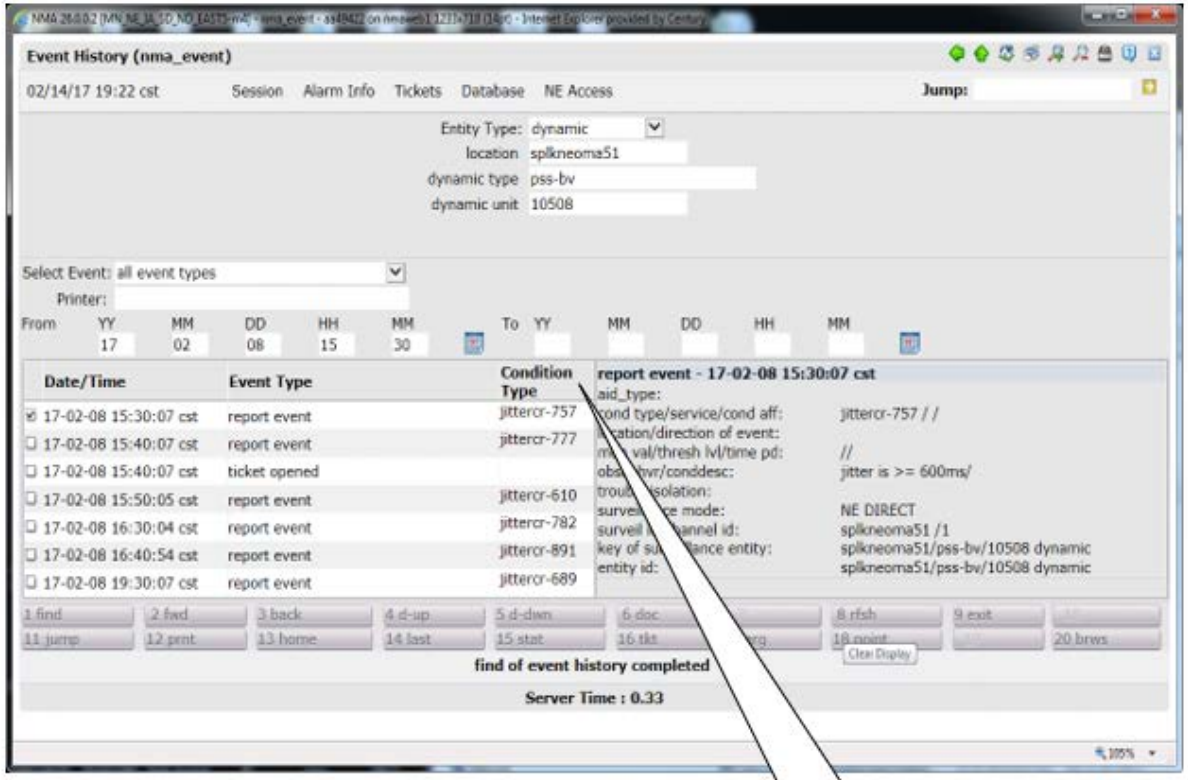
- Two of these ticket types from each probe could indicate a network outage.
- Packet Loss (PL)
- Historical condition types in the ticket events section of NMA may indicate a network problem.
- Jitter (JR)
- Historical condition types in the ticket events section of NMA may indicate a network problem
- Mean Operating Score (MOS).



NOC/SOC 14 Network probes logging event sample

The alarms are sectioned into 4 areas, (Heartbeat HB, Packet **Loss PL, Jitter JR, and MOS).**

This data is delivered to the CenturyLink Public Safety 9-1-1 NOC monitoring center via intelligent probes, data collectors, or VPN polling as required. The data is then analyzed by NOC personnel to identify fault occurrences and to determine the overall health of the managed portions of the Customer's network.



NOC/SOC 14 Network probes event log report sample

	4. Our ESInet network provides custom Quality of Service (QoS) for our managed private IP network which can prioritize any type of IP traffic; voice, data, and multi-media. Our solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic that provides additional logging events and the health of the network. QOS events are logged across the entire IP/MPLS network. QoS monitoring and reporting measures each media flow through the system, calculating quality scores (such as Mean Opinion Score) and aggregating the information into data for transmission to external reporting systems. Onboard QoS monitoring and measurement is also utilized for real-time functions such as QoS-based routing and load balancing. This does not compromise end-user QoS QoS in the CenturyLink ESInet is performed primarily through packet marking with DSCP on ingress to the switch ports attaching voice equipment to routers at remote and core sites. In some cases, the voice equipment manages its own marking, and the router/switch honors these QoS settings. In others, the router/switch will override the DSCP marking with a more appropriate setting. Typically, the audio stream (RTP) is marked with "Expedited Forwarding," the highest class of service available. This is appropriate for real-time media such as voice and is mapped to a priority queue. Signaling packets are placed in another queue, which will typically have a small but firmly reserved portion of bandwidth. Reported QoS data includes the following per-flow metrics events includes: – RTP Lost Packets – RTP Jitter – RTP Maximum Jitter – RTCP Lost Packets – RTCP Jitter – RTCP Latency

Any additional documentation can be inserted here:

NOC/ SOC 15	**NOC/SOC - Network Event Logging** **Management System Interface to Incident Management System** This system should be part of, or interfaced with, the bidder's incident management system, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract and provide copies of the data to the Commission on request, and at the end of the contract. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

CenturyLink maintains a problem management system for tracking and reporting trouble. We can also provide monthly trouble reports showing tickets opened, resolved, and unresolved.

In case of a service interruption and/or outage, we have instituted Incident Management processes and procedures for dealing with various severity levels during an event. Our incident response tools include use of the Incident Command System (ICS modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post-event review and root cause analysis. We manage incidents and provide customers with notifications and status of ongoing service affecting issues that may impact the CenturyLink NG9-1-1 ESInet Solution.

CenturyLink will prepare and submit a preliminary root cause analysis (RCA) for a Severity Level 1 or Severity Level 2 event. The preliminary report will provide an overview of all information known at that time. The Incident Command team will prepare and submit a final report of a Priority Level 1 or Level 2 event describing the impact of the event, the cause, resolution and any preventative steps that can be taken to eliminate future events.

Example of our Root Cause analysis. Focus on relevant objective assessment activities including:

a. Review of logs, forms, reports, and other incident documentation;
b. Identify recorded precursors and indicators;
c. Determine if the incident caused damage before it was detected;
d. Determine if the actual cause of the incident was identified;
e. Determine if the incident is a recurrence of a previous incident;
f. Calculate the estimated monetary damage from the incident;
g. Measure the difference between initial impact assessment and the final impact assessment;
h. Identify measures, if any, that could have prevented the incident.

Satisfy local, state and federal reporting requirements. This includes SLA reporting requirements

The CenturyLink NOC shall notify within 30 minutes of discovering an event or outage that may impact 9-1-1 services. CenturyLink's NGCS Solutions service assurance strategy places the highest emphasis on service restoration.

Communication will be supplied to all parties provided to CenturyLink by the Customer and its entities.

The following are key highlights for the notification system:

- The five state levels are as indicated: Critical, Major, Minor, Warning, and Normal
- We provide notification to the 24x7x365 NOC

- We provide notification by various means
- Notification levels are defined by the supporting entity
- We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications. For example, we can say "no more of a certain alarm for the next 30 minutes" or we can say "send me duplicate alarms every 5 minutes"

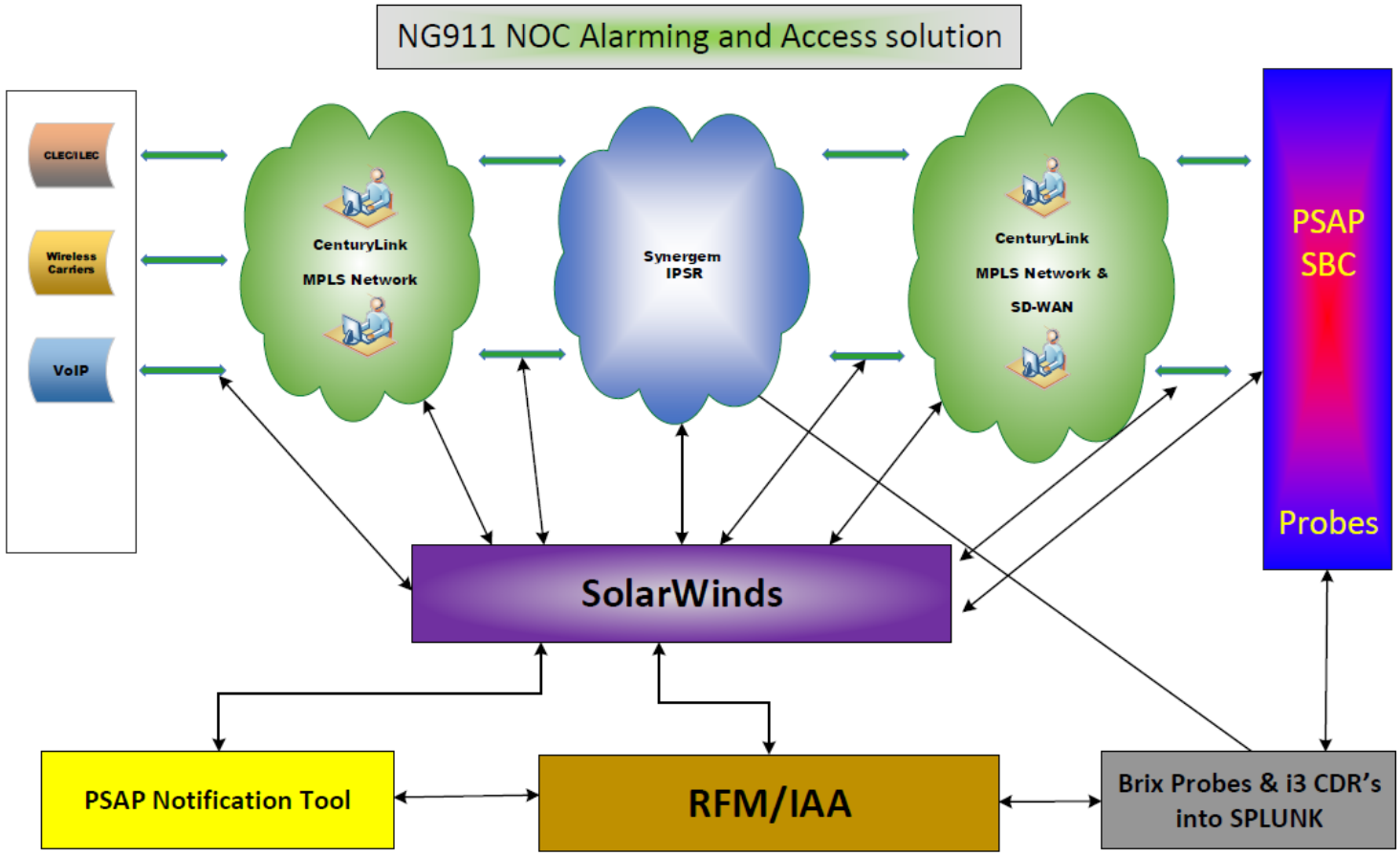
NOC/SOC 15 CenturyLink Severity Levels

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical	Any outage or condition that results in: • Loss of 911 call processing • End office or Remote Switch isolation from 911 network for 10 or more minutes • Loss of end office to 911 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major	Client is able to access the system, or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor	Client is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent	Client has an informational request or questions of a general nature concerning the overall product suite functionality or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours
Informational	ORT Testing, SMOP Events, non-customer impacting problems or informational types of trouble	N/A	N/A	N/A

Any additional documentation can be inserted here:

NOC/ SOC 16	**NOC/SOC - Network Event Logging** **Interfacing Between Solutions** Provide a detailed explanation and associated drawings explaining bidder's processes, tools, and procedures for interfacing with the bidder's monitoring solutions.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink has implemented processes and procedures for interfacing regarding event logging. To ensure high performance and reliable networking services for State of Nebraska, CenturyLink's IP networking framework is based upon the Information Technology Information Library (ITIL) principles. We use ITIL for service delivery including design, operation, and transitioning of services. We also conduct detailed IT needs assessments in an effort to identify specialized equipment and software that are required by customers in the public safety sector. CenturyLink's Network Operations Center (NOC) offer end-to-end service management using highly trained networking professionals who are available 24x7 for the monitoring and management of our network infrastructure. Our NOC services include service coordination, reporting, and logistical support. CenturyLink's NOCs analyze performance statistics for our network. We analyze network uptime, bandwidth utilization, and other performance metrics. CenturyLink's NOCs provide 24x7, services that deliver ongoing, real-time protection with an emphasis on the following elements: • Detect quickly • Respond appropriately • Restore critical services • Provide complete RCA (Root Cause Analysis) NOC operation can provide 24x7 geo-redundant network monitoring and reporting tools optimized by a team of highly trained experienced engineers and full-suite third-party vendor support. Our personnel have an average of eight years' plus network and system experience and service on design, implementation, and operational teams. Our network core- and carrier- grade NOC is located in our facilities. Both facilities are equipped with multiple internet service providers (ISPs), UPS and a dedicated diesel generator, closed-caption television, dual fire suppression systems, and secure access that ensures HA for all monitoring and support services. In addition, the NOC provides continuous system support and monitoring 24x7 to each ALI node and to the database management system. The NOC also monitors all PSAP connections into the ALI nodes at the application level. Staffing in the NOC is second to none in the industry with Tier 1 through Tier 3 support staff on duty 24x7x365. The following are key highlights for the network management system (NMS): • The five state levels from NMS are as indicated: Critical, Major, Minor, Warning, and Normal • We provide notification to the 24x7x365 NOC • We provide notification by email and SMS • Notification levels are defined by the supporting entity				

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



We are capable of alarm suppression by time, quantity and a combination for reducing alarm notifications. For example, we can say "no more of a certain alarm for the next 30 minutes" or we can say "send me duplicate alarms every 5 minutes"

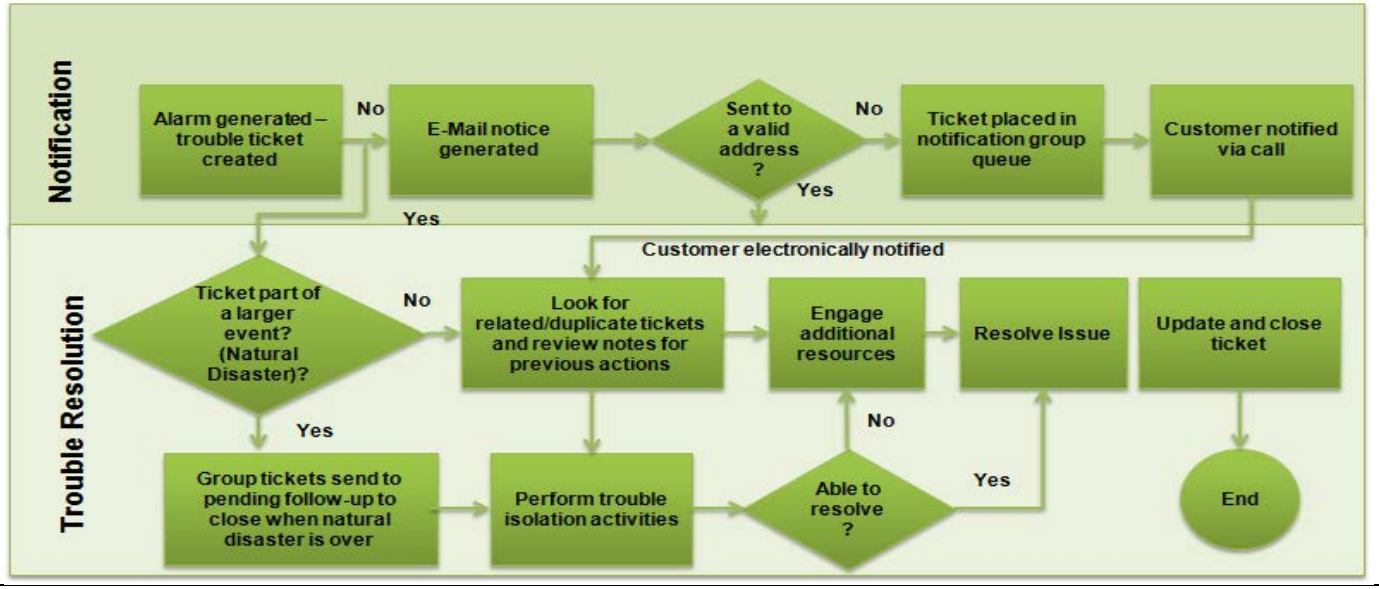
NOC/SOC 16 Solarwinds Event Log Manager Sample Report

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 17	**NOC/SOC - Access to Technical Staff** 1. Detail the procedures by which bidder communicates with technical personnel from participating subcontractors, the Commission, and the participating PSAPs. 2. Specify the level of assistance required from such technical personnel to resolve service-related issues.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1) CenturyLink will communicate with our technical personnel from our participating suppliers the Commission and PSAPs through phone calls, emails, conference bridge services such as Microsoft Teams, Zoom and ticketing system applications. A dedicated toll-free number has been established for the Commission, PSAPs, and our participating suppliers to utilize for reporting and obtaining/providing status on ESInet issues. CenturyLink has also established a dedicated toll-free number for use by the CenturyLink for ESInet issues. CenturyLink provides a web-based ticketing system for use by our customers as well and a ticketing interface tool between CenturyLink and our participating suppliers. From the outset, we try and involve authorized third parties in our project management program. They are invited to attend planning meetings; project plans are shared with them and their participation in joint deployment and test teams is solicited. They are copied, where appropriate, when report are issues. We need third-party technical representatives to understand the interface issues facing the integration of their tools with the remainder of the solution and to make their labs available for interoperability testing 2) Our CenturyLink Program Manager becomes the Single Point of Contact for the Commission and assists with all reporting questions as well as providing monthly/quarterly customer reviews and functions as the State's first point of escalation.				

Any additional documentation can be inserted here:

NOC/ SOC 18	**NOC/SOC - Notification** Specify how the bidder's NOC informs the Commission and the affected PSAPs or their designees of problems with the network, scheduled service and maintenance outages, and upgrades. Include all methods of notification used. Notifications for scheduled maintenance or outages shall be made no less than ten (10) business days in advance, except for emergency situations in which case, notification will be given immediately. Tickets related to the services delivered to subcontractors shall be forwarded automatically. Notification shall be provided via multiple communications means to the Commission and applicable PSAPs. Entities requiring notification may change, depending on the alarm or incident. Provide a detailed explanation explaining how the solution meets or exceeds the above requirements, including the methods of communications used.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink will communicate with our technical personnel from our participating suppliers and State of Nebraska and PSAPs through phone calls and ticketing system applications. A dedicated toll-free number has been established for the PSAPs, and our participating suppliers to utilize for reporting and obtaining/providing status on ESInet issues. CenturyLink has also established a dedicated toll-free number for use by the CenturyLink for ESInet issues. CenturyLink provides a web-based ticketing system for use by our customers as well and a ticketing interface tool between CenturyLink and our participating suppliers. **CenturyLink trouble notification process. The process is followed to keep customers well informed:** 				

CenturyLink maintains a problem management system for tracking and reporting trouble. We can also provide monthly trouble reports showing tickets opened, resolved, and unresolved.

In case of a service interruption and/or outage, we have instituted Incident Management processes and procedures for dealing with various severity levels during an event. Our incident response tools include use of the Incident Command System (ICS modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post-event review and root cause analysis. We manage incidents and provide customers with notifications and status of ongoing service affecting issues that may impact the CenturyLink NG9-1-1 ESInet Solution.

CenturyLink will prepare and submit a preliminary root cause analysis (RCA) for a Severity Level 1 or Severity Level 2 event. The preliminary report will provide an overview of all information known at that time. The Incident Command team will prepare and submit a final report of a Priority Level 1 or Level 2 event describing the impact of the event, the cause, resolution and any preventative steps that can be taken to eliminate future events.

The following are key highlights for the notification system:

- The five state levels are as indicated: Critical, Major, Minor, Warning, and Normal
- We provide notification to the 24x7x365 NOC
- We provide notification by various means
- Notification levels are defined by the supporting entity

We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications. For example, we can say "no more of a certain alarm for the next 30 minutes" or we can say "send me duplicate alarms every 5 minutes

Our CenturyLink Service Manager provides State of Nebraska and PSAP with a single point of contact for notification, escalating and tracking any major service outage. The Service Manager responsibilities includes:

- Hourly updates via telephone, emails and or on-site meetings of the event. Including details of the area effected.
- Provides current repair contacts and escalation guide to the PSAP and or State personnel
- Performs escalation function for customer during critical outages
- Ensures action plan is identified/executed in the event of recurring or chronic issues
- Maintains customer contact information for Network Maintenance activity
- Gathers and delivers Reason for Outage (RFO) explanation, post-event
  Participates in Service Reviews, presenting repair metrics as requested

For routine problems, stakeholders are notified through the ticketing process. If an outage occurs, SLA reporting is activated.

Here are five Change Management categories.

Change Category	Description

STANDARD	This change indicates a low risk and repeatable change that occurs frequently. Once it is deemed appropriate (3 successful) Change plans / MOPs are in place, a template will be built so the change can be entered as a Standard Change for future usage negating the need for a normal change. This change type does not require NG9-1-1Team approval.
NORMAL	Normal changes are often categorized according to risk and impact to the organization. A normal change will proceed through all steps of the change management process, including the NG9-1-1 Team for approval.
LATENT	This change should be utilized for unplanned work, resulting from a critical incident ticket &/or Major Incident.
EXPEDITED	An expedited change will proceed through all steps of the change management process and will be reviewed by the executive NG9-1-1. There is a valid business reason to bypass the 48-hour advance submittal time frame.
EMERGENCY	Utilized for a change that resolves a problem deemed critical to business continuity and for which a workaround is not enough. Examples are a router that could put voice delivery at risk and has a potential for an immediate threat to the production environment and /or to be a major impact to Business or Customer. Emergency changes are approved at an Emergency Executive NG911 Team.

CenturyLink will provide a notice in writing within ten (10) business days to the state in advanced on all Planned Maintenance changes except for any commission initiated, expedited and or emergency which take place immediately.

For Normal, Emergency, and Expedited changes, a change request is submitted to the NG9-1-1 Team. The request must include a step-by-step explanation of the purposed changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment.

The result of each change is tracked and available for future reference in our Change Management Module whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the NG9-1-1 Core Team. If the change was successful with deviation, this is also tracked with the deviations documented.

CenturyLink also utilizes Incident and Problem Management modules, which allows for tracking of break/fix issues as well as any resulting Problem Management requests.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 19	**NOC/SOC - Executive Dashboard** Contractor shall provide a web-based executive dashboard or similar tool, providing near real-time visibility of network status displayed geographically with service impact levels color-coded. Open ticket status shall be available to users through this dashboard. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response:				

Dashboard View

CenturyLink's solution provides a dashboard via a full-feature web portal-based functionality for ticket status, e-bonding data monitoring, reporting, and configuration management. The dashboard will provide a single pane of glass for monitoring and management of our NG9-1-1 solution.

Dashboard elements will include and incorporate the following:

- Our Dashboard will have visibility into various platforms included in the CenturyLink solution such as SDWAN and NG9-1-1 Networks

- The dashboard is customizable and provides a multi-tenant view
- Auto ticket and alarming thresholds customized based on negotiated SLAs and triggers
- Bandwidth, Inventory, ticketing, configuration data, are provided and accounted for in the CenturyLink response
- Order, Change, and Service Management
- Analytics, statistical data and reports will be developed based on requirements and agreed upon thresholds
- Application Programming Interface (API) integration to CenturyLink's ticketing platform
- CenturyLink's dashboard is capable of displaying data received in its ticket platform via E-Bonding from State and other providers
- Capture of all messages transiting the network using network probes linked to a correlation engine.
- 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.
- Reporting efforts are 100% passive, nonintrusive and vendor agnostic.
- For the manager, this dashboard provides an unprecedented level of network visibility in a variety of networks and devices. This depth of real-time visibility includes signaling messages – as they traverse through individual devices – media quality, message parameters, etc.
- The dashboard comes with a tool for producing a range of charts and graphs to display, track, and record traffic data. It also provides a data export facility for offline reporting tools, enabling raw data to be exported. E-Bonding ticket information is consolidated into a single viewing portal for access by the State and other authorized agencies
- Provides status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data.
- Network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP.
- Results and the dashboard are viewable through a portal that will be available to the State.

Benefits of Using the Public Safety 9-1-1 Customer Portal

- **Convenience**—at CenturyLink, we handle all 9-1-1 tickets and requests with the same level of care, whether our customers open them through the portal or call us directly. The portal offers convenience and saves time by enabling customers to manage tickets and requests online through this free online tool.
- **Support and Communications**—customers have access to comprehensive portal user support and education tools. Users can take advantage of our Portal Support Center or learn more about the portal capabilities with tutorials, webinars and user guides.
- **Security**—the portal is designed to provide secure and private access with three tiers of authentication to help ensure the protection and integrity of network data.
- **Reliability**—a dependable management tool, the portal provides transparent interactions with back-office source systems for timely delivery of information throughout a service lifecycle, as well as fast resolution and response times to issues.
- **Personalization**—customize views to see the information that is most important to you, save pages as favorites, assign personal IDs to tickets, manage your subscriptions, and more.

Any additional documentation can be inserted here:

NOC/ SOC 20	**NOC/SOC - Escalation Procedures** 1. Outline a detailed regional-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. 2. Describe how discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed. These procedures shall be maintained and accessible via an online portal. This escalation notification process shall be integrated with the notification processes described above, based on the problem reported.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink's Next Gen 9-1-1 Public Safety NOC will be the State and PSAPs' single point of contact for all service issues. The NROC is staffed 24x7x365, is accessible via a toll-free number. The NOC is staffed by highly trained 9-1-1 professionals. There unique skill set, coupled with advanced training and CenturyLink's refined logging and reporting functionality, means that CenturyLink's call agents are highly equipped and prepared to handle and supervise emergency service calls. CenturyLink uses a proactive monitoring and notification process (Error! Reference source not found.). The process uses platform-specific alarm thresholds to identify potential service impairments. CenturyLink network alarms are customer specific and generate trouble tickets that automatically notify customers via e-mail, text messaging, pager, and telephone. Proactive Customer Notification (PCN) also gives customers with flexibility to specify certain notification parameters on a service-by-service basis. To ensure rapid resolution of network issues, CenturyLink adheres to strict escalation procedures and measurable timeframes. If active progress and meaningful status updates are not being made, CenturyLink technicians are empowered to escalate issues internally and externally as required. CenturyLink and PSAPs may also request escalations. CenturyLink customer service is chartered to provide world-class customer support that attempts to resolve issues on a first contact basis. With geographically diverse NOC, CenturyLink provides ensures high availability of technical support personnel who provide rapid problem resolution and efficient work management in the event of natural or manmade disaster. CenturyLink also maintains records (log) of all trouble tickets. Our records allow our managers to review trouble tickets on a customer-by-customer, day-by-day, and criticality basis. When an incident impacts a CenturyLink customer our response is not complete until a CenturyLink representative contacts the customer with an explanation of the problem and a discussion of the actions that CenturyLink took to resolve issues and a discussion of how CenturyLink plans to keep the problem from occurring again. **Customer Notification** CenturyLink notifies affected customers and Nebraska of faults, restoration updates, and impact level. We include in our outage report information about impacted network switches and facilities. Our outage reports also include information about issues and concerns related to catastrophic events (i.e., fires at a transport site) and various other service issues. When a CenturyLink representative contacts a PSAP or CenturyLink, he/she will provide a tracking number, description of the fault, date and time the fault was detected, customers that are affected by the fault, and any peripheral information regarding faults and/or locations.				

	The CenturyLink representative will provide an estimated time to repair when possible and the circuit Telecommunication Service Priority (TSP) status. In order to allow CenturyLink personnel sufficient time to understand an issue, personnel are required to notify affected customers within 15 minutes. As more information about an issue is understood, CenturyLink will communicate that information to the customer. CenturyLink will utilize our WFA/OTTO ticketing system to track all NG9-1-1 proactive and reactive trouble reports. Escalation for all trouble reports occurs every 30 minutes or as appropriate if an ETA/ETR is provided. Tier 2 support is engaged within 30 minutes if no significant progress in the repair of the trouble is occurring. 1st Level Escalation = Supervisor or Duty Supervisor 2nd Level Escalations = Manager of the 9-1-1 PSS NOC 3rd Level Escalations = Director of the 9-1-1 PSS NOC 4th Level Escalations = VP of Service Assurance NOC RFO can be requested from the 9-1-1 Service Managers and they will submit an RFO request via internal systems. CenturyLink will provide a legally approved RFO within 10 business days that contains the following information.

Any additional documentation can be inserted here:

NOC/ SOC 21	**NOC/SOC -Statement on Standards for Attestation Engagement Number 16** Bidder shall demonstrate compliance with the Statement on Standards for Attestation Engagements Number 16 (SSAE 16). The applicable report from an SSAE 16 engagement is the Service Organization Controls 1 (SOC 1) report. 1. If bidder is proposing services, provide a detailed explanation of how bidder has complied with SSAE 16 for similar solutions, and how this would be implemented with the Commission's NG911 implementation. 2. Provide with the detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: If bidder is proposing services, provide a detailed explanation of how bidder has complied with SSAE 16 for similar solutions, and how this would be implemented with the Commission's NG911 implementation. All CenturyLink NGCS data centers are SSAE 16 compliant and we only use data centers for NG9-1-1 that meet these requirements. Provide with the detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement.				

Any additional documentation can be inserted here:

	NOC / SOC - Configuration Backup and Restoration 1. The bidder shall deploy and provide detailed descriptions of bidder and any subcontractors' capabilities to automatically or routinely back up configuration data and define the conditions under which the configuration of network elements, such as routers or switches, will be restored, and the process that will be used. A reporting process shall confirm regularly scheduled (e.g., monthly, quarterly) backup and restoration, and provide sufficient details on backup and restoration activity. 2. Describe the bidder's abilities to perform on-demand backups, such as at the end of a successful configuration change. A reporting process shall confirm on-demand backup and restoration and provide sufficient details on backup and restoration activity. 3. Describe bidder's COOP as it applies to the NGCS and delivery of 911 traffic via IP network to the respective host locations. 4. Provide a detailed explanation and any associated drawings explaining how the proposed processes and procedures provide the ability to manage these configuration backup and restoration processes in a manner that has no negative impact on the total Commission ESInet and NGCS solution.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NOC/ SOC 22	Bidder Response: **Configurations are backed up on every commit.** CenturyLink network configuration tools provides version control and backup functionality to all network elements, with backups of all network configuration performed daily and with changes. This allows the restoration of previously "known good" configurations or timely restoration of stored configurations in the event of equipment failure or disaster recovery. Using the above process, our network configuration management tools perform the following functions: • Detect and report on configuration policy violations or configuration backup failures to ensure compliance with corporate standards. • Utilize configuration templates and command templates, custom scripts, and configuration changes to provide consistent implementation of network configurations across similar site types. • Simultaneously modify configurations, change community strings, update ACLs, and block MAC addresses across many devices such as routers, firewalls and switches. • Compare start-up and running configuration files to troubleshoot device configurations issues. • Automatically check all network elements for changes and perform backup for all changed network device configurations on a daily or ad hoc basis, as needed. CenturyLink can provide reports confirming regularly scheduled daily backup and restoration files archived and provide additional details on backup and restoration activity as required. Our CenturyLink Program Manager can provide copies of all data upon requests to the commission. • CenturyLink can provide reports confirming on-demand backup and restoration files archived and provide additional details on backup and restoration activity as required. CenturyLink can provide copies of all data upon request.				

	• CenturyLink provides life-critical services supporting 9-1-1 and public safety and is strongly committed to continuous, sustained readiness of its applications, systems, networks, and processes 24x7x365. CenturyLink's business and service continuity plans, geographically diverse and redundant systems, and incident management processes and plans provide confidence that continuous operations will be sustained through planned or unplanned events. We maintain a robust and reliable data backup system that updates all NGCS and ESInet data nightly and store that data independently is all our datacenters and CenturyLink secure locations. We can affect a restoration of NG9-1-1 data from any or all of these sites. To summarize, CenturyLink backup and restoration process includes the following tasks: • Perform a daily backup of the data and systems. • Maintain a data backup as required in SLAs; • Secure backups in geo-diverse, separate locations. • Provide regular backup reports of all successful/failed system backups/archives per the SLAs • Provide data recovery services that are accomplished with no impact on operations; and, • Provide a copy of all data to designated recipients. • We also automatically back up configuration data especially before any changes in configuration are attempted. • Current complete backups are ALWAYS present prior upgrades to provide recovery capability in the event of system problems due to the changes. • Bluetooth is never used for backup of any medium or device which contains sensitive (internal data only) or greater data. • Automated system software and network of servers provide backup and recovery for subscribing customers • With SD-WAN we don't make configuration changes directly on the SDWAN appliance and therefore we don't have to worry about backing them up to allow us to recover from a device failure. The configurations are created & changed on the versa director and then pushed down to the appliance. Data in the versa director is replicated to a 2nd geographically diverse instance of the platform. • We back-up each edge and endpoint gateway device software, firmware, firewall, router and switches IOS as recommended by the manufacture via our VPN MPLS ESInet network. • Automatically check all network elements for changes and perform backup for all changed network device configurations on a daily basis • Configuration on the NG911 Host site backup equipment is based on documentation and configuration data held in geo-diverse repositories at every datacenter as well as the of engineering lab in LA and Chicago. 4. Network configuration management tools automatically check all network elements for changes and perform backup for all changed network device configurations on a daily basis, and may be performed on-demand, as needed. Network configuration management tools have been implemented with geo-diversity in place

Any additional documentation can be inserted here:

	NOC/SOC - Third-Party Management The Commission is seeking the optimum value provided by best-of-class products and services integrated as part of the total IP network solution. This may present a situation where no single manufacturer or supplier can provide a public safety-grade, unified NOC/SOC accountable for all components, products, and services that comprise the Commission's total IP network solution. Consequently, the Commission may find it beneficial to have a third party provide that overarching NOC/SOC service. A third-party NOC/SOC provider may be responsible for functioning as an umbrella for monitoring all of the Contractor's products and services, including collaboration with the Contractor's NOC/SOC. To facilitate that capability, the third-party NOC/SOC shall have a view into all elements that are under SLAs. Bidder's NOC/SOC NMIS and/or incident-tracking tools shall have the ability to perform eBonding, which enables bidirectional data synchronization. 2. Provide a detailed narrative discussing bidders experience in providing access to third-party NOC/SOC, overarching support as well as for each of the requirements in Third-Party NOC/SOC Support below.				
NOC/ SOC 23	Bidder Response: CenturyLink provides a single inclusive direct support when it comes to collaboration with 3rd party contractors. This support goes beyond the normal NOC'SCO support but also includes the development of interfaces through API's, E-bonding for monitoring and ticketing, synchronizing datasets, alert and monitoring tool integration, and tier 1-3 support with 3rd party NOC/SOC centers in order to provide an end to end monitoring solution to the State of Nebraska Examples of this collaboration with these 3rd party companies examples includes Synergem, Comtech, NG911 solutions for HG 9-1-1 in California, Atos Public Safety LLC, NGA911, Motorola Solutions, Intrado, and others. CenturyLink will work with State of Nebraska Commission and any selected third-party NOC/SOC for a functional requirements document for evaluation of CenturyLink and Nebraska commission compliance guidelines. No cost has been included in this proposal for any required integration work for the integration				

1. In support of the Commission's consideration of such an option, bidder shall indicate the compliance level of experience in providing access to third-party NOC/SOC overarching support, as related to the requirements identified in the table below.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Change management processes	X			
Coordinating and managing trouble tickets to resolution from bidder and multiple suppliers.	X			
Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly).	X			

	Notification processes for bidder and suppliers, and any other entities or people designated by the Commission.	X				
	System alarm access in the form of SNMP or syslog data.	X				
	Experience and processes for interworking of multiple public safety data system suppliers.	X				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	General Operations - Service Level Agreements **System Capacities and Performance** 1. Provide capacity levels of each element of the IP Network This may be in terms of busy-hour calls, network bandwidth, or any other applicable measure. The proposed solution shall be capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. 2. Specify lead times required to increase capacities on each element of the IP network.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SLA 1	Bidder Response: The CenturyLink ESInet is capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. CenturyLink can easily scale IP capacities through simple provisioning processes, eliminating the need for additional network buildouts, and enabling customers to increase capacities within a few weeks vs. months. CenturyLink will work with the State of Nebraska for capacity planning and to mutually agree on ordering timeframes. This methodology provides the State of Nebraska with a cost-effective solution in the near term and allows for growth based on coordinated agreements. The IP network transport used by CenturyLink's NGCS will initially be sized to comply with specified network bandwidth requirements. The CenturyLink MPLS IP network is monitored for capacity trends that indicate the need for proactive growth of the ESInet. As the needs of the State of Nebraska grow, local PSAP connectivity bandwidth will be scaled up or down by a change order process or through procedures as defined in the SLA and/or contract. Our solution provides a fully compliant, scalable environment in the existing LNG and ESInet core infrastructure. Currently the LNGs operate with redundancy at each location and the bandwidth is expandable in a short timeframe with no need for a forklift upgrade. The CenturyLink ESInet network is capable of bandwidth growth at each network element, existing end sites, and future end sites without sacrificing reliability of the solution. The solution is capable of interconnecting to other national- and/or state-level ESInets via open standards-based interfaces. The CenturyLink ESInet model is deployed from a network perspective with a 2N redundancy model – each remote site is provisioned with 50% more bandwidth as is required per the RFP to serve the total number of TDM voice trunks provisioned at the site. The network has the scalability to adjust bandwidth to changing needs easily, quickly, and with minimal operational impact. The bandwidth for each data center will support the bandwidth requirements and ease of future growth of the PSAP network. As it is proposed, our NG9-1-1 core is highly scalable capable of handling up to 4 million routes and up to 500,000 SIP-TLS sessions. As a carrier grade network, CenturyLink's NG9-1-1 Solution is easily scalable to a capacity that can support every 9-1-1 required by the local jurisdiction region or state deployment. CenturyLink's NGCS solution provides ethernet local access loops that can scale easily up to 1Gbps and larger with a few network interface device Network Interface Device (NID) dependencies.				

	Majority of the ethernet local access circuits that are deployed with a fiber media to the PSAP, this allows for the needed scalability of this solution. CenturyLink utilizes optical wave services, dark fiber leases and eNNI connectivity to provide a diverse POP MPLS delivered design. The network has the scalability to adjust bandwidth to changing needs easily, quickly, and with minimal operational impact. Ingress carrier network is designed to have multiple termination locations that can take 100% of the load in the event of a location failure. Connections to the PSAP are sized up to accommodate necessary bandwidth based on a concurrent G.711 SIP session (Call path). Each circuit is engineered to handle 100% of the call demand in the case of a failure of the primary or secondary circuit. Bandwidth is managed and monitored and can fluidly change as needed based on call volume. Our CenturyLink NG9-1-1 solution is capable of bandwidth growth at each network element, existing end sites, and future end sites without sacrificing reliability of the solution. The solution is capable of interconnecting to other national- and/or state-level ESInets via open standards-based interfaces. CenturyLink integrates a comprehensive set of tools for constant monitoring and management of the network. Multiple network management components will monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components will generate alarms to appropriate systems. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Delivery of monitoring reports, including bandwidth utilization and connectivity are provided as mutually agreed upon during contract negotiations. Traditional network management tools are complimented by active application monitoring and alerting. Application elements, BRIX probes and well as SDWAN deployment will also report network failures as detected by their monitoring activity, some of which is specific to managing the availability and integrity of the network

Any additional documentation can be inserted here:

	Service Level Agreements - System Performance **Network Latency** Specify the guaranteed maximum latency across the backbone network under a full-load condition, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

CenturyLink maximum latency across our backbone is based on 30-day average for the month of April and is provided in the blow table. Latency across the core network, which includes from the LNG to the PSAP.

For traffic that traverses AS209, the maximum one-way latency is 32ms across the backbone.

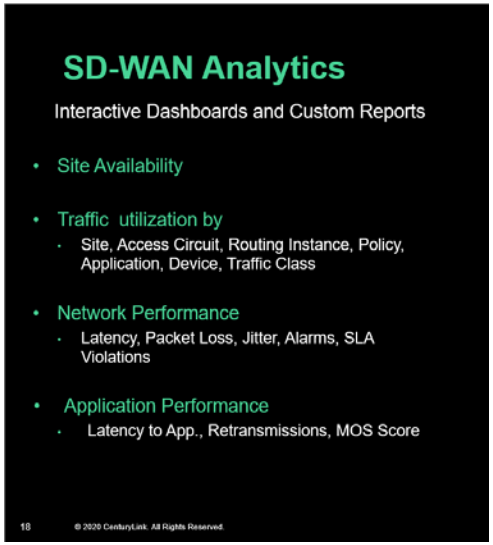
For traffic that traverses AS3549 the maximum one-way latency is 21ms across the backbone.

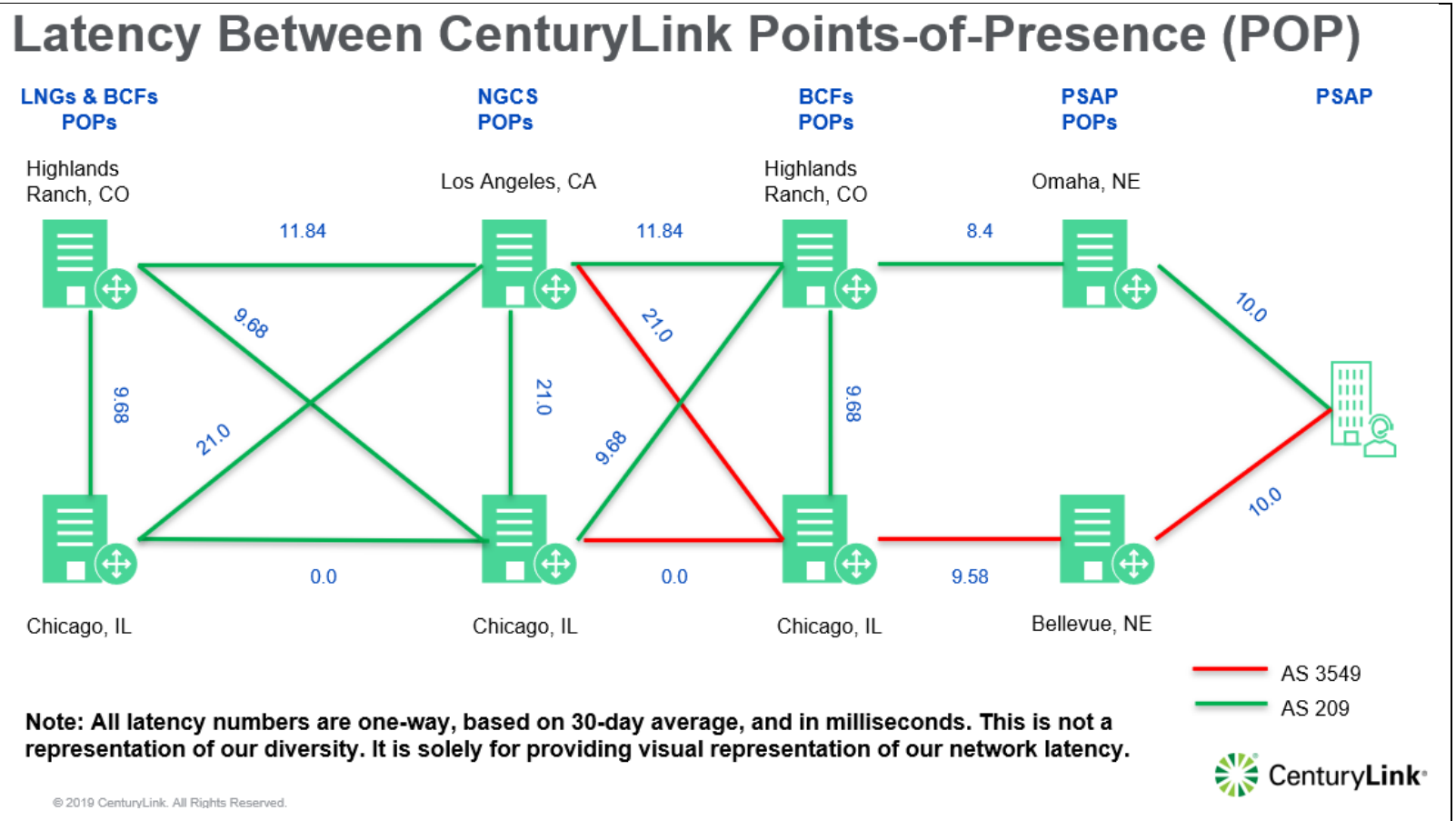
SLA 2

Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%

CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

	These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's. Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC. Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's Please see SLA 5 for examples of Active Probe reports	



Any additional documentation can be inserted here:

SLA 3	**Service Level Agreements - System Performance** **Point of Presence (POP) to POP** Specify the guaranteed maximum latency from interconnection facility to interconnection facility, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

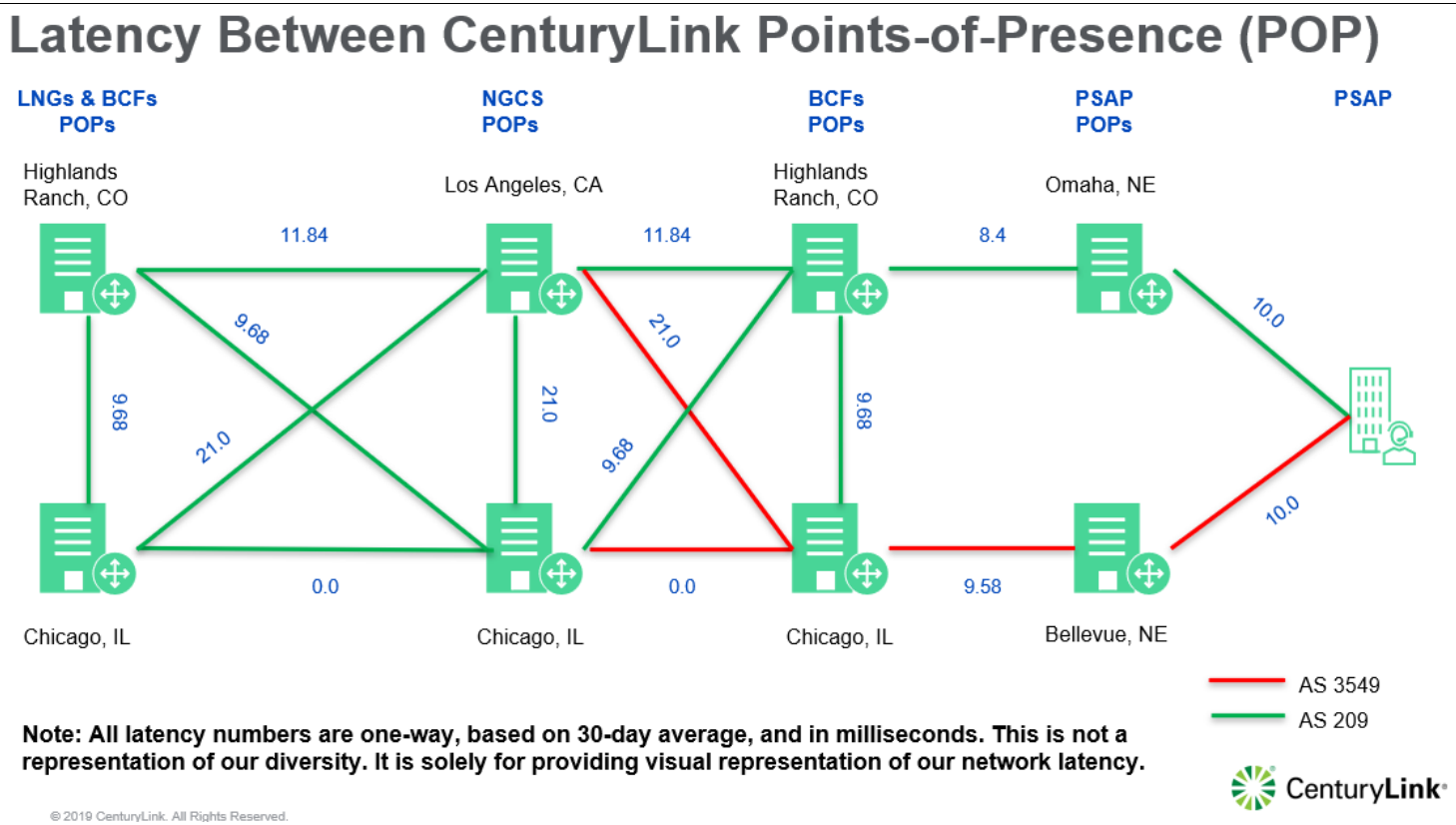
Bidder Response:

CenturyLink maximum latency from interconnection facility to interconnection facility is based on 30-day average for the month of April and is provided in the blow table.

Our maximum latency from POP to POP is 25ms.

The table below provides max latency from POP to POP.

Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%

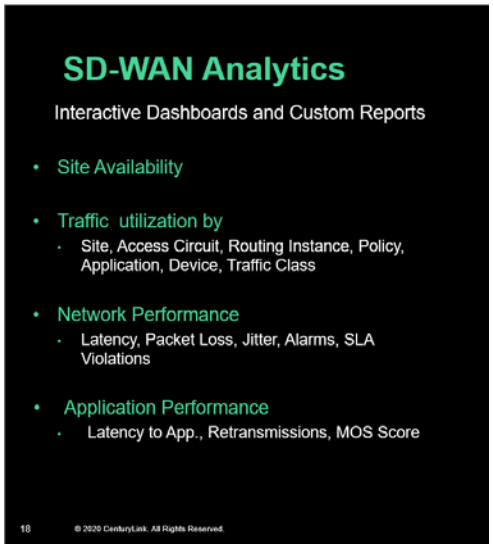


CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.



Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's

Please see SLA 5 for examples of Active Probe reports

Latency Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here:

SLA 4	**Service Level Agreements - System Performance** **POP to Endpoints** Specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

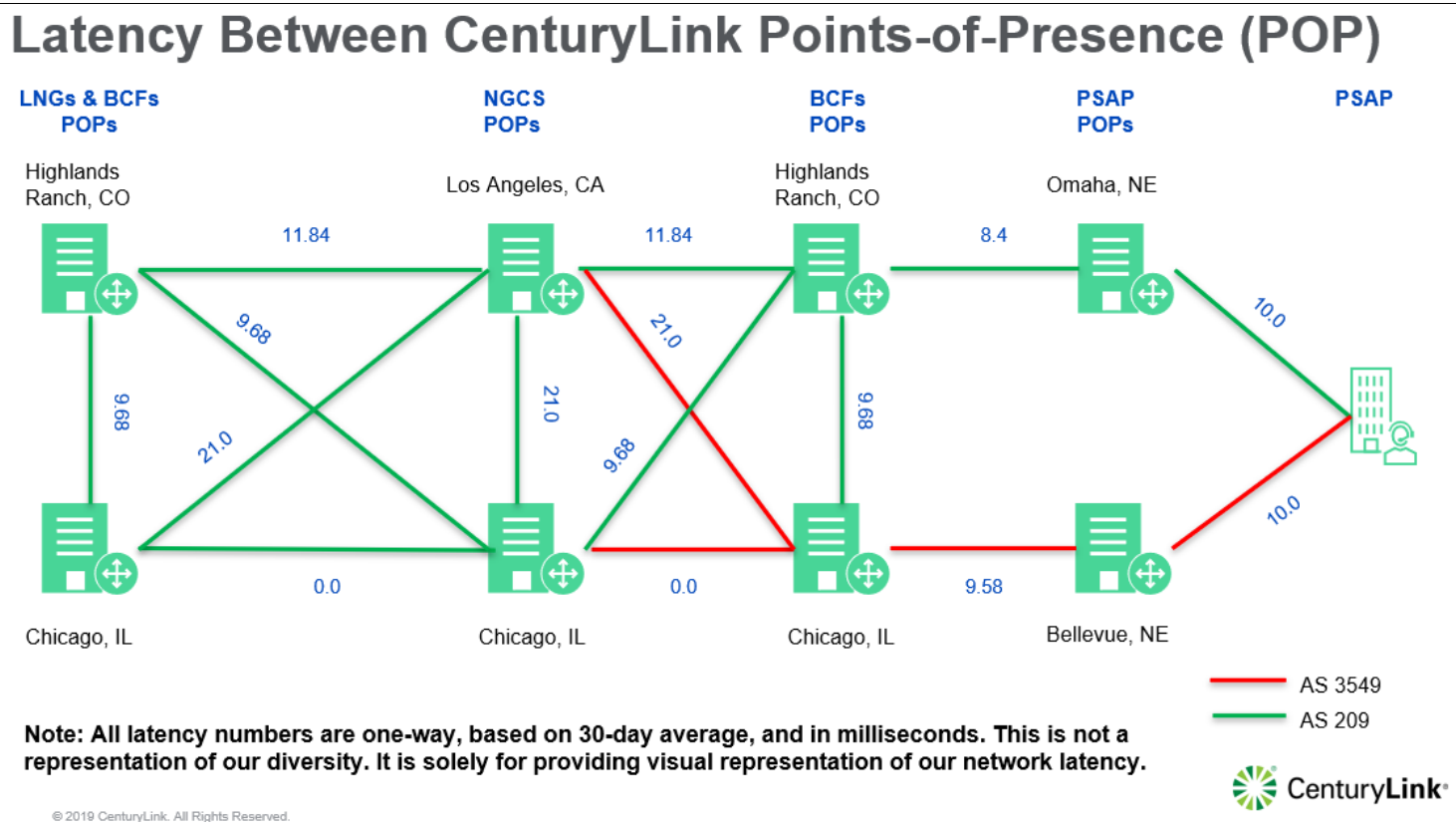
Bidder Response:

CenturyLink maximum latency from interconnection facilities to the network interface device located at the entrance to the host's premises is based on 30-day average for the month of April and is provided in the blow table.

POP to Endpoint maximum latency from interconnection facilities to the network interface device is 10 ms.

The table below provides max latency from POP to POP.

Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%



CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

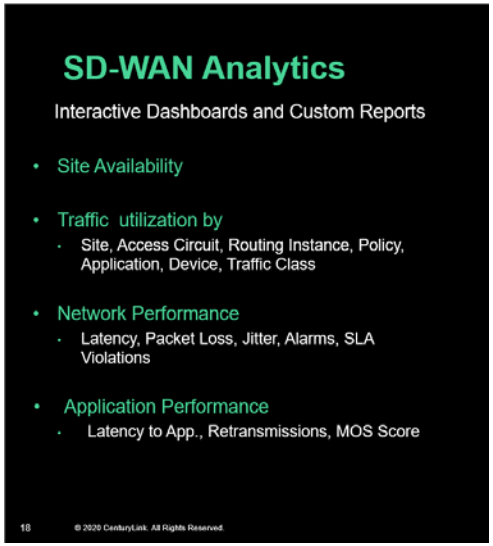
- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's



Please see SLA 5 for examples of Active Probe reports

Network Latency Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

SLA 5	**Service Level Agreements - System Performance** **Mean Opinion Score (MOS)** Bidder shall guarantee, in the response, a consistent MOS of 4.0 or better across all network links transporting media streams from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

Our NG9-1-1 solutions uses the G.711 codec, and the network supports voice quality that meets or exceeds ITU-T-P.830, maintaining an MOS standard rating of 4.0 or higher.

CenturyLink deploys active monitoring EXFO probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a test call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

When two consecutive test calls or MOS score fails, CenturyLink's monitoring system will auto-notify the CenturyLink NOC and PSAP customer of the failure and CenturyLink takes proactive remediation steps to resolve any service degradation as well as employing IP SLA's to remediate issues until the network path congestion or failure is resolved.

The attached document is an example of actual results for four PSAPs in different states. (See Copies of embedded attachments in Proposal 1 option C file 1 of 4 Attachments)

PSAP_Active_Test_Stats_v4-Example.pdf

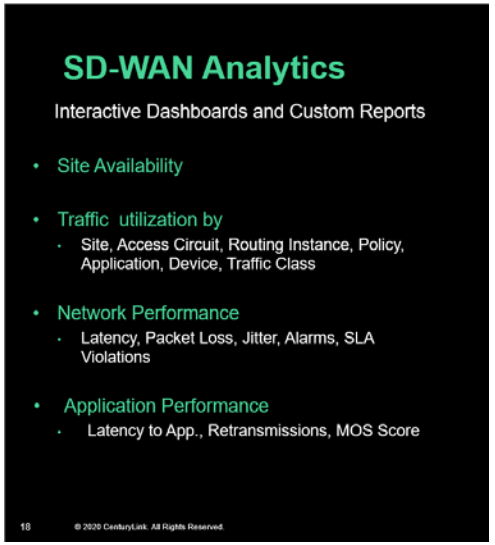
The following attachment contains actual results used for trouble resolution. . (See Copies of embedded attachments in Proposal 1 option C file 1 of 4 Attachments)

BRIX_probe__psap_id_troubleshooting-

Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's



Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

SLA 6

Service Level Agreements - System Performance **Packet Loss** Specify the guaranteed maximum end-to-end packet loss across the network. This specification also shall include any loss characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			

Bidder Response:

Proposal maintains a Packet Delivery >/=99.9%.

The below table provides a 30-day average for the month of April for Packet Loss.

Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%

CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

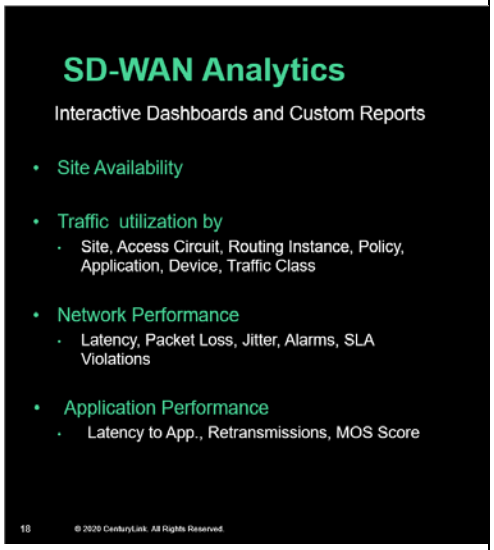
These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

Please see SLA 5 for examples of Active Probe reports

We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's



Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

SLA 7	**Service Level Agreements - System Performance** **Network Latency** Specify the guaranteed maximum end-to-end network latency across the network. This specification also shall include any latency associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

As also referenced in above section "SLA 2" "

NG9-1-1 network latency will be a monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less end to end across our network.

The below table provides a 30-day average for the month of April for Packet Loss.

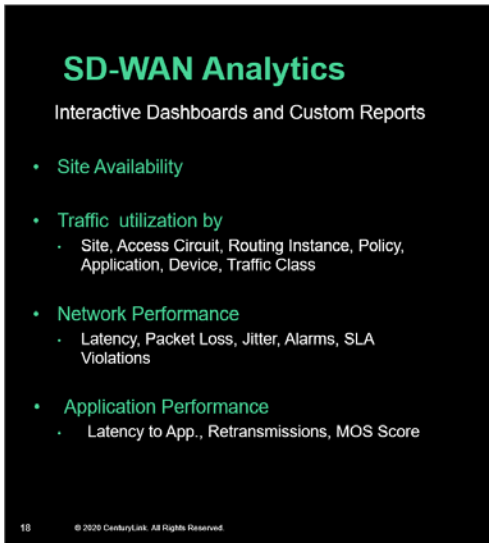
Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%

Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause intervention if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems.

CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring

- Latency
- Jitter
- Package Loss



These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

Please see SLA 5 for examples of Active Probe reports

Network Latency Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

SLA 8

Service Level Agreements - System Performance **Jitter** Specify the guaranteed maximum end-to-end jitter across the network. This specification also shall include any jitter characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			

Bidder Response:

Jitter shall not exceed twenty (20) milliseconds.

The below table provides a 30-day average for the month of April for Packet Loss.

Location A	Location B	AS Number	One Way Latency (ms)	Round Trip Latency (ms)	Jitter (ms)	Packet Delivery
Highlands Ranch, CO	Chicago, IL	AS 209	9.68	19.36	0.02	100%
Highlands Ranch, CO	Los Angeles, CA	AS 209	11.84	23.68	0.01	100%
Highlands Ranch, CO	Omaha, NE	AS 209	7.99	15.98	0.02	100%
Highlands Ranch, CO	Bellevue, NE	AS 209	9.58	19.16	0.02	100%
Chicago, IL	Los Angeles, CA	AS 209	21.01	42.02	0.02	100%
Chicago, IL	Los Angeles, CA	AS 3549	21.01	42.02	0.02	100%
Chicago, IL	Omaha, NE	AS 209	4.785	9.57	0.02	100%
Chicago, IL	Bellevue, NE	AS 3549	9.58	19.16	0.02	100%

CenturyLink deploys active monitoring probes to measure MOS scores from the ingress of the network to the PSAP. With this active monitoring, our host server places a call into the NG9-1-1 network every 6 to 7 minutes to a probe located at each core host PSAP. Every 6 to 7 minutes, we are testing the following:

- Logical connectivity to the host PSAP
- MOS scoring
  - Latency
  - Jitter
  - Package Loss

These network probes will alert our NG9-1-1 NOC whenever thresholds are exceeded. All tests are capture and stored and results are viewable through a web-architected GUI dashboard portal to the Commission and affected PSAP's.

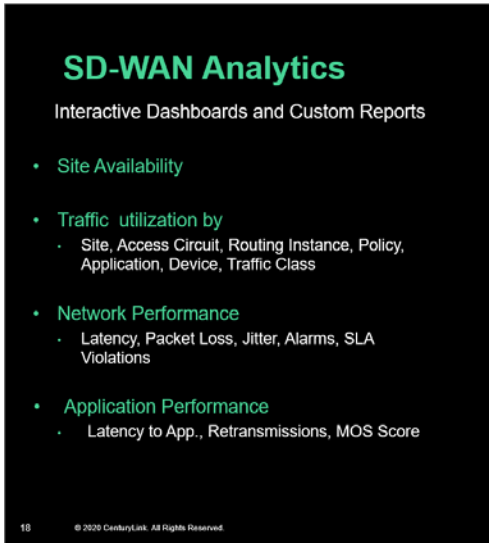
Our PSAP SD-WAN and SBC appliances will continuously monitor active calls in process. When MOS scores fall below threshold of 4.0, our monitoring system will alert our NG9-1-1 NOC and update our dashboards. Since we use packet replication with our SD-WAN appliance, all packets are sent over both MPLS circuits. If MOS score falls below the acceptable threshold over one of the two circuits, the SD-WAN has no problem recovering from this and passing on only the packets on the circuit that has not degraded. When this does happen, our monitoring system will alert our NG9-1-1 NOC.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

Please see SLA 5 for examples of Active Probe reports

Our NG 9-1-1 end to end solution currently uses a 40 ms jitter buffer for all voice calls. This means that all voice packets have been treated such that minimal end point jitter buffering would be needed (typically much less than 20 ms).

Our Project Management team will oversee the establishment of network system performance SLA's to meet external/internal customer business objectives, work plans, and ensures performance requirements are met across our NG9-1-1 ESInet solution. They will also develop methodologies, procedures, to produce performance reporting.



Jitter Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

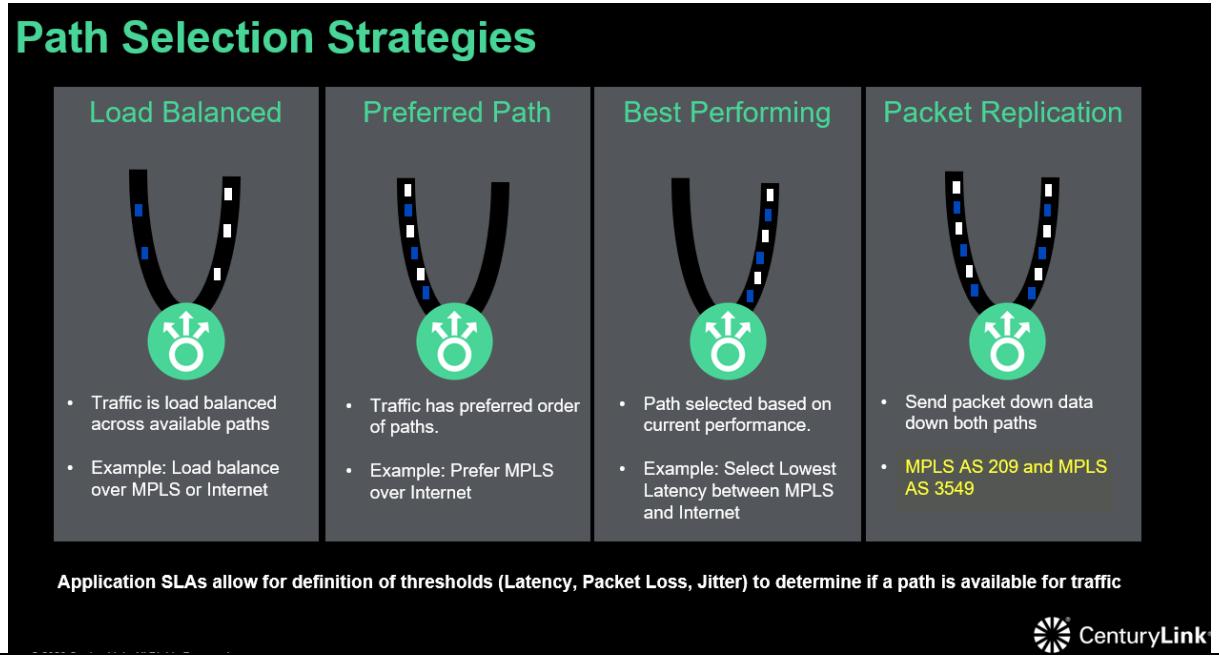
SLA 9	**Service Level Agreements – System Performance** **Network Traffic Convergence** Specify convergence protocols and the estimated or guaranteed network convergence time (less than 54 ms) of IP traffic at any point within the proposed solution, including how convergence information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

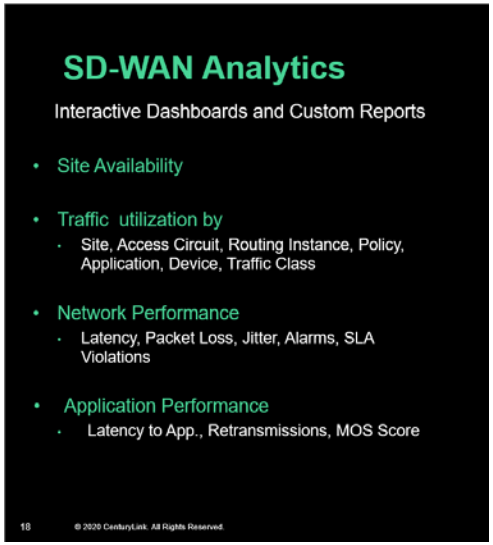
CenturyLink guarantees a network convergence time less than 54ms of IP traffic

Our NG9-1-1 core is engineered to produce the minimum possible convergence time While our MPLS network can and will support BFD timers, it is not what we depend on for resiliency or fast failover on our ESInet. We rely on our SD-WAN's ability to do "Packet Replication," which removes the dependency for failover with other protocols such as BFD.

SD-WAN with Packet Replication provides for near ~0ms convergence time.



Note: CenturyLink will only use MPLS for **NE ESInet. We will not use Internet connections. The above is for illustrative purposes for Path Selection Strategies only. Our ESInet will deploy Packet Replication.**



Packet replication enables real-time data packets to be duplicated and simultaneously sent over multiple flows to the endpoint destinations while maintaining high VoIP experience over these multiple connections.

Packet replication allows for data to be sent between SD-WAN appliances down in parallel down multiple paths. This provides for seamless recovery from degraded paths on UDP applications such as VoIP.

At each location, CenturyLink will provide two HA SD-WAN appliances. Circuit A will terminate on SD-WAN appliance 1, and circuit B will terminate on SD-WAN appliance 2. This HA configuration will replicate packets over both circuits. If circuit A was to fail, there would be no fail-over needed since we have replicated the packets on circuit B

Our solution can support any open-standard protocol on the PSAP side of the interface such as VRRP if the PSAP is configured to support a pair of HA routers.

We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes, Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's.

Our SD-WAN Interactive Dashboards and Custom Reports provides the following Network Performance analytics

Network Traffic Convergence Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

<table>
<tr><td rowspan="2">SLA 10</td><td>Service Level Agreements - System Performance
Mean Time to Repair (MTTR)
Specify the MTTR characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTTR information will be gathered, calculated and provided to the Commission and affected PSAPs.</td><td>Comply
X</td><td>Partially Comply</td><td>Complies with Future Capability</td><td>Does Not Comply</td></tr>
<tr><td colspan="5">Bidder Response:

We will follow standard MTTR operational guidelines for responding to customer troubles and providing updates on all products. Specific MTTR criteria will establish severity levels as part of the mutually agreed SLA. TTR times begin when a trouble ticket is opened after detection or report of an outage. Calculation of TTR service level will be based on the time taken to restore service following an event that results in the outage.

MTTR characteristics are commensurate with the appropriate level of service at which the ESInet system is functioning (i.e., system components in the call path are Life and Mission Critical Services (LCMS) while, peripheral systems are considered Business Critical Services (BCS). The MTTR characteristics are listed in the table below.

• Life and Mission Critical Services (LCMS)
• Business Critical Services (BCS)
• Business Essential Services (BES)
• Business Support Services (BSS)
• Unsupported Business Services (UBS)

Network Traffic Convergence Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and Oracle Operations control Monitor and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's.

<table>
<tr><th colspan="3">SLA 10: MTBF and MTTR</th></tr>
<tr><th>Service Class</th><th>MTBF (Service)</th><th>MTTR (Service)</th></tr>
<tr><td>LMCS</td><td>>5 years</td><td><2 minutes</td></tr>
<tr><td>BCS</td><td>>1 year</td><td><4 hours</td></tr>
<tr><td>BES</td><td>>3 months</td><td><40 hours</td></tr>
<tr><td>BSS</td><td>>1 month</td><td><3 days</td></tr>
<tr><td>UBS</td><td>Unspecified</td><td>Unspecified</td></tr>
</table>
</td></tr>
<tr><td></td><td colspan="5"></td></tr>
</table>

Any additional documentation can be inserted here

SLA 11	**Service Level Agreements - System Performance** **Mean Time Between Failures (MTBF)** Specify the MTBF characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTBF information will be gathered, calculated and provided to the Commission and affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

MTBF characteristics are commensurate with the appropriate level of service at which the system is functioning i.e., systems in the call path are Life and Mission Critical Services (LCMS) while peripheral systems are considered Business Critical Services (BCS). The MTBF characteristics are listed in the table below, where the following abbreviations are used:

- Life and Mission Critical Services (LCMS)
- Business Critical Services (BCS)
- Business Essential Services (BES)
- Business Support Services (BSS)
- Unsupported Business Services (UBS)

Table 1: MTBF and MTTR

Service Class	MTBF (Service)	MTTR (Service
LMCS	>5 years	<2 minutes
BCS	>1 year	<4 hours
BES	>3 months	<40 hours
BSS	>1month	<3 days
UBS	Unspecified	Unspecified

Based on our public safety experience, CenturyLink has found that measuring Service Availability from a call processing perspective is more applicable and relevant to 9-1-1 service vs. traditional methods of calculating availability thru MTBF and MTTR measures.

CenturyLink believes that the most relevant measure of service availability is evidenced by uninterrupted, reliable 9-1-1 call routing and delivery to the PSAPs.

Our NG9-1-1 availability is calculated from the time an outage begins that impacts call processing ability, until such time that the NG9-1-1 call processing ability is restored. This includes all NG9-1-1 downtime for the end-to-end service. This report will be made available on a monthly basis to the State of Utah.

Maintenance of and upgrades to the NG9-1-1 solution are done with no scheduled downtime. We schedule planned events for routine maintenance in ways that 9-1-1 operations are not impacted. A notification of the upcoming event will be sent to the customer as applicable. Planned events are fully staffed and managed with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event.

The CenturyLink team will conduct major and minor planned and critical un-planned events for all NG9-1-1 Services, system maintenance, or upgrades that may impact the NG9-1-1 Customer PSAPs. CenturyLink fully manages and completes these events with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. CenturyLink includes the required back-out time within the scheduled maintenance time frame.

Standard 9-1-1 availability as described in this response will be supported for all services offered in Next Generation ESInet solution. CenturyLink would like to point out that availability for the network is valid for diverse and redundant connectivity into the PSAP or third-party providers network.

	We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes, Splunk, and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

Any additional documentation can be inserted here

SLA 12	**Service Level Agreements - System Performance** **Network Reliability** Network reliability is defined as the ability for system endpoints to effectively communicate with each other, and all associated data and information is exchanged in usable formats. An IP-based network looks at reliability as an overall redundancy design, rather than component by component. Specify in the response the overall reliability service level of the IP network, including all bidder-provided components and facilities.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink's **overall reliability is 99.999%.** Our CenturyLink network is known for its reliability, security, and redundancy. It uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission; and it has an availability target of 99.999%. Our CenturyLink network is known for its reliability, security, and redundancy. It uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission; and it has an availability target of 99.999%. We accomplish this through problem detection, prevention, redundancy, and restoration offers to ensure that the network is always up and running. 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. Two connections are included in our ESInet design to each Host PSAP site supported by two separate edge routers and two separate IP VRF instances increasing the network reliability. All network routing infrastructure and equipment is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative making our network more reliable. Our two (2) physically diverse MPLS Network to each PSAP are predetermined, so packets travel only along the paths to which they are directed adding reliability to our network. Our NG9-1-1 ESInet is designed to meet more stringent requirements for security, resiliency, and reliability service levels than most other IP networks. CenturyLink ESInet utilizes an MPLS private IP network that includes the use of third-party network providers that provide the local access and path diversity. These networks are comprised of different components, multiple technical solutions, and various types of interfaces. Due to the nature of MPLS-based transport, WAN failures (within the carrier network or last-mile) may not be immediately detected by NGCS network equipment at the physical layer. Knowing this, the CenturyLink ESInet solution employs a more robust means of end-to-end failure detection to ensure the reliable delivery of 9-1-1 traffic All systems and components have redundant (parallel) capabilities into each of our CenturyLink facilities to provide additional reliability including: • Datacenters are widely separated, and are powered off of different power grids • Redundant Power systems				

- Telecommunications services
- Network electronics
- Cooling
- Fuel

SLA Reliablity - Assuming a 7x24x365 deployment (8,760 available hours), these ranges produce the following expected outage totals.

Nines	Availability	%	Downtime/ Year	Downtime/ Month*	Downtime/ Week
One	0.9	90%	36.5 days	73 hours	17.18 hours
Two	0.99	99%	3.65 days	7.30 hours	1.72 hours
Three	0.999	99.9%	8.76 hours	43.2 minutes	10.1 minutes
Four	0.9999	99.99%	52.56 minutes	4.32 minutes	1.01 minutes
Five	.99999	99.99%	5.3 minutes	25.9 seconds	6 seconds

Any additional documentation can be inserted here

	Service Level Agreements - System Performance **Network Availability** 1. Specify the service level offered as a percentage of time when the service is available, and the maximum period of total outage before remedies are activated. Availability is defined as MTBF/(MTBF+MTTR). 2. Include how system availability information will be gathered, calculated and provided to the Commission and affected PSAPs.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 13	Bidder Response: 1.End-to-end, the CenturyLink solution is architected to be secure, reliable, resilient, and robust. All applications and network in the 9-1-1 call path are designed to achieve 99.999% system availability using a number of techniques to improve resiliency such as geo-diverse redundancy, fail-over techniques, virtualization, high availability, etc. The solution utilizes redundant hardware components (network interfaces, hard disks, hot swap power supplies, etc.) wherever possible, and the solution has no single point of failure. NGCS services operate in an active-active configuration in two geo-diverse datacenters located in Ohio per this RFP request. This feature employs redundant, high-quality, fault-tolerant critical components operating continuously in tandem. If one should fail, the redundant component continues to carry the entire load with no interruption of service. No failover time is required. All applications are deployed on virtual servers and data is shared among and within each datacenter. These applications leverage high availability functionality within the hypervisor. DRS and HA features are utilized to ensure an "always on" architecture. Because of this, no single point of failure that will disrupt the ability to provide on-going call processing. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability. Core sites include redundant network transport and redundant network interfacing elements to ensure optimal operation and availability. Network interfacing elements include switches, routers, SBCs, firewalls, and other security devices. All network routing infrastructure is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology. Network probes and well as SDWAN deployment will also report network failures as detected by their monitoring activity, some of which is specific to managing the availability and integrity of the network. Network 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. CenturyLink's Statistic and Risk analysis reporting tools will be used to provide: Distribution of calls by destination; Call success rate; Average call length; Average number of calls per day; Ratio of incoming versus outgoing calls; and Average mean opinion score (MOS) value scores. The NG9-1-1 Service availability SLA measures the availability requirement of 99.999% for Call Processing ("Service Availability"). Call Processing is the ability of the Service to deliver calls from the inbound Service demarcation point into the Core Call Processing Nodes and from the Service demarcation point to a Valid Destination (for example a PSAP). The Service Availability is calculated from the time an issue is reported that impacts				

	Call Processing ability, until such time that the Service Call Processing ability is restored. The Service Availability downtime will not exceed 26.3 seconds per month. Customers are eligible for remedies and service credits when the Service Availability SLA is not achieved. 2.We use a combination of platforms for accomplishing monitoring, data management, and oversight tasks, including SDWAN, SolarWinds, Brix network probes. Splunk, and Oracle Operations control Monitor and others. Outputs from the various platforms are gathered, calculated and combined into single-pane views specific to the NG9-1-1 services arena using developed tools. This combined approach allows CenturyLink to tailor the solutions to the specific NG9-1-1 environment while leveraging best-in-class off the shelf tools where appropriate monthly results are viewable through our Web-Based customized dashboard to both the Commission and affected PSAP's. Network Availability Service Level Agreements (SLAs) will be provided as a part of our Program Development Plan (PDP). The CenturyLink Program Manager will work with the Commission and or PSAP's to track services against SLAs and provide monthly reporting to the customer. During the planning phase of the project the CPrgM will work with the state to define reporting criteria, format and frequency. Refer to Attachment labeled "2.d CenturyLink Sample Program Management Plan for Nebraska".

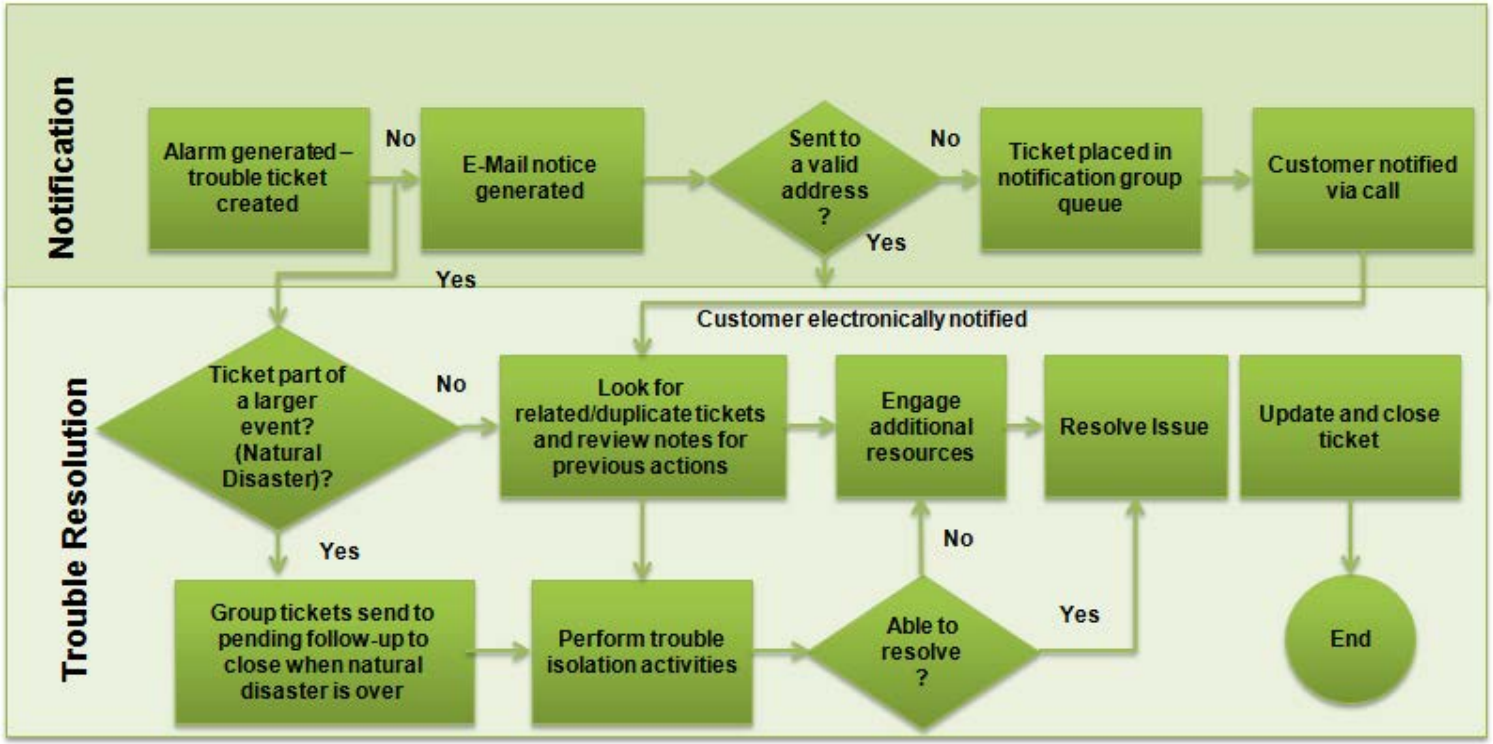
Any additional documentation can be inserted here

SLA 14	**Service Level Agreements - System Performance** **End-of-Support Equipment** Contractor shall proactively replace, at Contractor's expense, any hardware that has reached end of support (EOS) no later than 90 calendar days prior to the manufacturer's EOS date. All equipment must be new and of current manufacture, not refurbished. Describe your procedures for End-of-Support Equipment.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's NG9-1-1 solutions are a service and includes any hardware replacement in the cost that may occur to obsolescence within the good standing of contract term. This is an Infrastructure as a Service" proposal. Consequently, hardware and software are maintained by our team centrally and kept current with NENA standards as long as a support agreement is in place. CenturyLink Program Management CPrgM team will track the lifecycle of the equipment and alert stakeholders to the need for a refresh well before equipment becomes end of support.				

Any additional documentation can be inserted here

SLA 15	**Service Level Agreements –** **SLAs for Incident Management** The Commission requires the Contractor to establish processes and procedures for supporting a NOC/SOC that can rapidly triage and manage reported network incidents. Bidder shall develop an ITIL compliant severity-level scale that includes levels one through four, with level one being the most severe incident. The top two levels shall capture all incidents affecting the level of service of one or more endpoints. Include a description of incident severity-level attributes, including response and resolution times for each severity level, and how response and resolution times are measured.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The CenturyLink Network/Security Operations Center (NOC/SOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage CenturyLink's NGCS Solution associated services and connectivity. When a potential or actual customer-affecting event or outage is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established processes that are ISO 9001:2015-compliant for immediate escalation, notification, resolution, and reporting. In case of a service interruption and/or outage, we have instituted Incident Management processes and procedures for dealing with various severity levels during the course of an event. Our incident response tools include use of the Incident Command System (ICS modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post-event review and root cause analysis. We manage incidents and provide customers with notifications and status of ongoing service affecting issues that may impact the CenturyLink's NGCS Solution. **Notification** The CenturyLink support center shall notify the ISP and ICC within 30 minutes of discovering an event or outage that may impact 9-1-1 services. CenturyLink's NGCS Solutions service assurance strategy places the highest emphasis on service restoration. Communication will be supplied to all parties provided to CenturyLink by the Customer and its entities. CenturyLink complies with applicable FCC rules regarding outage notification and Reason for Outage (RFO) reporting. CenturyLink will prepare and submit a preliminary root cause analysis (RCA) for a Severity Level 1 or Severity Level 2 event. The preliminary report will provide an overview of all information known at that time. The Incident Command team will prepare and submit a final report of a Priority Level 1 or Level 2 event describing the impact of the event, the cause, resolution and any preventative steps that can be taken to eliminate future events. The following are key highlights for the notification system: • The five state levels are as indicated: Critical, Major, Minor, Warning, and Normal • We provide notification to the 24x7x365 NOC • We provide notification by various means • Notification levels are defined by the supporting entity • We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications. For example, we can say "no more of a certain alarm for the next 30 minutes" or we can say "send me duplicate alarms every 5 minutes" **Communication**				

	Communication will be supplied to all parties provided to CenturyLink by the Customer and its entities. We provide notification by various means. In the event of an outage CenturyLink applies immediate and sustained effort, 7x24, until a final resolution is in place. We use all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. If a temporary workaround solution is provided, we provide an action plan to be mutually agreed upon for the final resolution. We continue resolution activity until full service is restored. The primary objective of an incident is to mitigate impact. The Incident Commander and Incident Administrator are able to call upon whatever resources are required to identify and restore functionality. **Reason for Outage Reporting** In addition to tracking planned and emergent events, CenturyLink maintains a problem management system for tracking and reporting trouble. We can also provide monthly trouble reports showing tickets opened, resolved, and unresolved. CenturyLink will prepare and submit a preliminary root cause analysis (RCA) for a Severity Level 1 or Severity Level 2 event. The preliminary report will provide an overview of all information known at that time. A final report will also be provided that describes the cause, resolution and any preventative steps that can be taken to eliminate future events. CenturyLink uses a proactive monitoring and notification process (**Error! Reference source not found.**). The process uses platform-specific alarm thresholds to identify potential service impairments. CenturyLink network alarms are customer specific and generate trouble tickets that automatically notify customers via e-mail and telephone. Proactive Customer Notification (PCN) also gives customers with flexibility to specify certain notification parameters on a service-by-service basis.



Any additional documentation can be inserted here

SLA 16

Service Level Agreements – **Outage Notification and Reason for Outage (RFO) Report** **Outage Summary and Lessons Learned** Provide a summary of FCC reportable outage situations that interrupted 911 service to bidder's clients over the past three years, where 911 calls were not delivered or not delivered to the appropriate PSAP as a result of the issue. The response shall include the deployment type (legacy, ESInet, and NGCS), month, year, duration, number of PSAPs or population impacted, number of PSAPs or population served by the impacted system, impacted system, and lessons learned from each outage. **Regulatory Compliance** Contractor shall comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			

Bidder Response:

Limited to FCC outage reports for Nebraska
Limited to NE FCC outage reports where there was impact to 911 calls - ANI/ALI-only outages were excluded

Notes:– Numbers listed in "Population Impacted" represent who could not have used the service if they tried, not actual failed attempts.
– If 911 calls are rerouted to another PSAP with ANI/ALI, within 30 minutes of the start, it is not FCC reportable and not included here.

Deployment Type	Event Date	Duration	Number of PSAPs Impacted	Population Impacted	Area	RFO	Impacted System
Legacy	6/28/2017	25 hours, 13 minutes	1 - Dual ALI - 31 minutes	3898	Oakdale, O'Neill, Atkinson and Valentine	The cause of this outage was a damaged fiber cable due to rodent chew.	Transport
Legacy	8/29/2018	37 hours, 49 minutes	6	2426	North Platte, Lexington, Scottsbluff, Mitchelle, Oshkosh, Gering, Sidney, Gothenburg, Elm Creek, McCook, Denver, CO	The cause of this outage was a fiber cable cut by a mower. No locates were requested.	Transport
Legacy	4/9/2019	4 hours	1	3795	Randolph	The cause of this outage was a failure in the offnet provider's network.	Offnet

	Legacy	6/8/2019	15 hours, 28 minutes	0	1155	St. Paul	The cause of the outage was failed synchronization on the remote links.	Transport
	Legacy	7/5/2019	(911 rerouted in 41 minutes) event: 11 hours, 34 minutes	1	391	Laurel	The cause of this outage was a fiber cable cut.	Transport
	Legacy	9/12/2019	17 hours, 40 minutes	0	690	Elwood	The cause of this outage was a fiber cable cut.	Transport
	Legacy	10/8/2019	18 hours, 21 minutes	0	376	Elwood	The cause of this outage was a fiber cable cut by a mower	Transport
	Legacy	12/4/2019	(911 rerouted in 52 minutes) event: 11 hours, 15 minutes	1	1438	Scottsbluff	The cause of this outage was a fiber cut on a local providers network.	Offnet
	Legacy	4/3/2020	7 hours, 20 minutes	1	9999	South Sioux City	This outage was caused when AC Power took brief hits. The power hits confused the equipment so the generator wasn't engaged. Service did switch to battery and ran until battery power ran out and the switch failed.	Switch

Any additional documentation can be inserted here

	Service Level Agreements – **Outage Notification and Reason for Outage (RFO) Report** **Outage Notification** Contractor shall notify the Commission and affected PSAPs within a maximum 30 minutes of discovering an event or outage that may impact 911 services. All events that meet criteria for local, state, or federal reporting shall also be completed by the Contractor. At the time of initial notification, the Contractor shall convey all available information that may be useful in mitigating the effects of the event or outage, as well as a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. The Contractor is responsible for coordinating data gathering, troubleshooting and reporting on behalf of subcontractors. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SLA 17	Bidder Response: CenturyLink complies with applicable FCC rules regarding outage notification and Reason for Outage (RFO) reporting. In case of a service interruption and/or outage, our team has instituted Incident Management processes and procedures for dealing with various severity levels during the course of an incident. Our incident response tools include use of the Incident Command System (ICS), which is housed within our Ticketing System. The CenturyLink support center shall notify the Commission or affected PSAP within 30 minutes of discovering an event or outage that may impact 9-1-1 services. CenturyLink's NGCS Solutions service assurance strategy places the highest emphasis on service restoration. Communication will be supplied to all parties provided to CenturyLink by the Customer and its entities. CenturyLink complies with applicable FCC rules regarding outage notification and Reason for Outage (RFO) reporting. CenturyLink will prepare and submit a preliminary root cause analysis (RCA) for a Severity Level 1 or Severity Level 2 event. The preliminary report will provide an overview of all information known at that time. The Incident Command team will prepare and submit a final report of a Priority Level 1 or Level 2 event describing the impact of the event, the cause, resolution and any preventative steps that can be taken to eliminate future events. The following are key highlights for the notification system: • The five state levels are as indicated: Critical, Major, Minor, Warning, and Normal • We provide notification to the 24x7x365 NOC • We provide notification by various means • Notification levels are defined by the supporting entity • We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications. For example, we can say "no more of a certain alarm for the next 30 minutes" or we can say "send me duplicate alarms every 5 minutes"				

Any additional documentation can be inserted here

SLA 18	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Status Updates** The Contractor shall communicate any updated status information to the Commission and affected PSAPs no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 911 service is restored. This information shall include the nature of the outage, the best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected operations. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The CenturyLink Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage CenturyLink's NGCS Solution associated services and connectivity. When a potential or actual customer-affecting event or outage is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established processes that are ISO 9001:2015-compliant for immediate escalation, notification, resolution, and reporting. Initial notifications are sent within 30 minutes of any troubles discovered by the 9-1-1 Public Safety NON for Severity level 1 and Severity level 2. Updates occur every 30 minutes or as appropriate, and trouble resolution within 4 Hours. 86% of repairs completed in less than 4 Hours. The 30-minute notification is in compliance with the FCC requirement. To effectively support and handle customer questions, incidents or requests, we have adopted the ticket resolution procedure outlined below. The process is one that allows for continual improvement and ensures that all support requests are tracked and maintained in an efficient and effective way. Each of the steps is designed to allow for all types of questions, incidents or requests whether they are complicated or simple. Some of the steps can be removed if the nature of the inquiry is simple. CenturyLink repair procedures emphasize quality service for responsiveness and reliability to all the 9-1-1 centers. Our escalation policies and procedures allow for escalation to be invoked at any time deemed necessary by the customer, by the CenturyLink 9-1-1 Field Technicians, or by CenturyLink in-house Tier 2 technical support. CenturyLink will track all escalations via the CenturyLink repair web portal. Each escalation will be tracked during entire duration of the repair. CenturyLink agrees to begin Tier 1 support within 15 minutes of identifying a service affecting event. CenturyLink agrees to begin Tier 2 support within (2) hours of identifying a service affecting event and Tier 3 support with (4) hour or upon Center request. Under our normal protocol, for all Severity Level 1 & 2 (Critical and Major is your example) issues reported, we provide an immediate response, and will ensure the initiation of corrective action no longer than 30 minutes from time of notification. Within two (2) hours of any Severity Level 1 & 2 report, if the problem has not been corrected, we begin the escalation process and ensure an onsite dispatch, if required, has been affected. The escalation procedures are outlined as follows for previously reported problems: Step 1: Customer (PSAP) will call the CenturyLink 9-1-1 Public Safety Services Network Operations Center (NOC) and request a manager referencing the original repair ticket and escalation request. The manager will document the escalation in the CenturyLink 9-1-1 online repair system and call the local 9-1-1 CenturyLink Service manager.				

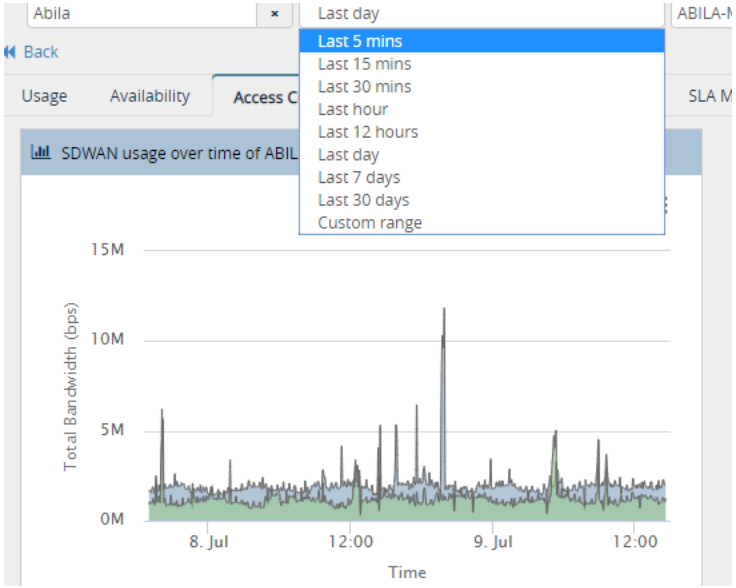
Step 2: CenturyLink Service manager will provide email and verbal updates to the customer

Step 3: if Customer (PSAP) is still not satisfied, the local CenturyLink 9-1-1 Account Team will be called. CenturyLink will provide a written action plan that outlines the steps that will be taken to resolve this escalation.

Additional conference calls or meeting(s) may be required to resolve the escalation.

CenturyLink meets monitoring and reporting time requirements for key SLA metrics listed above via our analytics portal associated with the SD-WAN devices in our proposed architecture.

CenturyLink's minimum reporting interval is "last 5 minutes as noted below.



CenturyLink Public Safety Service (PSS) Network Operations Center (NOC)

Group	Name	Title	Contact	Number
PSS NOC	PSS Network Operations Center	24x7	PSS NOC Center Main Number	800-357-0911
PSS NOC	1st Level Escalation	1st Level Escalation	PSS NOC Center Main Number	800-357-0911 – request a first level escalation
PSS NOC	2nd Level Escalation	PSS NOC Supervisor – Monday – Friday 7am to 3pm CST	Linda Capetz	612-256-6357 (O)
		PSS NOC Supervisor – Monday – Friday 3pm to 11pm CST	Will Cave	612-439-8968 (O)
		PSS NOC Duty Supervisor After hours, weekends and holidays	Duty Supervisor	833-291-4450
PSS NOC	3rd Level Escalation	PSS NOC Manager	Carl Klein	612-439-8841 (O)
				651-442-5999 (M)
PSS NOC	4th Level Escalation	PSS NOC Director	Sally Bakarich	720-888-8988 (O)
				303-507-4367 (M)
PSS NOC	5th Level Escalation	VP Centralized Services	Jorge Magana	404-526-4428 (O)
				404-384-1576 (M)

updated 2/19/2020

During the development of the final PMP, the escalation chart will be incorporated into the PMP as shown in the Sample PMP in the attachments section of this RFP

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 19	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Reason For Outage (RFO) Reporting** Following the restoration of normal 911 service, Contractor shall provide a preliminary RFO report to the Commission and affected PSAPs no later than three (3) calendar days after discovering the outage. An in-depth RFO report, including a detailed root-cause analysis, shall be provided to the Commission and affected PSAPs no later than ten (10) calendar days after discovering an outage. 1. Describe how bidder will comply with the notification and reporting requirements above. 2. Describe the NOC/SOC tools and techniques at bidder's disposal to ensure that bidder's various subcontractor perform troubleshooting and post-event analysis and provide associated reports.	X			
	Bidder Response: A detailed description of the RFO process is included in the attached Program Development Plan. An initial RFO is provided at ticket closure, when verifying service is restored. A formal RFO can be delivered, upon request, within 5 business days.				

Any additional documentation can be inserted here

SLA 20	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **PSAP Notifications** Outage notifications and follow-up analysis of outages are a critical element to understanding overall system health and preventing future service interruptions. Having awareness of issues that exist in a neighboring PSAP provides valuable insight into potential issues that may begin impacting another PSAP's operations. The Commission' is seeking an outage notification service that allows for each PSAP to elect the outage notification types and PSAPs for which it will receive outage notifications, outage updates and RFO reports. A web portal for authorized users to select/deselect outage notifications is required. Provide a detailed description of how bidder will support such an outage notification service.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink will work with the PSAPs to establishing the notification types available. Within the portal, the PSAPs can set permissions for any user to view that PSAP's trouble tickets. The PSAP can provide CenturyLink an email address in the form of a distribution list for all notifications. Authorized portal users will be able to select to receive notifications.				

Any additional documentation can be inserted here

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SLA 21	**Service Level Agreements –** **Media Contact** 1. Contractor shall provide a 24 x 7 spokesperson who will be available for media contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs. **Government & Regulatory Contact** 2. Contractor shall provide a 24 x 7 representative who will be available for government and regulatory contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs Describe bidder's experience in providing both a Media Contact and Government & Regulatory Contact for similar contracts.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

1. Our two (2) contact(s) for CenturyLink Media regarding 9-1-1 outages for the State of Nebraska our as follow:

Linda M. Johnson
Corporate Communications
CenturyLink
tel: 202.429.3130
cell: 202.538.9892
http://news.centurylink.com/public-policy

Mark Molzen
Global Issues Manager, Transformation, Legal
CenturyLink, Inc.
20 E. Thomas, Phoenix, AZ
O: 602-716-3389
C: 602-614-7476
Twitter: @mdmolzen

2. Our two (2) contact(s) for CenturyLink Government and Regulatory regarding 9-1-1 outages for the State of Nebraska our as follow:

Linda M. Johnson
Corporate Communications
CenturyLink
tel: 202.429.3130
cell: 202.538.9892
http://news.centurylink.com/public-policy

Mark Molzen
Global Issues Manager, Transformation, Legal
CenturyLink, Inc.
20 E. Thomas, Phoenix, AZ
O: 602-716-3389
C: 602-614-7476

CenturyLink also will follow the FCC rules regarding outage notification and Reason for Outage (RFO) reporting as outlined in this RFP and SLA's.

Any additional documentation can be inserted here

	Service Level Agreements – **SLA Violations** An SLA violation shall have occurred whenever: A. The Contractor fails to meet any single performance level; or, B. The average of any single performance item over the preceding two-month period fails to meet the service level stated in response to requirements SLA 1 through SLA 22. Contractor shall deliver an SLA violations report to the Commission on a monthly basis. **SLA Reporting** Provide a detailed description of how bidder measures and reports incidents, including immediate notifications and regularly scheduled reports. SLA results shall be delivered to the Commission on the 10th business day of the month. The report shall include all performance items identified in the bidder's proposal and documented in contract negotiations.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SLA 22	Bidder Response: Specific performance reports will be identified and mutually agreed upon during contract negotiations. **SLA Reporting:** The NG9-1-1 Public Safety NOC is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage the NG9-1-1 ESInet and associated services. When a potential or actual customer-affecting issue is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established processes that are ISO 9001:2008-compliant for immediate escalation, notification, resolution, and reporting. CenturyLink's monitoring system will auto-notify the CenturyLink NG9-1-1 Public Safety NOC and commission of a failure and CenturyLink takes proactive remediation steps to resolve any service degradation as well as employing IP SLA's to remediate issues until the network path congestion or failure is resolved. Via SolarWinds and other monitoring system 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 via our portal and dashboard. • 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. CenturyLink will provide monthly reporting on incidents, including open/closed ticket status, resolution times, and service level agreement (SLA) compliance to the commission.				

Any additional documentation can be inserted here

SLA 23	**Service Level Agreements –** **SLA Violation Financial Remedies** Contractor shall provide financial remedies to the Commission for each event in which service levels are not maintained. The Commission requires that all of the Contractor's network facilities, devices, and services will be measured on a rolling, 12-month calendar. Failure to meet SLAs shall be measured per service-affecting outage. Financial remedies shall be assessed for failure to meet SLAs. For service-affecting incidents, a 10 percent (10%) discount shall be accessed against the Monthly Recurring Charge (MRC) applicable to the source of the failure, whenever the initial period of resolution is exceeded. If the resolution period length of time doubles, then the discount shall increase to 20 percent of the MRC. If the resolution period length of time quadruples the initial period, then 50 percent of the MRC shall be assessed. The amount related to the damages is to be credited to the invoice for the month immediately following the violation. Bidder shall include how uptime information will be gathered, analyzed and provided to the Commission.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's solution includes "Near" Real Time Network Outage Monitoring and Reporting 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 with a Web browser which will connect to the dashboard made available to the state.				

Any additional documentation can be inserted here

Operational Scenarios

Safeguards shall be established to minimize the impact of human or system error. Describe bidder's risk-mitigation and issue-resolution strategies for the following hypothetical scenarios:

GEN SCEN 1

Scenario 1 At 0300 hours, a series of SBC alarms previously unseen by the NOC staff on duty begin to increase in volume and frequency. At 0330, multiple critical alarms are received. At 0345, a few PSAPs start reporting garbled audio while others report an inability to obtain location information. At 0600, some PSAPs are reporting that they have not received a call in the last 15 minutes.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			

Bidder Response:

CenturyLink would designate this as a Severity 1 (service impacting) issue.

CenturyLink actions would be as follows.

Restoration and Resolution Timeframes

CenturyLink and its subcontractors will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

GEN SCEN 1 Table 1. Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1*	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able to reach PSAP. Critical network or data communications problem on a system that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered	Immediately upon detection, but no longer than 10 minutes after determination of CTL impact	Target Mitigation = 30 minutes Target Resolution 2 hours	Hourly
Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every 4 hours or mutually agreed timeframe
Severity 3	Routing services are impaired, and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no longer than 1 hour after detection	</= 7 days	Every 8 hours or mutually agreed timeframe.

Root Cause Analysis Report:

Root Cause Analysis (RCA) report for Severity Level 1 or 2 service disruptions will be available within ten (10) Business Days following the resolution of a Severity Level 1 or 2 Service Disruption outlining the conditions that caused the trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

- Date/Time of the start of the service disruption.

- Date/Time of service restoration.
- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s).
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.
-

GEN SCEN 1 Table 2: Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1*	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able to reach PSAP. Critical network or data communications problem on a system that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered.	Immediately upon detection, but no longer than 10 minutes after determination of CTL impact	Target Mitigation = 30 min, Target Resolution 2 hours	Hourly
Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every4 hours or mutually agreed timeframe
Severity 3	Routing services are impaired, and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no longer than 1 hour after detection	</= 7 days	Every 8 hours or mutually agreed timeframe.

Any additional documentation can be inserted here

GEN SCEN 2	**Scenario 2** All originating service providers in the state are connected directly via Signaling System Number 7 (SS7) protocol to the bidder's LNGs that serve the PSAPs in Nebraska, as well as others outside the Commission's footprint. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. One of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of the prior day's logs, it is found that the two surviving LNGs only are processing 2,000 calls each.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

CenturyLink would initially designate this as a Severity 2 (routing services are impaired) issue, but upon review would change the classification to a Severity 1 (severely impacted). Once the perceived call volume mismatch is detected CenturyLink will, until proven otherwise, assume that calls were/are being impacted by this outage.

CenturyLink actions would be as follows.

Restoration and Resolution Timeframes

Initial Classification: CenturyLink and its vendors will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within four (4) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

Updated Classification: CenturyLink and its subcontractors will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

GEN SCEN 2 - Table 1. Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able to reach PSAP. Critical network or data communications problem on a system that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered	Immediately upon detection, but no longer than 10 mins after determination of CTL impact	Target Mitigation = 30 minutes, Target Resolution 2 hours	Hourly
Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every 4 hours or mutually agreed timeframe
Severity 3	Routing services are impaired and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no	</= 7 days	Every 8 hours or mutually

		longer than 1 hour after detection		agreed timeframe.

Root Cause Analysis Report

A Root Cause Analysis (RCA) for Severity Level 1 or 2 service disruptions will be available within ten (10) Business Days following the resolution of a Severity Level 1 or 2 Service Disruption outlining the conditions that caused the trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

- Date/Time of the start of the service disruption.
- Date/Time of service restoration.
- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s)
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.

GEN SCEN 2 - Table 2. Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able to reach PSAP. Critical network or data communications problem on a system that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered	Immediately upon detection, but no longer than 10 minutes after determination of CTL impact	Target Mitigation = 30 minutes, Target Resolution 2 hours	Hourly
Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every 4 hours or mutually agreed timeframe

	Severity 3	Routing services are impaired and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no longer than 1 hour after detection	</= 7 days	Every 8 hours or mutually agreed timeframe.	

Any additional documentation can be inserted here

GEN SCEN 3	**Scenario 3** As part of normal data-maintenance procedures, the bidder has uploaded six minor recent changes. The bidder's Quality Assurance/Quality Integrity (QA/QI) process provides a discrepancy report detailing 15,000 errors resulting from the updated file.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our NG9-1-1 Spatial Interface (SI) and Location Database (LDB) are built to deal with this exact scenario. Specific features are built within the interface to detect and prevent ECRF updates for errors exceeding a certain tolerance level. These levels are based on the specific layer: street, fire, ESX, etc. CenturyLink would not designate this as a Severity 1, 2 or 3 issue. Call routing would never be affected since the SI is designed to know when there is a problem and stops the changes from being committed to the ECRF. CenturyLink provides standard automated processing reports as part of the SI interface. If more information is needed, established processes and procedures would be utilized to reach out to the CenturyLink LDB/GIS analyst for further investigation and resolution.				

Any additional documentation can be inserted here

GEN SCEN 4	**Scenario 4** At 0700, the NOC has received an alarm reporting loss of connectivity for a single path to Host A. At 0705, the NOC contacts Host A to confirm the loss of connectivity. The PSAP has found that the link lights are off, but the system appears to be operational. At 0725, the redundant link appears to be bouncing for Host A. At 0900, the PSAP is reporting a decrease in typical call volume.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:
This incident would be initially designated as a Severity 2 (routing services are impaired) issue, but upon review would change the classification to a Severity 1 (severely impacted). Once the perceived call volume mismatch is detected CenturyLink will, until proven otherwise, assume that calls were/are being impacted by this outage.

CenturyLink actions would be as follows.

- As part of normal operations, The NOC actively monitors all paths between PSAPs and the core processing locations. When a path or device fails, the NOC sees alarms and begins troubleshooting. All alternate and paths for PSAP connectivity are pre-tested during integration and turnup. Any issues with failover will be addressed prior to turning the PSAP live.
- At 7:25, the team's priority would be to evaluate if there is any risk of 9-1-1 call or data degradation. Since the redundant path is not reliable(bouncing), and although the system is configured to do this in an automated fashion, the recommendation to force automated failover of all calls would be made. This would allow for reduced failover timing and/or other possible unforeseeable impacts.
- This situation would be worked at the highest priority with our NG9-1-1 team assigned to work the issue to resolution. CenturyLink would continue to work troubleshooting the issue from a circuit perspective and verify with internal test calls to the effected PSAP.
- Once a single link was brought back into service, a joint decision would need to be made by CenturyLink and the PSAP on whether or not to bring the PSAP back up one-sided (understanding the previous instability). In a typical environment, although not preferred, a one-sided solution is temporarily acceptable. For this particular situation and the history of one-sided issue with possible call impacts, a real-time decision would need to be made. Tools (call tracing, MOS evaluation, and test call validation) will be critical in determining next steps.
- After the event, CenturyLink NG9-1-1 team would perform a root cause analysis to determine the factors that led to the concurrent failure. While it is possible that they were unrelated coincidental events, CenturyLink's engineering staff is skeptical of such coincidences and so would strive to understand the situation so as to prevent a reoccurrence if possible.

GEN SCEN 4 - Table 1. Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able	Immediately upon detection, but no longer than 10 minutes after	Target Mitigation = 30 minutes,	Hourly

	to reach PSAP. Critical network or data communications problem on a system that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered	determination of CenturyLink impact	Target Resolution 2 hours	
Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every 4 hours or mutually agreed timeframe
Severity 3	Routing services are impaired, and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no longer than 1 hour after detection	</= 7 days	Every 8 hours or mutually agreed timeframe.

Root Cause Analysis Report

A Root Cause Analysis (RCA) for Severity Level 1 or 2 service disruptions will be available within ten (10) Business Days following the resolution of a Severity Level 1 or 2 Service Disruption outlining the conditions that caused the trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

Date/Time of the start of the service disruption.

- Date/Time of service restoration.
- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s)
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.

GEN SCEN 4 - Table 2. Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Resolution Time	Status
Severity 1	Inoperative/Severely Impacted - PSAP not receiving calls, audio is working on only one side of incoming calls, End Office traffic not able to reach PSAP. Critical network or data communications problem on a system	Immediately upon detection, but no longer than 10 minutes after determination of CTL impact	Target Mitigation = 30 minutes, Target	Hourly

		that prevents transmitting ANI to the PSAP, and/or network hardware, or circuit. All FCC reportable outages are considered		Resolution 2 hours	
	Severity 2	Routing services are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.	As soon as possible, but no longer than 30 minutes after detection identification	4 hours	Every 4 hours or mutually agreed timeframe
	Severity 3	Routing services are impaired and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 call delivery.	As soon as possible, but no longer than 1 hour after detection	</= 7 days	Every 8 hours or mutually agreed timeframe.

	Project Management and Ongoing Client Management Services **Project Management Methodology** 1. Describe bidder's project management methodology and support structure. 2. Describe the daily, weekly, and monthly interactions during the migration. 3. Include a proposed high-level project plan. 4. Include a schedule for the through implementation of this project.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
PM 1	Bidder Response: A detailed Program Development Plan has been included with this proposal, this document outlines both the implementation project management approach and the overall Program Management approach for the lifecycle of the contract. A regular communications cadence will be established with the State, to include weekly status meetings, a detailed order tracker to be delivered prior to the weekly status meetings, monthly overall Program level meetings and quarterly Program Review meetings will also be established. A draft schedule has also been included, as an attachment, outlining all tasks and timeframes necessary to complete the implementation of the project.				

Any additional documentation can be inserted here:

	Project Management and Ongoing Client Management Services **Post-Deployment Client Management** Describe the post-deployment client management service, including client management reports, executive briefings and the fielding of ad hoc support requests.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
PM 2	Bidder Response: As outlined in the attached Program Deployment Plan, the Program Manager will maintain both project and program level oversight for the entire lifecycle of the contract, The assigned support teams are provided in detail in the PDP, which also outlines their respective roles and responsibilities for the contract lifecycle.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

TRN 1	**General Requirements – Training** **Comprehensive Training** Contractor shall provide comprehensive training to designated Commission representatives responsible for varying layers of network/system monitoring and system maintenance. Describe bidder's training program for system implementation and ongoing operation and maintenance, including but not limited to the following topics: 1. user-configurable elements; 2. NOC/SOC procedures; 3. escalations; 4. trouble reporting; 5. help desk portal; 6. executive dashboard; and, 7. service monitoring tools. Training shall be available at the user level and delivered to the PSC and each region (up to 10) and also the train-the-trainer level (up to 25 individuals).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The CenturyLink Program Manager will work with the state to identify the individuals requiring training, as well as the types of training required. As outlined in the attached Program Development Plan the training programs include but are not limited to the above requested trainings.				

Any additional documentation can be inserted here:

TRN 2	**General Requirements – Training** **Attendees and Curriculum** 1. Describe the number and types of attendees required to attend training, training curriculum, number of training attendees included in the proposed price, and the duration of the training program per attendee (expressed in hours per day and number of days), as well as the location of the training and whether such training is available online or onsite. Preference is given to training that can be conducted in an onsite setting for attendees. 2. Provide Examples of the proposed training plans. 3. Provide a sample of the training materials to be used. Training classes shall be recorded for future reference and training of new Commission and PSAP employees.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The CenturyLink Program Manager will work with the state to identify the individuals requiring training, as well as the types of training required. As outlined in the attached Program Development Plan the training programs include but are not limited to the above requested trainings.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SRAR 1	**General Requirements – Service, Repair and Advance Replacement** The Commission shall not be responsible for the replacement and maintenance of hardware and software required to provide the NGCS or ESInet connectivity provided as part of the bidder's solution. The Contractor shall resolve all faults or malfunctions at no additional cost to the Commission. **Support Maintenance** 1. Describe in detail bidder's 24 x 7 x 365 maintenance support for the life of the contract. 2. Describe bidder's understanding of public safety maintenance windows and associated notification processes. 3. Describe bidder's problem resolution and change management processes, the supporting systems, and adherence to best practices, such as those described in the ITIL version 3 or most current version.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: A detailed description of trouble management, trouble ticket handling, planned maintenance and change management can be found in the attached Program Development Plan. CenturyLink maintains a 24 x 7 x 365 Public Safety NOC dedicated to ensuring that and service effecting event is minimized and resolved as quickly as possible. A full escalation matrix is provided in the draft PDP, as well as additional service management contacts that are available to the state at all time to ensure quick resolution of any issue.				

Any additional documentation can be inserted here:

SRP 1	**General Requirements – Software Release Policy** **Scheduled Releases** **Frequency of Scheduled Releases** 1. Describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release. 2. Include a current roadmap of feature updates and additions with projected release by quarter and year.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Since CenturyLink provides a NG9-1-1 solution tightly governed by demanding SLAs (which are based on current NENA doctrine), it is a core business imperative that we maintain compliance with relevant NENA standards. As industry standards evolve, this solution will be upgraded to maintain compliance with the current version of established industry standards. It will support new IP network and security industry standards within 18 months of ratification of applicable industry standards. Compliance requirements apply also to the supporting standards referenced within each standard. As solution updates are made to maintain compliance, the solution will not automatically abandon services or feature functionality in place at the time of the upgrade. Instead, we will identify the impact of any performance or feature changes prior to the upgrade and report them to the state approval Software provided by CenturyLink is tested and certified as free from defects in material, design, and workmanship. Software will be tested before it is considered ready for production. Our Microsoft base Team Foundation Server (TFS) tool will be used as the internal tool for tracking features and errors during the development process. Following the reception of a feature request or an error report in Freshdesk from a customer's or internally, an entry in TFS is created with as much details as available. Our NGCS operating system is based on the Microsoft 2010 platform. Patches, fixes and updates are provided per the MS schedule with all changes implemented within 30 days of notification. Immediate security fixes, however, will be implemented as soon as notification is received. CenturyLink software development process will be based on the Agile methodology and will use a 30-day sprint cycle. At the start of each sprint, a determination will be made of what content the sprint will consists of. The decision will be made using the backlog that contains feature requests and any errors previously identified. Unless the sprint contains customer features, customer raised errors or high severity features and requests, a release will not be scheduled. The criteria used to determine the content of the sprint is simple as follows: • Any high priority errors or features are automatically included in the sprint. • Less critical defects are considered by age, 30-180 days and included appropriately. • Customer raised features or errors are always given priority. Then, if the sprint capacity permits it, normal severity errors or features are included in the sprint. • The decision of including normal severity errors or features is based on criteria such as market demand for features, staffing level, workload and internal business direction.				

- In the event that a critical feature or error is reported, the error or feature will immediately be scheduled for enhancement, and all current work in the sprint will be postponed until the critical issue(s) is/are resolved. In this case, a new software release will be developed and released to customers following the successful completion of the new release.
- Automated unit tests are created and performed continuously by CENTURYLINK developers when a feature or defect is being implemented. When the new software release is built, the entire set of automated unit tests are performed again to ensure the build was successfully performed. Upon successful completion of the build, the software is tested in the CENTURYLINK lab. The CENTURYLINK lab environment is configured such that it is a replica of the CENTURYLINK production environment. Tests performed on the lab are two-fold: release content and regression tests. The tests performed for the release content ensures the requirements have been met for the new features or for resolving the defects. Regression tests are performed to ensure that no other system functionality has been affected by the new features or defects resolution.
- If a discrepancy is noted, the system automatically holds an update or flags the offending data and produces an automatic report to an establish call list. There are a number of reports available.
- If appropriate, documentation of release notes will be available to Customers at least thirty (30) days before implementation. This documentation will detail the deployment process and provide a timeline for scheduled and maintenance releases. It will also contain a description of how releases shall be tested.

Updates are issued according to the criticality of the issue confronted but generally will be made to ensure software conforms to NENA and industry standards. Upgrades are normally scheduled annually. Fixes are applied according to the criticality of issue confronted. Routine fixes will be addressed semi-annually or sooner if dictated by a software manufacturer. The chart below indicates how we manage software changes:

Nature of Change	Implementation
Reaction to immediate threat to basic call delivery	ASAP using patch or update testing and deployment
Projected threat	Included in current software sprint development process or in specially initiated sprint if no current sprint is ongoing (The STI software development process is based on the Agile methodology and will use a 30-day sprint cycle. At the start of each sprint, a determination is made on content the sprint will address).
Significant capability enhancement or elimination of major operating flaw.	Included in next sprint cycle, tested, approved and deployed usually within three to six months.
Routine change in standards	Included in annual update.

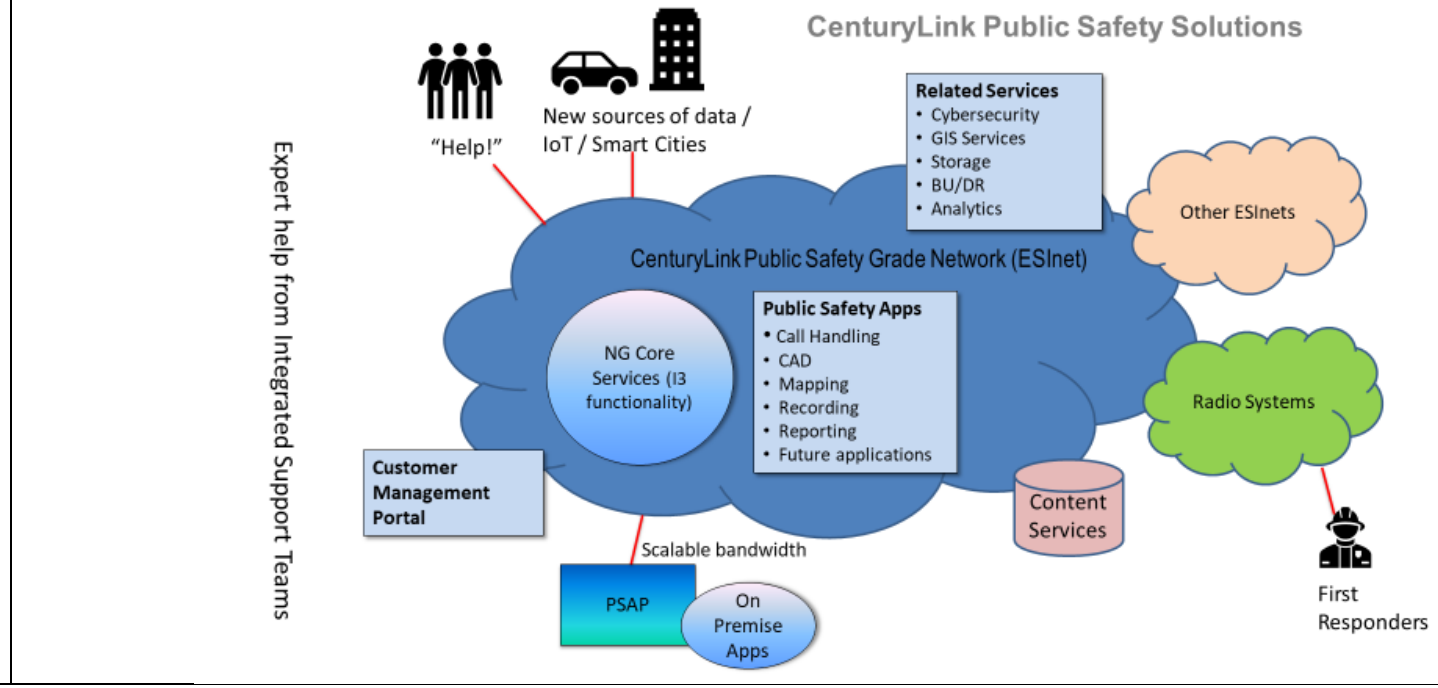
Regardless of the nature of the change, three rules apply:

1. Changes are tested in an isolated environment, never in the production sphere.
2. Any change is submitted for agency approval prior to implementation. Routine changes are often covered by an operating agreement.
3. Changes are implemented according to a plan that ensures no disruption of critical services.

The criteria used review a change is simple. Four factors will determine precedence: (1) Criticality; (2) Compatibility; (3) Operational Impact and (4) Budget:

	1. Criticality: A critical threat or deficiency identified by a reliable agency such as NENA or through verified customer reports will take precedence. Compatibility issues must be identified and resolved immediately, or workarounds devised. A fallback plan must be in place. Less critical issues will be dealt with through the sprint process, normal compatibility and acceptance test protocols and routine project management. 2. Compatibility: Any change impacts other programs and components. Normally, we rely on manufacturers to complete a robust compatibility test and then run the system with the change in a test environment to ensure compatibility. This might not be possible in emergencies. In such cases, we rely on compartmentalization of the change and limited compatibility testing involving major related programs. Our engineering team then runs a limited test environment review. 3. Operational impact: Any change is disruptive. Training may be impacted, other systems may require updating, cutover must be phased to guarantee no loss of operational integrity is experienced, etc. The degree of impact will influence the timing and nature of the implementation. 4. Budget: Critical changes excluded; an implementation must acknowledge the fiscal environment in which a client operates. That can dictate procurement, scheduling and cutover. Budget dictates whether parallel systems can be maintained during cutover. Clients are offered a cost/benefit analysis before routine changes are implemented. Our present roadmap is focused on ensuring our NGCS suite remains complaint with the NENA standards and other guidance that governs its usage. As such, our product enhancement effort is centered on draft changes such as those that might come with the publication of STA.010.3. We are looking at additional feature and functionality including: • E-bonding interfaces with other ESInet's and providers where we are working with major producers to enhance the scope of this product. • Dashboard and portal management which we expect will be influenced by emerging technologies that will improve the quality, scope and the user friendliness of our present portals and dashboards. ESRP queueing features is another significant initiative. While our GIS offering is quite robust, this is another area where improved technology is extending the reach of available data. Working with several GIS vendors, we are trying to simplify the user experience with machine learning and AI affects.

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



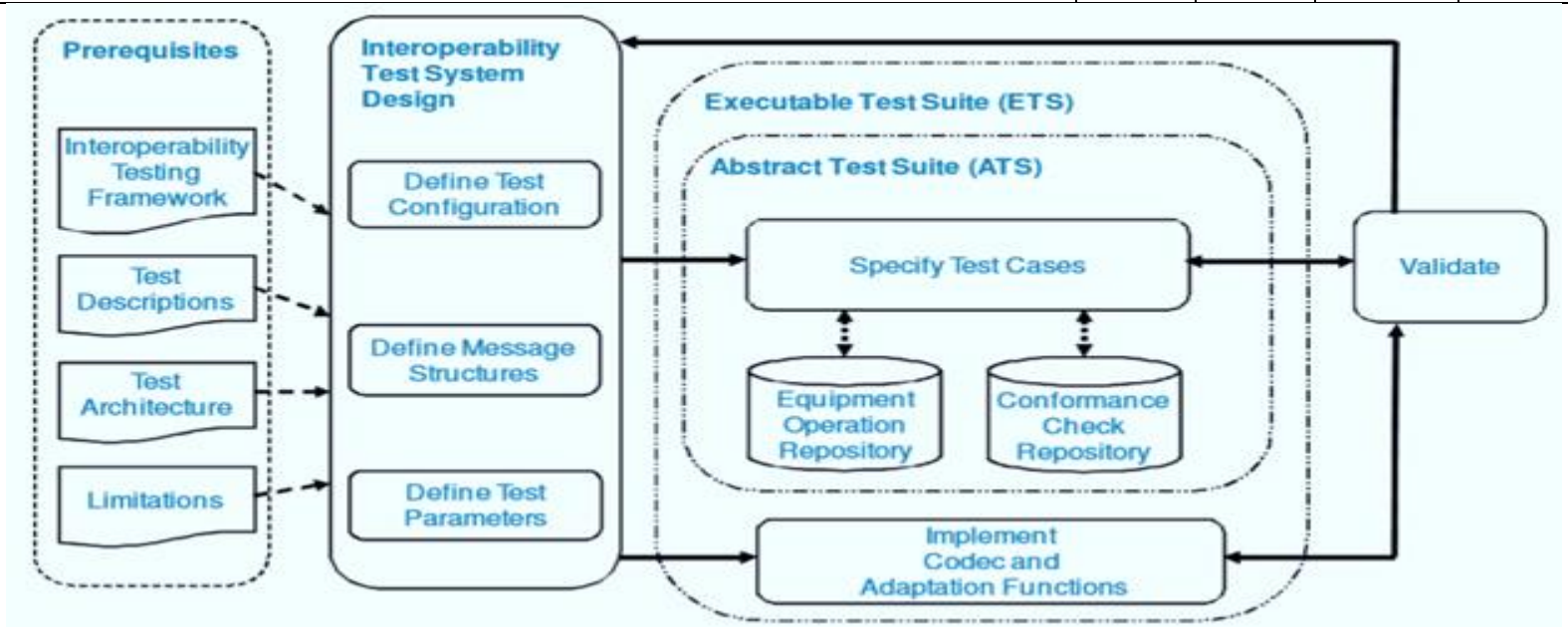
Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SRP 2	**General Requirements – Software Release Policy** **Maintenance Releases** Describe the frequency of defect-resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: As software maintenance updates and service packs are released by manufacturer, we test these release in our CenturyLink lab prior to releasing them into a live customer environment; this includes Approval For Use (AFU) which certifies new software release upon successful completion of FOA soak period. This ensures that our vendor solutions will work in a real-world environment and not just in the vendor's labs. The following defect-resolution occurs: (1) Ticket (change request) is created and reviewed by our technical architectural cross-functional team *(2)* A disposition will be made. Normally this can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. (*A disposition is typically made within two weeks or sooner depending upon the severity of the issue).* *(3)* Frequency of defect resolution includes must fix' defects (call delivery impacting) Normally these maintenance releases are rolled into the release immediately following the time of discovery within 6 months or earlier. *(Defects characterized by the customer as minor will be prioritized in vendorship with the customer.)* The decision-making process for choosing what features and defect resolutions to include in a scheduled release is primarily driven by customer guidance, market demand, and maintaining compliance with NENA, ATIS, and other organizations that contribute to standards for emergency call services including: • The decision-making processes involved in selecting which software features to provide are based on standards updates and market demand. • A typical annual release schedule includes one major software release with up to two minor releases as required. • The decision-making processes involved in selecting which software defects to fix is done in vendorship with the customer. All defects are assessed, managed, and scheduled by the Change Control Board. • Critical and Major defects are managed as soon as discovered and communicated by the customer. The initial solution may be a manual process. A long-term solution will be with the next ESInet platform code release. Minor defects are reviewed within three weeks of discovery and communication by the customer. The solution will be ranked against other defects and enhancements and road-mapped appropriately. • Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has installed in production, we will follow up with the customer to make sure the issue has been resolved. • The decision-making process for choosing what features and defect resolutions to include in a scheduled release is primarily driven by customer guidance, market demand, and maintaining compliance with NENA, ATIS, and other organizations that contribute to standards for emergency call services. Software releases occur approximately once annually for major releases and twice annually for minor releases.				

Any additional documentation can be inserted here:

SRP 3	**General Requirements – Software Release Policy** **Test Environment** Prior to install of new releases, bidder shall explain how Contractor replicates the production environment for software release testing to provide assurances that future software releases will not negatively impact PSAP operations.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			



SRP 3 - Interoperability test model. Note Not all elements are tested each time:

Any additional documentation can be inserted here:

SRP 4	**General Requirements – Software Release Policy** **Access to Defect Tracking System** Contractor shall provide the Commission with access to the Contractor's defect tracking system for the Commission to track the progress of defect resolutions. **Software Defect Tracking Process** Provide a detailed description of the software defect tracking process and describe how bidder will provide training for no more than ten (10) Commission staff prior to Final Acceptance Testing.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The frequency of defect resolution software releases is driven to some extent by the nature of the defect. 'Must fix' defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will typically make the fix available within 6 months if not earlier. Defects characterized by the customer as minor will be prioritized in vendorship with the customer. The decision-making processes involved in selecting which software defects to fix is done in vendorship with the customer. All defects are assessed, managed, and scheduled by the Change Control Board. Upon discovery and communication by the customer, a ticket (change request) is created and reviewed by a cross-functional team with representatives from CenturyLink Engineering, product and NE Representative. A disposition is typically made within 3 weeks or sooner depending upon the severity of the issue. A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has installed in production, we will follow up with the customer to make sure the issue has been resolved. CenturyLink will provide training to any commission staff and provide monthly reports on the defect tracking as required. This can will be accomplished via our CenturyLink Web Base training portal. CenturyLink includes training for this process to all Nebraska stakeholders.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SRP 5	**General Requirements – Software Release Policy** **Software Defect Aging** Describe how service-affecting software defects are aged. If minor problems (from the Contractor's perspective) are not identified and resolved immediately, these minor problems can become major or critical problems. Describe in detail how/when this minor problem gets scheduled or automatically escalated, and the feedback mechanism in place for keeping the Commission informed.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink has detailed comprehensive defect tracking process as part of our defect tracking tools, including Jira, Trac and others. . Critical and Major defects are managed as soon as discovered and communicated by the customer Critical and Major defects are managed as soon as discovered and communicated. The initial solution may be a manual process. CenturyLink utilizes our product roadmap and the Service Enhancement Request process to track the status and prioritize the enhancement with other Product Roadmap improvements. Must fix' defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will typically make the fix available within 3-6 months if not earlier. Any high priority software defect errors or features are automatically included in our development sprint. Less critical defects are considered by age, 30-180 days and included appropriately. The status of any defect is reflected in our ticketing program and is available for viewing by authorized individuals. Refer to section SRP 1 for additional information Minor defects are reviewed within three weeks of discovery and communication by the customer. The solution will be ranked against other defects and enhancements and road-mapped appropriately. Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has been installed in production, we will follow up with the customer to make sure the issue has been resolved. Upon discovery and communication by the customer of a "minor" defect, a ticket (change request) is created and reviewed by a cross-functional team. A disposition is typically made within three weeks or sooner depending upon the severity of the issue. A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. The decision-making processes involved in selecting which software defects to fix is done in vendorship with the customer. All defects are assessed, managed, and scheduled by our program manager in our Change Control Process (CCP). CenturyLink will provide monthly reports on defects to all Nebraska stakeholders and the commission.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

DOC 1	**General Requirements – Documentation** The Contractor shall provide the Commission with all pertinent documentation for the ESInet and/or NGCS connectivity provided as part of the Contractor's solution as implemented, No more than 30 days after completion of the network construction, and update the Commission as configurations change over the term of the contract. The required documentation shall include the following: **1.** Detailed project plan; **2.** Escalation procedures; **3.** Circuit identification; **4.** Single points of failure; **5.** Network path diversity drawings into each PSAP; **6.** Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system; **7.** PSAP backroom as-built drawings; **8.** PSAP demarcation point drawings; and, **9.** All user interface training and reference materials. **Network As-Built Documentation** Upon implementation, Contractor shall provide a network or solution diagram that clearly depicts the Contractor's solution as implemented. The Contractor shall provide all documentation in agreed-upon electronic format via a Contractor-hosted web portal. Please describe how bidder's solution meets or exceeds this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Documentation will be provided for our NGCS and ESInet components as implemented, and the State will be updated as configurations change are made over the term of the contract. A user interface to retrieve and customize reports upon request will be provided. Documentation will be provided in hard and soft copy format for the following elements: 1. All build-to documentation or planned drafts within 120 calendar days of contract execution 2. Final as-built documentation within 30 calendar days of the deployment of the first PSAP 3. Any documents related to changes to the solution within 30 calendar days of the completed change, or mutually agreed upon date of system acceptance/change/modification to the system as noted above				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

<table>
<tr><td rowspan="2">ESI 1</td><td>Emergency Services IP Network (ESInet)
Diversity
The network shall be designed with diverse entrances (e.g., east-west entrances) into specified buildings that are part of the ESInet. This requirement shall apply to the core network sites, including data centers and PSAPs specified in Attachment A - PSAP Host End-Point Locations, Equipment List and Selective Router Locations. Primary and redundant links shall not share common routes, trenches, or poles. If last-mile facility or building construction is required, bidder shall so indicate. If this is not possible at a given location, indicate how bidder intends to provide redundant and resilient connectivity to that location. Describe how bidder's solution meets or exceeds the above requirement.</td><td>Comply</td><td>Partially Comply</td><td>Complies with Future Capability</td><td>Does Not Comply</td></tr>
<tr><td></td><td>X</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">Bidder Response:

If last-mile facility or building construction is required, bidder shall so indicate.

Locations that require fiber build outs:

• South Central Region-Dawson
• South Central Region-Dawes
• Southeast Region-Windstream DC
• North Central Region-Cherry
• Metro Region-Douglas
• Metro Region-Pottawattamie
• West Metro Region - Fremont-New Region
• Northeast Region - City of Norfolk -New Region(Under Development)
• Northeast Region - City of South Sioux City-New Region(Under Development)
• Wayne County - City of Wayne

Note: All construction costs are included in our proposal.

If this is not possible at a given location, indicate how bidder intends to provide redundant and resilient connectivity to that location.

CenturyLink will be providing diverse entrances (east-west entrances) for core network sites, data centers, and PSAPs.

Describe how bidder's solution meets or exceeds the above requirement.

Core network sites

As a leading global network provider, all of CenturyLink's Points of Presence (POP) are designed with diverse fiber paths, redundant MPLS Priv routers that home to a pair of diverse MPLS PCore routers. To further diversify our solution, CenturyLink takes advantages of our purchase of Level 3's network assets to provide both POP diversity and carrier diversity.

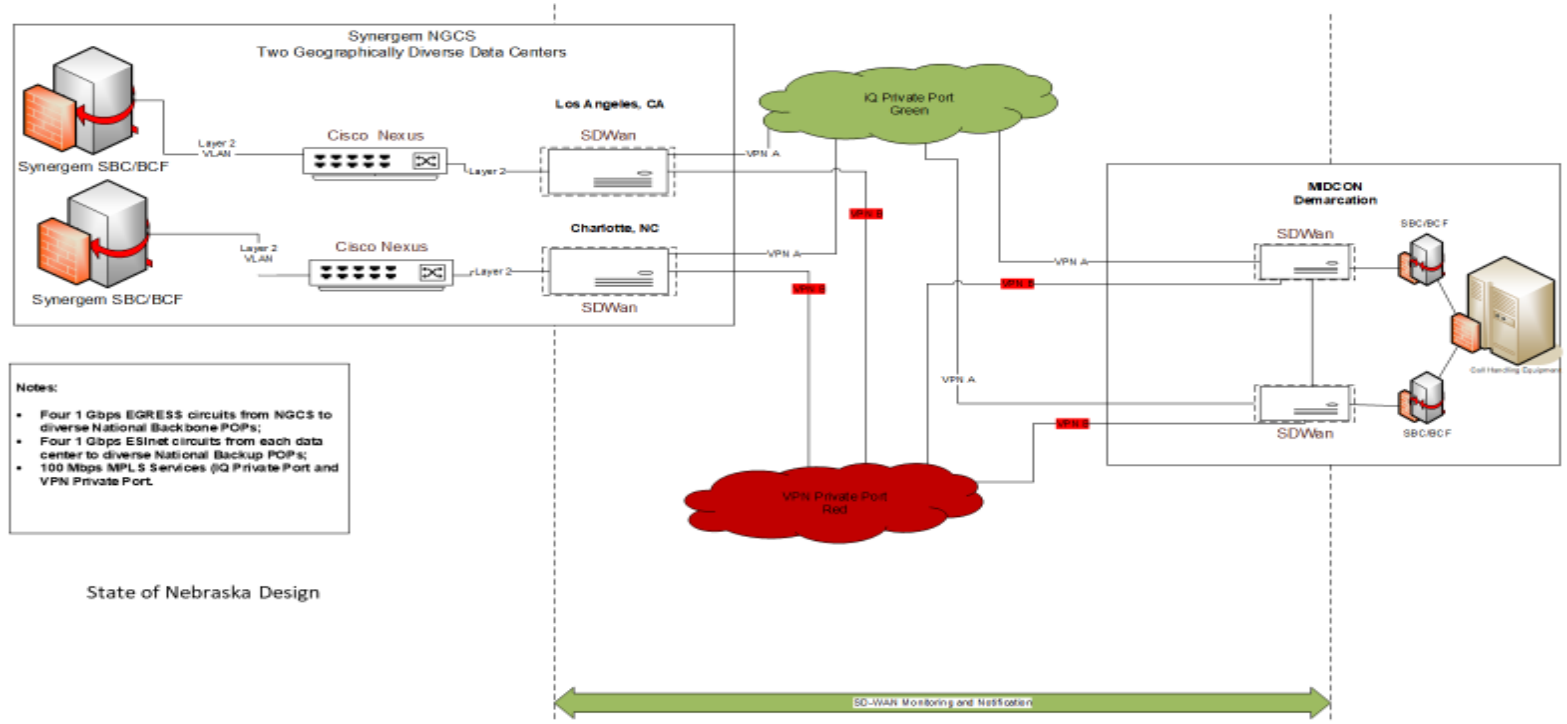
We do this by homing Circuit A to a geo-diverse POP using our IQ Private Port cloud, and Circuit B a geo-diverse POP to our IP VPN cloud. Each MPLS cloud runs on its own network core and backbone, have separate management systems, and are completely independent of each other.</td></tr>
</table>

Data Centers and PSAP

At data centers and PSAPs, we provide last mile diversity in one of three ways.

1. CenturyLink will build new fiber facilities to a new entrance at the PSAP
2. CenturyLink will provide our local access for circuit A and will contract with another provider to place a diverse fiber connection to the location
3. CenturyLink will contract with another provider to provide diversity, our build diversity to the location.

Where we do use a 3rd party provider, CenturyLink has established NNIs or meet points to connect to our two national MPLS networks. These NNIs are all fiber-based facilities.

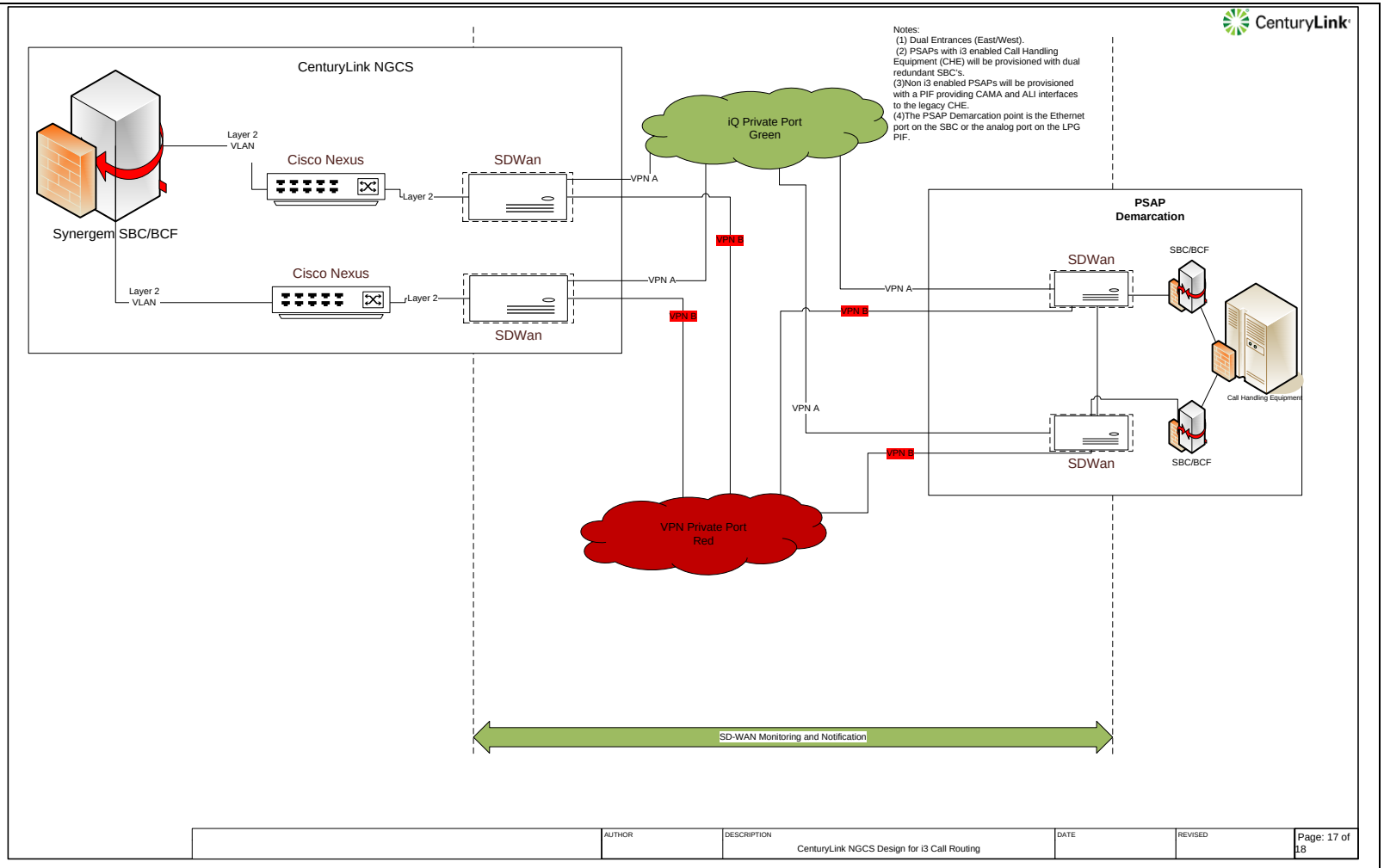


ESI 1 Diversity

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

ESI 2	**Emergency Services IP Network (ESInet)** **Network Design** Bidder shall design the physical network using the most robust facilities available. Use of fiber-optics is the preferred method for connectivity due to available capacity (bandwidth) and increased reliability. Given the amount of fiber-optic facilities and interconnections between the fiber-optic networks in Nebraska, the ESInet design should include as much fiber as possible, not only on the transport side but on the access side as well. Describe the design of proposed network with specific details on connectivity.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: **Describe the design of proposed network with specific details on connectivity.** As a global network provider, our Network Cores (POPs) are carrier grade and are serviced on multiple OC192 rings. CenturyLink will provide physically diverse fiber with a minimum of dual building entrances with 1G bandwidth to each datacenter from physically diverse CenturyLink Points of Presence (POP). CenturyLink will provide physically diverse fiber with 100mbps bandwidth, scalable to 1G bandwidth, to every host PSAP site from physically diverse CenturyLink POPs. Our handoff to the PSAP call handling equipment from our edge device can be either fiber or copper, depending on what the call handling equipment is able to accept. Please see ESI 1 for detail on POP and carrier diversity				

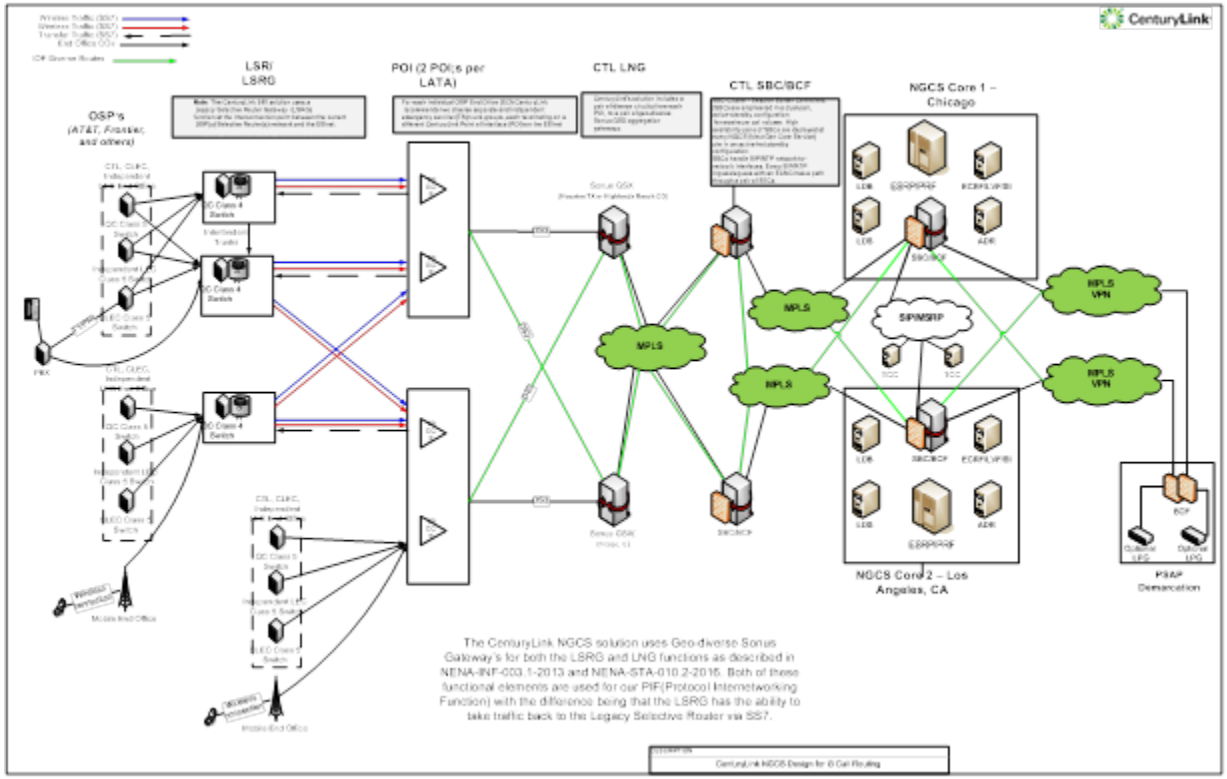


ESI 2 – Dual Entrance Drawing

Any additional documentation can be inserted here:

ESI 3	**Emergency Services IP Network (ESInet)** **No Single Points of Failure** The mission critical ESInet shall be designed with no single points of failure. All equipment shall include redundant processors and power supplies and be supported by an uninterruptible power supply (UPS) system and alternate power source in a properly conditioned environment. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our CenturyLink network is known for its reliability, security and redundancy. It uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission; and it has an availability target of 99.999%. We accomplish this through problem detection, prevention, redundancy, and restoration offers to ensure that the network is always up and running. CenturyLink ESInet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability. CenturyLink NG9-1-1 core and ESInet components are designed and configured for continuous operation. **Core sites** include redundant network transport and redundant network interfacing elements to ensure optimal operation and availability. Network interfacing elements include switches, routers, SBCs, firewalls, and other security devices. CenturyLink's NG9-1-1 solution operates within a highly survivable network architecture. Our solution operates in an **active-active** configuration in each datacenter with redundant, highly available fault-tolerant critical components operating continuously in tandem. If one should fail, the redundant components continue to carry the entire load with no interruption of service. No failover time is required. All applications are deployed on virtual servers and data is shared among and within each data center. These applications leverage H/A functionality within the vSphere hypervisor and associated Snapshots. vMotion, DRS and High Availability (HA) features are utilized to ensure backup and recovery. Our geographically diverse data centers monitor all critical systems automatically 24x7x365. Electronic logs are created and maintained in the system dashboard. This includes an historical record of availability and outage incident tracking. 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). Within each center, data is backed up and recovered based upon global standards and best practices. 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 High Availability (HA) functionality within the hypervisor, DRS and HA features are utilized to ensure an "always on" architecture. Data Center facility requirements address 24x7x365 secured physical access, secured floor space or locked equipment cabinets with controlled access, and monitoring and alarming for all facility elements, such as electrical, heating, cooling, etc. Data Centers include redundancy and diversity in electrical, to include power feeds and Uninterruptible Power Supplies (UPS). The CenturyLink ESInet network implements a design of redundancy upon redundancy. Individual processing elements are redundant at each Core Site and Core Sites are redundant to each other. The failure of any given component at a Core Site will not prevent that Core Site from processing 9-1-1 calls. If a dual failure does occur at a Core Site, or a Core Site somehow becomes unavailable, calls are processed at another Core Site. Any Core Site can process any 9-1-1 call.				

	The ESInet system design is a highly available and highly reliable distributed and redundant architecture with no single points of failure. Key components are redundant within a given geographic site and are also geographically redundant. The loss of any single element will not prohibit call processing functions. The architecture is also extremely scalable to meet current and future needs. The solution includes internal audits and background test capabilities to continuously ensure solution integrity and to detect abnormal conditions. The CenturyLink services maintain the highest system availability. CenturyLink embraces and creates all offerings based upon a "no single point of failure" principle, using fully redundant networks, multi-path, multi-protocol network linking all network elements and PSAPs within the ESInet. All the NGCS and network elements utilize dual power supplies so that a failure on the primary circuit will not disable the operation of the device. CenturyLink facilities and nodes are equipped with physically redundant data communications and power equipment so that any component can be maintained without overall service impact. The facilities and nodes that support the ESInet are equipped with physically redundant data communications and power equipment such that any component can be maintained without overall service impact. A minimum of two, entrances to each facility via diverse facility transport paths and diverse points of interconnection. CenturyLink NG9-1-1 systems are deployed in a redundant, geographically diverse configuration to ensure the highest reliability and survivability. All critical system components are redundant, and the application employs application level monitoring and automated failover to recover from system failures without impact to 9-1-1 call processing. In addition to physically diverse and redundant architecture, network components of the CenturyLink ESInet and associated core services have additional redundancy within each diverse location. CenturyLink carrier grade facilities including POI's and switching centers meet Tier III standards stipulated and developed by the Telecommunications Industry Association (TIA) and the Uptime Institute (UI).

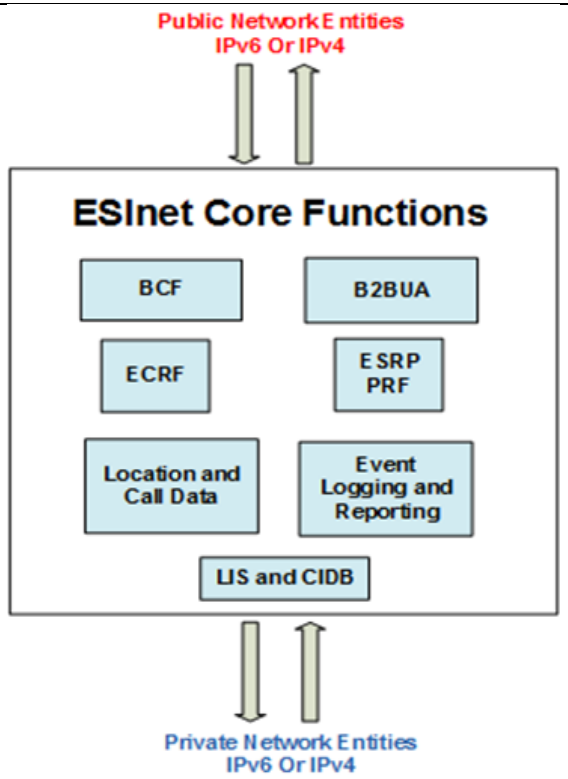


ESI 3 – ESINET Design – No Single Point of Failure.

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

ESI 4	**Emergency Services IP Network (ESInet)** **IPv4 and IPv6 Support** All network equipment shall be new and of current manufacture at the time of implementation. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IpPv6 and have the capability to run dual protocol stacks. Describe how the solution meets or exceeds the above requirement.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: All network **equipment shall be new and of current manufacture at the time of implementation** CenturyLink only provides equipment that is of current manufacture and new. We do not use refurbished, end-of-support, or equipment that is used or found on the gray market. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IpPv6 and have the capability to run dual protocol stacks. The CenturyLink ESInet supports either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards. All network equipment has the capability to utilize IPv4 and IPv6 addresses and is configurable to support dual stack operation. The IPv4 network and IPv6 interfaces are continuously monitored for availability and performance. This is accomplished with the use of a back-to-back user agent session border controller, rather than Network Address Translations (NATs). All devices within the network shall be assigned static addresses.				

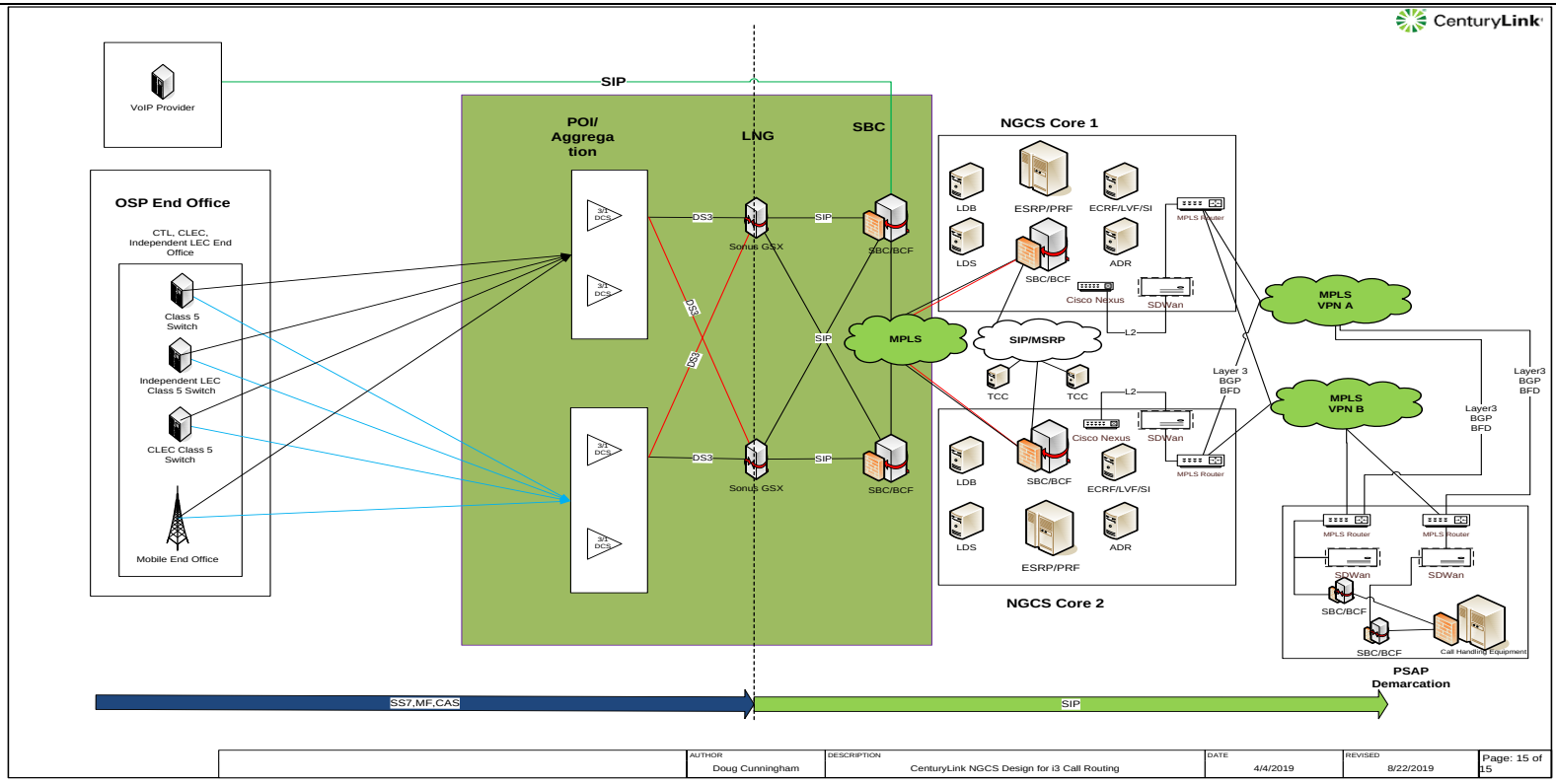


ESI 4: IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

ESI 5	**Emergency Services IP Network (ESInet)** **Open Standards** Open standards-based protocols shall be used, and the use of proprietary routing protocols is prohibited. **Resiliency** Resiliency, or fast failover, may be achieved through the use of the Bidirectional Forwarding Detection (BFD) protocol as defined in IETF Request for Comments (RFC) 5880 and RFC 5881, or other standards-based, non-proprietary methods. Describe how the bidder's solution will achieve resiliency.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink builds resiliency as follows: It starts with our global MPLS networks. Our MPLS network uses all open standard protocols for MPLS services. We route using only industry standard label switching in our core MPLS network. We use BGP (Border Gateway Protocol) as our routing protocol on our network between our network core and edge devices sitting at data centers and PSAPs. While our MPLS network can and will support BFD timers, it is not what we depend on for resiliency or fast failover on our ESInet. We rely on our SD-WAN's ability to do "Packet Replication," which removes the dependency for failover with other protocols such as BFD. Packet replication enables real-time data packet to be duplicated and simultaneously sent over multiple flows to the endpoint destinations while maintaining high VoIP experience over these multiple connections. Packet replication allows for data to be sent between SD-WAN appliances down in parallel down multiple paths. This provides for seamless recovery from degraded paths on UDP applications such as VoIP. At each location, CenturyLink will provide two HA SD-WAN appliances. Circuit A will terminate on SD-WAN appliance 1, and circuit B will terminate on SD-WAN appliance 2. This HA configuration will replicate packets over both circuits. If circuit A was to fail, there would be no fail-over needed since we have replicated the packets on circuit B Our solution can support any open-standard protocol on the PSAP side of the interface such as VRRP if the PSAP is configured to support a pair of HA routers.				



ESI 5 Resiliency - NG9-1-1 BFD Failover Drawing

Any additional documentation can be inserted here:

ESI 6	**Emergency Services IP Network (ESInet)** **Multicast Routing and Switching** Routers and switches must support multicast routing and switching. The applicable base protocols are Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's ESInet solution is capable of supporting multicast routing and switching. Through our SD-WAN appliances, our NG9-1-1 ESInet can support following protocols; Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). Our SD-WAN will support Multicast all variants of PIM: PIM Sparse Mode (PIM-SM), PIM Dense Mode (PIM-DM), Bidirectional PIM (Bidir-PIM), and PIM Source-Specific Multicast (PIM-SSM). Our SD-WAN will also support IGMP. With our SD-WAN devices, we can support both versions of PIM if required. Depending on the application requirement, CenturyLink can configure one or more multicast groups. CenturyLink will work with the Commission to design and configure any required multicast applications required for NG9-1-1 call delivery or to support non-NG9-1-1 applications.				

Any additional documentation can be inserted here:

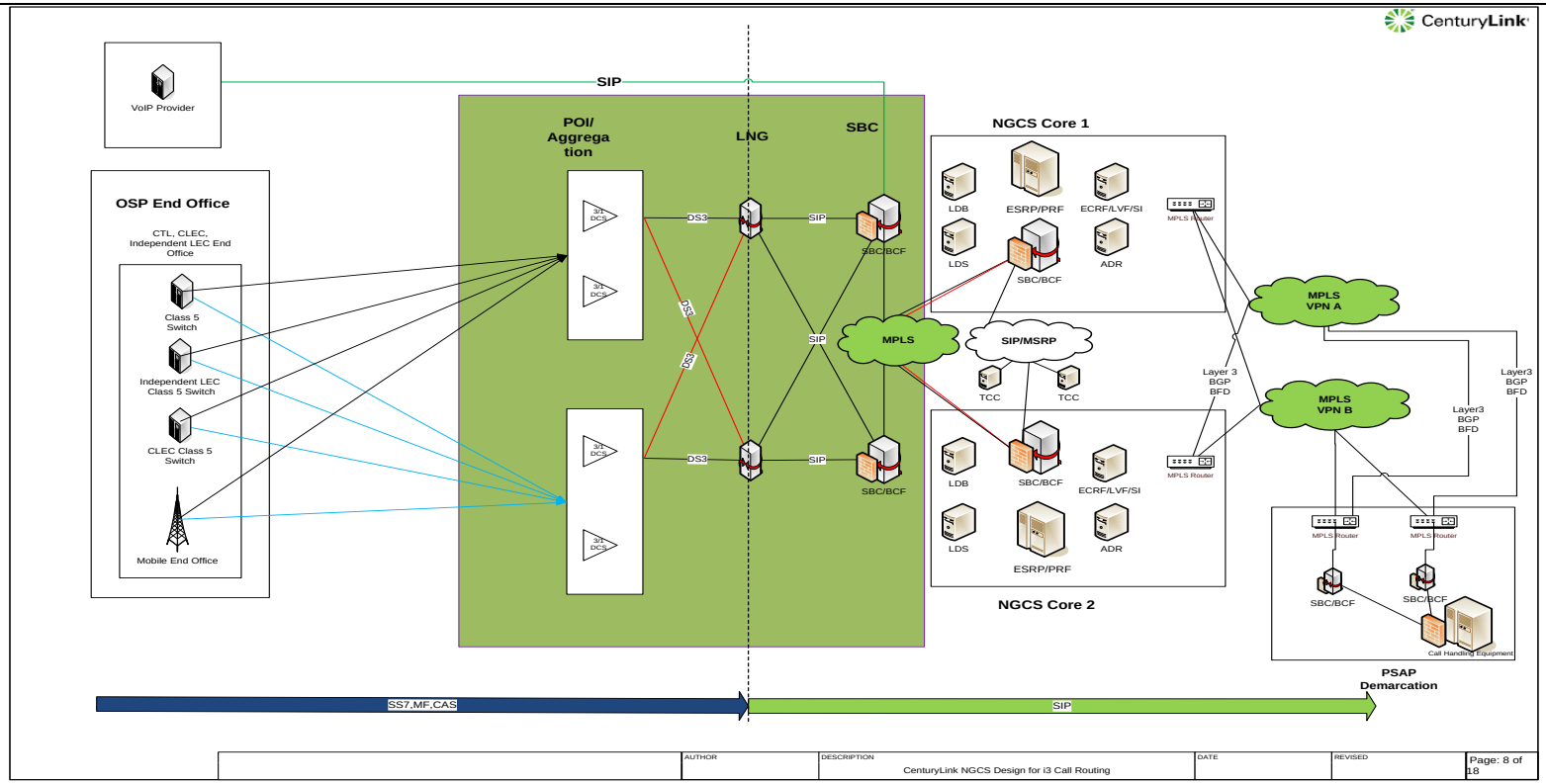
ESI 7	**Emergency Services IP Network (ESInet)** **Quality of Service (QoS)** The network equipment shall support Quality of Service (QoS) marking for prioritizing traffic in the network using the Differentiated Services Code Point (DSCP) protocol. While the network can change DSCP values through rules, the values typically are set by the system or functional element that originates the traffic. Network routers and switches shall not be configured in such a manner as to change DSCP values set by originating functional elements. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink will configure all routing devices and switches to honor DSCP markers and not modify them or reclassify them to other priority queues. If a DSCP marker is destined to a P2 queue, the marker will be preserved and placed into the P2 queue without the devices overriding marker or placing into a P1 queue based on the traffic type.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

ESI 8	**Emergency Services IP Network (ESInet)** **ESInet Properties** The proposed ESInet shall be private, robust, scalable, secure, diverse, redundant, sustainable, and self-healing. Bidder shall propose a network solution for all host sites listed in Attachment A - PSAP Host End-Point Locations and any future identified regions throughout the term of the contract. Describe how the proposed system meets each of these individual requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: **Private**- The CenturyLink ESINet IP network is known for its reliability, security and redundancy. It uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission; and it has an availability target of 99.999%. We accomplish this through problem detection, prevention, redundancy, and restoration offers to ensure that the network is always up and running. CenturyLink ESINet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability. CenturyLink ESINet components are designed and configured for continuous operation. All network routing infrastructure is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology. The CenturyLink ESINet network implements a design of redundancy upon redundancy. Individual processing elements are redundant at each Core Site and Core Sites are redundant to each other. The failure of any given component at a Core Site will not prevent that Core Site from processing 9-1-1 calls. If a dual failure does occur at a Core Site, or a Core Site somehow becomes unavailable, calls are processed at another Core Site. Any Core Site can process any 9-1-1 call. The Core Sites are geographically distributed across the United States and a regional disaster will not remove the ability for CenturyLink ESINet to process 9-1-1 calls, assuming telecommunication transport services for the impacted region are operable. **Scalable** - The core routing and intelligence of the CenturyLink ESInet provides immediate scalability in call routing and data delivery. The Core network and NG9-1-1 services are designed to support very large volumes with geographic diversity of the Core processing centers. The end result is an infrastructure that is public safety grade with respect to capacity, reliability, scalability, and redundancy. CenturyLink's NG9-1-1 Solution deploys on scalable ethernet local access connectivity using bandwidth-flexible infrastructure wherever possible. To accomplish this, we seek to provision connections on fiber facilities wherever possible. Host PSAPS in the proposed solution will be served on fiber connections These circuits are provisioned in an active-active configuration meaning, that under normal circumstances the full provisioned capacity of both circuits is available to handle calls, in contrast to failover type arrangements which only permit use of one circuit's capacity at any given time. Connections to the PSAP are sized up to accommodate necessary bandwidth based on a concurrent G.711 SIP session (Call path). Each circuit is engineered to handle 100% of the call demand in the case of a failure of the primary or secondary circuit. **Secure** - The MPLS VPN tunnels offer a stateful connection across the MPLS cores, so that both ends can quickly identify black holes or other network impairment. In addition, the tunnels are encrypted for security reasons, with AES 256-based IPSEC tunnel protection. Each router at a remote site has two tunnels built from that router over its attached MPLS network to the mGRE hub interfaces at each NG9-1-1 core site.				

	Diverse- The NG9-1-1 solution is designed with diverse entrances into each core call processing facility and each aggregation site (e.g., data centers). The solution uses MPLS networking between sites and avoids commonality of physical or virtual networks utilizing alternate POPs in all designs. CenturyLink's ESInet is designed with diverse entrances into each core call processing facility that is part of the State of Nebraska solution, e.g. data centers. Primary and diverse links do not share common routes or trenches PSAP connections to the ESInet are resilient, physically diverse, and logically separate for delivery of 9-1-1 calls. To meet diversity best practices, two diverse fiber connections are included with our proposal at each Host PSAP site supported by two (2) diverse east/west entrances, two (2) separate edge routers and two (2) separate IP instances. The CenturyLink service utilizes our MPLS private IP network that may include use of third-party network providers that provide the local access and path diversity. These networks are comprised of different components, multiple technical solutions, and various types of interfaces. CenturyLink will work to identify last mile options and if not feasible, design robust alternate route scenarios with neighboring PSAPs Redundant - CenturyLink's **NG9-1-1** core operates within a highly survivable network architecture. Our solution operates in an active-active configuration in each datacenter with redundant, highly available fault-tolerant critical components operating continuously in tandem. If one should fail, the redundant components continue to carry the entire load with no interruption of service. No failover time is required. All applications are deployed on virtual servers and data is shared among and within each data center. These applications leverage H/A functionality within the vSphere hypervisor and associated Snapshots. vMotion, DRS and H/A features are utilized to ensure backup and recovery. Our geographically diverse data centers monitor all critical systems automatically 24x7x365. Electronic logs are created and maintained in the system dashboard. This includes an historical record of availability and outage incident tracking. 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). 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 Self-healing - the CenturyLink NG9-1-1 solution is self-healing as every PSAP has connectivity to the geographically diverse NGCS core sites and diverse aggregation centers. Network connectivity is provided by CenturyLink MPLS network and is guaranteed to be diverse. CenturyLink's NGCS Solution deploys on scalable ethernet local access connectivity using bandwidth-flexible infrastructure wherever possible. To accomplish this, we seek to provision connections on fiber facilities wherever possible. Host - PSAPS in the proposed solution will be served on 100Mbps connections these would be provisioned on upgradeable facilities, allowing for significant future bandwidth growth without changing or adding facilities. These circuits are provisioned in an active-active circuit configuration meaning that under normal circumstances the full provisioned capacity of both circuits is available to handle calls, in contrast to failover type arrangements which only permit use of one circuit's capacity at any given time. Connections to the PSAP are sized up to accommodate necessary bandwidth based on a concurrent G.711 SIP session (Call path). Each circuit is engineered to handle 100% of the call demand in the case of a failure of the primary or secondary circuit.



ESI 8 - ESInet Properties Diagrams

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

<table>
<tr><td rowspan="2">ESI 9</td><td>Emergency Services IP Network (ESInet)
Special Construction
Bidder is responsible for any fees incurred through system commissioning, construction permits, make-ready costs, and other subcontracted activity.

Use of Existing Network Assets
There is already a microwave network in place that may be used as a backup network, as well as other local and state-owned network assets that may be suitable for inclusion in the ESInet. The final network design may make use of any of these facilities that are determined by the bidder to be suitable for inclusion in the ESInet. The bidder may support the router configuration necessary to make use of these facilities.

Network Design Documentation
Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end-state designs for the ESInet.</td><td>Comply

X</td><td>Partially Comply</td><td>Complies with Future Capability</td><td>Does Not Comply</td></tr>
<tr><td colspan="5">Bidder Response: Use of Existing Networks
Special Construction

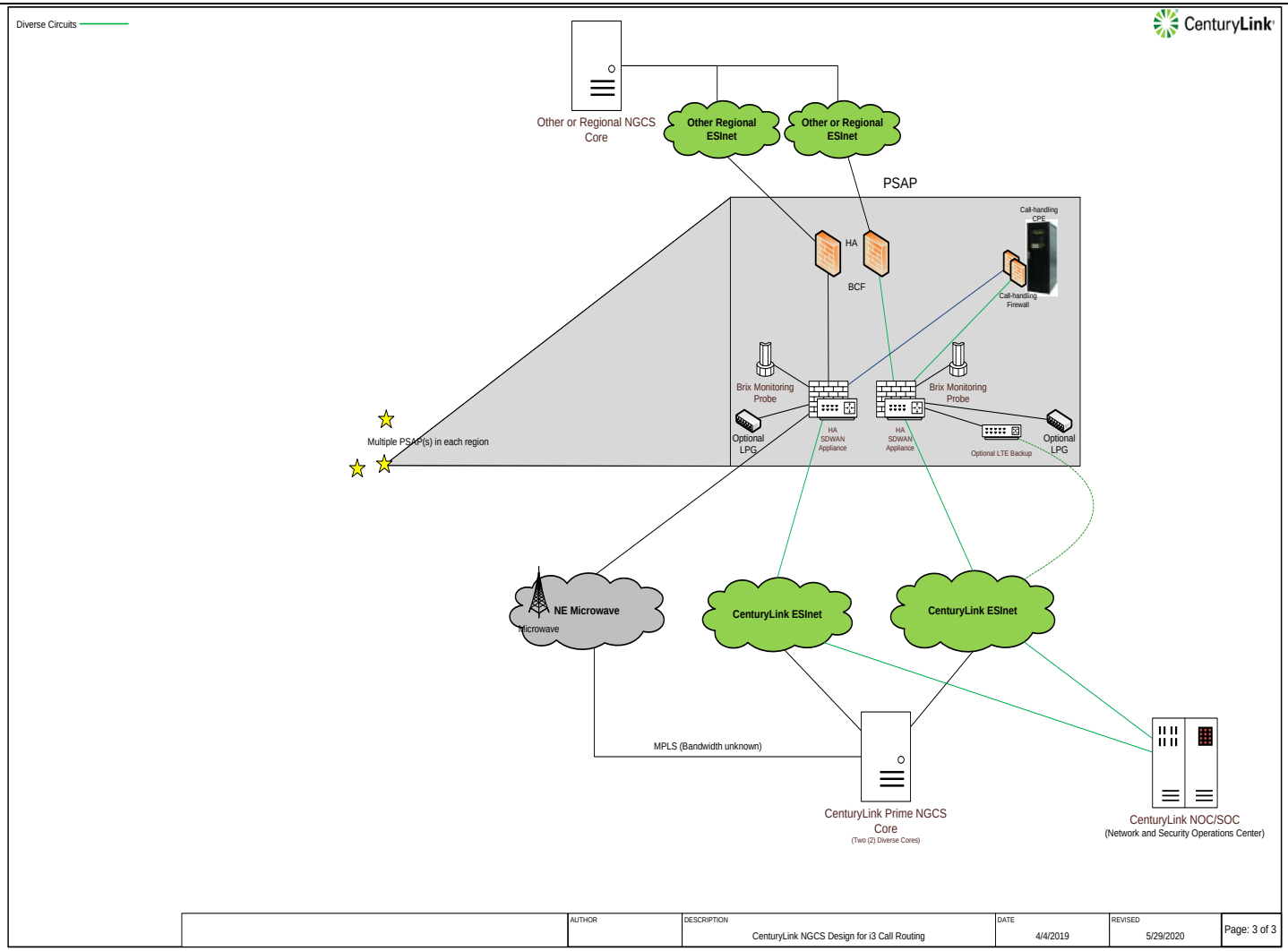
To meet diversity best practices, two diverse fiber connections are included in our design at each Host/PSAP site supported by two (2) separate edge SBC's, two (2) HA SD WAN devices and two (2) separate IP instances.

Our last mile MPLS 100M fiber design includes dual entrances (east/west), includes dual path circuits to all required Host/PSAP facilities identified in this RFP response, and traffic carried over diverse carrier networks. All Special construction charges have been identified and are included in our solution.

Each Host/PSAP site will require a site survey which will be performed by CenturyLink engineers and required Nebraska stakeholders. This task will be scheduled by our Program Manager and will be included in our final Project Development Plant (PDPD).

Use of Existing Network Assets

CenturyLink's design is capable of supporting additional third-party networks such as state microwave. This is one of many features our SD-WAN appliance provides in our solution. CenturyLink has included our SDWAN platform to terminate and interface any third-party networks including microwave. CenturyLink's SDWAN application will enable centralized configuration, security policies and if required application-based routing of traffic between disparate networks for resiliency.</td></tr>
</table>



ESI 9 – Dual Entrance and use of 3rd Party networks

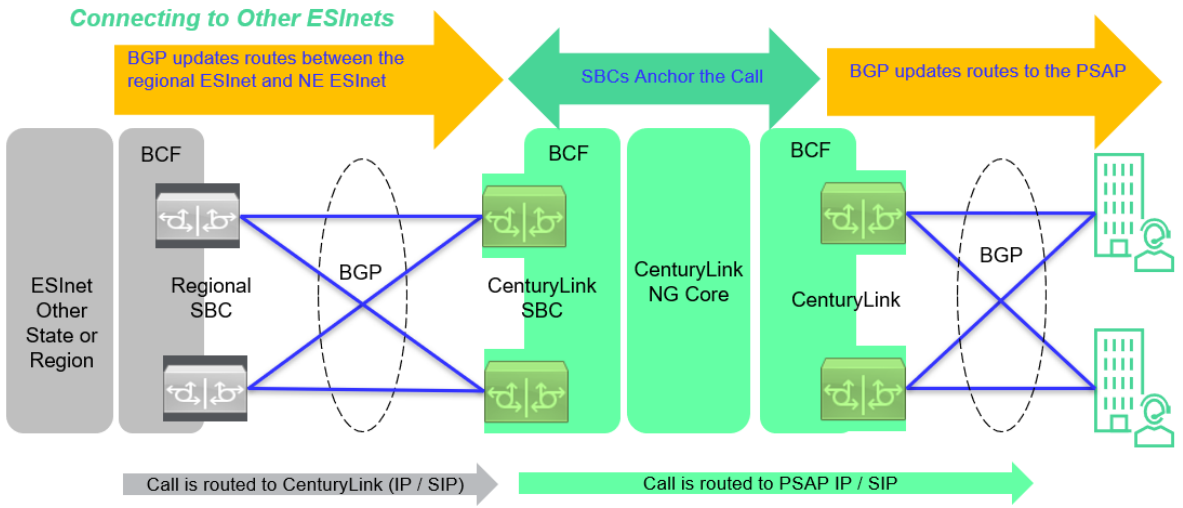
	Network Design Documentation

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

ESI 10	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** Contractor shall provide an ESInet solution capable of interfacing with neighboring state and regional NG911 IP networks as they are established, and capable of transferring voice and data between PSAPs. Describe how the solution will meet these requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our solution was designed in accordance with the NENA "Network of Networks" concept. It is natively capable of interfacing with any other NENA-compliance network. This is achieved by utilization of IPv6 for all ESInet interfaces. IF IPv4 interfaces are required, non-RFC1918 addresses are used. CenturyLink's NGCS Solution supports interconnection with Systems Service Providers (SSPs) in adjacent states as well as interconnection with State ESInets. The CenturyLink solution is capable of transferring voice and data between PSAPs in neighboring ESInets that may provide IP-based Selective Routing ("IPSR", i2) services or i3 NGCS to their PSAPs. Our solution is capable of transferring voice, ANI and ALI to States or Regions that are still using a legacy selective router (LSR) depending on the capabilities of the legacy 911 network. CenturyLink will interface to these other ESInet using a BCF that will incorporate required firewalls and session border controllers. We will apply zero trust security protocols at our BCF and will meet or exceed all NENA security requirements for interconnection to other ESInets. If the originating ESInet determines from their ECRF that the call should be routed to NE, the originating ESInet will need to send location information in PIDF-LO format, else, the regional and NE ESInets will need to share a location database to determine what PSAP the call. This works well for border areas where cell towers may receive wireless calls from two separate jurisdictions. This will help ensure the call gets routed to the correct PSAP without a transfer. For transfers between a regional ESInet and NE ESInet, star code transfers will be supported by CenturyLink or by URL. To summarize, any other ESInet that is NENA compliant can transfer voice and data in a standard NENA format.				

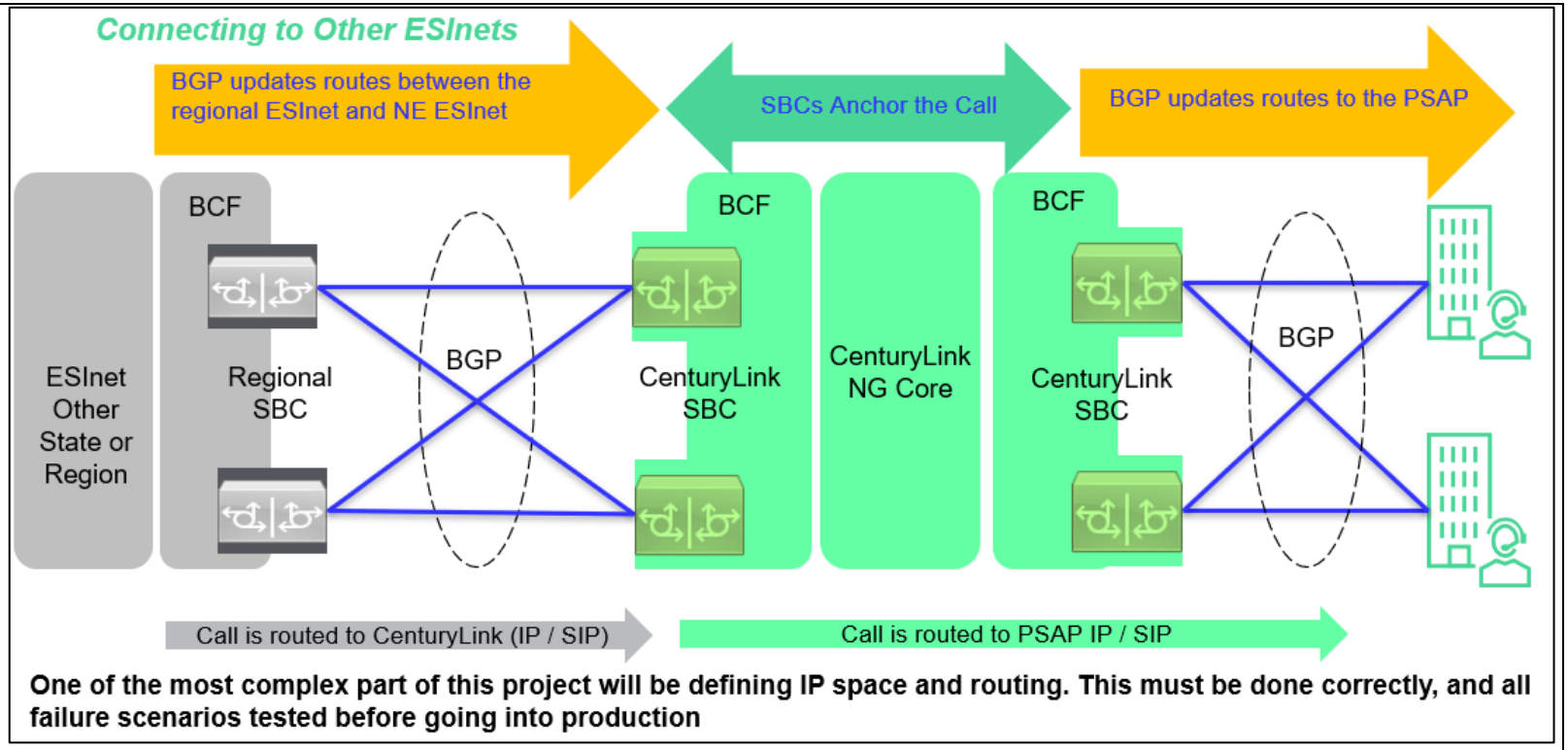
Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



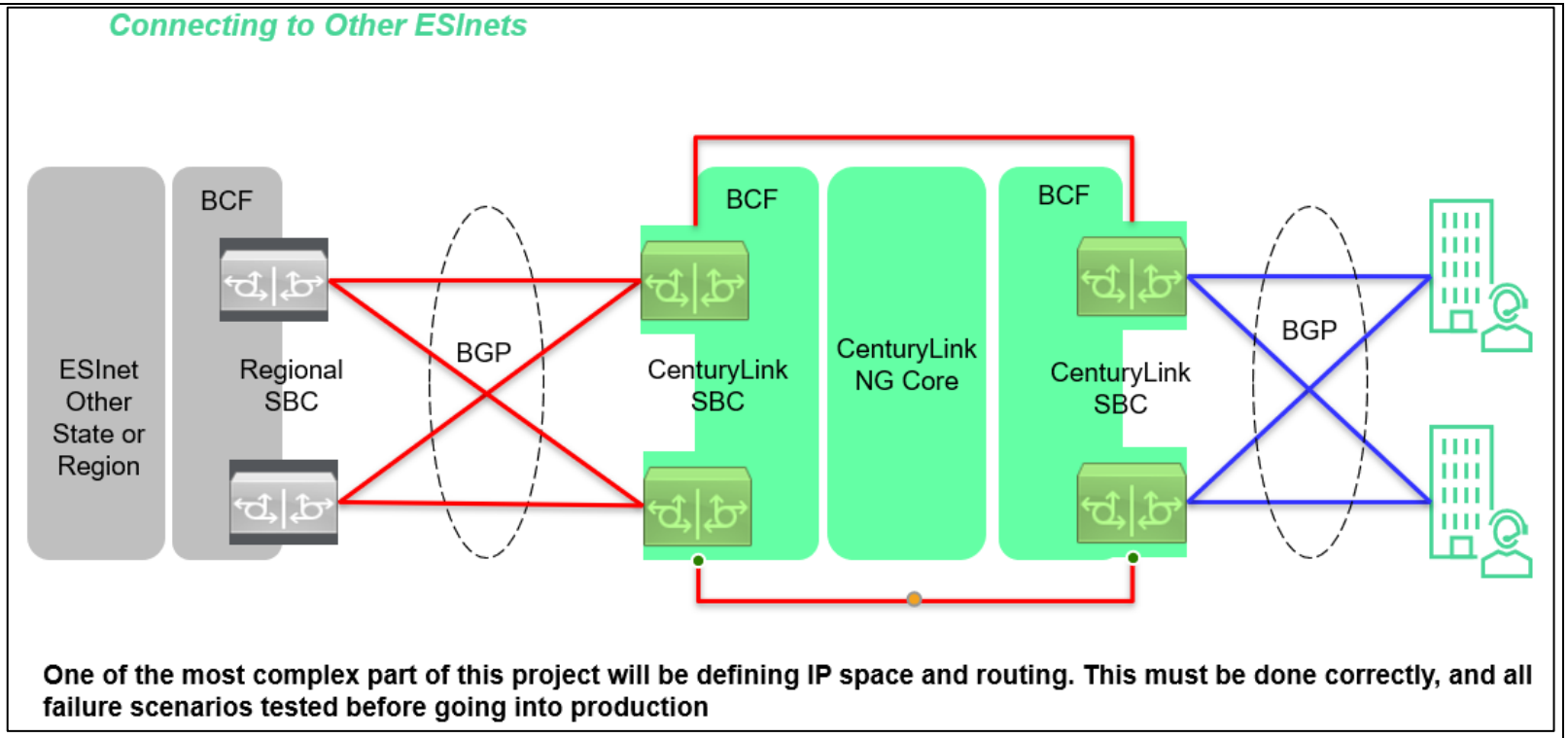
One of the most complex part of this project will be defining IP space and routing. This must be done correctly, and all failure scenarios tested before going into production

Any additional documentation can be inserted here:

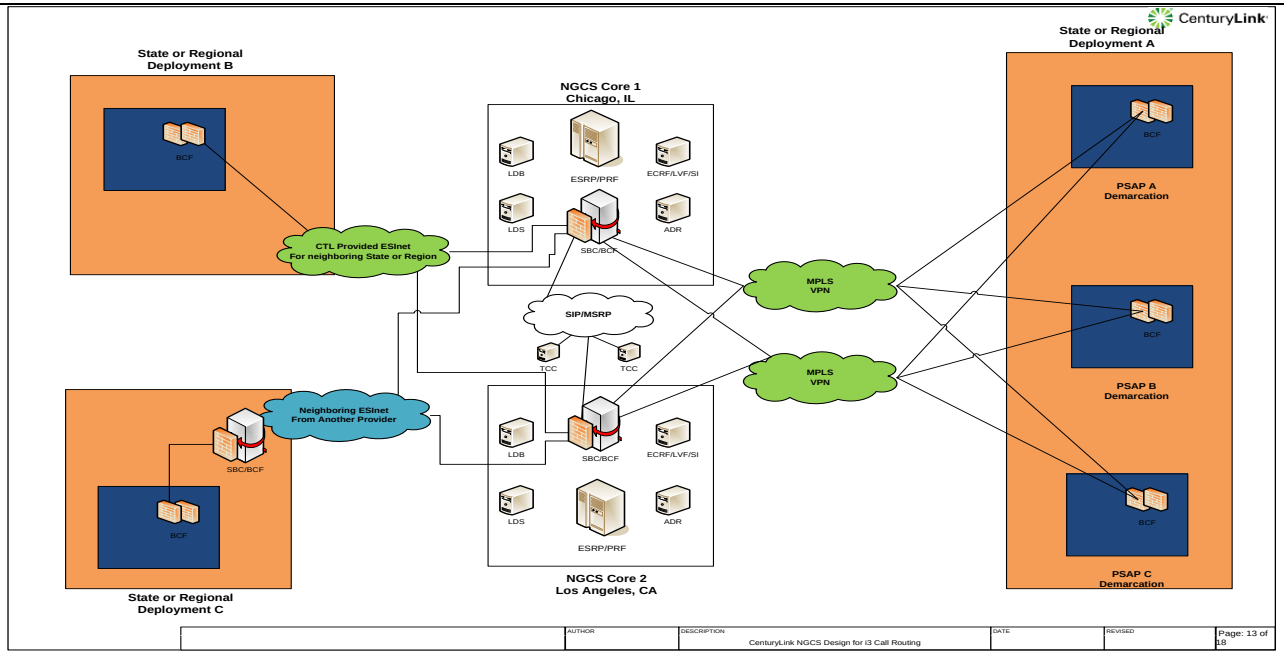
ESI 11	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** **Connecting to Other IP Networks** At such time as neighboring ESInets and NGCS systems are able to interconnect and exchange traffic, Contractor shall establish such connections and provide routing and security to allow traffic to be exchanged with neighboring ESInets and NGCS systems, regardless of the respective vendors of those systems. Describe how the solution meets or exceeds the above requirement.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink's i3 compliant, IP-based ESInet is designed to be reliable, resilient and secure and is designed to be interconnection with NENA compliant ESInets nationwide. CenturyLink will interconnect with external networks such that these connections provide routing and security. All ingress and egress from and to other ESInets will be through a secure BCF with firewalls, SD-WAN, and session border controllers (SBC), with network and security monitoring. All such interconnections will comply to current and future NENA NG9-1-1 security requirements. PKI will be employed in accordance with NENA standards and we can use a certificate authority specified by the Commission. We will use TLS as the protocol to provide communication security and ensure data integrity. TLS will have the following properties: • A private connection: All data is encrypted • Authentication: Provides authentication of the receiving and sending parties • Reliability: Protection of undetected loss or alteration of data during transmission CenturyLink's NGCS Solution supports interconnection with Systems Service Providers (SSPs) in adjacent states as well as interconnection with State networks. The CenturyLink solution supports interconnection to both legacy TDM emergency networks, i2 networks, and next generation i3 ESInets. CenturyLink's NG9-1-1 Solution ESInet was designed to fully integrate with other neighboring networks such as the State of Nebraska network and NENA-compliant interfaces. Regardless if traffic is originating from another ESRP on a neighboring ESInet and destined for the ESRP on the NE ESInet or is from an application to application such as CAD, the interconnection to those ESInets would not change. All traffic will need to enter the NE ESInet through the interconnection BCF. How that traffic is treated once it hits the NE ESInet depends on the application type and the security rules configured for such application traffic.				



ESI 11 – 911 Call between NGCS



ESI 11 – Other Application Traffic

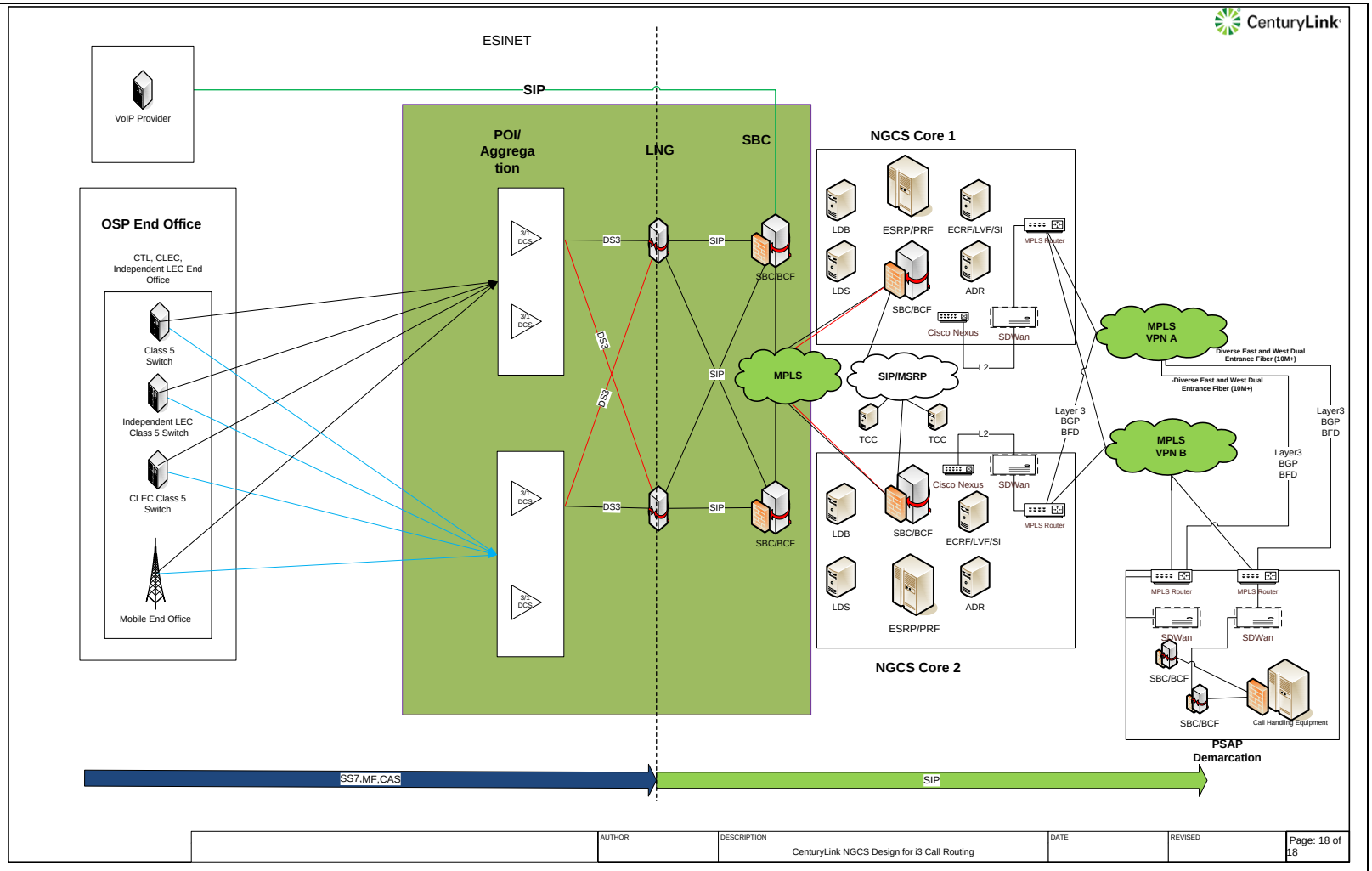


ESI 11 State and other Network to Network with Other IP Networks drawing

Any additional documentation can be inserted here:

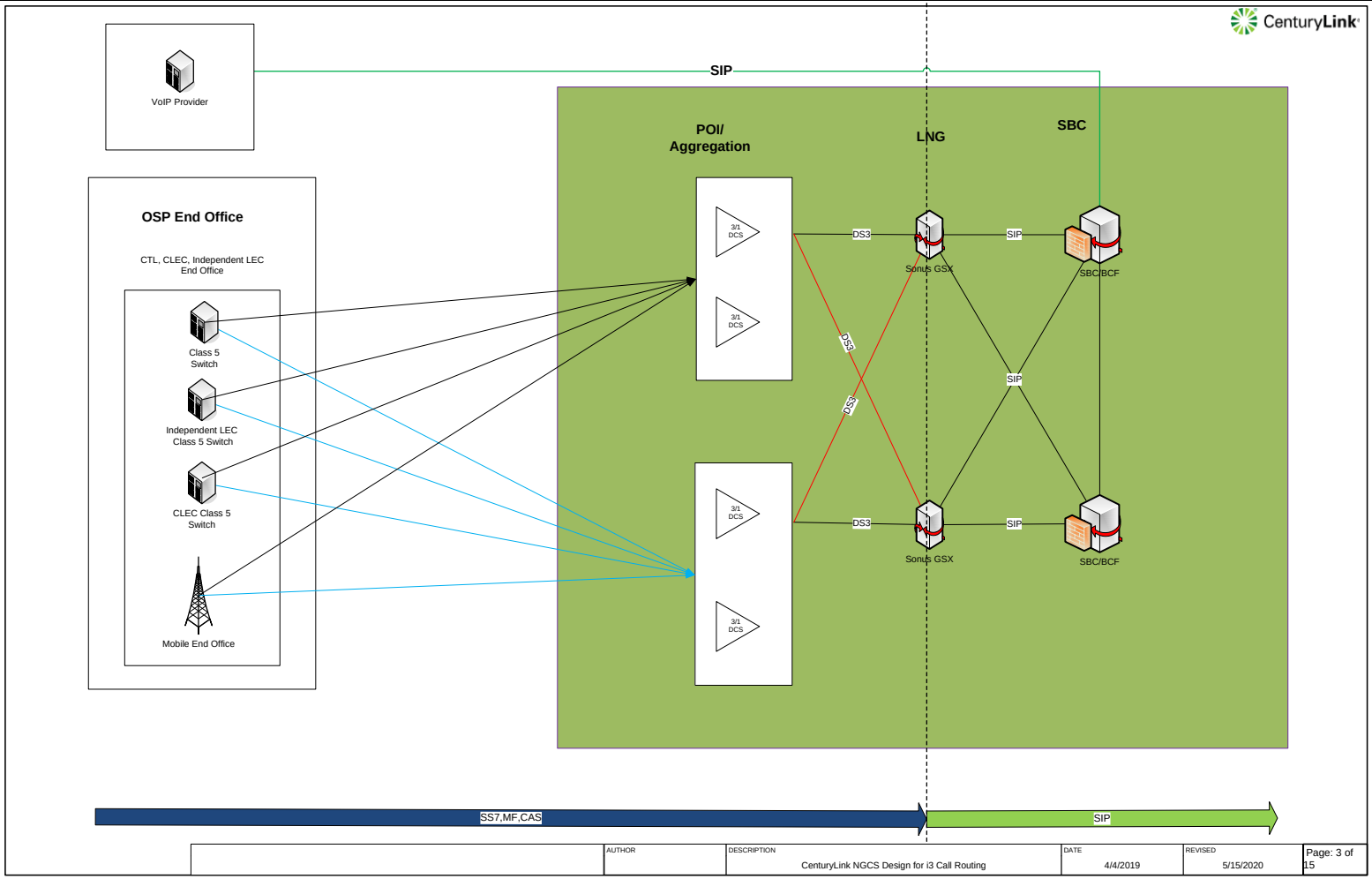
NGCS 1	**Next Generation Core Services Elements (NGCS)** Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end state for the Commission's ESInet and NGCS, taking into account the hosts and PSAPs listed in Attachment A - PSAP Host End-Point Locations. The following functional elements and services be included: a. Originating Service Provider (OSP) Connectivity; b. Legacy Network Gateway (LNG); c. Border Control Function (BCF); d. Emergency Services Routing Proxy (ESRP); e. Policy Routing Function (PRF); f. Emergency Call Routing Function (ECRF); g. Location Validation Function (LVF); h. Spatial Interface (SI); i. Location Database (LDB); j. Discrepancy Reporting; k. Logging and Recording; l. Time Server; m. Alarm Integration; and, n Message Session Relay Protocol (MSRP). **Originating Service Provider (OSP) Connectivity** **Due Authorization** Bidder shall possess a certificate of public necessity to operate as a telecommunications provider in the state of Nebraska. The Contractor shall provide a copy of current certificate of public necessity prior to award of contract. **Identification of Service Providers Connected to the Legacy Selective Router** Contractor shall be responsible for identifying and for connecting all wireline, wireless, Voice over IP (VoIP), telematics, and other third-party service providers currently connected to the existing legacy selective router. Contractor shall be responsible for updating this information quarterly for the term of the contract. Bidder shall identify each service provider that will be utilized by Contractor.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink NG9-1-1 ESINet provides an end-to-end network i3-capable 9-1-1 service, based on an IP infrastructure. Our Legacy Network Gateway consists of three elements: PIF, LIF and NIF. The PIF converts analog or TDM trunks to SIP and with our NIF and LIF, is provided as an element of our i3-Interconnect. Gateways supported by the CenturyLink NGCS solution are vendor agnostic. The LNG functions can support TDM traffic from OSPs, preferably SS7 but support MF and CAS signaling. Our LNG complies with the requirements of the i3 Standard, Section 7.1 (NENA-STA-010.2) and the RFCs cited therein (RFC 4904, RFC 3261, RFC 2392, RFC 2833, RFC 4244, RFC 3326, RFC 3515 and RFC 2616).2 It also satisfies a new section 7.1.1.3 in				

	NENA-STA-010.2, titled "Early Media" that requires an LNG to provide Early Media (referencing RFC 3960) to downstream elements whenever it is possible to do so. Additional Data dereference requests are also handled. Our LNG satisfies the requirements to provide a revised Internal Interface to the NIF Component Section (7.1.1.3 of STA010.2) and to provision the PIF component of the LNG to (1) Use standard interworking procedures as defined in ATIS-1000679.2015 (revised from ATIS T1.679-2004); and (2) Include in the SIP INVITE, an SDP offer that includes the G.711 codec. To support incoming TTY calls, the SDP offer will describe a media format associated with real time text as described in RFC 4103. Transcoding of TTY to real time text per RFC 5194 is provided as part of our i3-Interconnect service.



NGCS 1 NG9-1-1 Final End to End Drawing

	a. **Originating Service Provider (OSP) Connectivity**: CenturyLink will negotiate interconnection agreements and trunking arrangements with all service providers. CenturyLink will provide OSP's providers with a minimum of two (2) strategically and geographically diverse POIs (points of interconnect) for carriers that can send voice and data traffic via next generation protocols. CenturyLink will work with each OSP's to find the best way to connect and to help OSPs minimize the cost incurred to establish new circuits. If needed POI's can be extended into the LATA or long-haul transport can be arranged. Trunking configurations and signaling will be depended on the OSP's capabilities and will need to be coordinated, CenturyLink prefers to accept SIP or SS7, but can support other TDM deliveries such as MF and CAS. CenturyLink Core Sites interoperate with OSP aggregation sites to receive ingress TDM traffic at POI locations that will be diversely located and trunked to CenturyLink Legacy Network Gateway function. CenturyLink will: • Work with OSP's, PSAP's and State of Nebraska to develop a joint communication plan to each OSP outlining the scope of services to be implemented, a high-level implementation schedule, and key contact information for each entity. • Facilitate the establishment of OSP communication guidelines and adhere to these guidelines for the project implementation and service duration. CenturyLink establishes expectations with each OSP and manages communication to the OSP for items related to the proposed services on behalf of the State of Nebraska. • Provide transition planning and migration support to the OSP's through our assigned Project management team. Aggregation Plan for Wireless Carriers: • In the case of an OSP connecting to the CenturyLink NGCS infrastructure, the OSP is responsible for connecting to the CenturyLink aggregation points designated to that carrier via TDM (SS7 preferred, MF and CAS) and for SIP connectivity to Session Border Controllers for secure diverse IP connectivity. CenturyLink will have assigned personnel to coordinate with each carrier to provide key dates and timelines necessary for the transition of traffic. In the CenturyLink Solution, the aggregation services and POI will be common facilities in most locations and become OSP point of demarcation. • CenturyLink takes responsibility for facilitating the establishment of OSP communication guidelines and adhering to these guidelines for the project implementation and service duration. CenturyLink will establish expectations with each OSP and manages communication to the OSP for items related to the proposed services. CenturyLink will escalate to the appropriate County 9-1-1 groups regarding TSP initiatives and will request County intervention when necessary. • OSPs will connect to CenturyLink POIs using DS1 (T1) or higher transport facilities. OSPs will establish SS7, MF or CAS ES trunks (SS7 preferred) from OSP end offices to each of CenturyLink's diverse POIs. This is required to meet NENA 9-1-1 diversity rules "traffic will not ride on the same controller or shelf to maintain this diversity." SS7 point codes will be established for each trunk group the OSP connects to CenturyLink POIs. Refer to the drawing below.



NGCS 1 Originating Service Provider (OSP) Connectivity Drawing

Interoperability testing will be done between CenturyLink and each OSP that wishes to connect via IP SIP Connectivity into CenturyLink's network will be through a BCF function(s) with termination on CenturyLink Core Session Boarder Controllers for delivery to our NGCS.

- For this type of delivery, TDM / SS7 will not be involved and only IP / SIP will be used
- OSPs will have the ability to send PIDF-LO location data with the call when OSPs support this.

OSP Aggregation Service with Wireless Service Providers:

Wireless Service Providers (WSP) can connect to CenturyLink's NGCS several ways:

1. Through a CenturyLink aggregation point utilizing TDM
2. Through a CenturyLink aggregation point utilizing IP / SIP
3. Through CenturyLink's 9-1-1 Connect Solution. Currently, Sprint and T-Mobile deliver all their 9-1-1 calls to legacy selective routers across the United States using our 9-11 Connect Solution
4. Multiple small OSPs, VoIP Service Providers, and Cable operators use CenturyLink's 9-1-1 Connect Solution to deliver 9-1-1 calls from their subscribers to a legacy selective router
5. 9-1-1 Connect currently reach's 98% of legacy selective routers across the United States
6. CenturyLink will soon be able to provide a SIP-to-SIP connectivity into CenturyLink's NGCS
7. 9-1-1 Connect was purpose built and this network only handles calls from our OSP customers via IP SIP and deliver to the selective router as TDM
8. These OSPs connect to GSX gateways across the US as SIP. CenturyLink connects to the selective routers with a TDM handoff. Benefits for the State of Nebraska: CenturyLink has the capability to migrate our existing 9-1-1 Connect customer to: • An Aggregation point (TDM / SS7)
    - An Aggregation point (IP SIP)
    - CenturyLink's NGCS directly through our SBCs
    - TDM / SS7 to IP / SIP media conversions for any OSP

b. **Legacy Network Gateway (LNG)** Our Legacy Network Gateway consists of three elements: PIF, LIF and NIF. The PIF converts analog or TDM trunks to SIP and with our NIF and LIF, is provided as an element of our i3-Interconnect. Gateways supported by the CenturyLink NGCS solution are vendor agnostic. The LNG functions can support TDM traffic from OSPs, preferably SS7 but support MF and CAS signaling. LPG provided at the PSAP emulates CAMA delivery or supports CAS T1 and deliver serial ALI for the call handling equipment (CHE) at the PSAP to meet non i3 PSAP requirements. Our LNG complies with the requirements of the i3 Standard, Section 7.1 (NENA-STA-010.2) and the RFCs cited therein (RFC 4904, RFC 3261, RFC 2392, RFC 2833, RFC 4244, RFC 3326, RFC 3515 and RFC 2616).2 It also satisfies a new section 7.1.1.3 in NENA-STA-010.2, titled "Early Media" that requires an LNG to provide Early Media (referencing RFC 3960) to downstream elements whenever it is possible to do so.

Additional Data reference requests are also handled. Our LNG satisfies the requirements to provide a revised Internal Interface to the NIF Component Section (7.1.1.3 of STA010.2) and to provision the PIF component of the LNG to

1. Use standard interworking procedures as defined in ATIS-1000679.2015 (revised from ATIS T1.679-2004); and

2. Include in the SIP INVITE, an SDP offer that includes the G.711 codec. To support incoming TTY calls, the SDP offer will describe a media format associated with real time text as described in RFC 4103. Transcoding of TTY to real time text per RFC 5194 is provided as part of our i3-Interconnect service.

c. **Border Control Function (BCF):** Border Control Function/Session Border Controller (BCF/SBC) that we employ is the foundation of our security solution for call flow protection. It integrates fully with all other NGCS. Threats are detected by monitoring the NENA-defined Security Posture as well as predetermined threat profiles. Log events are created which 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. These will be configured to accomplish such goals as elevated trust of call flows and aggregation infrastructure.

This BCF provides both application and network layer protection and scanning. It will also mitigate lower layer protocol attacks and provide denial of service (DoS) and distributed denial of service (DDoS) detection and protection. The firewall component of the Oracle/Acme Packet BCF/SBC will inspect all traffic transiting the network edge. In accordance with NENA-STA-010.2, the BCF/SBC will ensure any connection involving a call origination sources, gateways, and similar elements outside the ESInet are properly screened.

a. Ensure the BCF supports an automated interface that allows a downstream element to mark the source of a call as a "bad actor". This would normally occur when a call is received that appears to be part of a deliberate attack on the system.
b. Ensure the BCF installs a "NENA-source" parameter in the Via header that in the outgoing INVITE message associated with every call. Calls are marked by the SBC in a way that allows a recipient to identify the BCF that processed the call.
c. The SBF/BCF functions are agnostic meaning the Nebraska i3 network will be able to connect to other providers' NGCS cores as long as those providers are i3 compliant.
d. Emergency Services Routing **Proxy (ESRP):** Our ESRP is the most robust element of its kind available on the market and scales to well over 200 call setups per second which equates to over 720,000 busy hour call attempts (BHCA). With software developed in collaboration between Synergem and Oracle; security, Quality of Service (QoS), and interoperability are "baked in" to the functional element. After the BCF security check, our ESRP provides routing based on the caller's location. It extracts the location of the caller from SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next hop route, and evaluates the route policy of that entity using its Policy Routing Function (PRF) to determine the actual next hop the call takes.

When calls arrive at one of the NGCS instances, the first step is an evaluation of the incoming call to determine if location information is already available in the SIP headers. If location is already known, then the call proceeds to ESRP processing. If the location is not known, then the calling number is used to transmit a HELD query to the LDB. The LDB responds with location information by reference or by value, and this info is then added to the headers for the call and it proceeds to the ESRP.

Once the call with location information enters the ESRP, that element determines whether the location provided is by value or by reference. If by reference, a dereference request is sent in order to obtain the current actual location for the call. Then, the next step is for the ESRP to submit a LoST query to the ECRF using the a fore mentioned location and service type SOS. The ECRF replies with a URI. The ESRP then uses the returned URI to process the call via the PRF.

In the PRF, the candidate destination URI returned by the ECRF is used along with other known data points (other header information, current time and date, etc.) to query against the currently active policy routing rule set. If this query returns any results, then the substitute URI provided in the policy rule is used as the definitive destination URI for the call. Otherwise, the candidate URI becomes definitive. The security protocol described in our replies to NGCS-75 and NGCS-210 protects the ECRF from attack.

e. **Policy Routing Function (PRF):** Our ESRP-supported PRF is the principal policy control tool with standardized methods to define/build and control Policy Rules. determines potential emergency call routes. Other rules the PRF can apply govern call termination and can include a route decision based on knowledge that a downstream ESRP is busy (call queue full) or that a PSAP is offline. Rules also may be used to "permit" or "deny" network access. With software developed in collaboration between Synergem and Oracle; security, Quality of Service (QoS), and interoperability are "baked in" to the functional element. Our ESRP provides final routing to a PSAP based on the caller's location. It extracts the location of the caller from SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next hop route, and evaluates the route policy of that entity using its Policy Routing Function (PRF) to determine the actual next hop. In the PRF, the candidate destination URI returned by the ECRF is used along with other known data points (other header information, current time and date, etc.) to query against the currently active policy routing rule set. If this query returns any results, then the substitute URI provided in the policy rule is used as the definitive destination URI for the call. Otherwise, the candidate URI becomes definitive

f. **Emergency Call Routing Function (ECRF):** CenturyLink's NGCS Solution Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) complies with all NENA and IETF standards and provides full migration into i3 without costly technology acquisition and process overhaul. Key aspects include:

- Allows data analysts to correlate street and community names from three data sources (Postal, MSAG, and GIS). • Allows authorized service providers to validate locations and route calls using real time data.
- Integration with the LDB, MSAG Conversion Service, and Spatial Interface.
- Identifies common error discrepancies between MSAG, GIS, and Postal.
- Extensive online help. • Extensive security mechanisms allow access and updating tailored to most organizations' GIS data or operations.
- Links to online mapping resources.
- Web-based user interface for ease of data management.
- Extensive reporting capabilities.
- • Allows establishment of translations.

g. **Location Validation Function (LVF):** The CenturyLink NGCS Solution ECRF contains a LoST server that validates location information against the system's database. This LVF is part of the NGCS suite provided in this service that will enable geospatial routing for call delivery to the correct PSAP boundary/jurisdiction. Both the ECRF and the LVF are compliant with applicable NENA and IETF standards. Key capabilities include:

- Data analysts can correlate street and community names from three data sources (Postal, MSAG, and GIS).
- OSPs can validate locations and route calls using real time data.
- Common error discrepancies between MSAG, GIS, and Postal are automatically identified.

- Extensive online help is available.
- Extensive security mechanisms allow access and updating tailored to most organizations' data operations.
- Links to online mapping resources are provided.
- Web-based user interface for ease of data management is available.
- ALI/Location Database (LDB) is fully integrated.
- Extensive reporting capabilities area available including 17 reports – all of which can be exported to Excel, PDF, etc. A Tracking agency and individual progress in data preparation. Translations can be established including County (e.g., "007" = "Boone County"), Community (e.g., "North Boone" = "Beaverton") and Street (e.g., "SH 76" = "Fairground Rd." = "State Line Rd.")

h. **Spatial Interface (SI)** is at the heart of the GIS to ECRF/LVF integration. Called the DataManager, this function supports the periodic loading of GIS data from external systems.

GIS data can be uploaded to the DataManager via an intuitive web interface enabling authorized users to provision the SI with geospatial data in ESRI shapefile or file geodatabase formats, verify that the data is in the expected schema, and initiate the load process into the SI. Alternatively, automated routines can be set up to populate the SI without having to upload via the web interface.

The load into the SI system does not do a complete overwrite; rather, it performs a change detection operation. As a result, an historical record of data changes can be maintained by the system, and detailed results of any load errors are provided. This process, either with the web interface or using automated routines, can be run as frequently as needed, although daily is recommended.

Once the data load is complete, DataManager performs numerous quality control checks on the data. The resulting QC errors can be viewed directly using any software capable of consuming ESRI-based web services. This will allow the viewing of any map data discrepancies in real-time.

Following the QC process, if the number and severity of any errors are within configurable limits, DataManager will automatically publish updated data to the master ECRF/LVF database. This database acts as a replication master, pushing all changes using Microsoft SQL Server replication to child databases that are used for ECRF/LVF functionality. All replication distributions run on the master database to minimize the load on the databases that are being actively used for LoST query processing. SQL Server replication occurs in near-real-time. The SI also provides reporting, allowing real-time access into the state of the datasets used by the ECRF/LVF.

Additional publishing routines can be set-up for other applications that may need GIS data. This allows administrators to create publishing tasks that export copies of the data into a format that is required by third-party applications. For example, CPE may require a certain data extract that is different from what CAD requires.

i. **Location Database (LDB):** A NENA compliant Location Database (LDB) that serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment will be provided. The LDB retains the current information, functionality, and interfaces of today's ALI, but also can utilize the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or gateway mobile location center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols.

	To successfully replace a legacy ALI system with an LDB, a mechanism must be provided to the Service providers to update the location information in the LDB. During the transition to i3, and to aid 9-1-1 authorities gaining cooperation from the Service providers, the LDB system includes a Service Order Input (SOI) processing function that matches existing SOI processing. This means that the Service providers do not have to change current processes to support the i3 system. Our solution provides a translation mechanism called the MSAG Conversion Service (MCS) to convert SOI records into the appropriate CLDXF format for comparison against the LVF). The LDB provides both legacy and NG9-1-1 location interfaces. To support NG9-1-1 capable PSAP's a HELD interface is provided. To support legacy PSAPs, a legacy ALI interface is provided, and location data within the LDB is converted into legacy formats using the MSAG Conversion Service (MCS). The HELD interface can support hundreds of queries per second. The legacy ALI interface requires the legacy CPE to maintain one or more TCP/IP connections. Each CPE instance must initiate and maintain the connection to the LDB legacy ALI interface. Each individual TCP/IP connection can handle one legacy ALI query at a time. This is a limitation of the legacy interface, not of the LDB. The LDB utilizes a web-based interface allowing authorized personnel access to the backend location database. From this web interface, users with the appropriate permissions can schedule reports and data extracts to be run. Key capabilities of the LDB include: – Support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501, and 08-502 related to ALI DBMS. Be capable of assuming the role of a location database as defined in the NENA NG9-1-1 Transition Plan Considerations (NENA INF 008.2-2013). – Support NENA standards (such as E2, E2+, NCAS, CAS). • Be able to provide location server functionality and interfaces as defined in NENA-STA-010.2-2016. • Be able to seamlessly interact with a NENA i3 ECRF/LVF for location validation, as described in NENA-STA-010.2- 2016. – Provide location by value or by reference, as defined in NENA-STA-010.2-2016. – Be able to dereference requests for additional information, as defined in NENA-STA-010.2- 2016. – Be able to interface simultaneously with multiple wireless callers. – Be able to interface simultaneously with multiple remote MPC/VPC databases. – Automatically detect, import and validate customer records (SOI records). – Convert legacy MSAG style addresses using an MSAG Conversion Service (MCS) as defined in NENA-STA-010.2-2016. Civic address data stored in the LDB database must conform to all PIDFLO and CLDXF standards. – Dynamically convert MSAG style address received over E2 using the MSAG Conversion Service so these calls can be routed using the ECRF which must contain CLDXF compliant data. – Natively support all CLDXF fields for each civic address stored, including all the street name elements (PRM, PRD, STP, STPS, RD, STS, POD, POM) and ALL of the address number and sub address elements (HNP, HNO, HNS, BLD, LOC, FLR, UNIT, ROOM, SEAT). • Provide Service Providers with the ability to update their location records using their existing processes (such as SOI), or a web-based user interface.

- Provide a legacy MSAG for Service Providers that still require it. To ensure that records in this MSAG will be valid after MCS conversion to CLDXF and LVF validation, it must be generated from the inverse operation (i.e., taking all the CLDXF GIS road centerline records and converting them back into legacy format using the MCS).
- Be able to be used simultaneously by both NG9-1-1-capable and E9-1-1-capable PSAPs. For E9-1-1 PSAPs, a legacy ALI service must be provided, with address data being "downgraded" from the LDB CLDXF compliant data into legacy MSAG style data using the MCS. NG9-1-1 PSAPs will utilize the HELD interface.
- Allow different E9-1-1 PSAPs to use different ALI formats based on individual needs.
- Use LVFs to validate civic addresses using CLDXF compliant PIDF-LO.
- Support location data formatting as defined in the NENA CLDXF.
- Periodically reevaluate the location information using LVF functions within the system.
- Communicate with NG9-1-1 functional elements using the HELD protocol.
- Provide a PIDF-LO based on both the wireless and VoIP E2 response. Wireless phase 2 should be represented with a circle in the PIDF-LO. • Be able to dereference additional data requests.
- Consistently respond to all requests within 400ms for data that is contained within the LDB.
- Provide Service Providers and GIS Users with the necessary workflows to correct civic address records that fail validation.
- Record all NRF conditions and provide a workflow for Service Providers for corrections. The system should query the NPAC database to determine ownership of the NRF TN and automatically assign the error to the owning Service Provider.
- Support the transition of existing PS/ALI customers to the LDB.
- Web interface allowing Service Providers or other authorized users to add additional data to each record as defined in IETF RFC 7852. At a minimum, an authorized user must be able to add, edit or delete additional data blocks for a record. Supported additional data blocks must include:
  a. Data Provider Information
  b. Service Information
  c. Device Information
  d. Owner/Subscriber Information Comments
- The HELD interface must support the delivery of additional data as defined in IETF RFC 7852.
- All changes to customer records in the LDB must include a full historical change history

j. **Discrepancy Reporting:** We accomplish discrepancy reporting in accordance with applicable SLAs employing a web-based portal for notification and correction. A discrepancy workflow will be available to all users to correct errors between the service provider records and the GIS (LVF).

k. **Logging and Recording**: We support logging and recording for relevant i3 event as define in Section '5.13 Logging Service' in NENA STA 010.2 2016 or its successors.

l. **Time Server**: CenturyLink's NG9-1-1 Solution processing elements achieve time synchronization via Network Time Protocol (NTP) from

redundant and geographically distributed sources within the CenturyLink's NGCS Solution domain. Time stamps are included in logs, system traces, and user reports.

m. **Alarm Integration:**: CenturyLink uses various different tools and Software packages are widely available for capturing, analyzing, and reporting the health of the network and NGCS functional elements based on the (Simple Network Management Protocol) SNMP traffic it receives. These include: Network Atlas, NetBrain, , Utility Tools (Ping, Tracroute, NSlookup, Power Tools, Commercial Scanners and Open Source type Tools SolarWinds, Monolith, and OpenView, as well as many full-featured open source packages, such as network probes and SD WAN. We set up platform-specific alarm thresholds to identify potential service impairments. CenturyLink network alarms are customer specific and generate trouble tickets that automatically opens up trouble tickets and reporting alarms to our CenturyLink, NOC/SOC and Nebraska customers. Proactive Customer Notification (PCN) gives customers with flexibility to specify certain notification parameters on a service-by-service basis.

n. **Message Session Relay Protocol (MSRP):** MSRP is the standard protocol specified for handling text in an NGCS structure and our systems are designed to support it. Because MSRP text is a native capability of CenturyLink's NG9-1-1 Solution, Policy Routing Rules in the ESRP can be based on the call type. This allows for such possibilities as routing text calls differently than voice, having different alternate routing rules for text, or making manual changes based on call type. Native MSRP delivery to capable PSAPs allows for handling of text calls with the same capabilities as voice calls. For instance, at ACD, PSAPs texts can be included in the normal voice queue, or they may be segregated into their own queue. Because text handling is not a separate service for CenturyLink's NGCS Solution reporting and logging capabilities are the same for text calls as for voice calls.

SMS/text messages received from the TCC can be delivered to any destination connected to CenturyLink's NGCS Solution.

To support incoming TTY calls, the SDP offer will describe a media format associated with real time text as described in RFC 4103. Transcoding of TTY to real time text per RFC 5194 is provided as part of our interconnect service. Other protocols such as XMPP may be supported if interworked to MSRP prior to NGCS presentation.

We comply with to NENA 08-003, NENA-STA-010.2-2016 that requires interworking real time text and TTY in our PIF component per RFC 5194, accepting DTMF signaling from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 4733, and recognizing Baudot tones in incoming media and replacing them with RFC 4103 real time text.

Tasks for provisioning SMS to 9-1-1 for PSAPs deploying the TTY method are the responsibility of the wireless provider, the TCC provider, and the PSAP or 9-1-1 Authority. CenturyLink's NGCS Solution will deliver TTY calls where the legacy 9-1-1 environment (SR/ALI DBMS) is being emulated by our solution. MSRP is the standard protocol specified for handling text in an NGCS structure. Other protocols such as XMPP may be supported if interworked to MSRP prior to NGCS presentation.

If a text message is presented to our network in the proper configuration, it will be handled just as any other call-for-service.

– The CenturyLink NGCS network is media agnostic and routes all inbound calls in the same way, whether voice, RTT (RTP) text (MSRP), video, or a mix of media types. Current i3 NENA standard limits direct SIP RTT delivery to MSRP according to NENA-STA-010.2-2016 Section 4.1.9. This specification notates that OSP delivery may use differing protocols (XMPP) but must be converted to MSRP for delivery into the ESInet for endpoint PSAP delivery. This function would be handled in the same fashion as any other media in the CenturyLink NGCS solution, presented with location our NGCS would apply the correct the Policy Routing Function (PRF) to enable direction of Real Time Text-to-9-1-1 to appropriate destination.

	– CenturyLink will be aggregating the connections from the nationally recognized TCCs at the NGCS. The communication and role of coordination to the TCCs will be managed through a CenturyLink Program Manager in conjunction with the locally relevant information for handling delivery to the PSAP. – CenturyLink's NG9-1-1 solution is committed to working within the specifications laid out by NENA, the PSAP communities and industry vendors for Next Generation 9-1-1 and NENA i3 standards. – Specific delivery options available today that allow RTT to be delivered via TTY (baudot) emulation will be supported in the CenturyLink NGS solution presented to the appropriately routed PSAP's. – CenturyLink's NGCS Solution supports RTT within the NG9-1-1 data stream natively. It is the role of the CPE equipment to decode this correctly.

Any additional documentation can be inserted here

NGCS 2	**Next Generation Core Services Elements (NGCS)** **Interconnection and Commercial Agreements, and Trunking** **Originating Service Provider (OSP) Connectivity** Contractor shall be responsible for negotiating interconnection or commercial agreements, and for data and network connection arrangements with each service provider identified in requirement NGCS 1. Interconnection or commercial agreements shall cover subjects including, but not limited to, split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and NGCS, Local Number Portability (LNP), National Number Portability (NNP), and Function of Code R (FoCR). Describe the process and provide timelines for meeting the requirements of this section, as well as the expected process for resolution of disputes.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink has a tremendous amount of experience in negotiating interconnection agreements and migrating agencies from existing systems to newer iterations. Our wealth of experience has produced innovations specifically designed to manage these concerns and mitigate migration risk. We will collaborate extensively with the state and PSAP stakeholders to develop a detailed migration strategy. Our nationwide ESInet, integrates with both legacy and NG9-1-1 infrastructures, which allows for migration to NG9-1-1 technology on your schedule without the need for a 'forklift' upgrade. During implementation of services, CenturyLink will provide a dedicated OSP Coordinator who works with the OSP and each telecommunication companies. The CenturyLink Project Manager is responsible for all implementation-related activities including creation and management of the implementation Program Development plan with the customer and coordinating activities with carriers and vendor/vendors such as establishing connectivity and test/migration schedules. Taking into account the State's needs and the constraints of the other Telecommunications Service Providers serving the State, the CenturyLink Project Manager creates and manages the project plan and milestone schedule tailored to the needs of the State's requirements with mutually agreed-upon timeframes. We have wide experience in negotiating Interconnect Agreements with a broad range of OSPs. We begin by meeting with each provider during the project kickoff phase to determine their needs and how we can take advantage of their existing operational strategy to facilitate transition to the ESInet environment. This includes a detailed review of all Local Area Telephone areas (LATA's), wireless cell sectors, Local Number Portability (LNP), National Number Portability (NNP), and Function of Code R (FoCR). The process for NEW interconnection between OSPs and CenturyLink NG9-1-1 ESInet solution is straightforward and consists of four steps that take an estimated 70 days. • Phase 1 – Design, Assign & Test (Timeline ~ 30 days). OSP inventories 9-1-1 connectivity and capacity requirements. Our team reviews end-to-end signaling design with OSP. OSP requests LOA/CFA (Letter of Authority/ Customer Facility Assignment); our team assigns: – (1) POI location. Review LATA, Split Center, cell sectors and other Environments. – (2) We provide cross-connect information when the OSP connecting to our NG9-1-1 solution via SIP and – (3) OSP circuit activation (BERT) by Network Delivery Team. OSP and team coordinate trunk activation. • Phase 2 – & Signaling (Timeline ~ 25 days). OSP submits SS7 ISUP orders to enable (possible 3rd Party). If SIP share host & IP with OSP and coordinate Inter-Op testing. OSP and our team coordinate end to end test calls to NG9-1-1 network - provisioned to our NG 9-1-1				

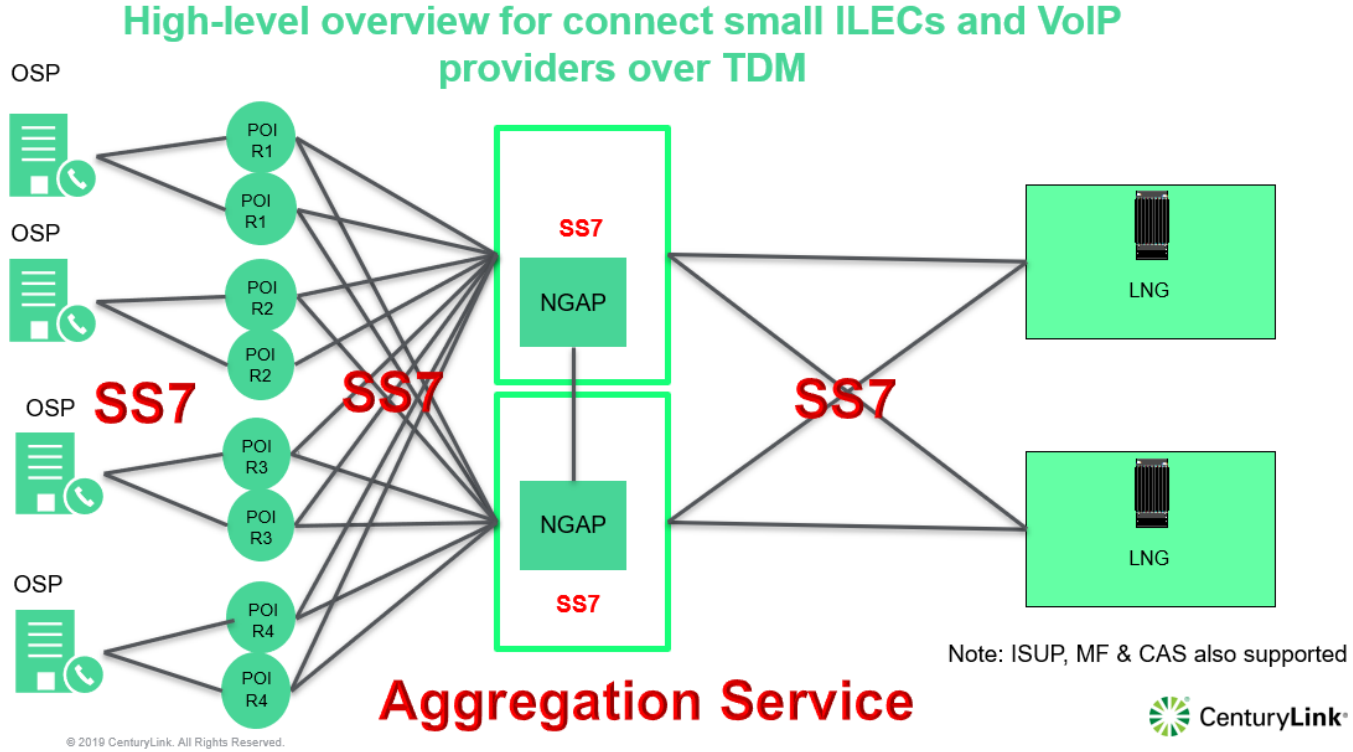
	solution. OSP and team ensure proper routing in place on the voice and signaling switches to deliver calls to our NGCS. OSP and team coordinate and execute the tests defined in the test strategy/acceptance test plan document. • Phase 3 – Cutover (Timeline ~ 15 days). FINAL Maintenance Operation Protocol (MOP) review w/OSP. Team coordinates cutover dates. Execute cutover. • Phase 4 – Disconnects – (Timeframe varies) After bi-directional connectivity is established to selective routers and an OSP is connected, it may immediately disconnect existing circuits from the SRs and discontinue monthly circuit, port and voice trunk payments to the ILEC. Interconnect with the OSPs and will receive SOI, MPC and VPC updates without the need for an ALI database or selective router. Per NENA i3, these obsolete components do not exist in an NG environment and can be decommissioned. Throughout the duration of the project implementation, our CenturyLink Project Manager(s) will keep the State of Nebraska informed of ongoing project status via regular project team meetings with each telecommunications provider. CenturyLink project management team will focus on "one team" approach with frequent project team discussions and written project documentation between the customer/CenturyLink and all participating subcontractors. The CenturyLink Project Manager, in coordination with the Program Manager, will take necessary actions to ensure the final project implementation exceeds the State's expectations.

Any additional documentation can be inserted here

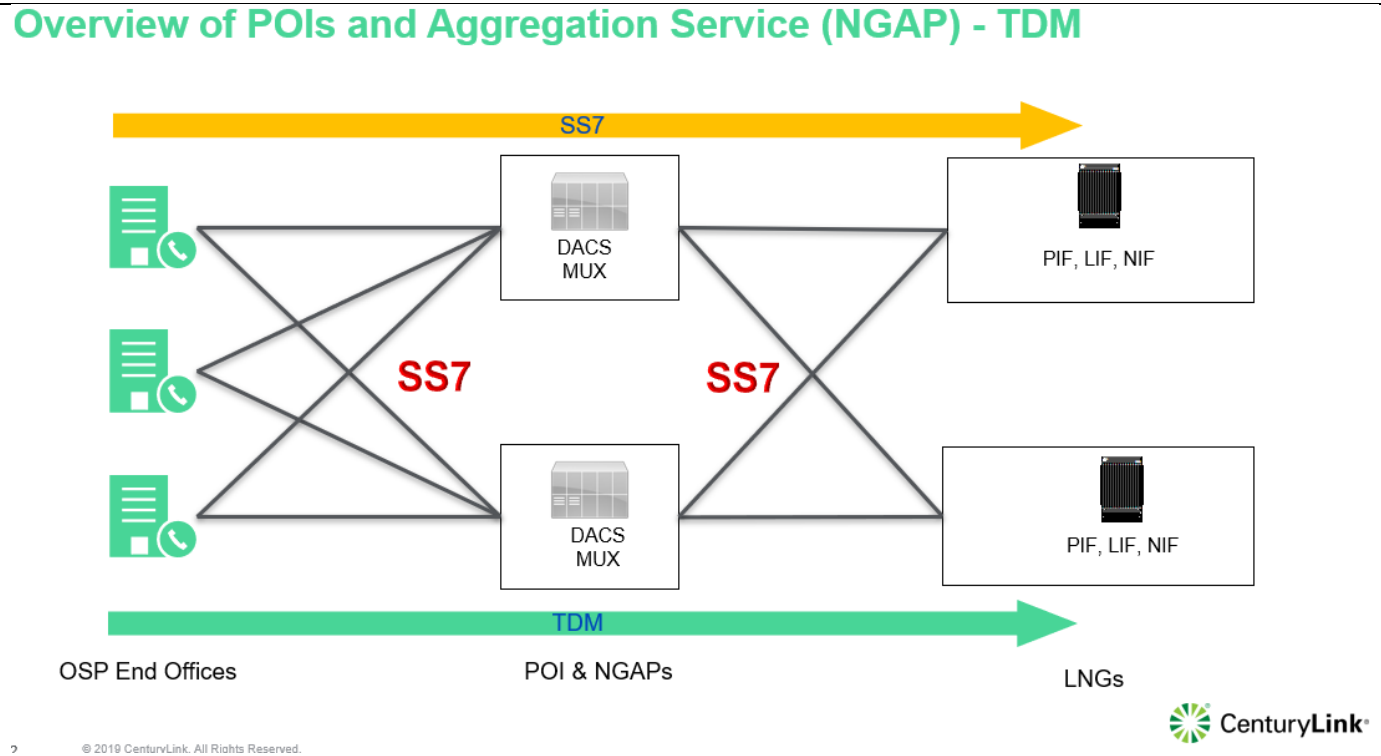
NGCS 3	**Next Generation Core Services Elements (NGCS)** **Originating Service Provider (OSP) Connectivity** **Management of OSP Connectivity** Contractor shall be responsible for managing moves, adds, changes, and deletions of the connections from the OSPs to the Contractor's systems for the term of the contract. Contractor shall allow for both Time-Division Multiplexing (TDM) and IP ingress to the network, proactively monitor these connections, and work with the respective service providers to resolve problems as they arise. Describe the process and provide timelines for meeting these requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Contractor shall be responsible for managing moves, adds, changes, and deletions of the connections from the OSPs to the Contractor's systems for the term of the **contract**. CenturyLink will provide an OSP Coordinator for the life of the project. The OSP coordinator will be responsible for managing all moves, adds, changes, and deletions of connections for the OSPs to the CenturyLink system. Contractor shall allow for both Time-Division Multiplexing (TDM) and IP ingress to the network, proactively monitor these connections, and work with the respective service providers to resolve problems as they arise. CenturyLink's solution will support the following types of TDM networks: SS7, ISUP, MF or CAS. CenturyLink's solution will support native SIP ingress from OSPs with this capability Describe the process and provide timelines for meeting these As one of the existing E911 Service Providers in the State of Nebraska, CenturyLink has a long history of successfully working with all OSPs in the state. In general, our approach would be to migrate each legacy selective router one at a time. Our Program Manager will work with the State of Nebraska on a schedule and timeline. Steps and typical timelines working to migrate OSPs pre-migration and migration **Step 1 - Design, Assign & Test (Timeline ~ 30** days): OSP inventories 9-1-1 connectivity and capacity requirements. Our team reviews end-to-end signaling design with OSP. OSP requests LOA/CFA (Letter of Authority/ Customer Facility Assignment); our team assigns 9-1-1 POI location. We provide cross-connect information when the OSP connecting to our ESInet via SIP. OSP circuit activation (BERT) by Network Delivery Team. OSP and team coordinate trunk activation. **Step 2 Signaling (Timeline ~ 25** days): OSP submits SS7 ISUP orders to enable (possible 3rd Party). If SIP, share host and IP with OSP and coordinate Inter-Op testing. OSP and our team coordinate end-to-end test calls to our NG9-1-1 ESInet. The OSP's and our CenturyLink Public Safety team will ensure proper routing is in place on the voice and signaling switches to deliver calls to the NG9-1-1 solution. The OSP's and CenturyLink Public Safety team will coordinate and execute the tests defined in the test strategy/acceptance testplan document. **Step 3 Cutover (Timeline ~ 15** days): FINAL Maintenance Operation Protocol (MOP) review w/OSP. Team coordinates cutover dates. Execute cutover.				

	Before and after system cutover, calls from any OSP serving a PSAP, must be able to be answered by that PSAP and transferred to, at a minimum, any other PSAP to which they were initially able to transfer. To ensure call integrity during the deployment, we execute a detailed NG9-1-1 testing plan that includes: • Extensive connectivity checks. • SBC Security Testing: – (1) Topology Hiding – The SBC will be configured to protect the identity of phones, computers and IP devices under test. (optional) – (2) 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. • SBC/SIP Call Routing/Policy Management tests (signaling and Media). Signaling and media will be generated by the OSP. • SIP Trunking Interoperability between our ESInet and NGCS • SIP Trunking Interoperability between our ESInet and NGCS Production Environment • TDM to SIP messaging conversion/Translation • SIP Message manipulation/Mediation – ESRN/ESQK. ESRN SIP Header Insertion • Media Transcoding – Testing Different Codecs, G.711, G.726 optional, G.729 optional. Ensuring the Media Codecs are supported. • DTMF/Fax Interworking – Dual-tone multi-frequency. IP based T.38 Fax Transmission functionality • Abandoned and Silent Calls: – (1) Abandoned call testing – (2) DTMF tone testing – (3) TDD/TT/TTY call testing • Basic T1 BERT Testing – ESF (Extended Super Frame), AMI (Alternative mark Inversion) or B8ZS (Bipolar 8 zero substitution) encoding methods, CRC error testing. • Redundant Components Failover Testing: SBC, Ethernet Switching TDM Conversion • Circuit Failover Testing • Site Failover Testing • End to end Validation testing - CSP to PSAP • Load Balancing – Distributing Traffic Load testing. SIP call load balancing vs failover functionality testing • Simulation of Peak Traffic Load. • Reporting/Monitoring Testing (Peak Load) • Alerting/Alarm Validation Testing (Peak Load) • SLA Compliance Testing (Peak Load). (1) Packet Latency – (20ms); (2) Packet Loss – (0.5%); (3) Jitter – (20ms) • MF trunk (CAS signaling) testing if required: – (1) Trunk seizure and wink back – (2) Feature group D testing

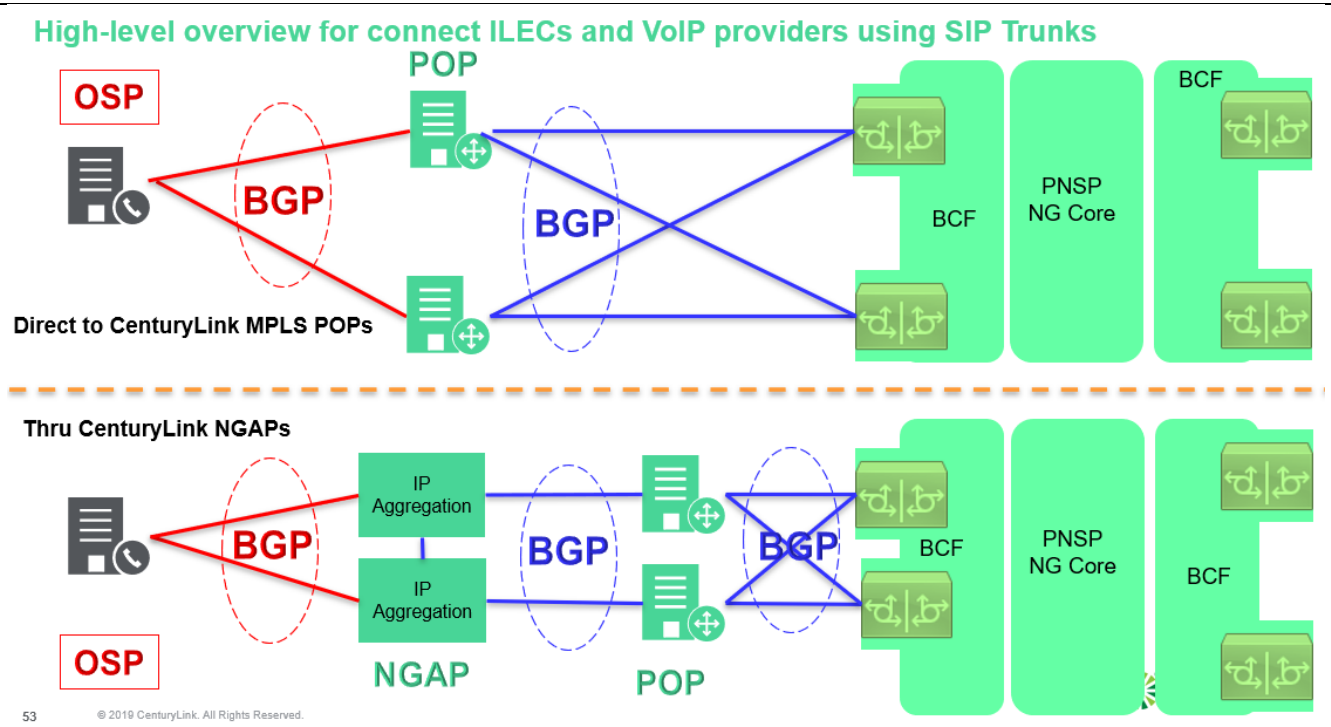
	– (3) Wireless emergency call routed via MSC over MF trunk (ANI and ESRD outpulse) – (4) Wireless emergency call routed via MSC and uses wireline compatibility mode – (5) On-hook indication to SIP BYE • SS7 interface. – (1) SS7 ISUP call end-to- end testing; Supervisory message testing (blocking/unblocking/ acknowledgement) **Call Transfer/Conference functionality** testing Refer to Attachment 2.e"CenturyLink Sample Nebraska Draft Project Schedule Gantt Chart Format" for the sample Gantt chart of this deployment's timelines Refer to the three (3) drawings shown below as "OSP TDM Connection Drawing, POI and Aggregation Service for OSP's Drawing" and SIP Drawing for OSP Connections Drawing:



NGCS 3 - OSP TDM Connection Drawing



NGCS 3 - POI and Aggregation Service for OSP's Drawing



NGCS 3 – Native IP SIP Ingress Drawing

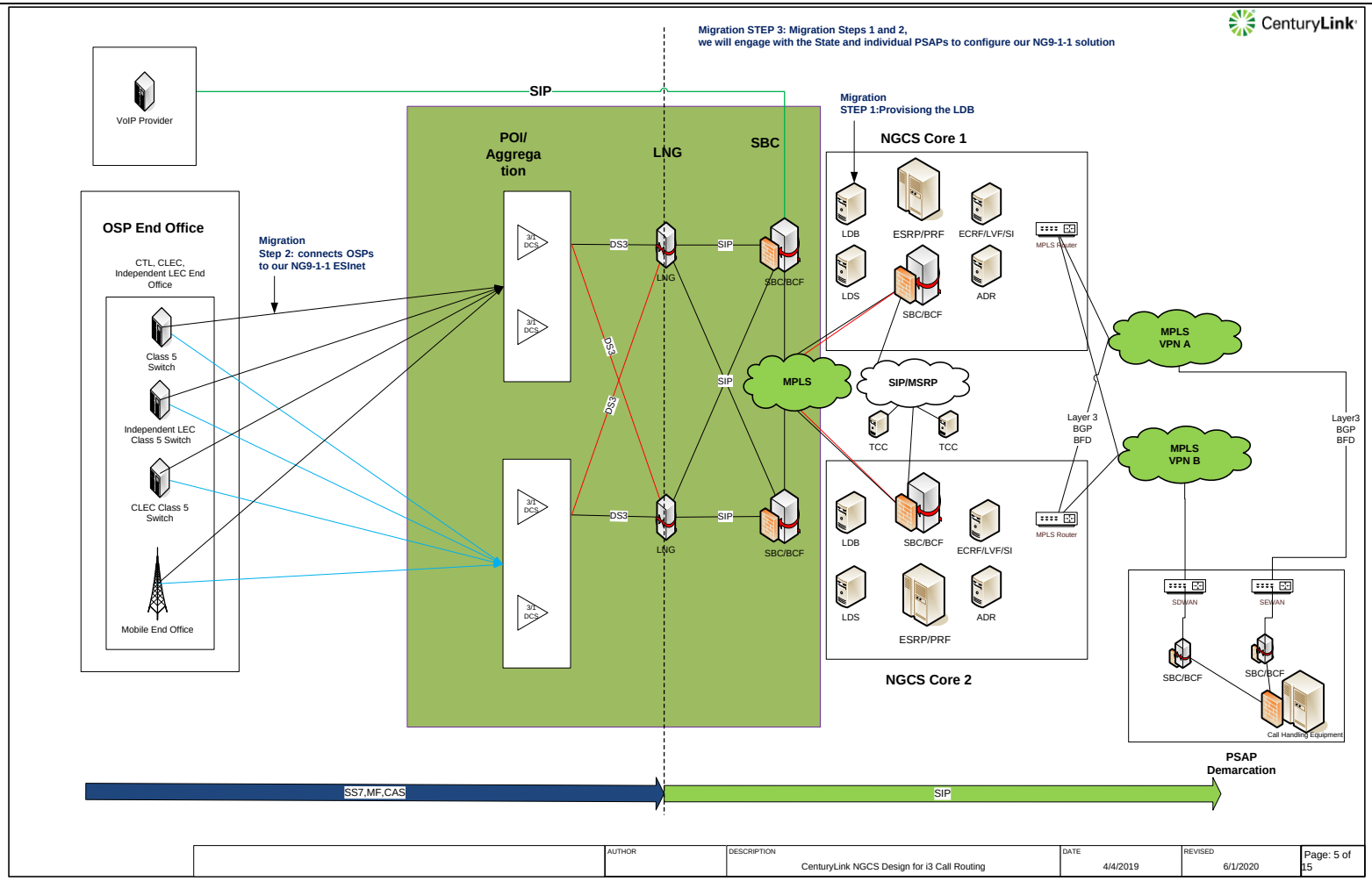
Any additional documentation can be inserted here

NGCS 4	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **LNG Description** The LNG is a signaling and media interconnection point between callers in legacy call-originating networks, i.e., Enhanced 911 (E911), and the NENA NG911 i3 architecture. The LNG shall log all calls it receives and processes and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (TDM) and the IP side of the LNG shall be logged. The LNG shall have Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) functionality to detect and mitigate Distributed Denial of Services (DDoS) attacks from both the TDM side and the IP side. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The LNG shall log all calls it receives and processes and shall permit the uploading of daily log files to a **network monitoring and management system for analysis.** CenturyLink collects all CDR logs from our LNGs for all calls received on TDM interfaces and transmitted upstream at the IP interface. CenturyLink collects and stores this data for monitoring and analysis of the LNG and upstream IP interfaces. This data is used to provide health statistics within our customer dashboards. The CDR captures all relevant call details such as TDM incoming trunk group and member, calling party, signaling parameters, date and time stamp, was call delivered for example The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response CenturyLink allows for ad hoc uploads of log files for troubleshooting and incident response The LNG shall have Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) functionality to detect and mitigate Distributed Denial of Services (DDoS) attacks from both the TDM side and the IP side. DDoS is relevant to only the IP side of our LNGs. CenturyLink does have controls for detecting and responding to TDOS attacks. When we detect a TDOS attack, CenturyLink will work with the Commission and affected PSAPs on the best method to employee to stop the TDOS attack. An example of this would be we determine that the attack is only coming from a small amount of NPA – NXXs, or a specific range of ES Trunks from one OSP, we can block traffic from only the sources we identify for a specific amount of time if this is the action the Commission and affected PSAPs would like implemented. From our LNG to our dedicated NG9-1-1 SBCs (LNG BCF), these circuits are completely private and not routable except from and to our NGCS BCF. We apply our IDS/IPS further downstream before any malicious traffic can reach the network domain between the LNG BCF and the NGCS BCF. Our CenturyLink network infrastructure is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. We employ high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/Application availability is safeguarded with clustering and load balancing techniques. Furthermore, our security architecture employs defenses that include, but are not limited to, Stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress.				

	We discuss our full solution security in the security questions above.

NGCS 5	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** Contractor shall provide redundant, resilient LNGs with legacy selective router gateway (LSRG) functionality to allow the legacy selective routers to transfer calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to deployed NGCS and vice versa. Legacy functionality and components shall be in place and operational during the NG911 transitional phase until all 911 authorities and PSAPs served by the legacy selective router have completed the transition. Describe the steps bidder will take to meet the transition timelines and minimize overlapping network costs.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: As one of the largest ILECs and operating four of the five legacy selective routers (LSR) in Nebraska, CenturyLink can minimize and provide significant cost savings to the Commission. Our proposal includes all ES Trunk connectivity to our POIs from CenturyLink serving wire centers with no cost recovery. CenturyLink will not bill cost recovery to the Commission under state tariff for this connectivity if CenturyLink is awarded the State contract to provide NG9-1-1 services. Included in our solution is an LSRG and all inter-tandem turnking needed to connect to all five state LSRs. Often missed and critically important in the migration to a NG9-1-1 solution is the migration of PS ALI customers. Without continuing to support the LSR for legacy PS ALI customers, these customers can be left scrambling to find an alternative solution that works with a NG9-1-1 system. CenturyLink will continue to maintain and support the LSR and LSRG until all PS ALI customers are migrated as the final phase to decommissioning the LSRs. CenturyLink has developed a process we call "Transitional, Consolidation and Transformation" (TCT) which provides a robust tried and tested framework. TCT projects have 3 broad phases: 1. Transition – CenturyLink will take-over customers' existing estates and enable them take advantage of instant cost savings. 2. Consolidate – CenturyLink will look to make efficiency savings and network improvements. 3. Transform – CenturyLink will work with the State of Nebraska to implement new NG9-1-1 technologies to agreed service levels. CenturyLink Project Management (CPM) adheres to Best Practices Methodology as prescribed by the Project Management Institute standards. The CPM charter underscores CenturyLink's commitment to facilitate a seamless transition for our customer's communications services to CenturyLink's network, ensure compliance with the terms of the contract, and maintain customer satisfaction throughout the project life cycle. We believe that by following these proven project management practices, the project milestones can be successfully achieved. **MIGRATION STEP 1:** In order to eliminate the current expense associated with the existing ALI DBMS, Migration Step 1 involves provisioning of the Location Database (LDB). Once this step is complete, the existing ALI DBMS can be eliminated. Our Proposal includes an LDB that can serve as both an ALI and a LIS. We provision a migration mechanism for both data and business processes, making the transition a flexible, yet controlled, evolution. We support current and future versions of location validation, emergency call routing, and location-based call routing. Our service consists of database and database management software. It provides request / response and is compatible with all leading Automatic Number Identification (ANI) / ALI				

	controllers as well as NG9-1-1 components such as Legacy Network Gateways (LNGs) and Emergency Service Routing Proxies (ESRPs). Our software can provision customer location data manually and in batches. **MIGRATION STEP 2**: In order to eliminate the current expense associated with State reimbursements to originating service providers for connectivity to selective routers, Migration Step 2 connects OSPs to our NG9-1-1 ESInet. Once that occurs, 9-1-1 calls will be routed through the NG9-1-1 ESInet to the selective routers. Existing OSP connectivity to the select routers can be disconnected. OSPs deliver 9-1-1 calls to the POI with the ESRN in the calling party 'to' field and ANI or ESQK/ESRK in the calling party 'from' field. The trunks are processed through a Protocol Internetwork Function (PIF). The PIF converts TDM trunks to Session Initiation Protocol (SIP) trunks with ANI, ESQK or ESRK in the P-Assert Identity field. The PIF also provides TTY transcoding for TDM trunks. The NG9-1-1 ESInet also provides a direct interface for OSPs able to connect via SIP with or without PIDF-Lo. **MIGRATION STEP 3:** In a parallel effort to Migration Steps 1 and 2, we will engage with the State and individual PSAPs to configure our NGCS. Our team will work with the user agency(s) to develop a Functional Specifications Document (FSD) that will establish in detail the specific goals, objectives, deliverables, and measures of success. At this point, a Project Management Plan (PMP) can be developed with a high degree of certainty. Once 9-1-1 calls flow through our NG9-1-1 service in step 2 above, PSAPs can be systematically and individually transitioned off the selective router and onto NGCS solution. This process mitigates transition risk by allowing for fallback to legacy connectivity. Once thoroughly tested, PSAPs can disconnect from the selective router and repurpose associated expense for NG9-1-1 services. PSAPs with CPE that does not currently support an IP interface will be equipped with an LPG. The PIF portion of the Legacy PSAP Gateway (LPG) will be provisioned on-site. Once the PSAP has upgrade their CPE to accommodate NENA i3 IP connectivity, the LPG will be replaced with an SBC. It is strongly recommended that the PSAP use their funds to upgrade their CPE instead of purchasing an LPG. CenturyLink will provide transition planning and migration support and timelines through our assigned Project management team. The detailed steps to transition to the NGCS LNG/LSRG is outlined in Attachment 2.d "CenturyLink Sample Program Management Plan for Nebraska" document.



NGCS 5 – MG9-1-1 Transitional Drawing

Any additional documentation can be inserted here

Attachment “C”
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 6	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Previous Work on Similar Solutions** 1. Explain how bidder has worked with legacy OSPs with similar solutions on similar projects. 2. Submit specific plans for working with established legacy 911 service providers in Nebraska.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

Explain how bidder has worked with legacy OSPs with **similar solutions on similar projects.**

CenturyLink has a long history of working with OSPs across the globe. We are ILECs and/or CLECs in all 50 states. Our most recent work with OSPs on a CenturyLink NG9-1-1 solution is in SD, CO, and CA. In SD and CO, CenturyLink provided all E9-1-1 services in the state. In CA, CenturyLink operates as a CLEC. We are currently in the deployment phase of the network and are working with OSPs to move their services to CenturyLink POIs.

Submit specific plans for working with established legacy 911 service providers in **Nebraska.**

CenturyLink is the major legacy 911 service provider in the state. For this response, we will detail our plan for working with the other state 911 service provider, Windstream. CenturyLink has a long relationship with Windstream in Nebraska and other states were CenturyLink and Windstream operate. CenturyLink has existing interconnect agreements with Windstream and existing process for order services between us.

Step 1 - Design, Assign & Test (Timeline ~ 30 days): OSP inventories 9-1-1 connectivity and capacity requirements . Our team reviews end-to-end signaling design with OSP. OSP requests LOA/CFA (Letter of Authority/ Customer Facility Assignment); our team assigns 9-1-1 POI location. We provide cross-connect information when the OSP connecting to our ESInet via SIP. OSP circuit activation (BERT) by Network Delivery Team. OSP and team coordinate trunk activation.

Step 2 Signaling (Timeline ~ 25 days): OSP submits SS7 ISUP orders to enable (possible 3rd Party). If SIP, share host and IP with OSP and coordinate Inter-Op testing. OSP and our team coordinate end-to-end test calls to our NG9-1-1 ESInet. The OSP's and our CenturyLink Public Safety team will ensure proper routing is in place on the voice and signaling switches to deliver calls to the NG9-1-1 solution. The OSP's and CenturyLink Public Safety team will coordinate and execute the tests defined in the test strategy/acceptance testplan document.

Step 3 Cutover (Timeline ~ 15 days): FINAL Maintenance Operation Protocol (MOP) review w/OSP. Team coordinates cutover dates. Execute cutover.

Before and after system cutover, calls from any OSP serving a PSAP, must be able to be answered by that PSAP and transferred to, at a minimum, any other PSAP to which they were initially able to transfer. To ensure call integrity during the deployment, we execute a detailed NG9-1-1 testing plan that includes:

- Extensive connectivity checks.
- SBC Security Testing:
  - (1) Topology Hiding – The SBC will be configured to protect the identity of phones, computers and IP devices under test. (optional)
  - (2) 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.
- SBC/SIP Call Routing/Policy Management tests (signaling and Media). Signaling and media will be generated by the OSP.

	• SIP Trunking Interoperability between our ESInet and NGCS • SIP Trunking Interoperability between our ESInet and NGCS Production Environment • TDM to SIP messaging conversion/Translation • SIP Message manipulation/Mediation – ESRN/ESQK. ESRN SIP Header Insertion • Media Transcoding – Testing Different Codecs, G.711, G.726 optional, G.729 optional. Ensuring the Media Codecs are supported. • DTMF/Fax Interworking – Dual-tone multi-frequency. IP based T.38 Fax Transmission functionality • Abandoned and Silent Calls: – (1) Abandoned call testing – (2) DTMF tone testing – (3) TDD/TT/TTY call testing • Basic T1 BERT Testing – ESF (Extended Super Frame), AMI (Alternative mark Inversion) or B8ZS (Bipolar 8 zero substitution) encoding methods, CRC error testing. • Redundant Components Failover Testing: SBC, Ethernet Switching TDM Conversion • Circuit Failover Testing • Site Failover Testing • End to end Validation testing - CSP to PSAP • Load Balancing – Distributing Traffic Load testing. SIP call load balancing vs failover functionality testing • Simulation of Peak Traffic Load. • Reporting/Monitoring Testing (Peak Load) • Alerting/Alarm Validation Testing (Peak Load) • SLA Compliance Testing (Peak Load). (1) Packet Latency – (20ms); (2) Packet Loss – (0.5%); (3) Jitter – (20ms) • MF trunk (CAS signaling) testing if required: – (1) Trunk seizure and wink back – (2) Feature group D testing – (3) Wireless emergency call routed via MSC over MF trunk (ANI and ESRD outpulse) – (4) Wireless emergency call routed via MSC and uses wireline compatibility mode – (5) On-hook indication to SIP BYE • SS7 interface. – (1) SS7 ISUP call end-to- end testing; Supervisory message testing (blocking/unblocking/ acknowledgement) • Call Transfer/Conference functionality testing

Any additional documentation can be inserted here

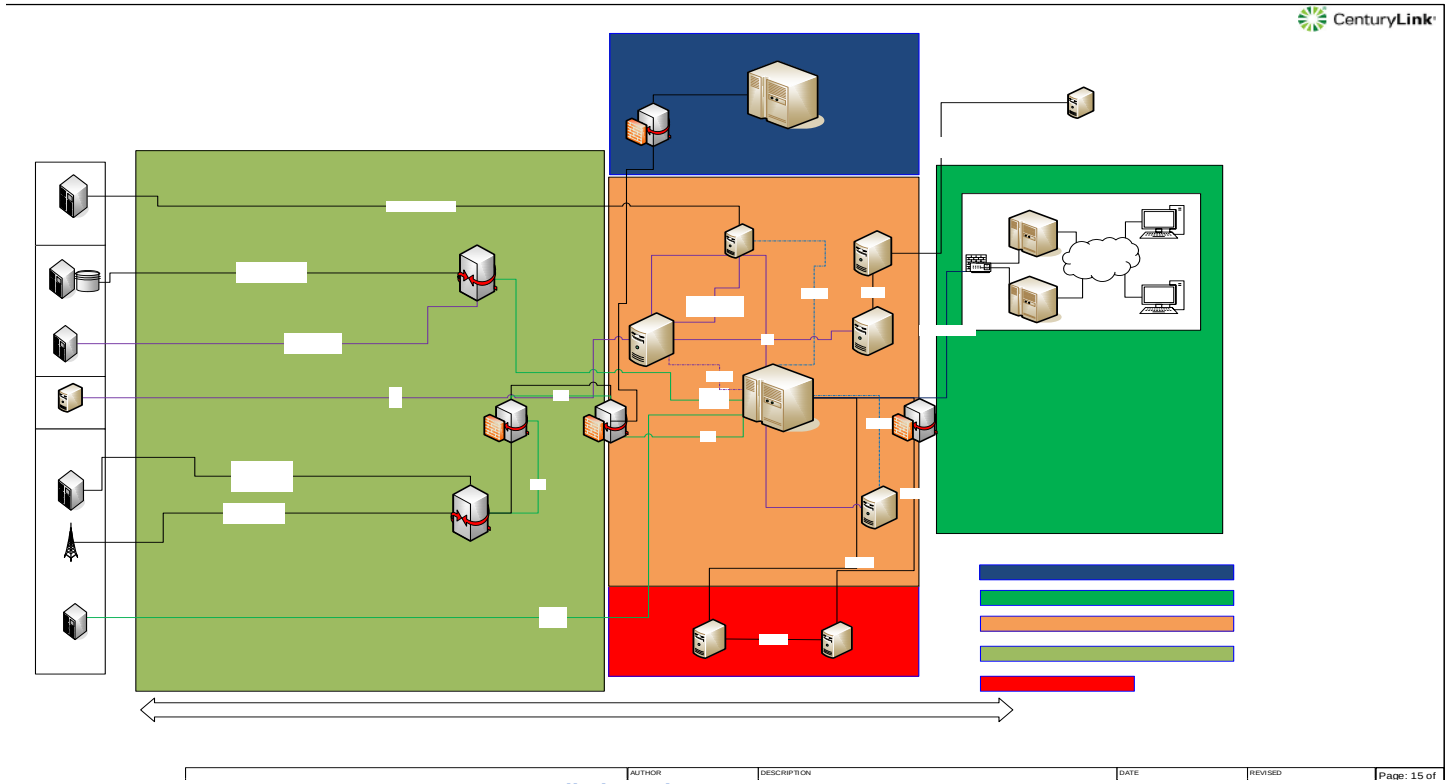
Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 7	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Traffic Engineering Process** Describe the process that will be utilized to analyze the current trunk engineering for 911 traffic, and to validate any applicable trunk rebalancing for public-safety grade service.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: As a 911 service provider for the State of Nebraska CenturyLink has existing knowledge of the current ES trunks that terminate on our legacy selective routers. For OSPs that don't currently terminate their ES trunks on one of the four CenturyLink selective routers in Nebraska, we use the Local Exchange Routing Guide (LERG) database managed by Telcordia, that provides all the existing wire centers within the state and the number of subscribers serviced out of those wire centers. In addition to traditional wireline services, these reports provide the subscriber base of VoIP and wireless OSPs. CenturyLink uses a long standing and proven industry standard to calculate the required ES trunks for wire centers based on the number of subscribers serviced by a serving wire center. The industry rule is for serving wire centers with 10,000 or less subscribers, 2 ES trunks must be provisioned to route 911 calls. For every additional 5,000 subscribers, one additional ES trunk must be provisioned. Therefore, a wire center with a subscriber base of 20,000, we would expect that OSP to deliver 4 ES trunks to our Point of Interfaces (POI). In this example, the OSP would deliver 2 ES trunks to POI A and 2 ES trunks to POI B. From the POI to our LNGs, we provision diverse DS3s, one to each of our geo-redundant carrier grade LNGs. Each DS3 is provisioned to carry 100% of the TDM traffic from the POI to the LNG in the event connectivity to an LNG is lost. The number of DS3s from each POI to the LNG is a function of the number of ES trunks terminating at the POI. Each DS3 can carry up to 672 DSOs or ES trunks. After the media has be transcoded to IP at the LNG, CenturyLink provisions diverse 10G IP circuits to each geo redundant dedicated NG9-1-1 SBC. Each link from the LNG to the SBC is provisioned to handle 100% of the traffic load. At implementation, we will adjust (rebalance) our POI capacity up or down based on the number of ES trunks OSPs will deliver. After implementation, CenturyLink monitors the ingress TDM traffic, validating we are delivering a P.01 grade service or greater on all trunk groups.				

Any additional documentation can be inserted here

NGCS 8	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Location Information** The LNG shall obtain location information to define, create, populate and send the correct Presence Information Data Format Location Object (PIDF-LO) parameter to the correct ESRP or terminating PSAP, as described within NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our solution to constructing an LNG is to utilize the NIF included with our BCF and move the LIF functionality to the ESRP. The ESRP immediately inspects the SIP INVITE for the presence of a PIDF-LO or location URI contained in the SIP Call-Info Header. If these two conditions are not met, the ESRP will submit a HELD query to the LDB and update the SIP Call-Info Header with the location URI, and use the PIDF-LO to query the ECRF for obtaining a call route to the appropriate PSAP. To overcome the problems of legacy ALI systems, NENA recommends the use of the Location Interwork Function, or LIF, within the Legacy Network Gateway, utilizing an internal location database with steering data as needed. This database is often referred to as an LDB, or Location Database (NENA-INF-008.2-2014). The LIF is a part of the LNG, although it can be physically separated. A Location Database (LDB) serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment and is included in this response to fully replace the existing ALI database and enable smooth transition to NG9-1-1. When legacy systems present ANI to the LNG, the LNG will utilize the LDB within the LIF to attach location to the call. The LNG issues a HELD query to the LDB, which will return a PIDF-LO adhering to the NENA CLDXF standard. Typically, the LNG will attach the location-by-reference URL into the SIP header allowing downstream elements (such as an ESRP or terminating PSAP CHE) to perform a dereference query over HELD to get location-by-value.				

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



NGCS 8 – Call Flow Diagram - PIDF-LO – ESRP to PSAP

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Protocol Conversion** **External Interfaces** The LNG external interfaces shall comply with NENA-STA-010.2-2016, requirements SLA 1-23, and other applicable standards and requirements. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 10	Bidder Response: CenturyLink's LNG supports protocol conversion as per NENA-STA-010.2-2016. Our LNGs support TDM to SIP conversion. CenturyLink LNGs and LSRG both support protocol conversion from TDM to SIP. Standard TDM interfaces we support are listed below: 9-1-1 Call Signaling Type • SS7 Wireline/NCAS (10 digits) • PRI/NI-2 (wireline, NCAS) • Analog CAMA I+7 (I always = 0) • DS1 CAMA I+7 (I always = 0)				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Baudot Code Transcoding** The bidder's BCF solution shall support transcoding of Baudot tones to real-time text (RTT), as described in IETF RFC 4103. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 11	Bidder Response: Our Legacy network Gateways transcodes Baudot to RTT as described in RFC 4103. We comply with NENA 08-003, NENA-STA-010.2-2016 that requires interworking real time text and TTY in our PIF component per RFC 5194, accepting DTMF signaling from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 4733, and recognizing Baudot tones in incoming media and replacing them with RFC 4103 real time text. CenturyLink's NGCS solution is committed to working within the specifications laid out by NENA, the PSAP communities and industry vendors for Next Generation 9-1-1 and NENA i3 standards. Specific delivery options available today that allow RTT to be delivered via TTY (baudot) emulation will be supported in the CenturyLink NG9-1-1 ESInet solution presented to the appropriately routed PSAP's. Our CenturyLink NGCS supports MSRP as the standard protocol for handling text. Other protocols such as XMPP may be supported if interworked to MSRP prior to NGCS presentation. We support RTT within the NG9-1-1 data stream natively. It is the role of the call-handling equipment to decode RTT correctly. CenturyLink will also work closely with Originating Service Providers, ESInet functional component vendors, and PSAP CPE vendors to proactively support end-to-end interoperability. Specific delivery options available today that allow RTT to be delivered via TTY (baudot) emulation will be supported in the CenturyLink NGS solution presented to the appropriately routed PSAP's. CenturyLink's NGCS Solution supports RTT within the NG9-1-1 data stream natively. It is the role of the CPE equipment to decode this correctly.				

Any additional documentation can be inserted here

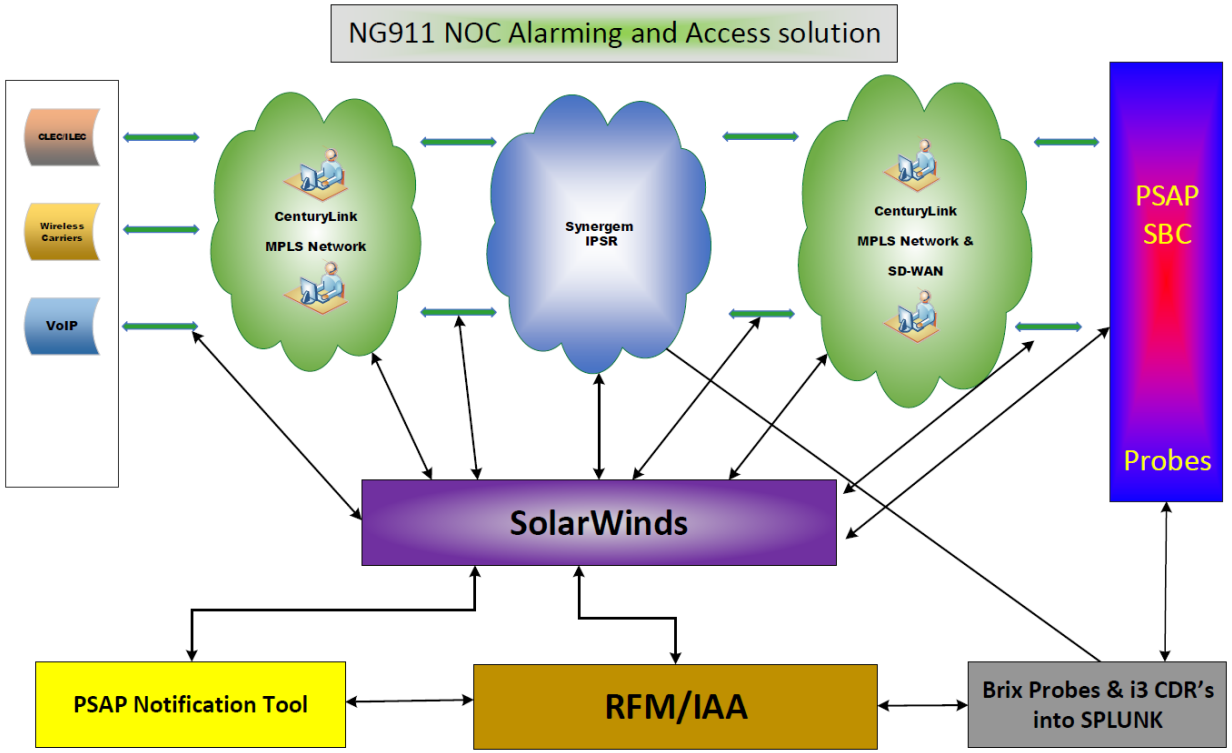
NGCS 12	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Callback Number** The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the Contractor to obtain the callback number from the wireless or VoIP provider and may include additional recurring and non-recurring costs that are independent of this RFP. The Contractor shall be responsible for all recurring and non-recurring costs associated with this requirement. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink complies to all NENA i3 standards as described in NENA-STA-010.2 Our NG9-1-1 solution uses a Legacy Network Gateway (LNG) that provides a mechanism to obtain the caller's location and callback number at the time of the call by using the Location Interwork Function (LIF) to query the OSP's appropriate transitional location database solution. Prior to the carrier's i3 transition, CenturyLink will continue to manage the location data retrieval solution on behalf of the OSP. The CenturyLink solution is designed to leverage the existing VoIP and Wireless legacy solutions during the transitional period while those carriers work towards i3 readiness. Prior to OSP i3 readiness, the provider will continue to send the pseudo ANI with the originating call to the current LNGs. Once received by the LNG, our NG9-1-1 solution will perform the proper NIF, LIF, and PIF functions to query the CenturyLink-managed LDB and steer queries to the external OSP location database to acquire the callback number and location information. The HELD interface into the CenturyLink Location Database (LDB, aka ALI) is leveraged by the NG9-1-1 system to retrieve PIDF-LO, by value, to be delivered to the PSAP within the SIP messaging. The HELD interface is also presented to the PSAP CPE to provide dereferencing services and/or provide location updates for wireless calls. Note that not all ALI fields map to PIDF-LO, for example Class of Service and Customer Name. As such, CenturyLink will also provide an ADR interface to retrieve this information to be included in the SIP signaling. For these fields, the LNG supports the Additional Data protocol (draft-ietf-ecrit-additional-data-28) to provide these data fields via the Additional Data Repository (ADR). This solution is in production with multiple live CenturyLink-managed i3 PSAPs.				

Any additional documentation can be inserted here

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Event Logging** The LNG shall facilitate logging of all significant events and 911 calls received and processed. Each call log shall contain all relevant parameters defined in Section 5.13.3 of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 13	Bidder Response: The LNG facilitates logging of all significant events and 9-1-1 calls received and processed. Each call log contains all relevant parameters as defined in NENA STA-010.2-2016. Our NG9-1-1 solution provides an i3 logging capability per the NENA STA-010.2 specification. The system can support near real-time log delivery and web service interfaces for log retrieval from authorized clients. Our NG9-1-1 solution logs hundreds of data points for each call that traverses the system to assist in tracking and troubleshooting calls. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. The Customer Management Portal provides participating PSAPs and approved personnel 24x7 access to call detail records through a secure, web-based portal. The call detail records provide the user with all of the pertinent information for each call. Additional Logging Events Includes: Provides logging of 9-1-1 metadata traffic to include Text-to-9-1-1. • Utilize SIP metadata and i3 logging to monitor, track and verify data flow. • Log the Events for Core Functional Elements within the network (BCF to PSAP) but not within the in the PSAP. • Support RFC 7865 and 7866 (previous known as SIPREC) to record only MSRP. • Use OAuth2 authorization. Users have a predetermined PSAP or set of PSAPs for which they are able to view statistics. For example, some users will only be able to view their own PSAP's statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping. Event data is time stamped upon ingress of payload entry through the LNG or BCF and at the time of answer and disconnect at the PSAP. Event data also tracks the time for each functional element to perform routing and PSAP assignment, by tracking the time it takes to traverse from the selective router to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics				

Any additional documentation can be inserted here

NGCS 14	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Extraction of Log Files** All LNG log files shall be capable of being extracted in near real-time and shall be in a format suitable for importing into a spreadsheet or word-processing program. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our Legacy Network Gateway (LNG) provides both CDR and Syslog output for off-line analysis. LNG log files are capable of being extracted in near real-time and are available in a format suitable for importing into a spreadsheet or word-processing program. Our LNG CDRs are captured using our SolarWinds monitoring and reporting system. These CDRs are passed through RFM / IAA as is data from all of our monitoring tools. All CDRs are stored in our SPLUNK application for operational analysis and troubleshooting. Reports in our SPLUNK tool are already capable of preparing reports in CSV and PDF formats.				

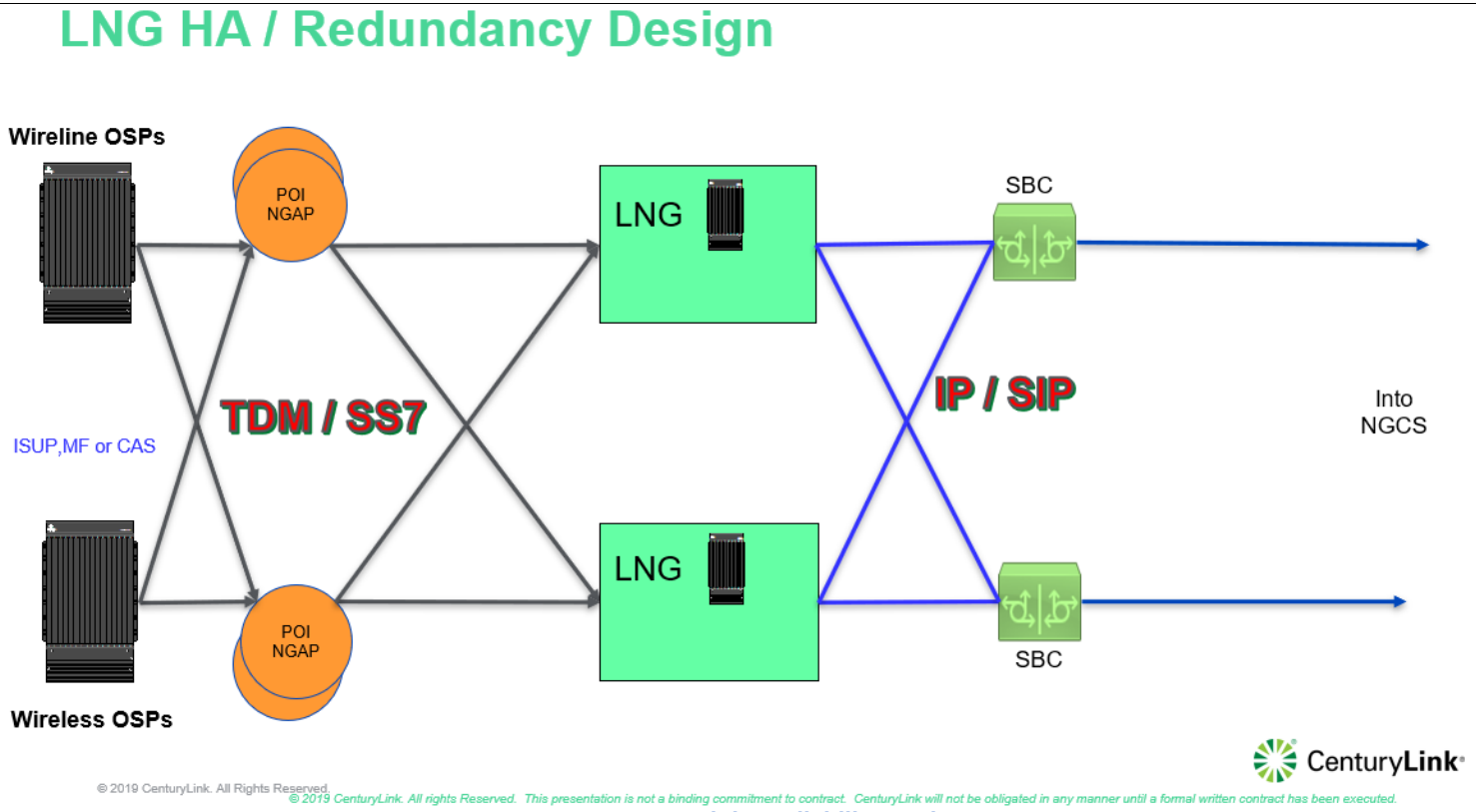


NGCS 14 - This diagram illustrates the operating components of the 7 and describes some of the reports that it generates.

Any additional documentation can be inserted here

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 15	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **High-Availability Design** The LNG solution shall be deployed in a high-availability design to meet public safety-grade resiliency and redundancy requirements, Section V.D.1.b. (General Requirements – Technical – Public Safety Grade). Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink's LNGs are designed with high availability and meet public safety-grade resiliency and redundancy requirements. CenturyLink deploys a minimum of two redundant POIs for OSP to connect their end offices to. OSPs connect half of their ES Trunks to POI A and the other half to POI B. From each POI, we provide a pair of diverse DS3 circuits with circuit A terminating at LNG A and circuit B terminating at LNG B. This design provides for 100% failover from one LNG to the other LNG in the event connectivity from a POI to an LNG experiences a service disruption. From each LNG, we configure a pair of diverse 1G MPLS circuits to each of our diverse session border controllers (SBC). This design provides for 100% failover of all traffic from one SBC to the diverse SBC. From our diverse SBCs facing the LNGs, we configure a pair of diverse 10G circuits to our diverse SBCs facing into our NGCS. This design provides for 100% failover of all traffic from the LNG SBCs to the NGCS SBCs. All terminating equipment at our POIs and LNGs are designed with high-availability and redundancy. There is not single point of failure in our LNG design. On the egress side of our LNGs, we deploy a set of HA routers for our MPLS network to a diverse pair of SBCs. At each SBC location, we have two active SBCs for additional redundancy. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology.				



NGCS 15 – LNG High Availability Design.

Any additional documentation can be inserted here

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Legacy Selective Router Gateway (LSRG) Functionality** The LSRG functionality shall support selective transfer, commonly referred to as "star code" transfers, made by legacy PSAPs for calls destined for the NextGen911 PSAPs or to neighboring legacy PSAPs outside of the ESInet. Describe how bidder's LNG solution provides for LSRG functionality.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 16	Bidder Response: CenturyLink will provide a LSRG to facilitate the transfer of 911 calls from a legacy PSAP to a NG911 PSAP and from a NG911 PSAP to a legacy PSAP with the capability of using star codes. The LNG/LSRG relationship is addressed in our NG9-1-1- ESInet Solution. It provides the transitional elements to convert traffic from TDM/SS7 to SIP. Through diverse Point of Interconnections (POIs) strategically placed across Nebraska. Our LNG functions for the legacy network (LNG, LSRG) as well as enhanced wireless Location Determination Services (LDS). This solution supports star codes natively as part of its design. Our NG9-1-1 network supports star code transfers made by legacy PSAPs for calls destined for PSAPs on the ESInet or to neighboring legacy PSAPs outside of the ESInet. A call taker can use a single button on the call taker's display to complete either a transfer or three-way conference. They can transfer an incoming 9-1-1 call to another agency by pressing a button labeled with the type of agency: for example, "Fire"-on the PSAP premises equipment. These transfers utilize pre-provisioned codes on a per-PSAP basis.				

Any additional documentation can be inserted here

NGCS 17	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Proposed LNG Locations** Provide the proposed locations for hosting the primary LNGs for the NextGen911 system, including the data center tier level for the host sites.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink uses our carrier grade Sonus gateways for our LNGs. We have three sets of gateways installed in tier 3 data centers our carrier hotels. The locations of our GSXs are as follows: • Huston, TX – Tier 3 • Chicago, IL – Tier 3 • Highland Ranch, CO – Tier 3 CenturyLink will terminate OSP using these three LNGs.				

Any additional documentation can be inserted here

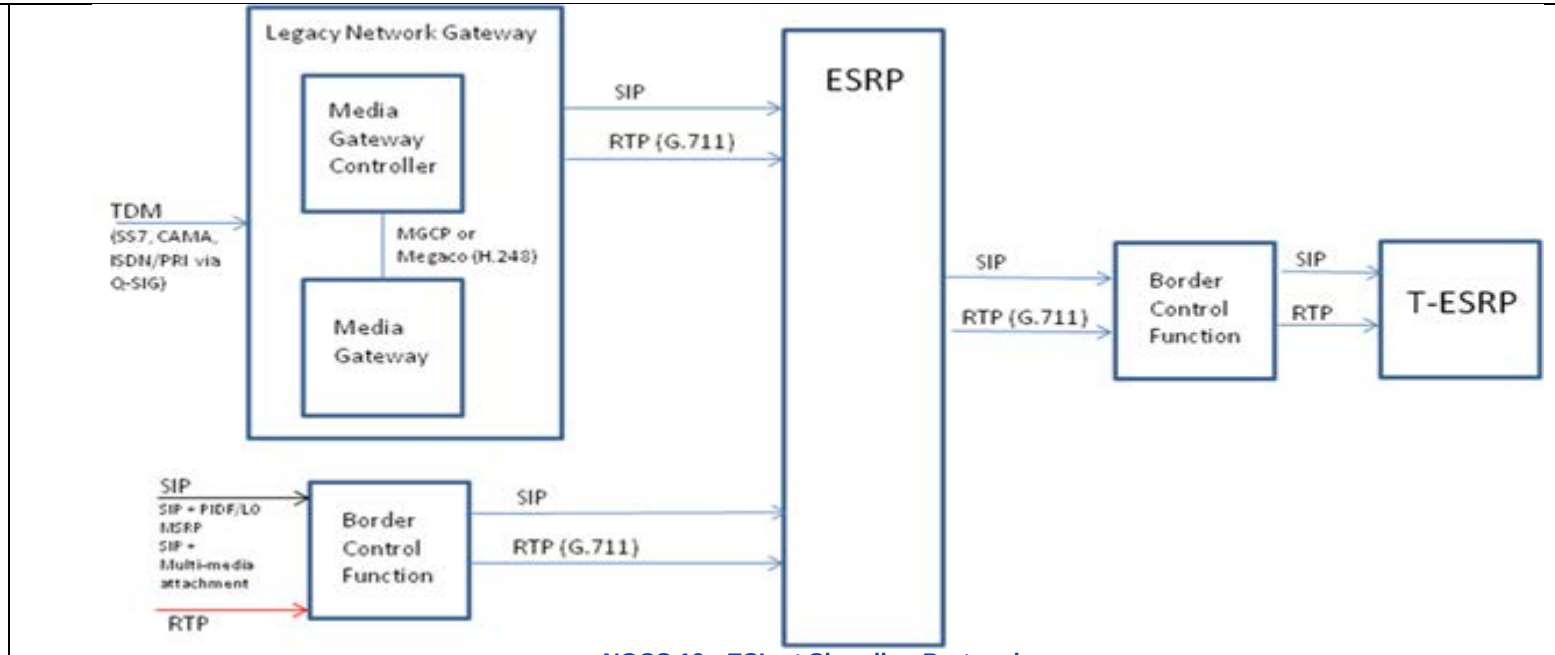
NGCS 18	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Charges for Dual Service** The bidder shall be responsible for meeting the timelines outlined above in requirement NGCS 2 and 3. If the transition from the legacy selective routers to NGCS exceeds the committed timeline, and is attributable to the acts or omissions of the Contractor, the Contractor will accept responsibility for financial support of the legacy network until such time as the full transition is complete. Describe how bidder's solution meets this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: All of our CenturyLink deployments includes a parallel installation when moving to a NG9-1-1 solution. We understand this requirement and accept financial responsibility				

NGCS 19	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Description** The BCF shall provide logical network security functions between external networks and the ESInet, and between the ESInet and PSAP networks. The BCF is responsible for numerous functions, including the following: a. Border firewall; b. VPN; c. IDS/IPS; d. Session Border Control (SBC); e. Opening and closing of pinholes; f. Limiting access to critical components through the use of VLANs. g. Call admission control; h. Media transcoding; i. Signaling protocol normalization and interworking; j. Network Address Translation (NAT); k. Codec negotiation; l. Support for QoS and priority markings; and, m. Media proxy. Provide details, including drawings, describing how the proposed BCF meets or exceeds all functions listed above and the requirements described in NENA-STA-010.2-2016, as well as additional firewall requirements described in NENA 04-503, NENA-INF-015.1-2016, and NENA 75-001, or the next subsequent version of the NENA documents listed that are publicly available at the proposal release date.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The BCF secures and segments the core functions to the transport network for the PSAP and external data sources which all remain in separate security domains. All messaging transiting the network uses SIP. If not delivered in SIP natively, it must be interworked to SIP using the Protocol Interwork Function (PIF) of the Legacy Network Gateway (LNG). This BCF provides both application and network layer protection and scanning. It will also mitigate lower layer protocol attacks and provide denial of service (DoS) and distributed denial of service (DDoS) detection and protection. In accordance with NENA-STA-010.2 (Section 6), the BCF/SBC will ensure any connection involving a call origination sources, gateways, and similar elements outside the ESInet are properly screened. • Ensure the BCF supports an automated interface that allows a downstream element to mark the source of a call as a "bad actor". This would normally occur when a call is received that appears to be part of a deliberate attack on the system. • Ensure the BCF installs a "NENA-source" parameter in the Via header that in the outgoing INVITE message associated with every call. Calls are marked by the SBC in a way that allows a recipient to identify the BCF that processed the call				

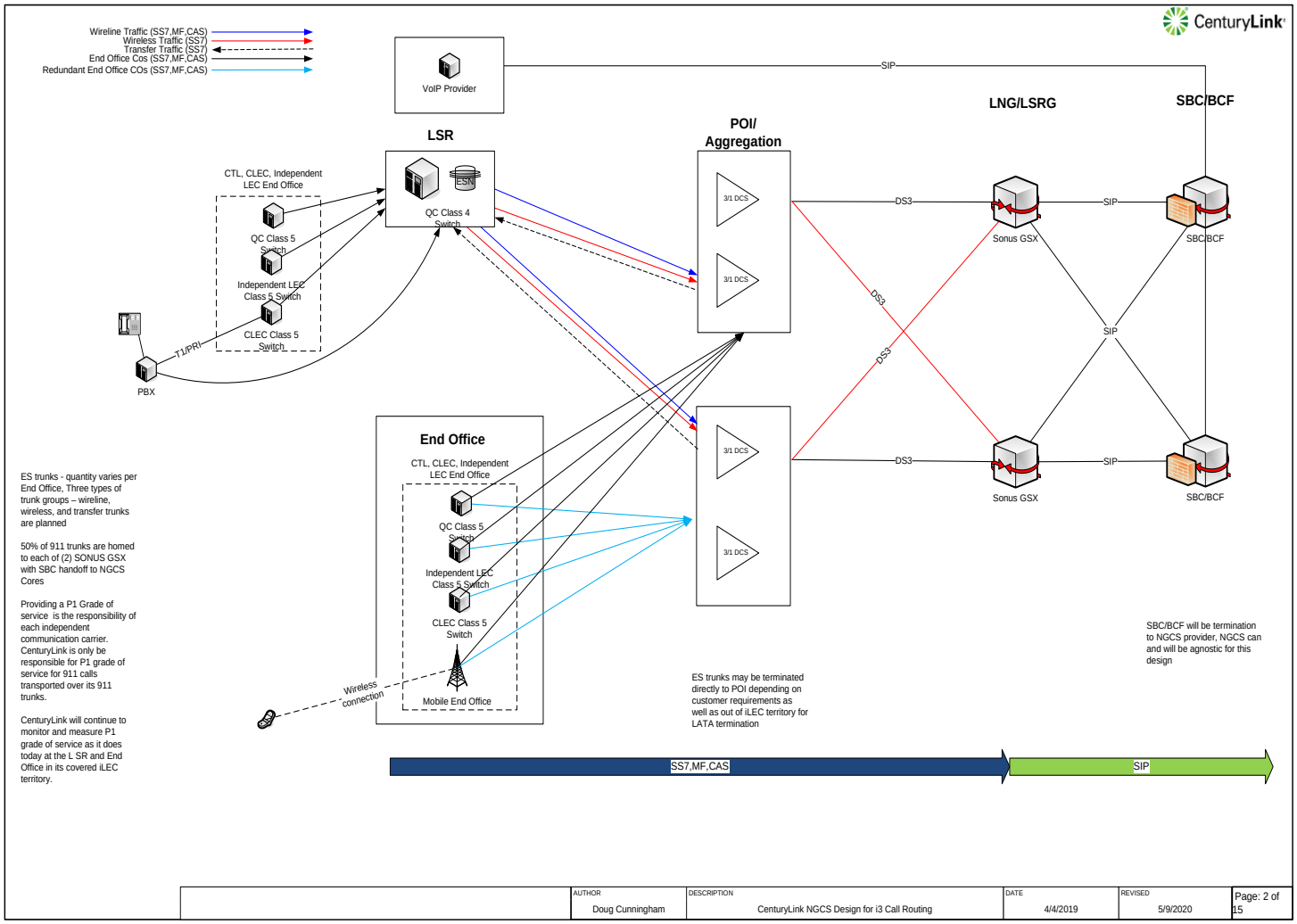
Additional functions and advantages of our BCF includes:

1. The **Border firewall** component of the our BCF/SBC will inspect all traffic transiting the network edge. Includes firewall rules, access control lists ("ACLs"), virtual local area networks ("VLANs")in accordance with NENA STA-010.2-2016. Our network supports standard 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.
2. **VPN** – the BCF's SBC supports encryption for calls that are not protected using Secure Sockets Layer (SSL), Transport Layer Security (TLS) Transport Layer Security over TCP (TLS-over-TCP) and Stream Control Transmission Protocol (SCTP) are supported and selectable for each SBC interface to external systems.
3. **IDS/IPS** - Each of our core emergency call processing sites includes border control and security functions including firewalls, intrusion detection systems, and intrusion protection systems. Security management personnel specialize in managing and operating these facilities and validate their operation.
4. We employ redundant **Border Control Function/Session Border Controller** (BCF/SBC) as the foundation of our security solution for call flow protection. It integrates fully with all other NGCS. Threats are detected by monitoring the NENA-defined Security Posture as well as predetermined threat profiles. Log events are created which include:
   - Normal operation: or the presence of suspicious activity that does not impact normal operations
   - The presence of fraudulent calls and events that are stressing a facility's ability to continue most operations
   - System under active attack and overwhelmed. These will be configured to accomplish such goals as elevated trust of call flows and aggregation infrastructure.
5. **PSAP BCF/SBC** are included part of this service as well that will terminate secure traffic to the PSAP and expect to hand off to the endpoint PSAP via customer provided call handling equipment firewall/BCF or SBC. The CenturyLink's NGCS Solution and ESInet are provided with an array of BCFs/firewalls that inspects all traffic transiting the network edge. This device will employ both application and network layer protection and scanning capability as well as mitigates lower layer protocol attacks.
   - The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or Access Control Lists (ACLs). CenturyLink continually investigates and upgrades with new advances in protective technology with tools such as Intrusion Detection System (IDS).
6. **Session Border Control (SBC)** - the SBC supports SIP over Transmission Control Protocol (TCP) primarily and recommended, User Datagram Protocol (UDP), Transport Layer Security over TCP (TLS-over-TCP), and Stream Control Transmission Protocol (SCTP). The SBC populates Layer 3 headers in order to facilitate priority routing of packets and enables interworking between networks utilizing IPv4 and IPv6.
7. **Opening and closing of pinholes** - Our NGCS BCFs are set to deny by default all traffic. Rules are built into the BCF/firewall such that pinholes between the firewalls will allow trusted/known traffic. Allowances go through rigorous scrutiny before being approved by BlackLab compliance NOC/SOC. Once approved, changes are made on a regular basis following standard procedures to ensure no other pinholes

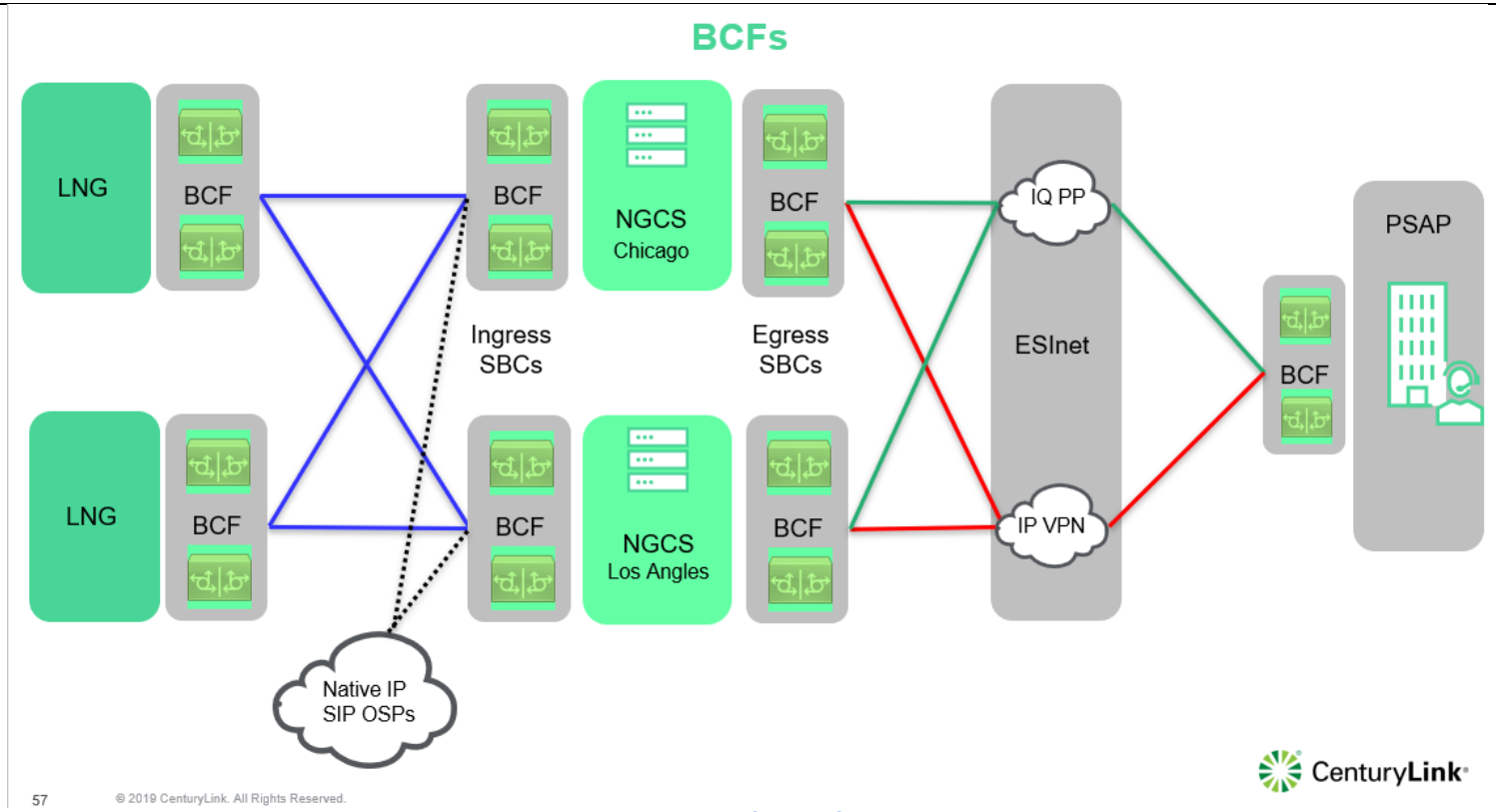
	are opened. Our CenturyLink NOC/SOC also does on-going traffic studies on the firewalls. If a pinhole is opened but not used, the NOC/SOC will close the pinhole if necessary. 8. **Limiting access** to critical components through the use of VLANs - The proposed ESInet is a Quality of Service (QoS)-managed private IP network which can prioritize any type of IP traffic: voice, data, and multi-media. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. These protective measures are supplemented with aggressive physical security for our datacenters and secure delivery of SIP traffic to the PSAP BCF. 9. **Call admission control** – Call admission control (CAC) is used when establishing connectivity to internal and external IP resources. 10. **Media transcoding** Our platform can use various different Codecs, G.711, G.726 optional, G.729 optional and we ensure that the Media Codecs are supported. 11. **Signaling protocol** normalization and interworking - Below is a detailed list of the various VoIP protocols and established multimedia sessions supported by the CenturyLink NG9-1-1 solution. As designed, the CenturyLink NG9-1-1 solution is evolutionary and will be able to support future i3 specifications. The Ng9-1-1 infrastructure is created to not only support an IPSR environment, but to support i3 NENA protocols, features. 12. **Network Address Translation (NAT)** - CenturyLink in national deployment model does not promote or practice the use of NAT within our ESInet infrastructure. As a specific egress carrier has unique needs, CenturyLink will work with that specific carrier to design a solution which best serves the State of Nebraska interests. Our BCF will provide logical network security functions between external ESInet and handle any NAT translations required between the external ESInet and CenturyLink provided ESInet. 13. **Codec negotiation** - The CenturyLink NG9-1-1 solution performs codec negotiation and upgrades all calls by defualt to a codec of G.711., Other codec's may be used. Refer to #11 Media transcoding in this section. 14. **Support for QoS and priority markings** - uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. 15. **Media proxy** – CenturyLink's solution will perform this function. Our BCFs work so that only authorized traffic to authorized end points and predetermined protocols interact with service critical components. The BCF does not impact compliance to the SIP or RTP standards. No impact to system extensibility is introduced by the BCF



NGCS 19 - ESInet Signaling Protocols



NGCS 19 . ESInet Border Control Function Drawing



NGCS 19 – End-to-End BCFs

As part of the CenturyLink's NGCS Solution's access control is provided through the Border Control Function/Session Border Controller (BCF/SBC) at the NGCS datacenters and secures and segments the core functions to the transport network for the PSAP and external data sources which all remain in separate security domains.

The BCF that we employ is the foundation of our security solution for call flow protection. All SIP interfaces to external components traverse through redundant BCF components. In addition to the BCF, firewalls exist for http traffic to external entities such as PSAPs for the PSAP Management Portal functional capabilities. The BCFs work so that only authorized traffic to authorized end points and predetermined protocols interact with service critical components

CenturyLink's BCF integrates fully with all other NGCS. Threats are detected by monitoring the NENA-defined Security Posture as well as predetermined threat profiles. Log events are created which include (1) Normal operation; or the presence of suspicious activity that does not impact

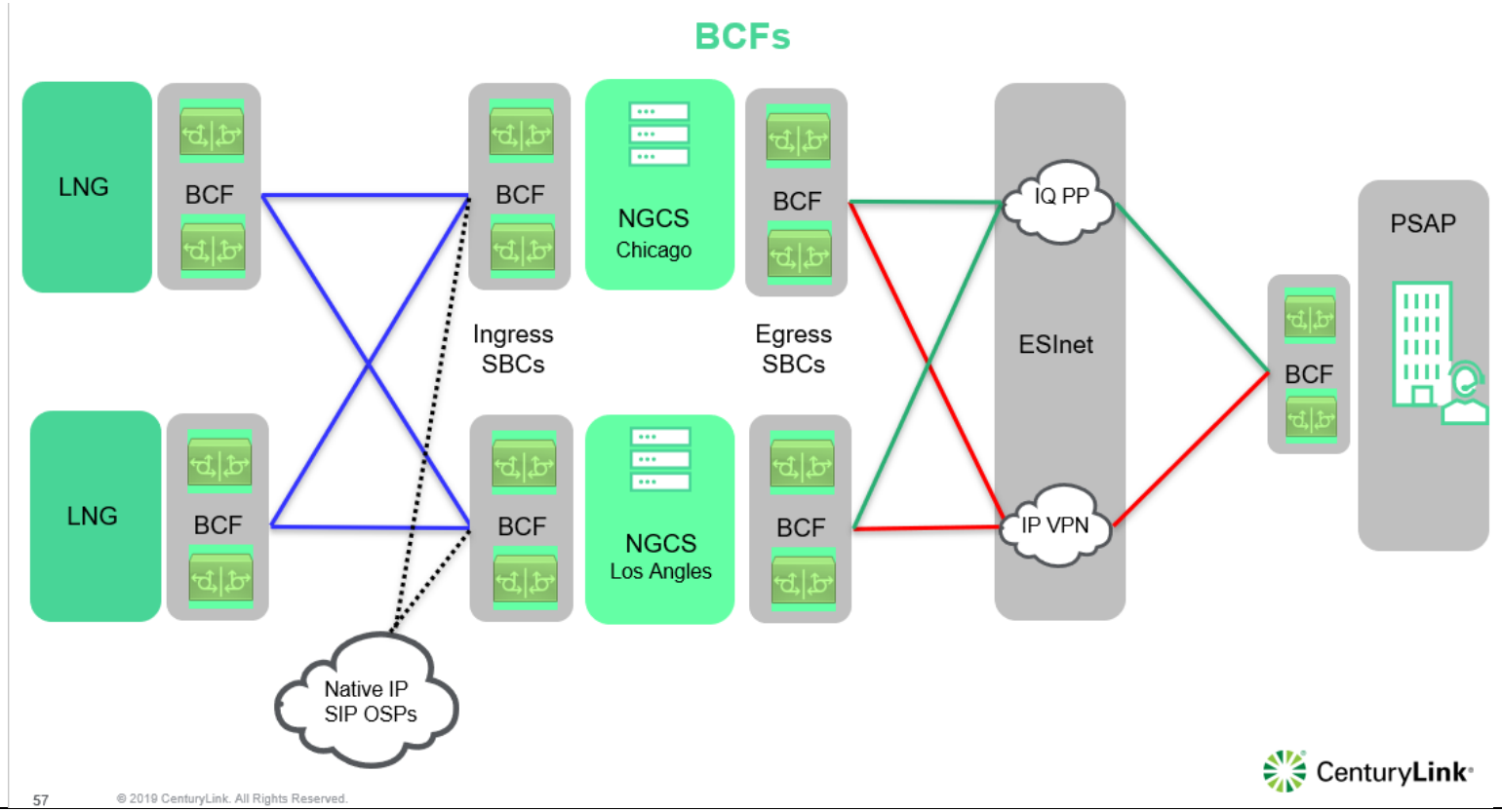
	normal operations; (2) The presence of fraudulent calls and events that are stressing a facility's ability to continue most operations; and (3) System under active attack and overwhelmed. The BCF provides both application and network layer protection and scanning. It will also mitigate lower layer protocol attacks and provide denial of service (DoS) and distributed denial of service (DDoS) detection and protection. The firewall component of the BCF/SBC will inspect all traffic transiting the network edge. 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 also supports an automated interface that allows a downstream element to mark the source of a call as a "bad actor". This would normally occur when a call is received that appears to be part of a deliberate attack on the system. PSAP BCF/SBC are included part of this service as well that will terminate secure traffic to the PSAP and expect to hand off to the endpoint PSAP via customer provided call handling equipment firewall/BCF or SBC. The CenturyLink's NGCS Solution and ESInet are provided with an array of BCFs/firewalls that inspects all traffic transiting the network edge. This device will employ both application and network layer protection and scanning capability as well as mitigates lower layer protocol attacks. Our network supports standard 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 datacenters and secure delivery of SIP traffic to the PSAP BCF

Any additional documentation can be inserted here

NGCS 20	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **High-Availability Design** The BCF solution shall be deployed in a manner to achieve 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

All our critical elements are deployed in an active-active mode. Each NGCS instance is paired with a redundant instance. Each redundantly paired instance is also paired with a geographically redundant, active-active pair. Our geographically diverse, active-active design means that up to three of the four NGCS instances can fail and the remaining instance will continue to carry the entire task load with no interruption nor degradation of service.



	NGCS 20 – HA BCF Design Each of our Core sites have redundant BCFs. The redundant BCF design and the overall redundant Core architecture of the CenturyLink ESINet solution allows for availability to meet or exceed 99.999%. Each of the two geographically diverse data centers have redundant BCFs. The redundant n+1 BCF design and data center locations in, North Chicago IL and Los Angeles, CA allow for availability to meet or exceed 99.999%. Each of the two geographically diverse data centers have redundant BCFs. The redundant n+1 BCF design and data center locations in datacenters in Chicago, IL and Highlands Ranch, CO allow for availability to meet or exceed 99.999%

Any additional documentation can be inserted here

NGCS 21	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Auditing of System Log Files** Management of the BCF shall include continuous auditing of the system log files for anomalies, and processes for responding to and managing security incidents. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink deploys our SD-WAN and SBCs at all our BCFs. We do this at our NGCS data centers, Network Core sites, and at the PSAP host sites. We gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Our operations team is staffed 7x24 and continuously monitors and responds to all events including security incidents. Using this and our network threat sensor and other data sources such as E-Bonding ticket information, are consolidated into a single viewing portal for access by the state. We monitor and audit all aspects of the network for threats from a variety of sources. This capability assists in troubleshooting and anomaly resolution as well as providing assurance of reliable performance.				


SD-WAN as a Service
Security
Routing
Realtime Visibility
Prioritization
Historical Analytics
Transformation Team
Best Practices
Project Management
Transformation Strategy
High Level Design
Low Level Design
Engineering Team
Standard Design Certification
In house tier 3 & 4 support
Release Testing & Certification
Operations Team
7x24 Operational Staff
Monitoring & Event Management
Change Management
Appliance Upgrades
SD-WAN Appliance
Futureproofing
Global Distribution
Sparing & Replacement
Cloud VMs
Universal CPE
Transport
CenturyLink
CenturyLink Aggregated
Customer Provided
Management & Control Plane
Infrastructure Deployment
SW Deployment
Monitoring
Release Management
3

NGCS 22	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Silence Suppression Detection** The BCF shall be capable of detecting when silence suppression is present in the 911 call and of disabling silence suppression if it is detected in the call. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our solution provides this capability. Our BCF can detect when silence suppression is present, which allows its continued use or disables it as circumstance dictate. if detected. Typically for 9-1-1 calls, an industry best practice is to preserve as much call detail as possible. Techniques such as voice activity detection (VAD) may not be sensitive enough to activate during low audio activity, and important background sounds may be missed. Additionally, some voice detection algorithms may not react in an expedient manner and may cut off the beginning of a word. The following comment is from NENA TID 08-501 in reference to silence suppression: "However, these techniques may not be appropriate for emergency calls in which "background noise" can be an important part of the call (both for the call taker and for logging recording purposes)." Some codecs also support silence suppression To that end CenturyLink does not enable silence suppression for any calls that use the CenturyLink ESINet service. Currently, when CenturyLink ESINet receives an emergency call with silence suppression requested, the ingress BCF answers with silence suppression disabled. Since we don't know if silence suppression was active or inactive for the upstream links, disabling silence suppression on the link into the CenturyLink ESINet solution prevents us from potentially being the only link with silence suppression active and dropping potentially important low-level background sounds.				

Any additional documentation can be inserted here:

NGCS 23	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Call Mediation** The BCF shall mediate all incoming 911 calls from VoIP providers to Session Initiation Protocol (SIP) calls and should be done in accordance with NENA-STA-010.2-2016. Any specific variations or non-compliance with this requirement shall be identified and documented below. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink ESINet BCF mediates all incoming 9-1-1 calls from VoIP providers to SIP calls in accordance with NENA STA-010.2-2016 a and the ATIS 0700015 standards. The CenturyLink ESINet specification is not only compliant with the NENA and ATIS standards, but also supports a transitional approach to accommodate the period until OSPs conform to the prerequisites identified in these standards. This transitional option is referred to as Selective Router Interface using SIP and it emulates SS7. The OSP Network SIP Interconnection option accepts emergency ingress calls to the ESInet via the BCF using SIP and then processes the call according to the routing logic determined by the 9-1-1 Public Safety Authority. Calls are routed either in conformance with the i3 specification or by equivalent legacy Selective Router logic. Calls from i3 compliant OSP networks interact with the ESRP and are processed in conformance with the i3 specification. Ingress SIP calls may only include the TN or pANI (ESRK or ESQK) or may include Location by Value or Location by Reference. CenturyLink ESINet will process these calls accordingly. Our solution not only meets but exceeds this requirement with our variations of SIP support. SIP mediation is one of the services it performs well.				

Any additional documentation can be inserted here:

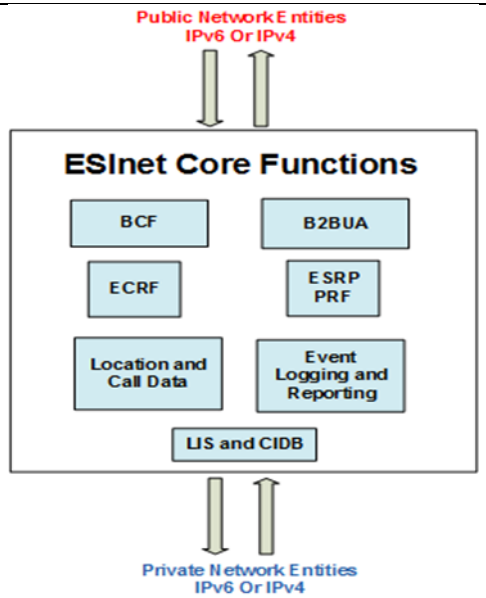
NGCS 24	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Event Logging** The BCF shall provide the functionality to maintain logs of all 911 sessions and all additional BCF logging and recording requirements, as specified in NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The BCF maintains logs of all 9-1-1 sessions and all additional BCF logging and recording requirements, as specified in NENA STA-010.2-2016. We support all of the Log Event Event Types described in NENA-STA-010.2, Section 5.13.3.2 A customer management portal is available for PSAP administrators to view end-to-end CDRs in real time. CDRs include the start time of the call as it enters the ESInet, answer time, end time, digits for ANI and any errors encountered. Additionally, i3 logs from all ESInet i3 components will be available per the NENA STA-010.2 specification. CenturyLink will support near real-time log delivery and web service interfaces for log retrieval from authorized clients.				

Any additional documentation can be inserted here:

NGCS 25	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **NAT/NAPT Detection and Mediation** Provide details on how the proposed Session Border Control (SBC) will recognize that a Network Address Translation (NAT) or Network Address and Port Translation (NAPT) has been performed on Open Systems Interconnection (OSI) Layer 3, but not above, and correct the signaling message for SIP.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink ESINet uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. When the SBC receives a message the rules are applied, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message. Our BCF will provide logical network security functions between external ESInet and handle any NAT translations required between the external ESInet and CenturyLink provided ESInet.				

Any additional documentation can be inserted here:

NGCS 26	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **IPv4/IPv6 Interworking** Provide details on how the proposed SBC shall enable interworking between networks utilizing IPv4 and IPv6 through the use of dual stacks, selectable for each SBC interface, based on NENA-STA-010.2-2016. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our SBC is natively designed to support IPv4 and IPv6, have the capability to run dual protocol stacks. This is true for our servers, systems, routers, switches, and other network equipment. We design to use IPv6 for all ESInet interfaces. IF IPv4 interfaces are required, non-RFC1918 addresses are used. CenturyLink ESINet will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards. All network equipment has the capability to utilize IPv4 and IPv6 addresses and is configurable to support dual stack operation. Whereas some components of internal systems only support IPv4; this will not be a limitation for this solution. When an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet Core strips down the IPv6 packet, removes the IPv6 header and adds the IPv4 header and passes it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. The IPv4 network and IPv6 interfaces are continuously monitored for availability and performance. This is accomplished with the use of a back-to-back user agent session border controller, rather than Network Address Translations (NATs). All devices within the network shall be assigned static addresses Since 2007, dual-stack design was chosen across the existing IPv4 infrastructure, which makes the end design for IPv6 exactly the same as IPv4. This provides a seamless transition by not requiring separate interfaces for IPv4 and IPv6 services. Several objectives were developed to ensure a phased approach to allow systems and the network to evolve: • Enable IPv6 on the production IP backbone to provide transit IPv6 services • Enable IPv6 equivalents of existing IPv4 enterprise services – Internet Port – public IPv6 connectivity to on-net and peer networks – Private Port – IPv6 Layer 3 VPN • Gain operational experience to minimize both operational and capital costs and gain developmental experience to support applications on IPv6 • Provide services to meet government mandated IPv6-ready dates • Implement IPv6 to not affect or degrade the performance of the existing IPv4 network and services				



NGCS 26. IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

NGCS 27	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Support Over Multiple Protocols** Provide details on how the proposed SBC shall support SIP over the following protocols: 1. Transmission Control Protocol (TCP), 2. User Datagram Protocol (UDP), 3. Transport Layer Security over TCP (TLS-over-TCP), and 4. Stream Control Transmission Protocol (SCTP). Protocols supported shall be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: All encryption mechanisms are supported in accordance with NENA STA010 and AES256. This extends to the following protocols: Transmission Control Protocol ("TCP"), User Datagram Protocol ("UDP"), Transport Layer Security ("TLS") over TCP, and Stream Control Transmission Protocol ("SCTP"). Protocols supported are selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems. Our SBC functions as part of our Oracle Acme Packet BCF. It supports SIP over all the listed protocols and this service is selectable. The solution uses Transmission Control Protocol (TCP) within the ESInet and highly recommends that PSAP call handling solutions support TCP. If the size of the SIP INVITE is within 200 bytes of the maximum transmission unit (MTU) of an Ethernet frame, fragmentation is likely to occur. Fragmentation may have impacts ranging from call setup delays of unknown duration and quantity, to blocked or abandoned calls. In some instances, fragmentation has no discernible impact to the call. Packet fragmentation is not unexpected, and it can be handled appropriately with the use of Transmission Control Protocol (TCP). Another protocol, User Datagram Protocol (UDP), is commonly used in VoIP implementations. This protocol differs from TCP, and its mechanisms for handling packet fragmentation are weaker. While CenturyLink ESINet can support both UDP and TCP, we recommend that TCP be used. This recommendation is based upon the packet size experienced within the CenturyLink ESINet solution, the anticipated growth of such packet sizes with forward-looking NG9-1-1 message sets, and applicable standards including the NENA i3 specification and IETF RFC 3261. Transport Layer Security over TCP (TLS-over-TCP) and Stream Control Transmission Protocol (SCTP) are supported and selectable for each SBC interface to external systems.				

Any additional documentation can be inserted here:

NGCS 28	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Packet Prioritization Based on Session Type** Provide details on how the proposed SBC shall be capable of populating the Layer 3 headers, based on call/session type (e.g., 911 calls) in order to facilitate priority routing of the packets.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our BCF's installs a "NENA-source" parameter in the Via header that in the outgoing INVITE message associated with every call. Calls are marked by the SBC in a way that allows a recipient to identify the BCF that processed the call.				

Any additional documentation can be inserted here:

NGCS 29	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Encryption of Unencrypted Calls** Provide details on how the proposed SBC supports encryption for calls that are not protected entering the ESInet, based on NENA-STA-010.2-2016.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The SBC analyzes the encryption employed on each inbound call and compares it with the minimum encryption required on our NG9-1-1 network (minimums set in accordance with STA010). If the call is unencrypted, or insufficiently encrypted, then the SBC re-encrypts the call as required. Currently, AES256 is employed, but CenturyLink routinely evaluates changes in encryption standards to ensure that the level of security maintained is adequate. CenturyLink ESINet provides a Border Control Function for encryption and interface with any non-trusted network components. The Border Control Function (BCF) provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification. The BCF inspects, modifies and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect and where the ESInet connects with service provider networks. The solution for border control functions includes both security functions for the ESInet as well as the applications that ride the ESInet which include but are not limited to the SIP traffic on the ESInet. The CenturyLink ESINet solution employs encryption-in-transit where possible on networks not under direct CenturyLink control. Encryption is achieved either using SSL/TLS or IPSEC VPN. The CenturyLink ESINet solution does not encrypt data-at-rest at the database level; as a compensating control, database servers are hardened at the operating system and application level and employ Principle of Least Privilege when assigning access for users and applications to database tables. Tunnels are encrypted for security with IPSEC tunnel protection.				

Any additional documentation can be inserted here:

NGCS 30	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Elements** 1. Provide details, including drawings, describing the different BCF elements that the proposed solution comprises. 2. As part of the details, identify all of the elements and/or interfaces to be provided by the Commission and/or PSAPs to the bidder.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The BCF inspects, modifies, and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect and where the ESInet connects with service provider networks. The BCF mitigates security threats, resolves interoperability problems and ensures reliable SIP-based communications. It is designed to protect and control real-time voice, video, and text sessions as they traverse IP networks between callers and Public Safety Answering Points (PSAPs). BCFs are included in the solution and interface to external components traversing through redundant BCF components. Each of the CenturyLink ESINet Core sites will have redundant BCFs. The redundant BCF components are market leading products that provide high reliability and high availability. The BCFs work so that only authorized traffic to authorized end points are allowed. The redundant BCF design and redundant Core architecture of the CenturyLink ESINet solution allows for availability to meet or exceed 99.999%. As part of our CenturyLink ESINet solution, we provide a Border Control Function to interface with any non-trusted network components. The Border Control Function provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification. Customer access to the BCF is provided via the Customer Management Portal allowing for review of real-time CDR data. The CenturyLink solution supports i3 specified NG9-1-1 interfaces and legacy interfaces. The ESInet supports all the specified protocols for ingress and egress call delivery, as well as post PSAP call delivery data retrieval. TDM ports on patch panels, installed by CenturyLink and connected to the CenturyLink-provided PIFs, will serve as the Physical Demarcation (Demarc) at each of the PSAPs and any POI facilities. The LNG functions can support TDM traffic from OSPs preferably SS7 but support MF and CAS signaling. LPG provided at the PSAP emulates CAMA delivery or support CAS T1 and deliver serial ALI for the call handling equipment (CHE) at the PSAP to meet non i3 PSAP requirements. Border Control Functions (BCF) are included in the ESInet solution and all SIP interfaces to external components traverse through redundant BCF components. CenturyLink deploys its ESInet solution on private MPLS connections yet still uses the BCF in conjunction with SBC deployments to minimize the security risk coming from external sources. Our CenturyLink designed NG9-1-1 system is composed entirely within the NENA i3 standard. One of the major advantages to this design is that calls are converted to SIP at the ESInet level before being delivered downstream to legacy or NG9-1-1 PSAPs. CenturyLink will design the call-routing functionality at the ESInet level to deliver SIP directly to each PSAP as each PSAP becomes NG9-1-1 ready, and from there the CPE will send the call on to each intelligent workstation.				

Any additional documentation can be inserted here:

NGCS 31	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **ESRP Description** The ESRP routes a call to the next hop. It also evaluates the originating policy rules set for the queue the call arrives on, extracts the location of the caller from the SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next-hop route, evaluates the route based on policy rules and queue states of the downstream entity queues, and then forwards the call to the resulting next hop. Bidder's proposed ESRP must meet or exceed NENA-STA-010.2-2016. Describe how the proposed solution meets or exceeds the standards.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our ESRP and PRF adheres to standards established in NENA-STA-010. We query the ECRF for the next hop, process the call against the PRF rules and subsequently forward the call to the resulting next hop. In compliance with NENA STA- 010.3, the first step is an evaluation of the incoming call to determine is location information is already available in the SIP headers and after the BCF security check, our ESRP provides routing based on the caller's location. It extracts the location of the caller from SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next hop route, and evaluates the route policy of that entity using its Policy Routing Function (PRF) to determine the actual next hop the call takes. CenturyLink's NGCS Solution ESRP is the most robust such element available on the market and scales to well over 200 call setups per second which equates to over 720,000 busy hour call attempts (BHCA). With software developed in collaboration with our vendor Synergem; security, Quality of Service (QoS), and interoperability are "baked in" to the functional element. Our ESRP provides final routing to a PSAP based on the caller's location. It extracts the location of the caller from SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next hop route, and evaluates the route policy of that entity using its Policy Routing Function (PRF) to determine the actual next hop the call takes. The ESRP supports both the server and client side of the "ElementState" event notification packages. The ESRP maintains "Subscriptions" for this package on upstream or downstream elements it serves. These "State" interfaces supply inputs to the PRF. The ESRP systems are deployed in a cluster, in which case the ESRP provides the greatest achievable level of call integrity by sharing the state of all calls in-progress across the cluster, ensuring that the failure of any node in the cluster shall have no impact on the survivability of any call. Our ingress call distribution algorithm ensures an equal distribution of calls is spread across all of the call processing elements, ensuring that no single call processing element is over utilized, as well as avoiding an unbalanced call processing profile where a disproportionate number of calls are processed in a network region that could be severed due to natural disaster or other catastrophic network event. Our ESRP provides final routing to a PSAP based on the caller's location. Each of the application systems reports its health to CenturyLink PSS NOC and alarms are generated for minor and major changes in system health. Alarms are also generated for all changes in the state of DNS and load balancer monitoring, as well as all changes in state within the ESRP cluster. Calls are automatically re-routed to an alternate data center when they can't access the local routing database or the local media server. Should one of the two core data centers experience a catastrophic outage, all calls will be automatically redirected to the alternate data center. The CenturyLink solution maintains multiple copies of the policy rules in addition to the diverse and redundant copies that reside within the call path systems.				

Any additional documentation can be inserted here:

NGCS 32	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Transition to Geospatial Routing** Bidder understands that all PSAPs and regions may not be ready for geospatial routing on day one of operations and shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. In bidder's separate cost proposal response, indicate the pricing difference between tabular and geospatial routing. Describe the process for transitioning each PSAP or region from tabular routing to geospatial routing as PSAP's becomes ready and the manner in which the solution provides for routing by both means simultaneously.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our NGCS solution does not route calls using Internet Protocol Selective Routing (IPSR) as this is not an i3 NGCS option. In our system, the readiness of the PSAP for geospatial routing is not an issue. If a PSAP is not ready for i3 calls, we employ an LPG. Establishing and migrating from the existing legacy system to the CenturyLink NG9-1-1 infrastructure is substantial. Interconnecting OSPs, designing the network, establishing redundant and diverse networks, testing, configuration, and turnup. Once the CenturyLink NG9-1-1 system is in operation, additional capabilities were designed to be configurable without and major disruption in service. Most of the work for the transition from IPSR routing to i3/geospatial routing occurs on the PSAP/regional side. Moving to i3 NG9-1-1 begins with a data assessment that includes GIS data. The 9-1-1 Authority must establish a strategy to move from legacy ESN-based call processing to the NENA i3 call processing model. The structure of that transition will affect how to evolve existing data. From a NGCS perspective, few modifications need to be completed. Incoming traffic will need to be re-designated as GIS routable. PSAP i3 configurations within the ESRP will need to be created and tested through to the CHE prior to deployment. A test plan is run to validate the i3 protocols are handled in the proper way and that calls can be transferred from i3 PSAPs to non- i3 PSAPs internal and external to the CenturyLink NG9-1-1 solution. Fallback to ESN routing with i3 call delivery is also validated during the testing process. The NGCS processes listed above are not theory, they have been and continue to be deployed in CenturyLink NG9-1-1 areas across the country.				

Any additional documentation can be inserted here:

NGCS 33	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Policy Routing Function (PRF) Description** The PRF is a required function of the ESRP. The ESRP interacts with the PRF to determine the next hop of a call or event. Before the ESRP sends the call to the next hop, it first queries the PRF to check the status of the next hop to determine if a unique routing rule or policy is in place that would direct the call to another location. The destination of the next hop is typically a queue. The PRF monitors the downstream queues of ESRPs for active understanding of the entity's queue status. Describe how the solution meets or exceeds the standards.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: If the downstream entity reports Queue State via a SIP NOTIFY, the ESRP will use the state of the queue to deliver calls. The PRF will be checked to see if the subscriber is permitted to subscribe. The ESRP-supported PRF determines potential emergency call routes. For calls correctly pointed to a PSAP that is 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 by the default routing instructions. Our ESRP-supported PRF determines potential emergency call routes. Other rules the PRF can apply govern call termination and can include a route decision based on knowledge that a downstream ESRP is busy (call queue full) or that a PSAP is offline. The ESRP supports https clients for the "Additional Call Data" services. These services may be invoked when the ESRP receives a call with a "Call Info" header with a "purpose" of "emergency Call Data," "emergency Caller Data" or "emergency PSAP data." The resulting data structure is an input to the PRF. The ESRP supports both the server and client side of the "Element State" event notification packages. The ESRP maintains "Subscriptions" for this package on upstream or downstream elements it serves. These "State" interfaces supply inputs to the PRF.				

Any additional documentation can be inserted here:

NGCS 34	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **PRF Policy Store and User Interface** The PRF shall allow defining of policy rules for distributing a wide range of calls in an efficient manner. 1. Describe the solution's Policy Store and the PSAP's ability to effect changes to the PRF. 2. Describe the user interface, role-based authentication, the ability of each PSAP or region to manage PSAP's own policy rules, and the types of policy rules available at the time of proposal submission, as well as those on the product roadmap. Roadmap items must include an estimated time of feature availability.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: **1)** Our ESRP-supported **PRF** is the principal policy control tool with standardized methods to define/build and control PolicyRules such as those that determine potential emergency call routes. Other rules the PRF can apply govern call termination and can include a route decision based on knowledge that a downstream ESRP is busy (call queue full) or that a PSAP is offline. Rules also may be used to "permit" or "deny" network access CenturyLink's PRF supports the full rule set defined by NENA-STA-010.2 A PSAP can update any rules over which it exercises ownership. This might include policies such as those that involve ESRP handling of overload and diversion when queues become full or call diversion to any available PSAP who registers to handle such calls **2)** Our interface structure complies with NENA 71-502, An Overview of Policy Rules for Call Routing and Handling in NG9-1-1 and NENA-STA-003, NENA Standard for NG9-1-1 Policy Routing Rules. These interfaces involve the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services and typical IP services such as DNS and DHCP. Our PRF is the principal policy control tool (PRF) with standardized methods to define/build and control PolicyRules. The following types of routing policies are supported and can be managed by the user via the CenturyLink portal. • **Abandonment/Night Service Routing.** The abandonment policy is engaged whenever the terminating ESRP (PSAP) operational state is defined as 'abandoned. The PSAP operational state may be modified by contacting the CenturyLinkNOC, triggered via a device installed at the PSAP, or modified online. • **Alternate Routing.** The alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout. The user can prioritize an alternate destination via the management portal and enable a PSTN back-up route on-the-fly. • **Diversion Routing** – The diversion routing policy is applied whenever the PSAP opts to engage alternate diversion routing rules. The PSAP operational state may be modified to engage the diversion routing policy by contacting the CenturyLink NOC or online • **Make Busy Toggle Switch** – Placed in the PSAP so they can control alternate routing that is predetermined by the PSAP. • **Overflow Routing** – The overflow routing policy is applied during overflow scenarios when a PSAP is receiving more calls than its occupied workstations can accommodate. Upon reaching the designated call capacity for the call type, cumulative calls, or if the target is unreachable, the ESRP engages the primary PSAP's overflow routing policy. Similarly, the alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout. • **Special Event Routing.** Special event routing is a special type of diversion routing that is applied during a scheduled time window. If a PSAP jurisdiction contains venues that host events that may warrant dedicated call handling (mobile command center or dedicated resources at the PSAP), special event polygons can be pre-provisioned				

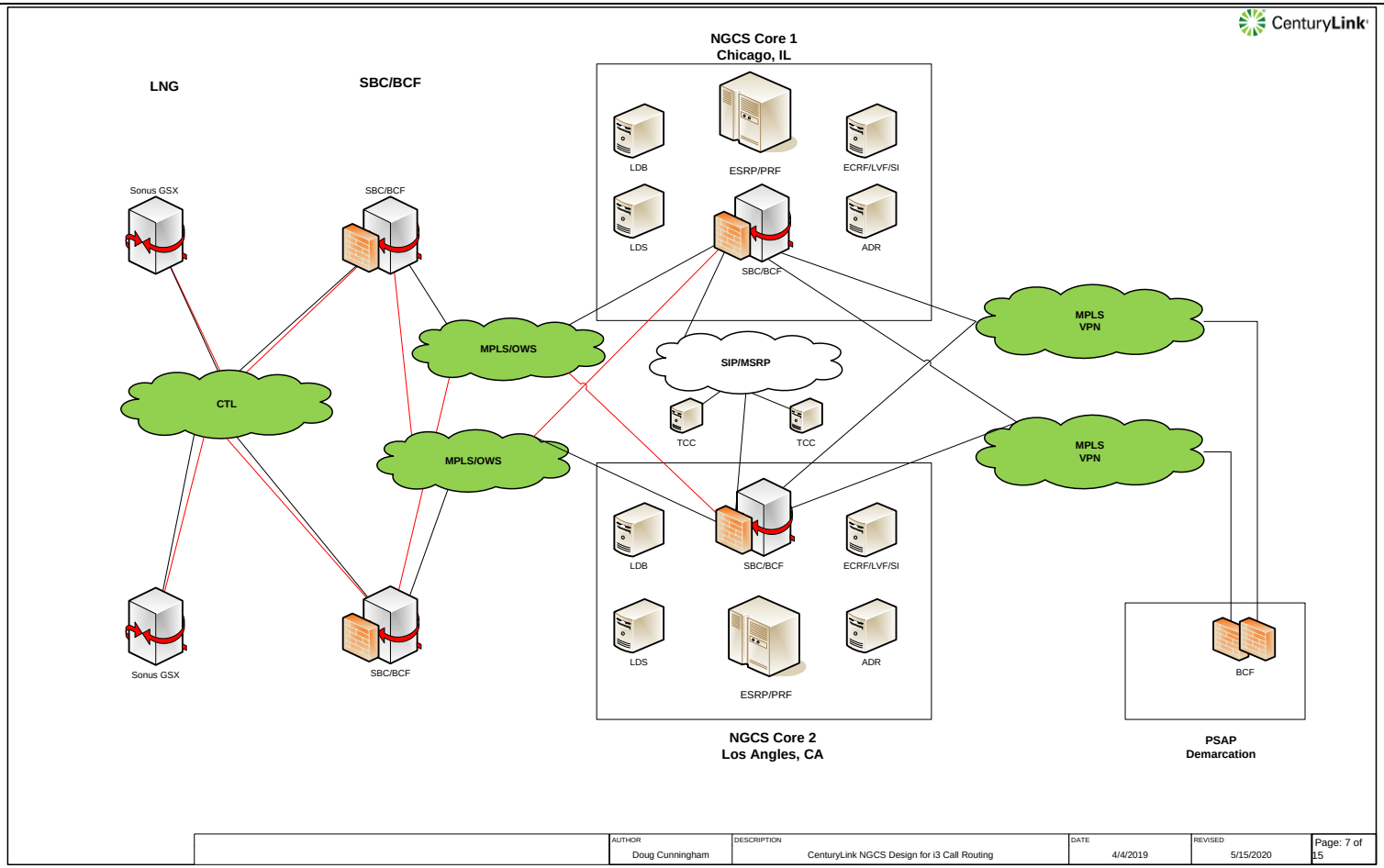
	• **Timers –** Routes calls not answered in a specific time to an alternate PSAP CenturyLink solution maintains multiple copies of the policy rules in addition to the diverse and redundant copies that reside within the call path systems.

Any additional documentation can be inserted here:

NGCS 35	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Next-Hop Queues** A next-hop queue may be a Uniform Resource Identifier (URI) that routes the call to an interactive multimedia response system (as described in IETF RFC 4240) that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via Dual-Tone Multi-Frequency (DTMF) signaling or other interaction protocols. Describe how the bidder's solution implements next-hop queueing.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Our proposed next-hop queue policy meets these requirements. Our system accepts DTMF signalling from the legacy PSAP and sends it to the NIF component in RTP packets, per RFC 4733. Our transition plan specifically tests tasks such as DTMF/Fax Interworking and DTMF tone testing. A next-hop queue that is a uniform resource identifier (URI) that routes a call to an interactive multimedia response system that plays a voice announcement and accepts responses via Dual-Tone Multi-Frequency (DTMF). DTMF signaling is supported. CenturyLink is happy to work with the State of Nebraska to assess and support use cases for when an announcement is negotiated by the caller to be played in a media format other than voice.				

Any additional documentation can be inserted here:

NGCS 36	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **High-Availability Design** The ESRP/PRF solution shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The redundant ESRP/PRF design and the overall diverse and redundant Core architecture of the CenturyLink ESINet solution allows for availability to meet or exceed 99.999%. All our critical elements are deployed in an active-active mode. Each NGCS instance is paired with a redundant instance. Each redundantly paired instance is also paired with a geographically redundant, active-active pair. Our geographically diverse, active-active design means that up to three of the four NGCS instances can fail and the remaining instance will continue to carry the entire task load with no interruption nor degradation of service ESRP high availability is achieved through an application processing complex consisting of multiple application servers, each of which operates independently of the others so that a single application processor failure does not disrupt the processing of the complex. There are two application processing complexes that operate independently of each other and are geographically distributed. Each component at an application processing complex has redundancy and high availability within its own domain. The ESRP application is highly redundant within each of the geographically separate sites. There are multiple computers running the ESRP application and the failure of any one or two of those computers do not affect calls in progress. Failure of a data center results in all future calls being processed by another geographically diverse data center and will still provide the total required call processing capacity requirement. At least two ECRF servers will exist at each of the geographically diverse locations, all with redundant and secure IP connections. Even if one server or even one location has a failure, the workload will be distributed to the other ECRF servers within the system. The redundant ECRF design and the redundant Core architecture of our NG9-1-1 solution allows for availability to meet or exceed 99.999%. The ECRFs exist within a highly available and geographically distributed application processing environment. A single hardware component failure at one of the application processing complexes will not interrupt processing of the ECRF. A single geographic site failure (either the communication to the site or elimination of the site itself) will not prevent further call processing from occurring. High availability is achieved through high availability software design, redundant ECRF instances, and transactions using dynamic client/server connections with multiple ECRF serving entities. The geographically diverse ECRFs utilize redundant data stores to support high availability. These systems are monitored 24x7x365 by our NG9-1-1 Public Safety Network Operating Center (NOC) and supported through our Incident Command System. All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. With the ECRF architecture including two separate servers at each geographically diverse location, upgrades and other maintenance can be performed one server at a time so that at no time will the system be one-sided.				



NGCS 36 - Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) High-Availability Design

Any additional documentation can be inserted here:

NGCS 37	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Keep-Alive Signaling Between Elements** Provide an explanation of how the proposed ESRPs use the SIP "options" transactions for maintaining "keep -alive" signaling between ESRPs, LNGs, Legacy PSAP Gateways (LPGs) and session recording services.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: All SIP functional elements in our ESInet and NGCS utilize SIP OPTIONS to provide the "keep-alive" signaling. Option messages are used in our CenturyLink ESINet solution to ensure path and element availability. In the event that an option response is not received, the solution will identify an alternate and /or resource to complete the transaction while maintaining 99.999% availability. SIP monitoring via SIP "Options" messages exists between the Core site call control application and each ingress (OSP) and PSAP endpoint. Continuity Tests (COT), loopback, and tone check testing is performed between the CenturyLink LNGs and OSP switching equipment before a circuit is established to detect failure of DS0 channels.				

Any additional documentation can be inserted here:

NGCS 38	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF** **TCP/TLS Implementation** The upstream interface on the proposed non-originating ESRPs shall implement Transmission Control Protocol/Transmission Layer Security (TCP/TLS), but shall be capable of fallback to UDP, as described in NENA-STA-010.2-2016. Stream Control Transmission Protocol (SCTP) support is optional. The ESRP shall maintain persistent TCP and TLS connections to the downstream ESRPs or User Agents (UA) that it serves. Provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: TCP/TLS with UDP fallback is implemented between all SIP functional element in our ESInet/NGCS. Our solution uses Transmission Control Protocol (TCP) within the ESInet, on both the ingress and egress of our CenturyLink provided network. Another protocol, User Datagram Protocol (UDP), is commonly used in VoIP implementations. This protocol differs from TCP, and its mechanisms for handling packet fragmentation are weaker. While our CenturyLink ESINet can support both UDP and TCP, we recommend that TCP be used. This recommendation is based upon the packet size experienced within our ESINet solution, the anticipated growth of such packet sizes with forward-looking NG9-1-1 message sets and applicable standards including the NENA i3 specification and IETF RFC 3261. The SBC also support SIP over Transport Layer Security over TCP (TLS-over-TCP), and Stream Control Transmission Protocol (SCTP). Protocols are selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems				

Any additional documentation can be inserted here:

NGCS 39	**Next Generation Core Services Elements (NGCS)** **NENA Compliance Chart** Provide a description of how the proposed ESRPs meet or exceed all functional requirements below as defined in NENA-STA-010.2-2016, which are listed below.	X			
	Bidder Response: CenturyLink complies with each provision as marked in the chart below.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Overview Section 5.2.1.1	X			
Call Queueing Section 5.2.1.2	X			
Queue State Event Package Section 5.2.1.3	X			
De-queue Registration Event Package Section 5.2.1.	X			
Policy Routing Function Section 5.2.1.5	X			
ESRP Notify Event Package Section 5.2.1.6	X			
INVITE Transaction Processing Section 5.2.1.7	X			
BYE Transaction Processing Section 5.2.1.8	X			
CANCEL Transaction Processing Section 5.2.1.9	X			
OPTIONS Transaction Processing Section 5.2.1.10	X			
Upstream Call Interface Section 5.2.2.1	X			
Downstream Call Interface Section 5.2.2.2	X			
ECRF Interface Section 5.2.2.3	X			
Location Information Server (LIS) Dereference Interface Section 5.2.2.4	X			
Additional Data Interfaces Section 5.2.2.5	X			
ESRP, PSAP, Call-Taker State Notification and Subscriptions Section 5.2.2.6	X			
Time Interface Section 5.2.2.7	X			
Logging Interface Section 5.2.2.8	X			
Data Structures Section 5.2.3	X			
Policy Elements Section 5.2.4	X			
Provisioning Section 5.2.5	X			

NGCS 40	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** Describe how the ECRF interfaces with other ECRF solutions which may interface with the bidder's solution. Awarded Contractor shall coordinate with other ECRF solution providers to ensure interoperability between the respective solutions.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The ECRF/LVF maintains both civic and geodetic coverage information. This information is used to determine who should answer a query. At a minimum, the ECRF/LVF must be loaded with coverage information for geographic areas for which it is authoritative. Our proposed ECRF can interface with any other ECRF solution that complies with NENA standards. The ECRF provisioning service will accept data (Roads, Addresses, and ESB polygons) from the Next Generation GIS Data Store or another ECRF. The data will be transformed and quality controlled. If the data meets publishing restrictions, then the ECRF database(s) will be updated with new data. Additionally, the data can also be exported for use in other applications like map display software. To support the envisioned i3 end-state, it is necessary that every authoritative ECRF/LVF logical node be accessible from every other ECRF/LVF server in the global forest as well as from query clients via the public Internet. It is a fundamental requirement of native i3 emergency calling that routing and validation queries be answered with service mappings from the authoritative ECRF/LVF, no matter where those queries originate. If a National Forest Guide is unavailable, CenturyLink will work with surrounding regions and states to obtain coverage data for their ECRF/LVF systems and attempt to establish connectivity between them. CenturyLink will provide the Nebraska coverage data to any surrounding region or state that would like to operate in the same LoST tree as the Nebraska system. 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 ECRF/LVF replicas will be deployed within the ESInet and will only receive queries originating internally or from other trusted ESInets. External ECRF/LVF replicas will be deployed within a DMZ and will handle all queries originating from untrusted networks and the public Internet. Coverage data can be added for areas where this ECRF/LVF is not authoritative. For these coverage entries an app string will be added to tell the ECRF/LVF what other LoST Server (ECRF) it needs to communicate with to get an authoritative answer. If all external ECRF/LVF replicas are attacked or compromised, the internal replicas will still be available to service internal calls and those from trusted networks. Both internal and external ECRF/LVF servers are critical to placing 9-1-1 calls in a Next Gen environment, and both tiers will be deployed in highly- available and redundant configurations				

Any additional documentation can be inserted here:

NGCS 41	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **ECRF Description** The ECRF shall be designed according to NENA-STA-010.2-2016 and be implemented using diverse, reliable and secure IP connections. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

Our Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) comply with all NENA and IETF standards and provides for complete migration into i3 without costly technology acquisition and process overhaul.

Key aspects include:

- Allows data analysts to correlate street and community names from three data sources (Postal, MSAG, and GIS).
- Allows authorized service providers to validate locations and route calls using real time data.
- Identifies common error discrepancies between MSAG, GIS, and Postal.
- Extensive online help.
- Extensive security mechanisms allow access and updating tailored to most organizations' data operations.
- ECRF/LVF is a critical functional element secured by diverse and reliable IP connections
- Links to online mapping resources.
- Web-based user interface for ease of data management.
- Extensive reporting capabilities.
- Allows establishment of translations including County (e.g., "007" = "Boone County"), Community (e.g., "North Boone" = "Beaverton") and Street (e.g., "SH 76" = "Fairground Rd." = "State Line Rd.")

GIS data can be uploaded via an intuitive web interface enabling authorized users to provision the SI with geospatial data in ESRI shapefile or file geodatabase formats, verify that the data is in the expected schema, and initiate the load process into the SI. Alternatively, automated routines can be set up to populate the SI without having to upload via the web interface.

A spatial interface (SI) is central to the provisioning of the GIS databases. The load into the SI system does not do a complete overwrite; rather, it performs a change detection operation. As a result, an historical record of data changes can be maintained by the system, and detailed results of any load errors are provided. This process, either with the web interface or using automated routines, can be run as frequently as needed, although daily is recommended.

Once the data load is complete, the system performs numerous quality control checks on the data. The resulting QC errors can be viewed directly using any software capable of consuming ESRI-based web services. This will allow the viewing of any map data discrepancies in real-time.

Following the QC process, if the number and severity of any errors are within configurable limits, the system will automatically publish updated data the to the master ECRF/LVF database. This database acts as a replication master, pushing all changes using Microsoft SQL Server replication to child databases that are used for ECRF/LVF functionality. All replication distributions run on the master database to minimize the load on the

	databases that are being actively used for LoST query processing. SQL Server replication occurs in near-real-time. The SI also provides reporting, allowing real-time access into the state of the datasets used by the ECRF/LVF. Additional publishing routines can be set-up for other applications that may need GIS data. This allows administrators to create publishing tasks that export copies of the data into a format that is required by third-party applications. For example, CPE may require a certain data extract that is different from what CAD requires. CenturyLink strongly supports the NENA i3 and other relevant standards and has been actively involved with the development of many of these standards, as well as interoperability testing at many of the NENA ICE events. The CenturyLink ECRF/LVF complies with the following standards: • NENA-STA-010.2-2016 compliant • RFC 5222 LoST protocol • RFC 4848 for LoST server name resolution • RFC 5031 for service names and format • RFCs 4119, 5139, and 5491 for location formats • RFC 5582 (informative) for LoST architecture

Any additional documentation can be inserted here:

NGCS 42	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **High-Availability Design** Bidder shall supply an ECRF function that meets a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements**.**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The ECRF/LVF system runs in a high-availability active-active architecture to achieve the required five-nines up-time metric. Each NGCS instance is paired with a redundant instance. Each redundantly paired instance is also paired with a geographically redundant, active-active pair. Our geographically diverse, active-active design means that up to three of the four NGCS instances can fail and the remaining instance will continue to carry the entire task load with no interruption nor degradation of service. Typically, four instances of the ECRF/LVF are deployed per data center, running behind load balancing hardware. Each instance runs on its own virtual machine, utilizing its own replica database instances. The load balancers perform a health check against each instance once per second and will automatically pull an unhealthy element from the pool and raise a system alert. A single instance of each element has enough capacity to run the entire system should there be multiple simultaneous element failures.				

Any additional documentation can be inserted here:

NGCS 43	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility by Outside Functional Elements** Contractors providing an ECRF shall ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, an LNG, an ESRP in a next-generation emergency services network, or by some combination of these functions. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Additional, non-call path, ECRF/LVF instances (usually two per data center) are deployed into the DMZ, and accessible from outside the ESInet. Note that these instances are still protected by firewalls, so that access must be granted to third parties to gain access. CenturyLink's proposed ECRF can interface with any other ECRF solution that complies with NENA standards. The ECRF provisioning service will accept data (Roads, Addresses, and ESB polygons) from the Next Generation GIS Data Store or another ECRF. The data will be transformed and quality controlled. If the data meets publishing restrictions, then the ECRF database(s) will be updated with new data. Additionally, the data can also be exported for use in other applications like map display software				

Any additional documentation can be inserted here:

NGCS 44	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility Inside the ESInet** Contractor shall provide an ECRF accessible inside an ESInet, which shall permit querying from any PSAP (or future entity authorized to connect to the ESInet) inside the ESInet. ECRFs provided by other entities may have their own policies regarding who may query them. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Access control to the ECRF/LVF instances within the ESInet is controlled by firewalls and other security measures. All other ESInet elements that need to access the ECRF/LVF will be granted access.				

Any additional documentation can be inserted here:

NGCS 45	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Origination Network ECRF** An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Describe the functionality of such an ECRF equivalent and document where this functional element resides within the proposed solution.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: It is recommended that an origination network use the ECRF/LVF instances in the DMZ. However, the GIS data used by the authoritative ECRF/LVF can be provided to origination networks at the discretion of the state. This process can be automated on a case-by-case basis. CenturyLink cannot speculate where this external functional element may reside within the origination network as it is not contained within the ESInet/NGCS deployed as part of this project. Furthermore, If the origination network routes an emergency call to the ESInet, then that origination network emergency calls "To" address is changed to "urn:service.sos". The NGCS uses the PIDF-LO sent with the call or in the absence of a valid location, would execute a LIS/LDB HELD lookup and validate the origination and termination using the appropriate PRF rules				

Any additional documentation can be inserted here:

NGCS 46	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Routing Query Interface** The ECRF shall support a routing query interface that can be used by an endpoint, ESRP or PSAP to request location-based routing information from the ECRF. Additionally, it shall support both iterative and recursive queries to external ECRF sources. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink's ECRF/LVF provides the required interface and is fully compliant with NENA-STA-010.2-2016 and RFC 5222, providing the Lost query interface to any functional element capable of performing a LoST query. The ECRF/LVF can also be configured to perform recursive queries to other ECRF/LVF servers for locations that it is non-authoritative. Alternatively, it can return the URI to the authoritative ECRF/LVF allowing any LoST client to perform a cycle of repetitive queries. CenturyLink will configure the appropriate civic and geodetic coverage data into the state ECRF/LVF to support queries up (and potentially down) to local or regional LoST Servers that might be deployed in the state, the LoST tree and to the National Forest Guide when available and appropriate. Our ECRF/LVF instance can handle approximately 250 queries per second.				

Any additional documentation can be inserted here:

NGCS 47	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **LoST Protocol Support** The ECRF shall interface with the Location-to-Service Translation (LoST) protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CHE, or any other permitted IP host. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

The proposed solution includes an ECRF/LVF system that is fully compliant with RFC 5222 to provide a LoST protocol query and response interface.

The ECRF/LVF employed by i3-Route™ complies with RFC 5222 LoST Protocol, and additionally complies with other relevant standards:

- NENA-STA-010.2-2016 compliant
- RFC 4848 for LoST server name resolution
- RFC 5031 for service names and format
- RFCs 4119, 5139, and 5491 for location formats
- RFC 5582 (informative) for LoST architecture

The ECRF/LVF also implements requirements that are specific to NENA i3, including:

- Configurable service names, for services beyond those specified in RFC 5031
- Logging of LoST queries and responses to an i3-compatible logging service
- Discovery of additional data associated with a location.

The ECRF/LVF allows queries from any functional element capable of performing an RFC 5222 compliant LoST request, as permitted by other security elements, such as firewalls.

The LoST protocol also provides extension points for errors, warnings, and location validation. The I3-Route™ ECRF/LVF already includes several such extensions used to better characterize the quality of the response and anticipates that similar or equivalent extensions will be standardized by NENA at some point in the future.

Additionally, there is a standards-track draft "draft-ietf-ecrit-similar-location" extension to LoST which will allow a LoST server to respond with suggested locations when the location used in the findService query is invalid or incomplete. This has been implemented in the I3-Route™ ECRF/LVF and can be used by the LDB to provide users with help in resolving discrepancies.

The ECRF/LVF is designed to answer queries with the most useful possible response for the given query parameter and takes full advantage of the errors and warnings defined for the LoST protocol when needed. If the location in the query is malformed in such a way that it cannot be understood, the server will return a descriptive error message documenting the problem to the best that it could determine.

If a civic location is correctly formed but is simply invalid, meaning that it cannot be uniquely resolved to a particular GIS feature, then there are several possible outcomes depending on how much of the location is considered valid. It is possible that the query may still return correct call routing information, multiple sets of call routing information (if the location is ambiguous), or default call routing information with a warning.

	The ECRF/LVF fully supports both the civic and geodetic profiles. During the transitional phase, the LDB will provide all location, either directly or indirectly (via an E2 connection). For wireline calls, the LDB will contain an LVF valid and CLDXF compliant address location. For wireless, the LDB will contain a shell record, and will attempt to get more granular location over E2 from the Mobile Positioning Center (MPC). The location from the MPC will be a point and a confidence radius. This location is converted by the LDB into a circle that can be used by the ECRF for determining call routing. For VoIP, the LDB may contain either a civic address location or a shell record. If it is a shell record, the LDB will attempt to query the VoIP Positioning Center (VPC) for a more granular location. For VoIP, the E2 provided location could be geodetic or civic, or both. If the VPC provides a civic address location, it will be in the legacy MSAG format, so the LDB will utilize the MSAG Conversion Service (MCS) to convert the location into a CLDXF compliant PIDF-LO. Different service polygons can be used to represent different service request types, represented by the service URN in the LoST query. The ECRF/LVF fully supports the service naming conventions defined in RFC 5031, including the top-level services and sub-services defined therein. Support for services defined in the future is provided via configuration updates. Service substitutions are also supported and may be configured to return a mapping for an alternate service if the desired service is not available for the queried location. For example, if the ECRF receives a query for urn:service.sos.physician, but no physician service polygon is defined for that location, the ECRF can be configured to respond with a mapping for another service, such as urn:service.sos. Multiple levels of logging are implemented by the ECRF/LVF in order to capture all relevant information. All connections and connection attempts are recorded by the logging mechanisms built into IIS. All LoST queries and responses are logged both to the i3 event logging service (if one is available) and to an independent ECRF logging database. Debug logging can also be enabled on the ECRF with minimal impact and provides more specific detail regarding query processing. The ECRF/LVF system runs in a high-availability architecture to achieve the required five-nines up-time metric. Typically, two to four instances of the ECRF/LVF are deployed per data center, running behind load balancing hardware. Each instance runs on its own virtual machine, utilizing its own replica database instances. The load balancers perform a health check against each instance once per second and will automatically pull an unhealthy element from the pool and raise a system alert. A single instance of each element has enough capacity to run the entire system should there be multiple simultaneous failures of elements.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **Query Rate-Limiting** The proposed ECRF shall allow for rate-limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 48	Bidder Response: CenturyLink typically uses a DNS solution to have call flow related queries (LNG, ESRP, etc.) go to a certain group of ECRF/LVF instances and non-call flow related queries go to a different group of ECRF/LVF instances. Another route might be the following: All LoST connections, queries and responses are logged to debug log files and a centralized logging database. Additionally, LoST queries and responses can also be logged to a NENA compliant i3 logger. A utility tool called Log Analysis and Retrieval Tool (LART) can be provided to mine logging data from the database logging stores as needed. The ECRF/LVF is hosted by Microsoft IIS and will be deployed using reverse-proxy load balancers. The load balancers provide options for rate-limiting of queries and IIS offers a Dynamic IP Restrictions module which allows for rate-limiting of queries. The ESRPs will be configured as exceptions to the rate-limiting rules.				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **Supported Functions** The ECRF shall support each of the following items. Describe how the solution meets or exceeds each of the requirements below:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 49	Bidder Response: 1. **Logging**. Multiple levels of logging are implemented by the ECRF/LVF in order to capture all relevant information. All connections and connection attempts are recorded by the logging mechanisms built into IIS. All LoST queries and responses are logged both to the i3 event logging service and to an independent centralized ECRF logging database. Debug logging can also be enabled on the ECRF with minimal impact and provides more specific detail regarding query processing. GIS data updates are all logged, and a history of recent GIS edits are stored for every GIS feature. 2. **Error Correction**: Aggregation of independently maintained datasets requires an extra level of error checking, may present challenges in obtaining a consistent level of quality throughout the dataset, and requires the data aggregator to deal with any boundary/edge issues in order to present a single, usable set of data to the ECRF/LVF. Placing individual datasets into their own ECRF/LVF nodes requires coverage regions to be created that accurately describe the areas for which each node is authoritative but establishes a more direct line of responsibility and isolates any GIS issues so that they cannot block updates to data contained in other nodes. We recommend data aggregation be used if the combined data represents a contiguous area of similar quality, the aggregator can be treated as the authoritative source of that data and is effective in correcting errors in the data. If those conditions are not met, it may make more sense to keep the datasets isolated. Any errors found within the data are published out as an ESRI ArcGIS web service feature layer (although the errors can also be sent in a file-based format), allowing the GIS users to add this layer to ArcMap to provide real context to the location and nature of the errors.. 3. **SI Updates:** The SI provides the interface for provisioning updated GIS data to the ECRF/LVF. Upon receipt of updated GIS data, the SI performs a substantial amount of quality control checks to avoid provisioning the ECRF/LVF with bad data. The time it takes to run these checks varies based on the number of changes in the GIS data. Once the quality control has completed its checks, actual provisioning of the GIS data to the live ECRF/LVF instances is relatively quick. The SI and ECRF/LVF system use a concept of master and replica databases. The master database is not used in live call flow and is the location that any intensive processing takes place, such as the quality control workflows. When an update is committed to the master database by the SI, it is replicated using the RDBMS native replication process to each of the live call flow ECRF/LVF database	X			

	instances. This happens in the background and has little to no impact on the ECRF/LVF query performance. 4. **Geospatial call routing:** Our solution supports current and future versions of location validation, emergency call routing, and location-based call routing. Our service consists of database and database management software. It provides request / response and is compatible with all leading Automatic Number Identification (ANI) / ALI controllers as well as NG9-1-1 components such as Legacy Network Gateways (LNGs) and Emergency Service Routing Proxies (ESRPs). Our software can provision customer location data manually and in batches. If a civic location is correctly formed but is simply invalid, there are several possible outcomes depending on how much of the location is considered valid. It is possible that the query may still return correct call routing information, multiple sets of call routing information (if the location is ambiguous), or default call routing information with a warning. The ECRF/LVF fully supports both the civic and geodetic profiles. During the transitional phase, the LDB will provide all location, either directly or indirectly (via an E2 connection). For wireline calls, the LDB will contain an LVF valid and CLDXF compliant address location. For wireless, the LDB will contain a shell record, and will attempt to get more granular location over E2 from the Mobile Positioning Center (MPC). The location from the MPC will be a point and a confidence radius. This location is converted by the LDB into a circle that can be used by the ECRF for determining call routing. For VoIP, the LDB may contain either a civic address location or a shell record. If it is a shell record, the LDB will attempt to query the VoIP Positioning Center (VPC) for a more granular location. For VoIP, the E2 provided location could be geodetic or civic, or both. If the VPC provides a civic address location, it will be in the legacy MSAG format, so the LDB will utilize the MSAG Conversion Service (MCS) to convert the location into a CLDXF compliant PIDF-LO. Different service polygons can be used to represent different service request types (such as police, fire and EMS), represented by the service URN in the LoST query. The DDTi ECRF/LVF fully supports the service naming conventions defined in RFC 5031, including the top-level services and sub-services defined therein. Support for services defined in the future is provided via configuration updates. Service substitutions are also supported and may be configured to return a mapping for an alternate service if the desired service is not available for the queried location. For example, if the ECRF receives a query for urn:service.sos.physician, but no physician service polygon is defined for that location, the ECRF can be configured to respond with a mapping for another service, such as urn:service.sos.				

	5. **GIS Boundaries**: Our SI executes a program to collect, evaluate, and improve GIS data. This data is checked to ensure it meets the standard for CLDFX, but also that is contiguous and matches all segments and boundaries. Our GIS Ddata normalization service validates that road centerlines break at shared intersections, validates that no gaps or overlaps are in polygon boundaries. 6. **LoST queries:** Different polygon layers can be used to represent different service request types (such as police, fire and EMS), represented by the service URN in the LoST query. At a minimum, a layer that represents the top-level urn:service.sos is required. 7. **NENA Compliance:** All of our NGCS are designed from the outset to comply with applicable NENA standards. That is the core of business model. NENA 02-010 (now NENA STA-015.10-2018) is a legacy standard and has been superseded by NENA-STA-006.1.1-2020 (NENA Standard for NG9-1-1 GIS Data Model) and NENA-STA-004.1-2014 (NENA Next Generation United States Civic Location Data Exchange Format CLDXF). The ECRF/LVF fully complies with the new standards. NENA 02-014 is also a legacy standard. For example, it requires an Emergency Service Zone (ESZ) layer, which has no role in a NG9-1-1 deployment. 8. **Dynamic Updates:** The ECRF/LVF supports dynamic override service polygons. This feature allows authorized users to draw polygons on a map display and specify a new call route for any calls that fall within that polygon. 9. **Data Validation:** The SI, provides the interface for provisioning updated GIS data to the ECRF/LVF. Upon receipt of updated GIS data, the SI performs a substantial amount of quality control checks to avoid provisioning the ECRF/LVF with bad data. The time it takes to run these checks varies based on the number of changes in the GIS data. Once the quality control has completed its checks, actual provisioning of the GIS data to the live ECRF/LVF instances is relatively quick. More extensive detail on this data validation is provided in the SI section of this response.				

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions	X			
Location error identification.	X			
Updates from the SI in near real-time with no degradation of LoST services	X			
Routing of calls based on geographic coordinates, geodetic shapes, and civic addresses	X			

Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS).	X			
Permitting of LoST queries for find service request association with each layer.	X			
Compliance with NENA 02-010 and NENA 02-014.	X			
Dynamic updates to GIS without disruption of the ECRF.	X			
Validation of GIS updates before they are provisioned into the ECRF.	X			

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **User Interface and Provisioning** Define bidder's method for: 1. provisioning the ECRF; 2. updating the ECRF (including the frequency of updates); 3. validating data provisioning; 4. performing error logging; 5. performing gap and overlap analysis; and 6. supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet. 7. Provide a clear description of the functionality of the ECRF; list features and capabilities; 8. describe the error handling, default mechanisms, and logging; and 9. provide an overview of deployment recommendations to achieve 99.999 percent reliability.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 50	Bidder Response: Provisioning the ECRF; updating the ECRF **(including the frequency of updates); validating data provisioning** The GIS data provisioned to the ECRF/LVF can be updated as often as the state desires. It is recommended a frequency of at least weekly, with daily being optimal. Provisioning of the ECRF/LVF is accomplished using the Spatial Interface product. CenturyLink will work with each jurisdiction that is providing GIS data to determine an automated process for receiving data updates. This is typically accomplished by the secure transfer of a file-based GIS format, such as an ESRI File Geodatabase. There are multiple layers of testing performed when new GIS is received. Initial tests check layer availability and subsequent tests evaluate completeness. If the data passes the import checks, it will be loaded into the SI where more granular and spatial quality controls are performed. If there are any discrepancies, this process updates the quality control tables. Data that passes quality control can then be provisioned in near-real time to other systems within the network, including the ECRF/LVF. Custom publishing of data can also occur for use in other systems, such a Computer Aided Dispatch (CAD) or a PSA Tactical Map Display. Any errors found within the data are published out as an ESRI ArcGIS web service feature layer (although the errors can also be sent to the county in a file-based format), allowing the GIS users to add this layer to ArcMap to provide real context to the location and nature of the errors. The following screenshot shows a sample quality control error layer displayed in ArcGIS Online. A web interface is provided within the solution that allows authorized users to configure the GIS quality control checks, set quality control thresholds, and view reports on quality control metrics. The following screenshot shows the quality control configuration page of the SI web interface. Each jurisdiction will have its own set of layers within the SI, and there will also be one aggregated state-wide dataset. When changes occur to a jurisdiction GIS layer, and those changes pass the quality control checks, those changes will be pushed to the aggregated state-wide dataset, where additional quality control checks will run (something might not be an error at the local dataset level but could be an error at the aggregated dataset level, such as a duplicate address). The Spatial Interface system will attempt to publish GIS data updates to the target ECRF/LVF systems based on publishing rules. Publishing rules are configured within the quality control configuration. For example, if there are gaps or overlaps in the datasets and a zero tolerance for gaps and overlaps has been agreed upon, then the data will not publish to the ECRF. The errors, with their locations, will be sent to the appropriate entity and resolution must be achieved and data resent to the system after remediation. Performing error logging				

	Multiple levels of logging are implemented by the ECRF/LVF in order to capture all relevant information. All connections and connection attempts are recorded by the logging mechanisms built into IIS. All LoST queries and responses are logged both to the i3 event logging service and to an independent centralized ECRF logging database. Debug logging can also be enabled on the ECRF with minimal impact and provides more specific detail regarding query processing. Additionally, informational and error messages can be written to other tools, such as DataDog or Seq. **Performing gap and overlap analysis** As part of the GIS data provisioning the Spatial Interfacer product performs checks on polygon layers for gaps and overlaps. Typically, publishing thresholds are set to block a polygon layer from being published to the ECRF/LVF if it contains a gap or overlap. Additionally, just like point and line quality control errors, polygon error can be shared back to the appropriate GIS authority as a map layer, either file based or as a web service. **Supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet** The ECRF/LVF supports all query and response types defined in the LoST protocol RFC 5222. The ECRF/LVF allows access to the LoST interface with firewall rules, preventing unauthorized access. **Provide a clear description of the functionality of the ECRF; list features and capabilities** The ECRF/LVF system utilizes a Microsoft SQL Server backend, and utilizes Microsoft IIS for the http(s) interface. A master ECRF/LVF receives GIS data updates from the SI product. These updates are then replicated to each ECRF/LVF instance, each of which use their own replica of the database. Any failure in the master database would have no impact on the replica databases, allowing each ECRF/LVF instance to continue to be fully functional (although no GIS data updates would process until the master database is back online). The ECRF/LVF is a fully standards compliant LoST Server as defined by RFC 5222. The LoST protocol also provides extension points for errors, warnings, and location validation. The ECRF/LVF already includes several such extensions used to better characterize the quality of the response and anticipates that similar or equivalent extensions will be standardized by NENA at some point in the future. Additionally, there is a standards-track draft "draft-ietf-ecrit-similar-location" extension to LoST which will allow a LoST server to respond with suggested locations when the location used in the findService query is invalid or incomplete. This has been implemented in the ECRF/LVF and can be used by the LDB to provide users with help in resolving discrepancies. Describe the error handling, default mechanisms, and logging The ECRF/LVF is designed to answer queries with the most useful possible response for the given query parameter and takes full advantage of the errors and warnings defined for the LoST protocol when needed. If the location in the query is malformed in such a way that it cannot be understood, the server will return a descriptive error message documenting the problem to the best that it could determine. If a civic location is correctly formed but is simply invalid, meaning that it cannot be uniquely resolved to a GIS feature, then there are several possible outcomes depending on how much of the location is considered valid. It is possible that the query may still return correct call routing information, multiple sets of call routing information (if the location is ambiguous), or default call routing information with a warning. Multiple levels of logging are implemented by the ECRF/LVF in order to capture all relevant information. All connections and connection attempts are recorded by the logging mechanisms built into IIS. All LoST queries and responses are logged both to the i3 event logging service and to an independent centralized ECRF logging database. Debug logging can also be enabled on the ECRF with minimal impact and provides more specific detail regarding query processing.

	Provide an overview of deployment recommendations to achieve 99.999 percent reliability The ECRF/LVF system runs in a high-availability architecture to achieve the required five-nines up-time metric. Typically, two to four instances of the ECRF/LVF are deployed per data center, running behind load balancing hardware. Each instance runs on its own virtual machine or container, utilizing its own replica database instances. The load balancers perform a health check against each instance once per second and will automatically pull an unhealthy element from the pool and raise a system alert. A single instance of each element has enough capacity to run the entire system should there be multiple simultaneous failures of elements.

Any additional documentation can be inserted here:

NGCS 51	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Hierarchical Integration with Other ECRFs** The ESInet will be part of an overall hierarchical plan that includes interconnectivity to other regions and ECRFs. Provide details regarding bidder's vision for how this interconnection will include replicas of ECRF/LVF at different levels of the hierarchy, as well as access/origination networks.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink will deploy an ECRF/LVF system that is authoritative for the state and any other jurisdictions that become part of the project. Internal ECRF/LVF replicas will be deployed within the ESInet and will only receive queries originating internally or from other trusted ESInets. External ECRF/LVF replicas will be deployed within a DMZ and will handle all queries originating from untrusted networks and the public Internet. Once neighboring state-level ECRF/LVF's are provisioned, tabular and spatial authoritative coverage regions will be provided to each state-level ECRF/LVF vendor so that their state-level ECRF/LVF can be provisioned with this information. The state-level neighboring ECRF/LVF's will also need to provide coverage data for provisioning in the Nebraska ECRF/LVF. IP connectivity will need to be established between each neighboring state-level ECRF/LVF and the Nebraska ECRF/LVF defined for this project to allow recursion between the systems based on the authoritative coverage data. A similar process is required for geodetic queries. A polygon will be loaded into the Nebraska ECRF/LVF that defines the geographic area for which it is authoritative. This same polygon will be provided to the neighboring state-level ECRF/LVF's. If a neighboring state-level ECRF/LVF receives a geodetic query that falls inside that polygon, it will know to recursively send the query to the Nebraska ECRF/LVF for the authoritative answer (or using an iterative approach, respond to the query with the application string of the Nebraska ECRF/LVF so the client can directly query it). This approach will create a multi-state LoST tree and can be used until a National Forest Guide is available to create LoST tree hierarchy. Also, if all external ECRF/LVF replicas are attacked or compromised, the internal replicas will still be available to service internal validation and calls and those from trusted networks. Both internal and external ECRF/LVF servers are critical to performing location validation and placing 9-1-1 calls in a Next Generation environment and both tiers will be deployed in highly available and redundant configurations.				

Any additional documentation can be inserted here:

NGCS 52	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Forest Guide** Provide explanations of any tradeoffs between aggregations of data at higher-level ECRFs versus the use of Forest Guides (as defined in NENA-INF-009.1-2014) to refer requests between ECRFs that possess different levels of data. As part of that explanation, provide details on how the appropriate ECRF/LVF data will be managed and provisioned for use in overload and backup routing scenarios in the current environment, and any dependencies that might impact provisioning.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The LoST protocol is designed for servers to be organized in hierarchical trees and for queries to automatically navigate the tree structure until the authoritative server for the queried location is reached. The tree structure of the LoST system allows GIS data to be maintained in any number of independent, authoritative datasets for different regions, each with its own logical ECRF/LVF node. These nodes may or may not reside on the same physical servers as other ECRF/LVF nodes. Forest guides are LoST servers which facilitate navigation between trees in the LoST hierarchy but are not authoritative to answer queries on their own and are not provisioned with data other than coverage regions of the root nodes. The LoST hierarchy is built as a collection of LoST trees, each represented by a root node which is authoritative for one or more areas designated by coverage regions. Each root node publicizes its coverage regions via forest guides. Each root node may optionally delegate some or all its authority to one or more lower level child nodes. This delegation is also expressed using coverage regions which are narrower in scope than those representing the entire root node. These smaller coverage regions must be shared between a parent and child but are not distributed to forest guides. Each child node, in turn, may further delegate authority to children of its own. There is no requirement that a root node ECRF/LVF be authoritative for a size or scope of area, although it is generally suggested that root nodes be on the scale of a country or state. This allows individual jurisdictions flexibility in determining how to deploy ECRF/LVF services. Deployment can be in cooperation with other ECRF/LVFs in an existing tree structure, or a new root node can be declared. Smaller jurisdictions that are prepared to move forward earlier than others in their region may initially deploy an ECRF/LVF as a root node, but have that node moved under a larger parent in the future. This is what will affect the coverage regions represented in forest guides, and to a lesser effect how often a forest guide is needed to allow a query to navigate the LoST hierarchy. The question of GIS data aggregation does not directly determine whether a node is a root node or a child node, but rather determines whether a given area is represented by one logical ECRF node or many (which may or may not fall under a common parent). The LoST protocol is designed to work seamlessly in any case. There are some tradeoffs, however, between aggregation or non-aggregation. Aggregation of independently maintained datasets requires an extra level of error checking, may present challenges in obtaining a consistent level of quality throughout the dataset, and requires the data aggregator to deal with any boundary/edge issues in order to present a single, usable set of data to the ECRF/LVF. Placing individual datasets into their own ECRF/LVF nodes requires coverage regions to be created that accurately describe the areas for which each node is authoritative but establishes a more direct line of responsibility and isolates any GIS issues so that they cannot block updates to data contained in other nodes. A logical ECRF/LVF node can essentially be hosted with as many replicas and at any locations that the responsible authority wishes. Smaller nodes may be able to better take advantage of the performance benefits of distributed computing when placed on separate physical hosts but incur virtually no penalty when co-hosted versus the same data combined into a single dataset.				

	It should be noted that every ECRF/LVF query must be answered with a service mapping from the authoritative logical node. ECRF/LVFs that are not authoritative for a queried location can answer using cached mappings in some cases but cannot independently generate a result in the case that the authoritative node cannot be reached. Further, because the expiration time of cached mappings is typically very short (minutes), it is unlikely that non-authoritative servers will be of any substantial benefit in the event of a failure of the authoritative node. There is no mechanism for one logical ECRF/LVF node to "take over" for another. The requirement to have reliability and high availability of the ECRF/LVF service should not be a factor in decisions regarding aggregation of data. Rather, every logical node should simply be deployed in a geo-diverse manner using as many replicas as needed to obtain both the desired performance and reliability. Some or all replicas could conceivably be hosted on common hardware with other logical ECRF/LVF nodes. Provisioning of all replicas of a logical node must be identical but is completely independent (aside from shared resources such as disk space) of provisioning for any other nodes that happen to be hosted in the same place.

Any additional documentation can be inserted here:

NGCS 53	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** An LVF is a LoST protocol server where civic location information for every call originating endpoint is validated against the SI-provisioned GIS data Describe how the LVF solution interfaces with other LVF solutions which may interface with bidder's solution. Contractor shall coordinate with other LVF solution providers to ensure interoperability between the respective solutions.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Our Spatial Interface (SI) is at the heart of the GIS to ECRF/LVF integration. This function supports the periodic loading of GIS data from external systems. GIS data can be uploaded via an intuitive web interface enabling authorized users to provision the SI with geospatial data in ESRI shapefile or file geodatabase formats, verify that the data is in the expected schema, and initiate the load process into the SI. Alternatively, automated routines can be set up to populate the SI without having to upload via the web interface. The load into the SI system does not do a complete overwrite; rather, it performs a change detection operation. As a result, an historical record of data changes can be maintained by the system, and detailed results of any load errors are provided. This process, either with the web interface or using automated routines, can be run as frequently as needed, although daily is recommended. Once the data load is complete, our SI performs numerous quality control checks on the data. The resulting QC errors can be viewed directly using any software capable of consuming ESRI-based web services. This will allow the viewing of any map data discrepancies in real-time. Following the QC process, if the number and severity of any errors are within configurable limits: the system will automatically publish updated data the to the master ECRF/LVF database. This database acts as a replication master, pushing all changes using Microsoft SQL Server replication to child databases that are used for ECRF/LVF functionality. All replication distributions run on the master database to minimize the load on the databases that are being actively used for LoST query processing. SQL Server replication occurs in near-real-time. The SI also provides reporting, allowing real-time access into the state of the datasets used by the ECRF/LVF. Additional publishing routines can be set-up for other applications that may need GIS data. This allows administrators to create publishing tasks that export copies of the data into a format that is required by third-party applications. For example, CPE may require a certain data extract that is different from what CAD requires.				

Any additional documentation can be inserted here:

NGCS 54	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **LVF Description** The SI is responsible for provisioning and updating the information used for location validation in the LVF, which shall contain a standardized interface to the SI. Describe how the LVF solution meets the above requirements**.**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The GIS data provisioned to the ECRF/LVF can be updated as often as the state desires. This is accomplished using a SI database management system. We will work with each jurisdiction that is providing GIS data to determine an automated process for receiving data updates. This is typically accomplished by the secure transfer of a file-based GIS format, such as an ESRI File Geodatabase. There are multiple layers of testing performed when new GIS is received. Initial tests check layer availability and subsequent tests evaluate completeness. For example, the system will test new GIS data to ensure required fields are complete prior to loading. The load process performs a change detection against the data that currently exists in system, and only processes records that have changed. If minimum data requirements are not met (e.g., expected layers are missing from the source data, duplicate unique IDs are present, or spatial inconsistencies such as invalid geometry or multi-part features are detected), email notifications will be sent identifying the errors. As a result, processes can be placed on hold until corrections are made and remediated data is uploaded. If the data passes the import checks, it will be loaded into the database management system where more granular and spatial quality controls are performed. If there are any discrepancies, this process updates the quality control tables. Data that passes quality control can then be provisioned in near-real time to other systems within the network, including the ECRF/LVF. Custom publishing of data can also occur for use in other systems, such a Computer Aided Dispatch (CAD) or a Tactical Map Display. Any errors found within the data are published out as an ESRI ArcGIS web service feature layer (although the errors can also be sent to the county in a file-based format), allowing the GIS users to add this layer to ArcMap to provide real context to the location and nature of the errors. The following screenshot shows a sample quality control error layer displayed in ArcGIS Online. A web interface is provided within the solution that allows authorized users to configure the GIS quality control checks, set quality control thresholds, and view reports on quality control metrics. Each jurisdiction will have its own set of layers within The Database Management System, and there will also be one aggregated region-wide dataset. When changes occur to a jurisdiction GIS layer, and those changes pass the quality control checks, those changes will be pushed to the aggregated region-wide dataset, where additional quality control checks will run (something might not be an error at the local dataset level but could be an error at the aggregated dataset level, such as a duplicate address). The database management system will attempt to publish GIS data updates to the target ECRF/LVF systems based on publishing rules. Publishing rules are configured within the quality control configuration. For example, if there are gaps or overlaps in the datasets and a zero tolerance for gaps and overlaps has been agreed upon, then the data will not publish to the ECRF. The errors, with their locations, will be sent to the appropriate entity and resolution must be achieved and data resent to the system after remediation.				

Any additional documentation can be inserted here:

NGCS 55	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **Location Validation** The LVF shall be available to validate civic locations at the time a wireline device is ordered— e.g., Service Order Interface (SOI) validation—when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB shall be allowed to periodically revalidate the civic location information against the GIS data contained within the LVF. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Location validation prior to the use of that location in an emergency call is one of the fundamental principles in NG9-1-1. The ECRF/LVF is designed to be deployed as a highly available service that can run without interruption. The ECRF/LVF will be available for validation of locations fitting the civic location profile as described in RFC 5222. The ECRF/LVF will be accessible to all endpoints within the ESInet and trusted networks as well as made publicly accessible via the internet. This is necessary both for call routing and so that any device or location server can pre-validate civic locations. Please note that SOI records do not fit the civic location profile required for LoST queries and contain data that does not follow CLDXF standards. To ensure SOI records to be directly validated by a compliant ECRF/LVF, a Location Database (LDB) must be used to first convert (with the use of the NENA defined MSAG Conversion Service) the SOI data to a CLDXF-compliant PIDF-LO. Although the ECRF/LVF itself cannot initiate the revalidation of civic locations contained within the LDB or any other location server (it can only respond when queried), periodic revalidation of all civic location records is expected and the ECRF/LVF will be sized with sufficient capacity to handle such ongoing revalidation activity. The ECRF/LVF is fully RFC 5222 compliant, supporting the optional "validateLocation" attribute of a LoST query. Additionally, the ECRF/LVF has been extended to include the ECRIT Similar and Complete Location standard, allowing additional useful information to be passed back to clients making validation queries. The LDB has three different mechanisms for revalidation: • A full revalidation runs as a scheduled job to periodically revalidate every civic address record in the LDB against the GIS using an LVF query. • A discrepancy revalidation runs more frequently and revalidates LDB records that were previously flagged as being LVF invalid. • A targeted revalidation runs when GIS data in the ECRF/LVF system has been updated and revalidates civic address records in the LDB that may have been affected by the specific changes to the GIS data.				

Any additional documentation can be inserted here:

NGCS 56	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **High-Availability Design** The LVF shall support all functionality as defined in NENA-STA-010.2-2016, shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability, and shall be provisioned with the same data as the ECRF. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: As previously described, the ECRF/LVF system is deployed as a series of LoST Servers, so each server is identical regardless of what its primary use will be (live call-flow routing or civic address validation). The ECRF/LVF system runs in a high-availability architecture to achieve the required five-nines up-time metric. Typically, two to four instances of the ECRF/LVF are deployed per data center, running behind load balancing hardware. Each instance runs on its own virtual machine, utilizing its own replica database instances. The load balancers perform a health check against each instance once per second and will automatically pull an unhealthy element from the pool and raise a system alert. A single instance of each element has enough capacity to run the entire system should there be multiple simultaneous failures of elements.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) **Location Validation Function (LVF)** **Public-Facing LVF** Outline options for a public-facing LVF provisioned for use by service providers outside the ESInet.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 57	Bidder Response: Location validation prior to the use of that location in an emergency call is one of the fundamental principles in NG9-1-1. This means that location validation must be available to all devices and service providers via a public interface. Because the ECRF/LVF is a critical functional element used both within and external to the ESInet, separate internal and external ECRF/LVF replicas will be deployed at each data center designated for handling queries that originate outside the ESInet. Internal ECRF/LVF replicas will be deployed within the ESInet and will only receive queries originating internally or from other trusted ESInets. External ECRF/ replicas will be deployed within a DMZ and will handle all queries originating from untrusted networks and the public Internet. The public facing servers will be part of the same SQL Server replication tree as the internal ECRF/LVF servers, so will contain identical data. The border control function (BCF) must allow externally originating LoST queries from any source unless the BCF deems that traffic to be malicious in nature. The authoritative coverage regions of the ECRF/LVF will be exported to a higher level ECRF/LVF node or Forest Guide. Service providers supporting nomadic devices will interact with the same public facing ECRF/LVF as service providers offering fixed devices, described above. Service providers will initiate a LoST query for all new and changed locations for nomadic devices, and the ECRF/LVF will respond in real time. If all external ECRF/LVF replicas are attacked or compromised, the internal replicas will still be available to service internal validation and calls and those from trusted networks. Both internal and external ECRF/LVF servers are critical to performing location validation and placing 9-1-1 calls in a Next Generation environment and both tiers will be deployed in highly available and redundant configurations.				

Any additional documentation can be inserted here:

NGCS 58	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **User Interface and Security** Describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined in NENA-STA-010.2-2016, with particular attention to: 1. the arrangement of the proposed components; 2. user interface and features; 3. and security aspects.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

The ECRF/LVF is a scalable LoST (Location-to-Service Translation) server that adheres to IETF and NENA standards and provides both call routing and location validation functions. The ECRF/LVF is hosted within Microsoft Internet Information Services (IIS), and connects to a Microsoft SQL Server backend database. The solution leverages numerous Microsoft technologies to provide reliable, highly available, and highly performant service. Hosting the service within IIS also provides timely access to security updates and a rich set of options related to security and management (LoST is transported over HTTP and HTTP-over-TLS).

The LoST protocol is specified in RFC 5222, and the ECRF/LVF implementation was designed for strict compliance with that specification in order to assure correct functionality and interoperability with LoST clients as well as other ECRF/LVFs. Several related specifications are referenced directly or indirectly by RFC 5222, with which the ECRF/LVF also complies. Those include:

- RFC 4848 for LoST server name resolution.
- RFC 5031 for service names and format.
- RFCs 4119, 5139, and 5491 for location formats.
- RFC 5582 (informative) for LoST architecture.

The ECRF/LVF also implements requirements that are specific to NENA i3, including:

- Configurable service names, for services beyond those specified in RFC 5031.
- Logging of LoST queries and responses to an i3-compatible logging service.
- Discovery of additional data associated with a location.

The design of the ECRF/LVF allows for flexible hosting options including multiple replicas. To achieve the availability and reliability needed for NG9-1-1, multiple ECRF/LVF replicas will be deployed, each on datacenter-grade hardware having redundant network connectivity. Redundant load balancers will serve as reverse proxies for all incoming queries, and https requests will be secured with TLS according to industry best practices.

Because the ECRF/LVF is a critical functional element used both within the ESInet and by validation and calls originating external to the ESInet, separate internal and external ECRF/LVF replicas will be deployed for each logical node. Internal ECRF/LVF replicas will be deployed within the ESInet and will only receive queries originating internally or from other trusted ESInets. External ECRF/LVF replicas will be deployed within a DMZ and will handle all queries originating from untrusted networks and the public Internet. This helps minimize the security risk associated with operating a service that must be accessible via the public internet and allows internal functionality to continue unimpeded even if all externally facing replicas are under are attack.

	Please note that specifications for the ECRF/LVF do not include a traditional user interface. The specified point of interaction for location validation is the LoST query interface, which is an XML-based query/response mechanism using HTTP. While the results of a LoST query can be read by humans, normally a third-party application is responsible for generating the query and presenting the result to a user. The Location Database (LDB) Manager website is an example of such an application, and allows users to enter a location, test its validity, and visualize the results. A user interface is provided for the SI, which provides full insight into the GIS data within the ECRF/LVF.

Any additional documentation can be inserted here:

NGCS 59	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **SI Description** The SI is responsible for provisioning and updating authoritative GIS data to the ECRF, the LVF, the map viewer, the PSAP tactical map display, CAD systems, and similar applications that consume GIS data. GIS data provisioned by the SI shall undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: NENA 02-010 and NENA 02-014 are mostly legacy standards and are superseded by NG9-1-1 standards, including NENA-REQ-002.1-2016, NENA-STA-005.1.1- 2017 and NENA-STA-006.1-2018. Adherence to the updated standards and data models is preferred. NENA Next Generation 9-1-1 Data Management Requirements (NENA-REQ-002.1, Section 3.3) states: "It is expected that 9-1-1 Authorities will perform Quality Assurance/Quality Control (QA/QC) processes listed above prior to provisioning the data into the SI thus minimizing the errors and resolution timeframe for the provisioning process." Some issues that could be reported back to the 9-1-1 authority from the SI are: • Invalid geometry • Gap/overlap • Duplicate attribute as defined by the SI system • Mandatory field(s) missing or mismatched data types • Address range issues on centerline • General provisioning failure to SI or ECRF/LVF • Malformed Uniform Resource Identifier (URI) There are many more data quality control checks that should be performed, and with different data QC gateways the GIS department(s) and 9-1-1 authority have the flexibility to identity errors at a much earlier stage than the SI. GIS Data QCs occur at multiple stages. It starts before data is provisioned and it is recommended the MSAG and ALI are rigorously synchronized to the NG9-1-1 Authoritative GIS layers which will be used for call routing before procurement or implementation of a NG9-1-1 system. After that is complete, it is important that an iterative QC occurs each time data is submitted to the system. Between the time a GIS departments data is submitted and before the data is provisioned to the ECRF and LVF, there are two gateways where error trapping can occur which provides flexibility in QC configurations and allows for critical errors to be identified as early as possible in the replication process. As a GIS department who is responsible for maintaining the authoritative GIS data for the service area being provisioned and along with a 9-1-1 Authority, they will have the choice of what QC errors should stop publishing to the ECRF and LVF so the error(s) can be corrected and data re-submitted to the system as soon as possible.				

	The first data gate is the Data Importing Service which upon success then passes the data to a secondary QC process where if any discrepancies exist, then a QC file will be updated. QCs are returned to a subscribing GIS group who would then be responsible for fixing the data. The Data Importing Service recognizes and reports general errors from each GIS layer the earliest and analyzes and reports on issues with: • Data file names • NG9-1-1 schema constraints • Primary Key inconsistencies • Unique ID • Allowable <Null> values • Default Values • Spatial Reference Identifier • Partial dataset detection (configurable) • Records which break spatial validity rules • Records that containing multi-part features • Data type incompatibility • Alias record duplication The value of these QCs allows the GIS provider to stop processing and replication before data is entered into the Spatial Interface and the subscriber group will be notified at the earliest stage possible. Upon successful quality control, data from the SI can be provisioned confidently to any downstream element which consumes the authoritative GIS data, including PSAP map display, CAD, and other ECRFs.

Any additional documentation can be inserted here:

NGCS 60	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Web Feature Service and Updates** The SI shall convert the GIS data into the format (data structure and projection) used by the ECRF and LVF, in real-time or near real-time, using a web feature service. The SI shall be able to provision and perform incremental updates, in near real-time, to the ECRF, LVF, the map viewer service, the PSAP tactical map display and similar applications that consume GIS data. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply

Bidder Response:

Data Publishing

There are several processes for updating data to internal and external systems. The first is the update process to the primary data sources which consist of the ECRF database(s), the ESRI Server database(s), and the creation of ESRI file formats for potential external distribution. In addition, there are administrative controls to manage and report on the process from the SI web site. Finally, there are several potential methods that can be used for data distribution beyond the ECRF and ESRI databases.

Data Update Overview

ECRF/LVF database(s) Updates

The Spatial Interface publishing mechanism operates by detecting changes made to data held within the SI (through the Data Import process, or by editors directly), determining the resulting differences compared to the current ECRF/LVF database, and then executing SQL transactions to bring the ECRF/LVF database up to date. All change comparison operations involving the ECRF/LVF data are performed on the ECRF/LVF master database, which is not used in LoST query processing. All operational ECRF/LVFs use local replica databases to answer queries. This means the change comparison portion of the ECRF/LVF updates cannot impact live LoST services. The update portion of the process uses SQL transactions specifically designed to minimize the impact to concurrent queries used to answer LoST requests. This minimizes the impact on individual ECRF/LVF replicas when the update transactions are applied. All guaranteed service levels are maintained during an ECRF/LVF data update.

ESRI Server(s) Updates for Tactical Map Display

The current map datasets are exported from the Spatial Interface. These are then migrated to Esri Server to be processed. First, the new Roads and Addresses data is used to update the locator data that is used by the Esri Geocoding service. If the Esri server is providing a map tile service, the new data set is compared to the previous version. These are compared to detect which map tiles need to be updated. Once the map tiles have been updated for the master server, the new tiles are copied to any additional Esri Servers that are providing a map tile service. Finally, the reference data is updated for the next iteration of updates and data comparisons.

Custom Export Files

When the publishing is initiated in SI, it can also generate custom exports in standard ESRI file formats or non-spatial formats. These can be used for legacy systems or to distribute the data for systems outside of the Next Generation system.

Administration

	The Spatial Interface website provides a secure process for administrative users to manage their data publishing rules, determine which QCs are performed on the data, control QC and Publishing jobs, and get current status reports related to QC and Publishing. *Publishing Rules* Publishing rules can be setup for any layer that will be published. Each QC has an assigned severity level and based on these, an administrative user can create rules that will allow or disallow automated publishing of the data. There are two types of rules: 1. An absolute rule that is based on the total number of errors for a particular severity for a particular layer. For example, the fire service polygon may be blocked for publishing with a count of critical errors > 0 (or any positive integer). 2. A rule based on the percentage of records with errors at a particular severity level. For example, the Roads layer may be blocked from publishing when the percentile of records with medium severity errors is > 10%. **QC** *Tests* An authorized administrative user can set whether the QC test will be performed by turning the QC on or off and can set the severity level of a QC process (i.e., the severity level used in publishing rules). **Monitoring and Control** The current status of any QC or publishing jobs is reported in the website. In addition, the last successful job(s) completed are also reported. QC and publishing jobs can be stopped and initiated from the SI website. **Data Distribution** There are several methods that can be used to either distribute the GIS data directly or provide access to the data via services. The ECRF database(s) are tightly coupled to the Spatial Interface, so data is directly provided to the ECRF via the publishing processes. Further data access can be provided by the Esri server(s). This can include map tile services, web feature services and other Esri methods as required. For data users outside of the NG9-1-1 system, spatial or non-spatial files can be made available via SFTP. For example, the Roads can be used to generate a MSAG 3.1 file that can be distributed to TSP entities for use in their phone databases.

Any additional documentation can be inserted here:

NGCS 61	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Data Provisioning and Validation** Describe the functionality of the proposed SI solution in sufficient detail to explain the validation of GIS data and data updates prior to provisioning into the ECRF and LVF, along with the means of real-time or near real-time provisioning of incremental updates to the GIS data provisioned to the ECRF and LVF.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: **Spatial Interface (SI)** There are four core areas of functionality for the SI Service: Data Quality Control, Data Publishing, System and Data Reporting, and Administrative Control. *Data Quality Control* • The SI includes a quality control (QC) process that runs continuously and evaluates updates as they are incorporated into the core database. The output of these checks is one or more (depending on the QC checks that are used) QC error layers in the SI system. • Users can view QC error layers directly using the Data Maintenance Service user interface, and/or the QC error layers can also be exported to Esri file-based formats. In addition, an Esri server layer can be used to distribute the QC error data (requires appropriate Esri licensing). • The QC checks can be assigned to several different classifications: geocoding, standards, internal consistencies, and external consistencies (if any). These checks include most of the tests that were used during the data quality control and synchronization phases as previously described. *Data Publishing* • The Data Publishing function transforms, formats, and exports the data from the core database into files or other databases based on the client's needs. The publishing of the data can be restricted based upon errors detected during the QC process. Individual QCs are assigned to a customizable severity level, and individual thresholds can be configured for each severity level and GIS layer. These thresholds can be based on either the absolute count of errors or the relative rate of errors in the layer. If the any of the QC error thresholds are violated, the publish process will be blocked. It is also possible for an administrator to configure a given publishing task to ignore the QC error thresholds, if needed. • Data publishing tasks can be initiated on demand, scheduled as a one-time publish, scheduled as a reoccurring publish, or can be triggered automatically by any changes following the completion of QC checks. • A database layer can be setup to be published to multiple user defined export files. Each one of these exports can be customized in a limited way. The specific fields to export can be designated, and the output field name and format can be configured. • The Data Publishing will directly update the master ECRF database. The other ECRF databases will be update via replication from the master ECRF database. *System and Data Reporting* • QC error summary counts are available via the SI website, as well as detailed counts by error type/description. • Change report summaries and counts are available on a scheduled basis.				

	• Publishing failures (due to excessive QC errors, for example) can be configured to generate email notifications. • The system contains all the historical data along with a time stamp and user ID for any changes. *Administrative Control* • The Spatial Interface website provides a secure administrative interface. • Administrators can configure quality control and data publishing from the website. • Administrators can also control users, permissions, and display options. • Administrators can request a rollback to a previous database state if necessary.

Any additional documentation can be inserted here:

NGCS 62	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Use of the Commission's GIS Data Model** 1. Describe how the bidder's solution will use the Commission's GIS data model (Attachment B) without modification to the schema. 2. Define bidder's processes and methods to receive and incorporate the updated SI datasets. 3. Describe bidder's proposed workflow for receiving GIS updates from regions to allow for a smooth transition. 4. Describe all security and monitoring aspects, and any additional features supported by the proposed SI.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The ECRF/LVF, LDB and MCS solution has been built form the ground up as a NENA i3 solution. The Commission's GIS data model is closely aligned with the Next Generation 9-1-1 GIS Data Model and can therefore be used directly in our solution with no modification. CenturyLink will work directly with each region to determine the best method to receive data updates. Typically, this involves some sort of secure and automated file transfer, but other mechanisms are available too (such as database replication). The Spatial Interface system offers two possible solutions for the workflow. It can either process each jurisdiction's data in complete isolation, and then publish each dataset to individual ECRF/LVF instances (each of which would share each other's authoritative coverage information allowing them to do recursive queries amongst themselves), or SI can aggregate each jurisdiction's data set into an state-wide dataset. The workflow process from local jurisdictions and progressing to the ECRF/LVF dataset is integrated with the following processes: *The Local Data Editing Environment* This is the where the local jurisdiction(s) edit and maintain their GIS data that will eventually populate the ECRF database. There are several options for services in this category. Each local jurisdiction can pick the option that best fits their needs and existing processes. In addition, it is possible to mix the options within the jurisdiction by layer. For example, the Road layer could be maintained by one local agency and the ESB layers could be maintained by a different agency. Each of these agencies can pick the option that best suites them. The basic requirement is that a given local GIS layer can only be maintained via one option. *Data Submission* This service facilitates the submission of data updates for the GIS layers by the local jurisdictions. There are several options that can be selected and like the data editing options, this can be customized down to the local GIS layer level. In addition, non-GIS data (MSAG and ALI data for example) can be submitted via SFTP. Data Import Services The Data Import Service consists of six core areas of functionality: Data Update Monitoring, Data Schema Verification, Data Transformation, Data Coalescence and Regional Data Updating. There is an instance configured for each local data provider. The only client requirement for the Data Import service is a valid email account for error and job status reporting.				

- Data Update Monitoring
  - The Data Import Service monitors a configured destination location for the data submission process. If an update is detected, the Data Import processes will automatically start.
- Data Schema Verification
  - The submitted data is checked against the configured local schema and verified that the data transformation can be applied.
  - If there are any schema issues or specific record issues, they will be reported to the local data provider via email. The email will include detailed information concerning the specific errors.
    - A schema issue is usually caused by a change in the submitted data fields. For example, if a field name has been changed then the configured data transformation may no longer be valid.
    - Individual record issues are usually caused by specific data values. For example, if submitted record contains a non-integer value in an integer target field then there will be a data conversion issue for the individual record. Additionally, invalid geometry is also checked and would be reported for the individual records with invalid geometry.
- Data Transformation
  - The submitted data is transformed to the ECRF data set schema using the configured transformation(s).
- Data Coalescence
  - The set of the most current transformed local datasets are coalesced to form the Next Generation Map data set for updating the Spatial Interface database. This coalescence transformation may include some topological based transformations depending on the configuration beyond that this functionality is at its core a union operation.
- Regional Data Updating
  - The current ECRF data set is compared to the current SI data set. The changes in the two data sets are detected and are classified as a delete, add, or modify. The ECRF data set is modified based on the changes detected above.

Spatial Interface Software

The SI software is tied to the ECRF data set. Each ECRF data set will have its own instance of the SI service (it is expected there will be one instance for this project). There are three main functions that the Spatial Interface performs. First, it is the primary Data Quality Control engine for the ECRF. In addition, the Quality Control results will be prepared and served back out through one of the Data Discrepancy Reporting Options. The Spatial Interface service has the export transforms that will be necessary for exporting the data to the ECRF data set and for other custom exports (for example, the mapping application in the Dispatch Centers). The next function is the publishing function which will verify that the data meets the quality constraints (customizable) for publishing data to the ECRF and other systems (if applicable). It then will perform the necessary transformations and export the data. Finally, there is an administrative website that will enable registered users to control these functions and view reports on the system.

Next Generation Services

This will consist of two independent services: the ECRF/LVF service and the Location Database (LDB) Service. The ECRF database will have the current ECRF data set and will provide the LVF query service. The Location Database will have the Next Generation phone data. It will initiate the

	LVF queries and store the LDB discrepancies (i.e. phone records that have discrepancies from the LVF query). The LDB website provides functionality for managing the discrepancies including assignment to different groups, resolution and auditing. GIS Data Discrepancy Reporting There are several options for reporting discrepancies. Most of the services will provide website access to the discrepancies. In addition, the discrepancies can be exported into various formats so that the local user can access them in their Data Editing environments. Alternatively, if the discrepancies have a spatial component then they can be provided as an Esri data service.

Any additional documentation can be inserted here:

NGCS 63	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** Describe how the solution interfaces with other LDB solutions which may participate in or interface with bidder's solution. Contractor shall coordinate with other LDB solution providers to ensure interoperability between the respective solutions. Also explain how the proposed solution would deal with multiple ALI/MSAG databases and the locations where ALI steering may be in place.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The LDB can interface with any neighboring ESInets, but it is unlikely to need to interface directly with other LDB solutions. If a call originates in NE and is transferred over a state line to another NENA i3 compliant ESInet, the location dereference URL will go with the transfer in the SIP header. The CHE across the state line can use this dereference URL to obtain the callers location directly from the NE LDB, without the need to utilize any LDB within their own state. As an example, a wireless call placed from South Dakota may hit a cell tower in Nebraska. This call will likely hit an LNG in Nebraska which will in turn query the Nebraska LDB. Once at the Nebraska ESRP one of two things can happen. The ESRP will dereference the location from the Nebraska LDB. If the LDB is only able to return a cell tower location at this point, the call will be routed to a Nebraska PSAP. From there, the PSAP can transfer the call to the South Dakota PSAP. This transfer will include the location dereference URL that the South Dakota PSAP can use to get updated location information from the Nebraska LDB. Alternatively, if the Nebraska LDB can return the actual caller's location to the Nebraska ESRP and the ESRP can route the call directly to the South Dakota ESInet (to either the South Dakota ESRP or directly to the appropriate South Dakota PSAP). If sent to the South Dakota ESRP, it can use the dereference URL to request updated location from the Nebraska LDB and use that to determine which South Dakota PSAP the call should go to (using the South Dakota ECRF). If a neighboring state is still legacy or not fully NENA i3 complaint, other mechanisms can be put in place, such as legacy style FoCR. In this situation, pANI records in the Nebraska LDB are shared with the neighboring state for them to provision in their ALI database. Conversely, the neighboring state will share their pANI records for provisioning in the Nebraska LDB.				

Any additional documentation can be inserted here:

NGCS 64	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** **LDB Description** An LDB serves as both a legacy ALI database and as a LIS in an i3-compliant NG911 environment. The LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can utilize the new protocols required in an NG911 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or Gateway Mobile Location Center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols. Describe the functionality of the proposed LDB, including additional features and capabilities, error handling, FoCR capabilities, logging and deployment recommendations in detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface, and features, and security aspects.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: For an LDB to function correctly and allow interoperability between legacy and Next Generation 9-1-1 formats, a MSAG Conversion Service (MCS) is needed (as defined in NENA-STA-010.2-216). An MCS is included as part of this response. **MCS Overview** The MCS is designed to bridge the gap between legacy (ALI/MSAG) and Next Generation (PIDF-LO/CLDXF) data schemas and formats. An MCS is a required functional element if interoperability is required between legacy and Next Generation data. In the situation where the legacy ALI database is wholly replaced by a transitional Location Database (LDB), the MCS is used by the Service Order Input (SOI) process to convert the legacy address records submitted by the service providers to the NG9-1-1 CLDXF format. The LDB stores all records in CLDXF format and is therefore closely aligned with the data in the ECRF/LVF. Additionally, the MCS is used to convert dynamically received address data that is received over an E2 connection (typically for VoIP). E2 will return address data in a legacy format, which needs to be converted to a CLDXF compliant PIDF-LO before being sent to the ECRF for call routing instructions. If legacy CHE exists in the deployment, the MCS will also be used to provide legacy ALI services to this CHE. Without the MCS, location data associated with each call will not be aligned with the GIS data that is in the ECRF/LVF, as this data is required to be in the NG9-1-1 GIS Data Model (which is closely aligned with CLDXF, and very different from legacy ALI/MSAG data models). Failure to align call location data with ECRF/LVF data will result in significant call routing issues.				

	Additionally, the MCS can provide translation services to gateway elements when calls need to be transferred with location between legacy and NG PSAP's. **LDB Overview** To overcome the problems of legacy ALI systems, NENA recommends the use of the Location Interwork Function, or LIF, within the Legacy Network Gateway, utilizing an internal location database with steering data as needed. This database is often referred to as an LDB, or Location Database (NENA-INF-008.2-2014). The LIF is a part of the LNG, although it can be physically separated. A Location Database (LDB) serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment and is included in this response to fully replace the existing ALI database and enable smooth transition to NG9-1-1. The LDB can provide the same functionality as a legacy ALI database, but also provides i3 processes and interfaces. A single state-wide LDB would provide numerous advantages over the current ALI database system(s), including: • All location records that contain a civic address are pre-validated against the LVF, ensuring that at the time of a 9-1-1 call they will properly route. LDB response times are measured in milliseconds, not seconds (note that for wireless and nomadic VoIP, the LDB must still communicate with MPC/VPC which will introduce delay). • Service providers would not have to change their workflows, as the LDB supports the legacy SOI provisioning interfaces. Service providers can continue to send their records in this legacy format, and the MCS will be used to convert the record into the NG9-1-1 data model before provisioning the data into the LDB. This means that legacy service providers can continue "business as usual", without having to change their existing processes. • All data would be stored in native NG9-1-1 formats. A legacy MSAG, at the state level, can still be created for service providers that wish to use it. The MSAG is generated from data in the ECRF/LVF and converted into a legacy format using the MCS.				

Any additional documentation can be inserted here:

The LDB shall meet the following requirements:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI Database Management System (DBMS).	X			

Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI Database Management System (DBMS). NENA 02-010 Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-010. The LDB supports Service Order Input (SOI) processing of files in the 2.1 and 4.0 exchange formats. Support for version 3.0 is not implemented as it is not commonly used within the industry. The GIS data model is not directly relevant to the LDB. NENA 02-011 NENA Data Standards for Local Exchange Carriers, ALI Service providers & 9-1-1 Jurisdictions The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-011. NENA 02-015 *Standard for Reporting and Resolving ANI/ALI Discrepancies and No Records Found for Wireline, Wireless and VoIP Technologies* The LDB meets, and in many cases exceeds, all relevant requirements of NENA 02-015. All "No Record Found" reports are automatically generated for service providers, and the LDB Manager web interface provides a full NRF workflow. Location discrepancies (such as those reported by a PSAP) are tracked in the standard ticketing system. NENA 04-005 NENA ALI Query Service Standard The LDB stores location data in a format compliant to the NG9-1-1 data models. This means an intermediate process is required to convert this data for legacy ALI. If an AQS is required, an MSAG Conversion Service (MCS) is used to convert the CLDXF compliant PIDF-LO from the LDB back into the NENA ALI 4.0 format. At this time the AQS is not fully supported but can be if required. It is recommended that CPE use the NG9-1-1 HELD protocol wherever possible. Legacy ALI interfaces do not support the same rich data format as HELD. If all CPE can support the HELD protocol, there is no need for an AQS to be deployed. Standard legacy ALI is fully supported. NENA 08-501 NENA Technical Information Document on the Network Interface to IP Capable PSAP The entire LDB is built to communicate over IP networks, and fully supports both IPv4 and IPv6. Legacy ALI queries can be supported over a TCP/IP connection, and the HELD interface also runs over a TCP/IP connection. The LDB also supports additional data when using the HELD protocol. The latest standards are used for this, which supersede the information in this document. *NENA 08-502 NENA Generic E9-1-1 Requirements Technical Information Document*				

The LDB supports section 2.6.2, with the exception that the location information is LVF validated rather than MSAG validated. The LDB provides callback information as described in section 2.6.3, providing the callback information is available from the MPC/VPC. The LDB supports section 2.7.2 in that it will store static location data, as well as steer E2+ queries as appropriate for nomadic location data, such as wireless and nomadic VoIP. The LDB can process SOI files from Service providers in either the NENA 2.1 or NENA 4.0 formats, as described in section 2.7.2.1. A full range of error and validation checks are performed on each file and each record and errors are returned to the Service provider for resolution. LVF generated discrepancies are returned to the GIS group responsible for the data in the ECRF/LVF. Local number portability (LNP) is fully supported using the Unlock and Migrate process, and NPAC databases are queried to verify TN ownership to ensure the accuracy of the database. The LDB supports section 2.7.2.2, offering both legacy and i3 interfaces for location queries. NG9-1-1 compliant CPE can use the HELD interface, whereas legacy systems can perform a legacy ALI dip. The ability to steer queries to other databases is supported, as described in section 2.7.2.3, but requires full cooperation of other database providers. The LDB includes a full ESME subsystem, allowing it to communicate over E2/E2+ to positioning centers for wireless and nomadic VoIP. The LDB can be deployed in a multiple node system, allowing it to achieve 99.999% availability as described in section 2.7.2.5. The LDB meets the requirements of section 2.7.2.6, as most queries for static records take 100 ms or less. Queries to outside systems (such as an MPC/VPC) may take longer and are beyond the control of the LDB. The LDB supports data provisioning as described in sections 2.8.2.1 and 2.8.2.2, using either standard SOI type file processing or a web interface				
Shall be capable of assuming the role of a location DBMS as defined in NENA-INF-008.2-2013, NENA NG9 1-1 Transition Plan Considerations. The LDB was developed to provide all the relevant transitional database functionality as defined in section 11.5 of the NG9-1-1 Transition Plan Considerations document. Unlike other solutions on the market, our LDB was built from the ground up as an LDB, not an ALI database system repurposed as an LDB.	X			
Shall support NENA standards J-036, E2, E2+, non-call-associated signaling (NCAS) and call-associated signaling (CAS).	X			

The LDB, in conjunction with the ESME, can provide all the necessary processing to handle legacy wireless and nomadic VoIP calls. In a typical scenario, each pANI record within the LDB is assigned to an E2 connection (E2 steering). The ESME sub system maintains all E2 connections to the appropriate MPC or VPC. When a pANI query is presented to the LDB, it determines which E2 connection it needs to use, and passes a query onto the ESME. The ESME, which has dual IP connections to each MCP or VPC, performs the actual E2 (or E2+) query to the appropriate positioning center, and passes the response back to the LDB. In the case where the E2+ response contains an address (often occurs with nomadic VoIP), a further call in placed to the MCS to convert this address from a legacy format to the PIDF-LO equivalent				
Shall be able to provide LIS functionality and interfaces as defined in NENA-STA-010.2-2016 The LDB supports all LIS functionality and interfaces as defined in NENA-STA-010.2-2016. Specifically, the LDB supports the HELD protocol, as specified in NENA-STA-010.2-2016, and detailed in RFC 5985, and HELD location dereference RFC 6753.	X			
Shall be able to seamlessly interact with a NENA i3-compliant ECRF, as described in NENA-STA-010.2-2016. The LDB, as part of data provisioning, uses the LoST protocol to validate all civic address data against the ECRF/LVF. All civic address locations that return invalid elements will generate a discrepancy and will enter into the LDB discrepancy workflow system. In terms of call flow, the LDB and ECRF act independently. The ESRP will issue a dereference HELD query to the LDB and await a response. Once the response is received, the location will be sent by the ESRP as a LoST query to the ECRF.	X			
Shall be able to dereference a location by reference, as defined in NENA-STA-010.2-2016. The LDB supports both GET and POST location dereference queries using the HELD protocol. The initial query will need to take place by value, with the initial response including the location dereference URL. Future location requests can use the location dereference URL to retrieve updated location information.	X			
Shall be able to dereference requests for additional information, as defined in NENA-STA-010.2-2016.	X			

Both location by value and location by reference queries include additional data in the response. The LDB currently supports the ECRIT additional data standard (RFC 7852), which includes most of the additional data structure defined in NENA-STA-010.2-2016 (such as ProviderInfo and ServiceInfo).				
Shall be able to interface simultaneously with multiple wireless callers. The LDB supports legacy wireless location delivery using an Emergency Services Message Engine (ESME) connected to one or more Mobile Positioning Centers. Each multi-threaded ESME instance can handle multiple simultaneous queries, with the ability to handle hundreds of wireless calls per second.	X			
Shall be able to interface simultaneously with multiple remote ALI databases. Providing that the remote ALI database provider can provide steering data (in some agreed upon mechanism, such as FoCR), the LDB is able to steer queries to remote ALI databases. The MSAG Conversion Service (MCS) is used to convert legacy ALI response from the remote ALI database into PIDF-LO. Additionally, the LDB can be provisioned with pANI from neighboring ALI databases, allowing it to perform E2 queries to retrieve location information for calls that have been transferred into Nebraska. Data sharing agreements must be in place with neighboring ALI database providers for the sharing of these records. A legacy ALI interface can also be provided, allowing the legacy ALI database to perform queries for data contained within the LDB. The MCS will be used to convert the LDB PIDF-LO data into the legacy ALI 4.0 format, which can then be formatted into other legacy ALI formats	X			
Shall automatically detect, import and validate customer records (SOI records). To successfully replace a legacy ALI system with an LDB, a mechanism must be provided to the Service Providers to update the location information in the LDB. During the transition to i3, and to aid 9-1-1 authorities gaining cooperation from the Service Providers, the LDB system includes a Service Order Input (SOI) processing function that is like existing SOI processing. This means that the Service Providers do not have to change current processes in order to support the i3 system (an MSAG Conversion Service is provided to convert SOI records into the appropriate CLDXF format for comparison against the LVF). Service providers can submit their SOI files for processing via some agreed upon, secure method. Asynchronous back end server processes run to process the SOI files. Multiple SOI processing agents can be configured on a single database, allowing multiple SOI files to be processed at the same time. Unlike SOI processing for E9-1-1 ALI databases, each SOI record must be validated against the GIS, by way of an LVF, prior to the record being committed to the database and being made available for HELD queries. This ensures the civic address location provided by the Service Provider can be mapped, and thus routed and	X			

plotted. If a record fails validation, the Service Provider is notified (various notification mechanisms exist, including an error report). The group responsible for the GIS map data can also be notified, so the map data can be checked for accuracy. Each SOI record can be looked at individually also. Records that are rejected can be directly edited within the LDB Manager web interface, or a new and correct SOI record could be submitted. Scheduled, periodic revalidation of existing LDB records will also be performed by the system. This process checks all LDB records that have previously been flagged as LVF valid and submits a new LVF query to verify each record is still valid. Records that fail validation will be flagged in the LDB as invalid but will still be returned in HELD queries for a configurable time period (by default, this is 30 days), allowing the Service Provider or GIS department time to investigate and resolve the issue. The LDB utilizes a web-based interface allowing authorized personnel access to the backend location database. From this web interface, users with the appropriate permissions can schedule reports and data extracts to be run. Key functionality of the web interface includes: • Role based security, restricting users to what they can do and what data they can see. For example, a Service Provider will only be allowed to view their location records and job reports from SOI jobs they have submitted. • Ability to query data by telephone number and address. • Ability to modify location records and validate the changes against the LVF in real time. • View reports. Workflow for resolving data discrepancies for records that have failed LVF validation (for example, if, after review, the Service Provider has determined that the location data is correct, the discrepancy can be routed to the appropriate GIS department for resolution). Users can be defined and managed via the LDB web interface. Users will have permission-based access to their subscriber data and be able to schedule daily data extract				
Shall have the ability to be used simultaneously by both NG911-capable and E911 capable PSAPs. The LDB provides both legacy and NG9-1-1 location interfaces. To support NG9-1-1 capable PSAP's a HELD interface is provided. To support legacy PSAPs, a legacy ALI interface is provided, and location data within the LDB is converted into legacy formats using the MSAG Conversion Service. The HELD interface can support hundreds of queries per second. The legacy ALI interface requires the legacy CPE to maintain one or more TCP/IP connections. Each CPE instance must initiate and maintain the connection to the LDB legacy ALI interface. Each individual TCP/IP connection can handle one legacy ALI query per position at a time. This is a limitation of the legacy interface, not of the LDB.	X			

Shall allow different PSAPs to use different ALI formats based on individual needs. It is expected that NG9-1-1 capable PSAPs will not use ALI at all and should be capable of consuming data provided in the HELD response. Data provided in this way cannot be reformatted into different formats as it is controlled by a well-defined XML schema. For legacy PSAPs that use the legacy ALI interface, the response can be formatted on a PSAP by PSAP basis.	X			
Shall utilize LVFs to validate civic addresses. As civic address data is provisioned into the LDB (either through SOI or by manual input using the web interface), it is validated against the LVF. If the civic address is submitted via SOI, it is converted from legacy MSAG format to the LVF compatible CLDXF format before being validated by the LVF. If a civic address fails validation, it is placed into the discrepancy workflow process for resolution. Discrepancies are marked with a severity that is determined from the response from the LVF. A civic address that fails to return a mapping will be flagged as critical, allowing these types of discrepancies to be worked first.	X			
Shall support PIDF-LO location data formatting as defined in NENA-STA-010.2-2016. The CLDXF standard describes the PIDF-LO format for the United States. This standard is strictly observed in both the LDB and ECRF/LVF systems. To support legacy processes (to convert between PIDF-LO in the CLDXF format and legacy ALI) an MSAG Conversion Service (MCS) is used. The MCS is included as part of this response. All GIS data within the ECRF/LVF will be in the CLDXF format. As a result of this, the civic address data stored within the LDB must also be in this format, otherwise it would fail LVF validation. If SOI is used to provision civic address data into the LDB, it undergoes transformation from the legacy format to CLDXF during file processing, with a result of CLDXF compliant civic address in the LDB. Additionally, if civic address data is provided from a MPC/VPC during call flow (such as a nomadic VoIP call), it is converted during the call flow by the LDB from the legacy format into CLDXF compliant PIDF-LO (using the MCS).	X			
Shall periodically reevaluate the location information using LVF functions within the system. A back-end server process runs continually against the LDB database. This back-end process is configured to periodically perform revalidation tasks. It is typically configured to revalidate open discrepancies with a	X			

frequency similar to the frequency that the GIS data is updated in the ECRF/LVF. Additionally, full database revalidation is typically configured to run weekly or monthly. The LDB has three different mechanisms for revalidation: • A full revalidation runs as a scheduled job to periodically revalidate every civic address record in the LDB against the GIS using an LVF query. • A discrepancy revalidation runs more frequently and revalidates civic address records that were previously flagged as being LVF invalid. • A targeted revalidation runs when GIS data in the ECRF/LVF system has been updated and revalidates civic address records in the LDB that may have been affected by the specific changes to the GIS data.				
Shall be able to communicate with NG911 functional elements using the SIP and HELD protocols. The LDB provides full support of the HELD protocol, secured with TLS. The LDB can accept HELD queries from all authorized NG9-1-1 core elements, as well as dereference requests from NG9-1-1 capable CPE performing a "re-bid". The LDB does not have a SIP interface at this time as none of the other functional elements offered in this solution can request location using SIP SUBSCRIBE/NOTIFY. In general, the industry seems to have standardized on the HELD protocol. If clients capable of SIP SUBSCRIBE/NOTIFY for location exist, support can be added to a future release of the LDB.	X			
Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response. The LDB converts E2/E2+ responses to PIDF-LO. In the case of wireless E2, the Position Result, which contains latitude/longitude coordinates, as well as an uncertainty, is converted to a GML circle in the PIDF-LO response, and the E2 confidence is also included in the PIDF-LO. In the case of a E2+ response that includes a civic address (in a legacy format), the legacy address is converted into a CLDXF compliant PIDF-LO using the MSAG Conversion Service. As the HELD protocol can support multiple locations per response, the LDB is able to provide all location data received in the E2/E2+ response. Additionally, the shell record location can also be included if appropriate.	X			
Shall be able to dereference additional data requests. The LDB can also act as an Additional Data Repository (ADR) as defined in NENA-STA-010.2. When responding to a location request, either by value or by reference, the LDB will include available additional data blocks inside the <provided-by> element of the PIDF-LO. The additional data blocks conform to the IETF ECRIT Additional Data Related to an Emergency Call standard, and may include:	X			

• Data Provider Information • Service Information • Device Information • Owner/Subscriber Information • Comments Clients can retrieve the additional data by performing a dereference query to the LDB using the URI received in the initial location response.				
Shall consistently respond to all requests within 400 milliseconds (ms). Average query latency is less than 50 ms for data stored locally within the LDB. If data must be retrieved from other systems, response times will vary and are dependent on the remote system (such as a remote ALI database, RapidSOS or an MPC/VPC). The HELD protocol supports a parameter in the query to tell the LDB how long the query client is willing to wait for a response. This is a useful feature, particularly for legacy wireless calls. In this scenario, the LNG may initiate a query to the LDB, with a maximum wait time of 3 seconds. The LDB will, via the ESME, query the remote Mobile Positioning Center. After 3 seconds, the LDB will respond with the best data it has available. At this point, it is possible that the MPC was only able to return Phase I location data. However, by the time the call reaches the ESRP, and the ESRP performs a dereference request, the ESME may have received Phase II wireless data, and so the LDB will now respond to the ESRP with this updated information.	X			

NGCS 65	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** **Integration of Multi-Line Telephone System Data** The LDB shall support the Integration of Multi-Line Telephone System (MLTS) databases. As part of this migration, Contractor shall be responsible for migrating records from the current MLTS databases to the LDB. Provide details on the database migration process and the user interface for management of these MLTS data records.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The LDB has full support for PS/ALI. Each PS/ALI customer must have its own registered NENA ID, as this is used to uniquely identify and securely partition their data within the LDB. The PS/ALI customers will be given access to the LDB Manager web interface, allowing them full read and write access to their records. Additionally, the LDB can be configured with blocking ranges, restricting the access to a specific range of TN's for which the PS/ALI customer can create new device records. Each PS/ALI customer can manage their records in the LDB by either a SOI process (if their MLTS system supports the generation of these files) or by direct editing using the LDB Manager web interface. Not all PSAPs will transition to being i3 capable at the same time. As a result, the LDB will provide legacy ALI style services to these PSAPs until such time as the PSAP is able to consume PIDF-LO style data. During the transitional phase, the LDB will provide all location, either directly or indirectly (via an E2 connection). For wireline calls, the LDB will contain an LVF valid and CLDXF compliant address location. For wireless, the LDB will contain a shell record, and will attempt to get more granular location over E2 from the Mobile Positioning Center (MPC). The location from the MPC will be a point and a confidence radius. This location is converted by the LDB into a circle that can be used by the ECRF for determining call routing. For VoIP, the LDB may contain either a civic address location or a shell record. If it is a shell record, the LDB will attempt to query the VoIP Positioning Center (VPC) for a more granular location. For VoIP, the E2 provided location could be geodetic or civic, or both. If the VPC provides a civic address location, it will be in the legacy MSAG format, so the LDB will utilize the MSAG Conversion Service (MCS) to convert the location into a CLDXF compliant PIDF-LO. During the transition period, service providers do not have to change the way they operate regarding populating a location database. Prior to transition, they would submit SOI files to the ALI database provider. During transition, they will continue to provide the same SOI files, only now the data will be loaded into the LDB. The LDB is stricter in terms of the quality of the data, due to the LVF validation checks, so initially service providers may see more SOI failures than normal.				

Any additional documentation can be inserted here:

NGCS 66	**Next Generation Core Services Elements (NGCS)** **Discrepancy Reporting** 1. Provide details regarding the proposed solution's report functions for notifying PSAPs any time a discrepancy is detected concerning the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, explain how a report will be sent for the purpose of reporting the discrepancy to multiple responding PSAPs, as determined by the Commission. Discrepancy reporting is outlined in Section 4.7 of NENA-STA-010.2-2016. 2. Describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: To track and report any discrepancy in the performance of the NGCS, we employ an exceptional monitoring, security and event management platform. Working in a complementary way, these two tools gather a comprehensive set of data about the status of the network, including device reachability, SIP endpoint behavior, predicted MOS performance, routing topology, security threats, infrastructure alarms, SLA compliance, and a host of other relevant data. Both tools have a network-wide view starting at the TDM trunks at the aggregation infrastructure and all the way through the call flow to the demarcation device at each PSAP. Then, these and other data sources such as E-Bonding ticket information are consolidated into a single viewing portal for access by the state. Physical access to IP network and these reports is extremely limited and dual authentication is in place. Any access is logged and reported in real-time to the STI Chief of Engineering. Access to network logging reports is granted through the credentialing program. CenturyLink's monitoring system will auto-notify the CenturyLink NOC and PSAP customer of a failure and CenturyLink takes proactive remediation steps to resolve any service degradation as well as employing IP SLA's to remediate issues until the network path congestion or failure is resolved. 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 via our portal and dashboard. 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. CenturyLink's dashboard is a portal-based functionality for ticket status, e-bonding data monitoring, reporting, and configuration management. The dashboard will provide a single pane of glass for monitoring and network management. CenturyLink employs a combination of products both custom in-house built and purchased monitoring platforms to allow our engineers to see the whole pictures end to end, from call traces to power supply status and voltage levels. Alerts sent to our NG9-1-1 NOC allow technicians to monitor and mediate problems before they cause issues impacting the customer or caller.				

	Our reporting package is designed to provide critical path hop-by-hop analysis and visualization all along the complete delivery track. Users can quickly see maps of network connections, dependency relationships, and topology information, and know who, what and where devices are connected to the network. This application ensures devices are configured and operating in compliance with regulatory standards and that network managers are prepared to recover quickly from hardware faults and human errors using automatic backups. Dashboard elements will include and incorporate the following: • Capture of all messages transiting the network using network probes linked to a correlation engine. Results and the dashboard are viewable through a portal that will be available to the State. • Reporting efforts are 100% passive, nonintrusive and vendor agnostic. The Oracle EOM 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. • Our other monitoring tools will also allow end-users to gain visibility into signaling and media interactions, and leverage key indicators to identify, troubleshoot, and resolve issues that can reduce the efficiency of enhanced IP network service. Our monitoring tools captures all messages transiting the network using network probes linked to an unrivaled correlation engine. Results are viewable through a web-architected GUI. This Monitor runs on commercial-off-the-shelf hardware and software components that are integrated into our session border controller (SBC) service delivery platforms.

Any additional documentation can be inserted here:

NGCS 67	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** PSAPs may have a variety of logging recorders capable of recording SIP traffic and associated media. PSAPs will use the Emergency Call Tracking System (ECaTS) for call logging and capture event details. The Commission will gather statistical data from PSAPs through ECaTS. Describe how the solution interfaces with logging recorders and ECaTS.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's NG9-1-1 Solution ESInet was designed to fully integrate with other networks and databases featuring NENA-compliant interfaces. The endpoint delivery is determined by the call handling equipment (CHE) capabilities however, the preferred method is direct SIP handoff via SBC or boarder control function (BCF) at the site to a call handling security appliance or SBC. An LPG (Legacy PSAP Gateway) can be deployed for PSAP CHE that is not direct SIP capable. The LPG ensure that any traffic entering our network from outside sources meets interconnection standards. This interconnectivity extends to CADS, logging records, clocks and other NENA-compliant components. Also, CenturyLink's ECRF, LVF, LDB, ESRP, PRF functional elements provide logging events to the i3 Logging Services and will interface with any NENA-standard logger recorder and ECaTS. Multiple levels of logging are implemented by the ECRF/LVF to capture all relevant information. All connections and connection attempts are recorded by the logging mechanisms built into IIS. All LoST queries and responses are logged both to the i3 event logging service and to an independent ECRF logging database. Debug logging can also be enabled on the ECRF with minimal impact and provides more specific detail regarding query processing.				

Any additional documentation can be inserted here:

NGCS 68	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Event Logging Description** Extensive logging of NG911related events, transactions, media, and operations is required. All log entries shall be accurately time-stamped. Logging must include all elements in the call flow including logging of NG911related events within ESInets, the NGCS, the PSAP, and related operations, and is a standardized function used throughout ESInets, NG911 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress, and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. Describe how the solution meets or exceeds the above requirements.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: The CenturyLink NG9-1-1 Operations Center is tailored specifically to meet the requirements of the Nebraska RFP. CenturyLink will leverage several highly sophisticated monitoring tools to ensure the CenturyLink's system components and networks maintain the highest quality and availability. These tools include CenturyLink Remedy, SolarWinds, Oracle Enterprise Operations Monitoring, 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. CenturyLink provides API feeds from monitoring tools such as SolarWinds, Brix Probes and integrate SDWAN network monitoring and reporting tools. Regional ticketing information via e-bonding will be presented 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. 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 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 to provide monitored data • CenturyLink will monitor and display the network and performance data for SLA compliance. • Via APIs the Dashboard will have visibility into various platforms included in the CenturyLink solutions such as SDWAN, NGCS and CenturyLink's ticketing platform. • Analytics, statistical data and reports will be developed based on requirements and agreed upon thresholds, displayed via dashboard. The system monitoring program and MIS effort will recognize the State as an authorized customer.

Any additional documentation can be inserted here:

NGCS 69	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Integration with Call-Handling Equipment** 1. Describe how bidder's event-logging solution may integrate with the each PSAP's call-handling equipment, to provide a complete, end-to-end view of a call. 2. Describe how the Commission can gain access to information in the event-logging solution. 3. Describe the requirements of the PSAP's call-handling equipment, software license agreements, and interfaces required to support integration with the bidder's event-logging solution.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1. CenturyLink can integrate with PSAP log events by having the PSAP log events to the ESInet/NGCS Log function as well as the PSAP logger. 2. The State could consolidate the ESInet/NGCS logging information with a scheduled extract 3. The PSAP equipment must comply with NENA-STA-010.2-2016 Logging Services XML schema (XSD).				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 70	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Access to Event Logging Data** 1. Describe how the PSAPs and the Commission will gain access via role-based authentication to the event-logging solution data and run statistical and other MIS reports. The PSAP is the custodian of such data for purposes of the Nebraska Public Records Statutes, Neb. Rev. Stat. §§ 84-712 to 84 712.09. The PSAP is responsible for maintaining such data pursuant to the PSAP record-retention schedule applicable to such data as provided in the Nebraska Public Record Statutes, Neb. Rev. Stat. §§ 84 1201 to 84 1229. The state is implementing the ECaTS MIS solution statewide. Upon deployment, the Contractor shall coordinate with ECaTS, the state, and the PSAPs to deliver event logging data to the ECaTS solution. An existing data-sharing agreement (DSA) between the state and the PSAPs governs what data the state may access along with notifications of records requests. This DSA will govern data collected by the NGCS and ESInet provider whether that data is delivered to ECaTS or directly to the state or PSAPs. 2. Describe the reports, MIS tools, and performance metrics made available to each PSAP, the user interface for retrieving or receiving reports, role-based authentication to limit access to data and reports, and the ability to customize reports based on individual PSAP needs. These reports may be used as a basis for changes to bandwidth and capacity. The required reports and metrics will include, but is not limited to: a. Timing b. Call-delivery time c. Call-processing time between elements d. Volumes e. Call volumes by call type f. Alternate-routed calls g. Text-to-911 h. All NGCS element usage volumes i. Bandwidth/trunk utilization j. Calls per trunk k. Trunk utilization l. Circuit utilization	X			
	Bidder Response: 1.Our ECRF, LVF, LDB, ESRP, PRF functional elements provide logging events to interface with ECaTS MIS solution. It will interface with any NENA i3 standard compliant MIS solution such as ECaTS. Our logging events will be collected and pass on to the ECaTS MIS software application for data aggregation, data analytics and reporting.				

	2.Multiple levels of logging are implemented by the NGCS to capture all relevant information such as call delivery time, call types, etc. All calls are recorded by the logging mechanisms. All call events are logged to the i3 event logging service for logging/recording. CenturyLink will work with ECaTS and the State to integrate our i3 logging events interface into the ECaTS MIS software application for data aggregation, data analytics and reporting. All logging events are XML schemas, using SOAP as the transport mechanism, that are conformant with the NENA XML schemas definition provided in the NENA-STA-010.2-2016 and are readily available for interfacing with ECaTS. All reports including performance metrics listed above will be readily available through the CenturyLink's NG9-1-1 Public Safety dashboard portal. Our Project Management team will oversee and ensure performance requirements are met across our NG9-1-1 ESInet solution and collaborate with each PSAP and the Commission of any ad hoc reports as needed.	

Any additional documentation can be inserted here:

NGCS 71	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **NENA Standards Compliance** The bidder's proposed logging solution shall meet the requirements set forth in NENA-STA-010.2-2016. **Third-Party Certification Fees** Bidder is responsible for any third-party certification fees. Describe how the solution meets or exceeds these above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink Logging solution adheres to all the standards set forth in NENA-STA-010.2 and responsible for Third-Party fees.				

Any additional documentation can be inserted here:

NGCS 72	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** Bidder's solution shall sync with existing time sources to maintain consistent time stamps across the network and systems. Describe how bidder's solution complies with this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's solution will sync with any time source that provides an i3 interface and will maintain time stamps. Time stamps are included in logs, system traces, and user reports				

Any additional documentation can be inserted here:

NGCS 73	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Master Clock Description** The bidder shall provide redundant, resilient network-attached Stratum 2-time sources ("master clocks") capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's NGCS Solution processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the CenturyLink's NGCS Solution domain. Time stamps are included in logs, system traces, and user reports. The two servers are dedicated to NTP services. Customers can neighbor directly with those servers for time services. CenturyLink utilizes Symmetricom's GPS NTP solutions with Stratum 1 synchronization.				

Any additional documentation can be inserted here:

NGCS 74	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Accessibility by PSAP Equipment** The master clock time source(s) shall be accessible to the PSAPs for synchronizing call-handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the NTP for maintaining system clock accuracy. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink's NGCS will interface with a standard timing device. Sync would be through that device and its interface within the PSAP. All functional elements support the use of the NTP for maintaining accuracy. CenturyLink utilizes Symmetricom's GPS NTP solutions with Stratum 1 synchronization.				

Any additional documentation can be inserted here:

NGCS 75	**Next Generation Core Services Elements (NGCS)** **NG911 Application Integration** Bidder shall describe other NG911 applications, additional data integrations, and personal safety applications that may be integrated with the NGCS solution. The bidder's system must be capable of integration with Additional Data Repositories (ADR), Identity-Searchable Additional Data Repositories (IS-ADR) or commercial third-party LIS, as described in NENA STA-010.2-2016, within two years of the deployment of the first PSAP. Describe how the solution will accomplish integration, information storage, and use/transmission of data to PSAP CHE.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink is actively involved negotiating with several ADR providers, telematics service providers, NG9-1-1 reporting and Over-The-Top (OTT) video delivery tools to add value to our ESInet/NGCS offerings and will offer additional information and functionality for PSAPs and first responders. The LDB included in this proposal can act as an ADR out of the box, providing additional data in the HELD response in compliance with IETF RFC 7852 Additional Data Related to an Emergency Call. Additionally, the LDB can query the external RapidSOS ADR for additional location information for a wireless call. Further development might be needed to support other external ADR's as they become available, particularly if they do not support the HELD protocol. If the CHE is i3 ready, it should be able to receive PIDF-LO as part of the call payload (or issue a dereference request to the LDB for that information). The LDB will provide all the location information it can to the CHE. The following screenshot shows a call handling tactical map display that has received a PIDF-LO from the LDB with three locations for a single call. The RapidSOS location is shown, with buttons available to switch to the wireless phase I and wireless phase II locations if desired.				

Any additional documentation can be inserted here:

NGCS 76	**Next Generation Core Services Elements (NGCS)** **Message Session Relay Protocol Text (MSRP) Integration** The PSAPs have deployed short messaging service (SMS)-to-911 service. 1. Describe the ability to integrate existing web-based and MSRP-integrated SMS-to-911 and Real-Time Text (RTT) services into the solution. 2. Explain whether the solution supports location-by-reference and/or location-by-value. This requirement is for the integration of text messaging with MSRP and not a requirement for procuring text services.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1. The CenturyLink solution supports RTT and Baudot to RTT according to RFC 4103. 2. CenturyLink currently supports either location-by-reference or location-by-value. The ESRP checks for either value being present before initiating its own HELD request for a routable location.				

Any additional documentation can be inserted here:

Attachment "C"
Option C Revision One
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 77	**Next Generation Core Services Elements (NGCS)** **1. Make-Busy Functionality** Some PSAPs have a physical make-busy switch that can be activated in the event of an emergency evacuation. Bidder's solution shall support this functionality to all PSAPS.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	2. Ringdown Functionality Bidders' solution shall support ringdown functionality, either through the call-handling system or through the NGCS.	X			
	3. Near-Simultaneous Transfer The solution shall support near-simultaneous conference and transfer capability, with up to at least 12 parties in the conference. This feature shall allow transfer or conference buttons to be programmed to automatically establish a conference with multiple parties. For instance, one button at a police department might establish a conference between the police, fire, and EMS PSAPs and the original caller, without having to add each additional party individually. Describe how bidder's solution meets or exceeds these requirements.			X	
	Bidder Response: 1. If the PSAP does not respond to the initial INVITE, the ESRP will direct the call to the next hop in sequence. Once all the alternate routes are exhausted, it will attempt to send the call to the final default route. If those steps fail, the ESRP will respond with a 480 temporarily unavailable, please try later. 2. CenturyLink would use a third-party COTS solution if needed to route the call through the ESInet/NGCS. 3. CenturyLink's ESInet solution will have the capacity to handle that many legs of a call.				

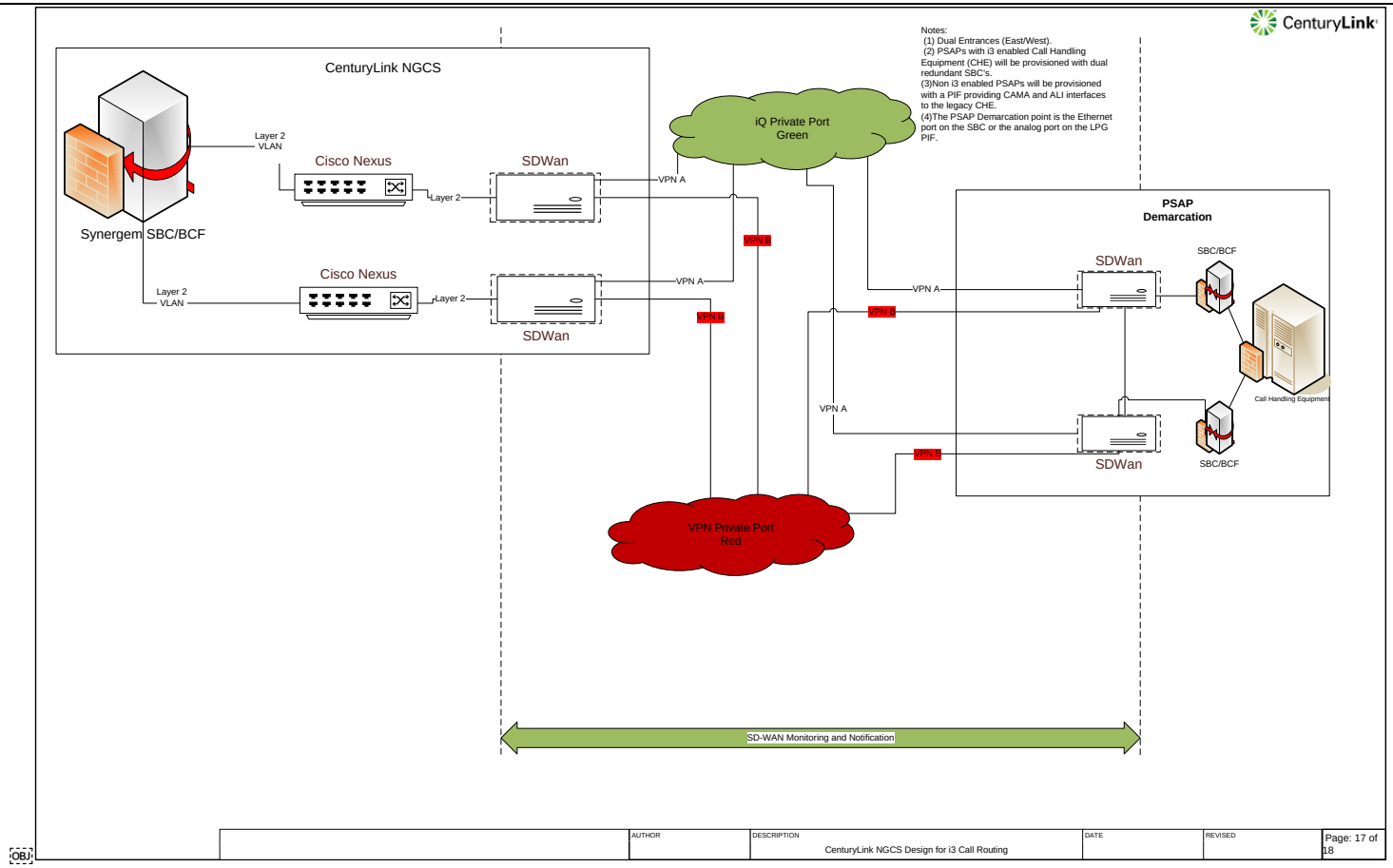
Any additional documentation can be inserted here:

NGCS 78	**Next Generation Core Services Elements (NGCS)** **PSAP Interfaces and Backroom Equipment Requirements** **Support of PSAP Interfaces** Bidder's solution shall have the ability to support PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the following: a. SIP calls b. NGCS call delivery c. Web services d. All baseline media and multimedia (as described in NENA STA-010.2-2016, Section 4) e. NTP time services interface, accurate to 1 ms f. Transport layer security g. Discrepancy reporting Describe the functionality of the PSAP interfaces in detail to address the requirements outlined above, with particular attention to the user interface, additional features, and security aspects.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: a. All SIP messages are supported in CenturyLink's ESInet/NGCS b. The egress of all calls is supported by a BCF that protects the ESInet from a security viewpoint c. All NGCS web services are currently SOAP end points. The ECRF and LIS/LDB are HTTP web endpoints. d. Our ESInet/NGCS supports all media and multimedia defined in NENA-STA-010.2-2016 e. CenturyLink's NTP solution will provide time accurate to 1 msec. f. CenturyLink supports TLS with fallback to UDP as needed g. CenturyLink supports Discrepancy Reporting in the LDB/LIS				

Any additional documentation can be inserted here:

NGCS 79	**Next Generation Core Services Elements (NGCS)** **PSAP Interfaces and Backroom Equipment Requirements** **Support of Call Handling Equipment (CHE) Platforms** 1. Provide a list of CHE platforms for which bidder has successfully implemented the interfaces listed above in a live production environment, noting any interfaces that have not yet been tested with each CHE vendor/model. 2. Where interfaces with CHE vendors/models have yet to be deployed and/or tested, please describe the integration testing process that the bidder will perform prior to acceptance testing of the solution. 3. Describe the physical interface handoff required at the PSAP CHE demarcation point.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1. CenturyLink can interface with any call-taking solution that complies with NENA standards. We have interfaced with Motorola ECW, Motorola VESTA, Intrado VIPER, and Evo911 using native SIP, IP or a Legacy PSAP Gateway. In northern California we are integrating with Tritech, Motorola, Zetron and others. The CHE vendors we have supported on our NG9-1-1 solution(s) using CAMA, RFAI and i3 interfaces as appropriate are: 2. This variety of call-taking partners demonstrates the flexibility of our network architecture when working with a NENA-compliant vendor. For those vendors with whom we have not yet interfaced, we test our software with their solution in our lab and in theirs to ensure compatibly. Our protocol requires us to establish interoperability and then to test the call and data delivery interfaces specified in STA010. CenturyLink supports both field testing at PSAP sites with CPE vendors using interfaces they have not yet deployed and Lab testing in our Colorado lab. In both cases, the Call Handling Equipment Provider (CHE) would create a non-live profile on the customer CPE, or stand up a new non-live version of their CPE, enabling the full suite of pre-migration testing to be performed within the customer environment using the exact production configuration and equipment that will eventually be deployed. Prior to this parties agree to specific test cases. These tests are done under increasingly stressful environments and conclude with tests under operational conditions. The specifics regarding Demarc. and handoffs vary from vendor test to vendor test and it is difficult to offer one all-inclusive answer. Suffice to say, our test procedures match those outlined in relevant NENA doctrine. We design our testing to discover: • Loss of data • Unreliable performance • Unreliable operation • Incorrect operation • Low maintainability In general, the test protocol involves: • Connect two or more devices or programs from different vendors • Check connectivity between devices • Check if device can send/receives packets or frames from each other • Check if data is handled correctly in the network and facility layers				

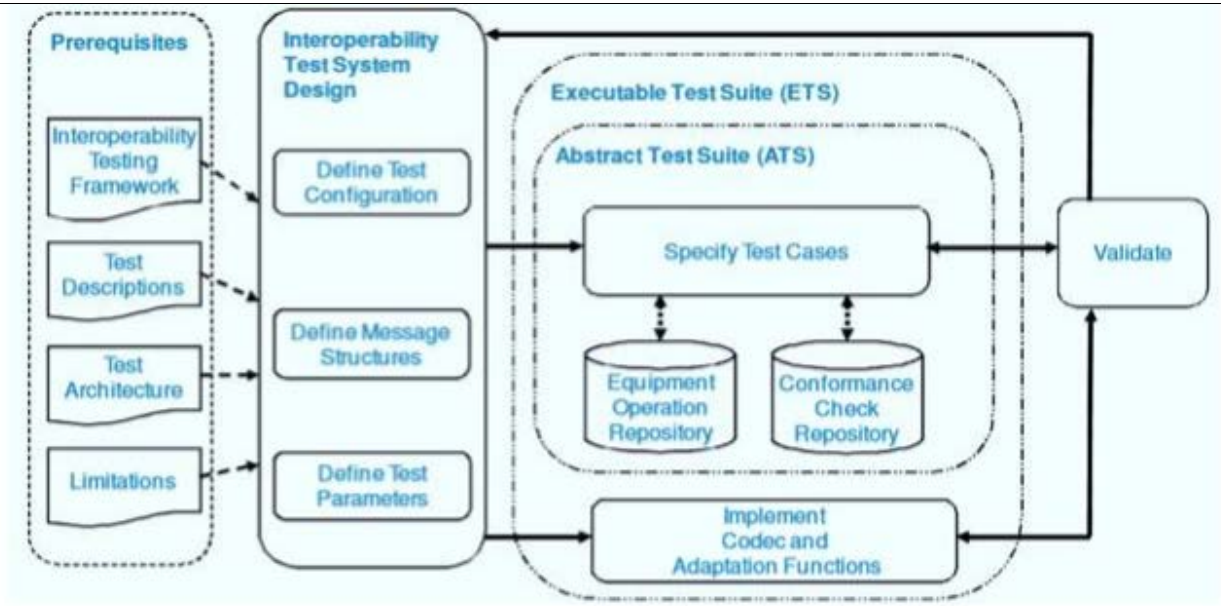
	• Check if implemented algorithms work correctly • Result ok: check next result • Result not ok: Use monitor tools to detect source of error • Report result in Test reporting tool. Connectivity for this method of testing uses our CenturyLink MPLS network and or internet VPN and follows a suite of suggested test cases within a defined testing window. CenturyLink would assist with provisioning, enabling call tests, and confirming messaging in our logs. CenturyLink's role is to provide a method for the CPE vendor to pre-validate that their equipment is ready to deploy in the field. CenturyLink 911 lab and upon successful testing, would provide a detailed Approved for Field Use (AFU) document once testing is completed to both our tier 2 and vendor partners. 3. CenturyLink interfaces with PSAPs in several ways: – I3 – Standards based IP interface either electrical or copper. – IP PSAPs – IP connectivity for voice/data via electrical or copper, TCP Legacy AII or IP to Serial based ALI supported via LPG. – Digital CAMA – TDM copper hand off with TCP or Serial ALI support – Analog CAMA – TDM copper hand off with TCP or Serial ALI support In the Legacy CAMA interface, the demarcation point between our NG9-1-1 solution and the PSAP environment is the ingress side of the CPE 66 block for CAMA trunks. – In the i3 or RFAI IP interface the NG9-1-1 demarcation point is a LAN port on the CenturyLink network edge routers. PSAPs with i3 enabled Call Handling Equipment (CHE) will be provisioned with dual redundant SBC's. Non i3 enabled PSAPs will be provisioned with a PIF providing CAMA and ALI interfaces to the legacy CHE. The PSAP Demarcation point is the Ethernet port on the SBC or the analog port on the LPG PIF.



NGCS 79 Physical interface handoff required at the PSAP CHE demarcation point.

CenturyLink can also provide a *PSAP Installation Overview* document after contract award that details the physical interface handoff and PSAP equipment requirements. This document covers PSAP data collection, site survey information, PSAP Network Edge Equipment requirements and also includes General Facility requirements and Equipment Room requirements. These documents describe in detail the physical requirements needed to support the installation of the PSAP routers and the connectivity between the NG9-1-1 ESInet and the PSAP's Call Handling Equipment.

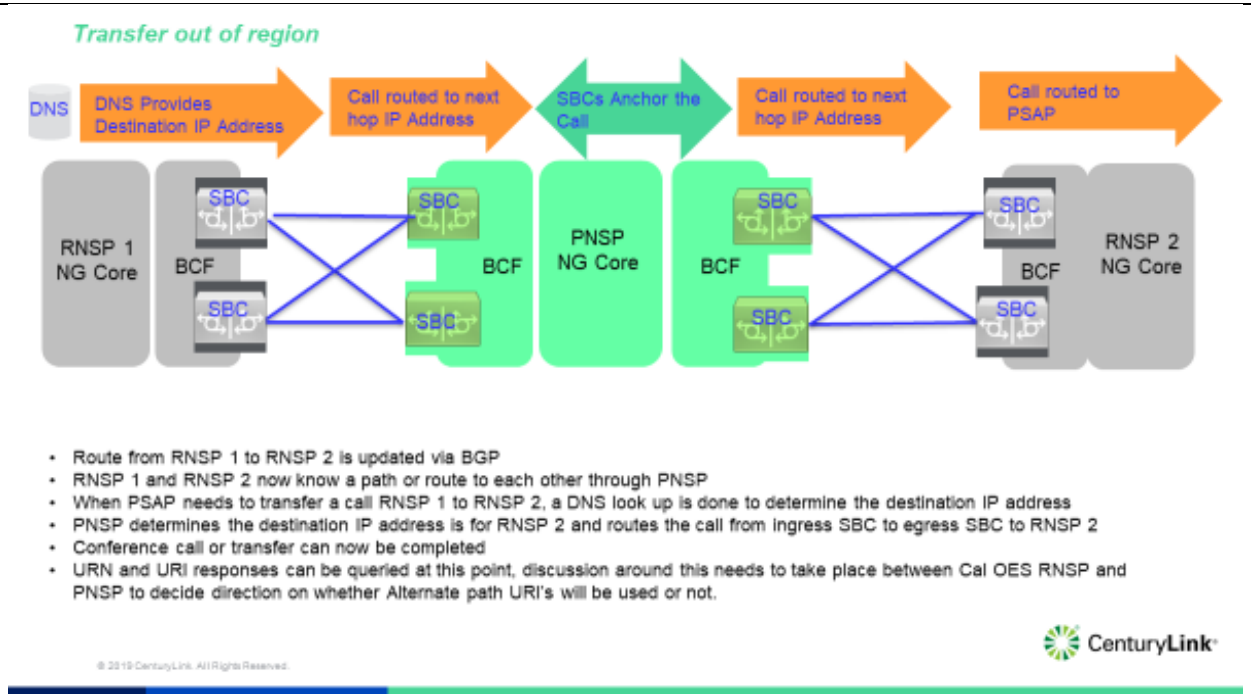
The following charts depicts the difference interoperability test protocols:



NGCS 79 – ESInet to ESInet Transfer

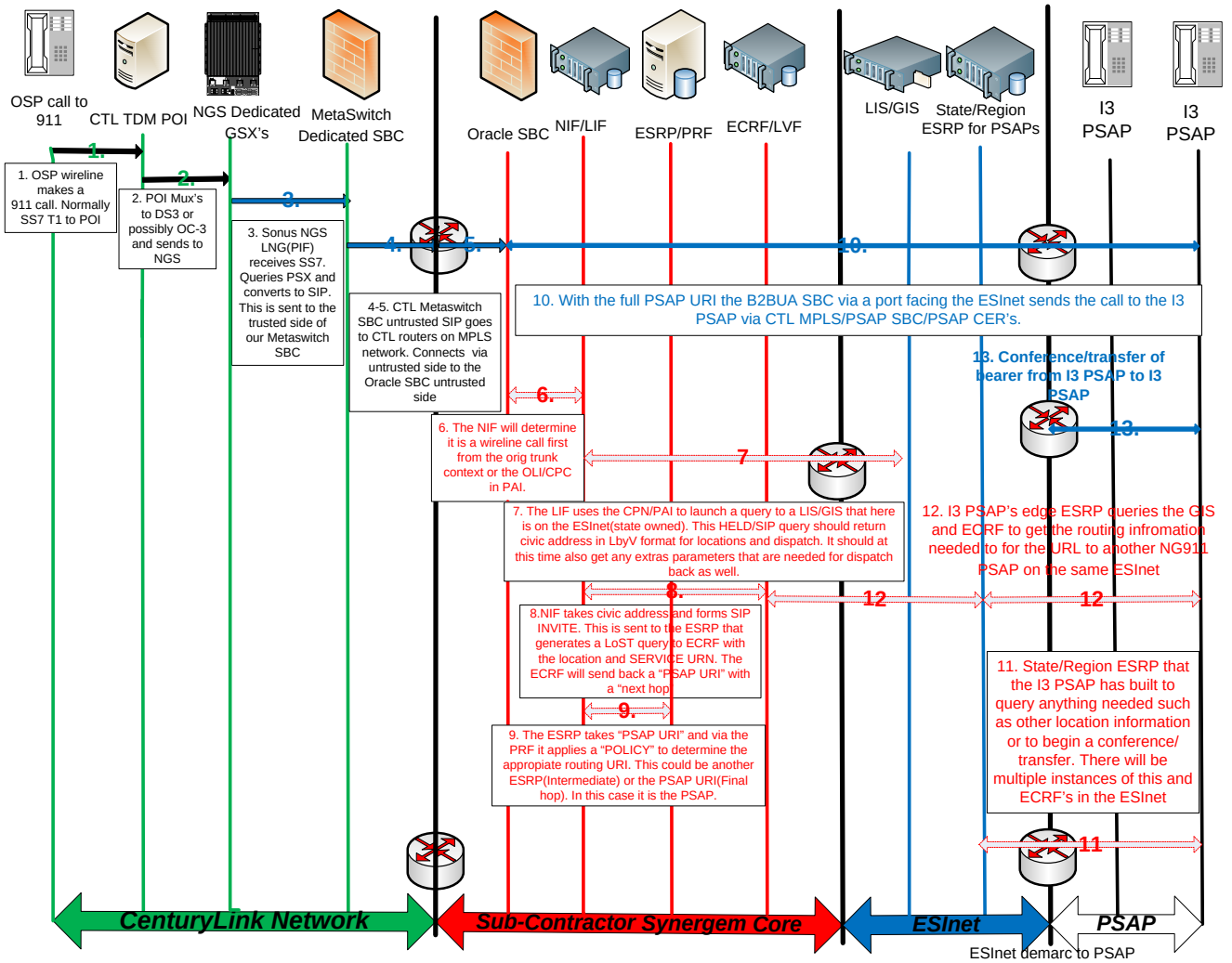
ESInet to ESInet Transfer: For a PSAP to transfer a call out to another ESInet it needs to route the call through the CTL Core. This is accomplished via the following:

- Route from ESInet 1 to ESInet 2 is updated via IP routing.
- RNSP 1 through 4 will know a path or route to each other through CTL Core sharing its routing tables to the attached ESInet networks.
- When PSAP needs to transfer a call from ESInet 1 to ESInet 2, a DNS look up is done to determine the destination IP address.
- CTL Core determines the destination IP address is for ESInet 2 and routes the call from ingress SBC to egress SBC to ESInet 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 the ESInet(s) and CTL 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.



NGCS 79 Transfers out of Region

CenturyLink utilizes the prototypical architecture as specified in NENA STA-010 for routing calls. When a call needs to be transferred to a PSAP, arriving calls would be evaluated to determine whether they have location information in the arriving SIP headers; if they do not, a HELD query 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 PSAP destination determined.



NGCS 79 NG9-1-1 PSAP Traffic Transfers to NG9-1-1 PSAP DIAGRAM

	Route from PSAP to other ESInet is routed via next hop/default URI based on the transfer to PSAP entry loaded into the host PSAP's GIS that is queried. If it is in the same GIS DB and in iterative mode, the ECRF should return a full URI to the PSAP with a default next hop of the first ESRP on the transfer to ESInet. If it is not managed by the same GIS such as neighboring state it should get a default route to that states non-trusted facing ESRP and BCF such as sos@default.WI.us.net as an example for Nebraska • Determines the destination IP address is for PSAP 2 and routes the call from ingress SBC to egress SBC to PSAP 2 regardless if the final destination is known or not • Conference call or transfer can now be completed o URN and URI responses can be queried at this point, discussion around this needs to take place between CTL and different NG9-1-1 system to decide direction on whether Alternate path URI's will be used or not.

Any additional documentation can be inserted here:

NGCS 80	**Next Generation Core Services Elements (NGCS)** **Transfer to 7/10-Digit Numbers** The bidder's solution shall be capable of transferring 911 calls to 7 or 10-digit numbers with the Calling Party Number (CPN). Describe how the solution meets or exceeds this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	CenturyLink can transfer 9-1-1 calls in various fashions which will include with the 7- or 10-digit Calling Party number. These transfer methods include fixed transfer, PSAP DN transfer, 2-3-digit star code transfers, and PSTN transfer. Additionally, for i3, CenturyLink will follow the appropriate NENA-STA-010.2-2016 protocols for transfers and is doing so in live i3 environments today.				

Any additional documentation can be inserted here:

SVAL-1	**Service Validation** Throughout the life of the contract, upon request of the Commission, Bidder shall allow for network testing and validation by a third-party entity, to verify that the service(s) and/or solution(s) are in compliance with the contract's scope.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: CenturyLink would welcome a third-party testing and validation entity and will offer its full cooperation upon request from the commission. We would only ask for a Statement of Work (SOW) to review the test plan and processes to be used.				

OPTIONAL SERVICE

NGCS 81	**Next Generation Core Services Elements (NGCS)** **OPTIONAL SERVICES** **NG911 Applications and Alarm Integration** **Alarm Integration Description** NG911 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and associated data. Describe bidder's experience with integrating alarms, sensors, and other non-interactive call types with bidder's NGCS solution and include separate pricing.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: CenturyLink and its partners have had experience integrating multiple "non-traditional" systems into the NG9-1-1 infrastructure. These include, but are not limited to, Telematics, VoIP Services, Text, Multimedia, and Sensors. If the participating technologies can use traditional TDM/ALI protocols or NENA standard i3 protocols to connect and provide address information to the NGCS infrastructure, then the solution and interoperation should be seamless. With the information available today, it seems as though alarm data and call center support would fit the NG9-1-1 mold well. In order to fully understand the support (and therefore financial) impacts, CenturyLink would need to know the interoperability requirements from the Alarm Provider, as well as the expectation for the result from the PSAP. If alarm companies provide either legacy TDM/ALI or i3 standard protocols, the integration would be seamless, and the call flow should be identical to that of a typical legacy and/or i3 call. If for some reason, the alarm company is unable to provide the voice and location information in an industry-standard format, additional resources would need to be expended to design, test and implement a non-standard solution. ASAP is a is an alarm-based protocol that is tied to the INLETS message switch with INLETS assigned IDs and is how alarm companies route alarm calls to the appropriate PSAP CAD. These IDs are not transferable or usable in/on an ESInet or with NGCS because they are not defined in the NENA specification. Until APCO ratifies the protocol to be used on a common IP transport and uses common NGCS services for routing of calls based on location elements, ASAP cannot be used on an ESInet. CenturyLink is working with Alarm and IOT companies to standardize calls for service in an i3 methodology. If there is an expectation to provide functionalities or capabilities that are not currently supported by the legacy and/or NENA i3 model, CenturyLink would need to fully understand the requirements from both the OSP in question as well as the Commission to establish a support model to satisfy the end user's needs. CenturyLink can work through engineering requirements discovery with the Commission to develop a mutually agreed upon scope of work that would be priced separately upon completion of functional requirements analysis.				

Any additional documentation can be inserted here: