



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

Kim VanDenTop
Public Safety / 911 Account Director

P: 605-496-5800

E: kim.vandentop@lumen.com

Legal Statement**INFORMATIONAL PURPOSES ONLY**

Lumen has endeavored to provide responses as requested by the RFP, but Lumen's response is not intended to create a binding contractual commitment between the parties without further discussion between and execution of appropriate contract documents by the parties. Specifically, Lumen's responses and proposal 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 Lumen's signature on its submission, the responses are informational only and are provided for your evaluation.

CONTRACT AND SERVICE TERMS

Lumen proposes to provide its Services pursuant to the State of Nebraska Contract Terms and Conditions subject to negotiation between the parties when those terms are provided upon award pursuant to the State of Nebraska's answers to questions provided in Addendum 2 to this RFP. Lumen also requests the inclusion of its service attachments, service exhibits and SLAs, and SOW attached to this bid response (the "Lumen Attachments") in the final, negotiated contract between the parties. If there is any conflict between the responses provided and the Lumen Attachments, the Lumen Attachment controls and contains the complete Lumen terms. Lumen is confident that the parties will reach a definitive agreement in the context of an award. By presenting this proposal, Lumen does not agree that the RFP or Lumen's response will be a part of a final agreement in whole or in part.

AFFILIATED COMPANIES

Lumen services are provided through affiliated companies. In some instances, Lumen's response or attached documents may include references to "CenturyLink" or names of other Lumen affiliated entities. All references to CenturyLink or other affiliated entities mean "Lumen" for purposes of the response. The Lumen Contract and/or the applicable Service Exhibits attached thereto will identify and be executed by the Lumen affiliate contracting for and/or 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). Lumen policies require tagging of any circuits or equivalent data paths used to transport 9-1-1 Data. It is required that customers agree to cooperate with Lumen regarding compliance with these rules and policies and to notify Lumen of all Services customers purchase under the Agreement utilized as Critical 911 Circuits or for 9-1-1 Data.

INSURANCE

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

Table of Contents

1. Corporate Overview 1

 1.1. Bidder Identification and Information 1

 1.2. Financial Statements..... 1

 1.3. Change of Ownership 3

 1.4. Office Location 3

 1.5. Relationships with the State 3

 1.6. Bidder’s Employee Relations to State 4

 1.7. Contract Performance 5

 1.8. Summary of Bidder’s Corporate Experience 5

 1.9. Summary of Bidder’s Proposed Personnel/Management Approach..... 7

 1.10. Subcontractors..... 14

2. Factors Used To Evaluate Corporate Overview 16

3. Response to Scope of Work 18

 3.1. ESInet Architecture and Design 18

 3.2. NG911 Core Services (NGCS) 29

 3.3. GIS and Location-Based Routing 31

 3.4. Call Flow and Media Session Handling 33

 3.5. Security, Privacy, and Trust 34

 3.6. Logging, Reporting, and Call Detail Records 35

 3.7. Interoperability, Testing, Conformance, and System Acceptance 37

 3.8. Operational Support and Service Level Agreements (SLAs)..... 38

 3.9. Applicable Standards..... 39

4. Response to Work Plan and Project Planning 53

 4.1. Project Management 53

 4.2. Staffing and Qualifications 73

 4.3. Implementation..... 80

 4.4. Transition 90

 4.5. Testing and Acceptance 99

5. Response to Technical Requirements 106

5.1. ESInet Requirements 106
Deliverables - ESInet Architecture and Design..... 145
5.2. Next Generation Core Services (NGCS) Requirements..... 146
Deliverables - NG911 Core Services (NGCS)..... 178
5.3. GIS and Database Services Requirements 179
Deliverables - GIS and Location-Based Routing..... 191
5.4. Security Requirements..... 191
Deliverables - Security, Privacy, and Trust..... 246
5.5. Reporting Services Requirements..... 246
Deliverables - Logging, Reporting, and Call Detail Records..... 277
5.6. Installation Requirements..... 277
Deliverables - Training..... 283
5.7. Training..... 283
Deliverables - Interoperability, Testing, Conformance, and System Acceptance..... 288
5.8. Operations and Service Management Requirements 289
Deliverables - Operational Support and Service Level Agreements (SLAs) 328
5.9. Value Add and Optional Services..... 329
5.10. Use Case Examples for Use with Response..... 330
6. Cost Proposal..... 343
7. Response to Terms 344
8. Contractual Agreement Form..... 345

List of Tables

Table 1.8-1. Corporate Experience Summary Matrix..... 6
Table 1.9-1. Lumen Account Team..... 10
Table 3.9-1. OSI Layer Mapping for Nebraska ESInet Network Segments..... 41
Table 3.9-2. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 46
Table 3.9-3. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 47
Table 3.9-4. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 48
Table 3.9-5. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 49
Table 3.9-6. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 51
Table 3.9-7. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix..... 52
Table 4.1.3.1-1. Lumen’s High-Level Work Breakdown Structure 58
Table 4.1.3.3-1. Lumen Risk Register 64
Table 4.1.3.6-1. PSAP-by-PSAP Work Plan Phased Activities..... 71

Table 4.4.1.5-1. Risk Assessment and Avoidance Matrix	96
Table 5.4.1.1-1. Responsibilities Matrix.	194
Table 5.4.1.2-1 Lumen's Identity Management Approach.....	198

List of Figures

Figure 1.9-1. Lumen's Proposed Organization Structure.....	9
Figure 3.1-1. Lumen System Diagram.....	20
Figure 3.1-2. Lumen NGCS Single Core Architecture.....	22
Figure 3.1-3. Core Site (ECMC) Architecture Illustration.....	23
Figure 3.1-4. Lumen ESInet Architecture Design.....	24
Figure 3.6-1. Individual CDRs by Date/Time	36
Figure 3.6-2. PSAP State Configurable CDR Options	37
Figure 4.1.3.6-1. Modernized NG911 Schedule Timeline.....	72
Figure 5.1.6-1. Executive Network Dashboard Statistics - Real-time and Downloadable.....	110
Figure 4.1.3.6-1. Lumen's Proposed ESInet Solution.....	113
Figure .1.12.4-1. Lumen ESInet Architecture Design.....	132
Figure 5.1.14.1-1. Organizational placement of Lumen's NG9-1-1 NOC.....	139
Figure 5.1.14.1-2. Summary of NOC Tools and Systems	140
Figure 5.1.14.1-3. State of Nebraska Monitoring Portal.....	141
Figure 5.1.14.1-4. Ticket/Issue Problem Resolution Flow	142
Figure 5.4.1.2-1. PCA Trust Hierarchy and Certificate Issuance Model	200
Figure 5.4.10-1. NGSC Core Redundant Design.....	245
Figure 5.4.10-2. NGSC Core Redundant Design.....	246
Figure 5.5-1. Management Portal - Call Detail and Trace - Individual Messages Available.....	247
Figure 5.5-2. Management Portal - Abandonment, Alternate, and Backup Routing	248
Figure 5.8.3.1-1. Visibility of Lumen's Realtime Fault Manager.....	304
Figure 5.8.3.1-2. NG911 NOC Alarm Ticketing	305
Figure 5.8.3.1-3. NG911 HiPer Architecture.....	305
Figure 5.8.3.2-1. Lumen SOC Network Monitoring Capabilities.....	308
Figure 5.10.1-1. i3 OSP w/LIS/ADR not using NFG.....	334
Figure 5.10.1-2. i3 OSP not using NFG using Lumen LIS/ADR.....	334
Figure 5.10.1-3. i3 OSP using NFG.....	335

April 15, 2026

David Sankey – State 911 Director
Nebraska Public Service Commission
300 The Atrium, 1200 N Street
Lincoln, Nebraska 68509

Dear Evaluation Committee,

Lumen submits this proposal in response to the State of Nebraska’s (SoNE) Request for Proposal (RFP) for Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS), offering an Intrado-based NG911 solution that emphasizes continuity of service, standards conformance, and accountable operations. We recognize that NG911 is a mission-critical public safety service, and our approach modernizes Nebraska’s emergency communications environment while minimizing transition risk, operational disruption, and uncertainty for PSAPs and State oversight entities.

Lumen is a leader in the telecommunications industry, operating a nationwide, carrier grade Internet Protocol (IP), fiber network engineered for geographic diversity, redundancy, and high availability. This network provides the resilient transport foundation required for NG911 ESInet services and supports deterministic performance, rapid fault isolation, and controlled traffic behavior under both normal and degraded conditions.

Intrado is a recognized industry leader in E911 and NG911 solutions, supporting emergency communications for public safety agencies, enterprises, and government entities across diverse geographic regions and operational environments. Together, Lumen’s ESInet capabilities and Intrado’s NGCS platforms are deployed at scale, interoperate with Originating Service Provider (OSP) and peer networks, and actively support next-generation call routing, policy control, analytics, and emergency services delivery.

SoNE NG911 - Designed for Resiliency and High-Availability

Lumen delivers a fully IP-based ESInet architecture enhanced with SD-WAN to eliminate single points of failure and strengthen statewide NG911 resiliency from day one. As the incumbent provider, Lumen modernizes an already operational ESInet rather than rebuilding one, avoiding the disruption and risk associated with restarting OSP integrations. Lumen is on track to complete all remaining OSP migrations by November 2026, with national carriers already delivering calls via SIP and local carriers supported through TDM. Additionally, Lumen’s modernized NG911 architecture incorporates optional tertiary connectivity using Dejero multi-carrier wireless and Starlink low-earth-orbit (LEO) satellite services, providing continuity even when terrestrial infrastructure is disrupted and supporting sustained 99.999% availability objectives for NG911 services.

Benefit to the State of Nebraska: Nebraska benefits from immediate resiliency improvements without restarting OSP migrations, reduced exposure to single-point failures, enhanced operational visibility, faster fault isolation, and assured, redundant call routing continuity even during large-scale terrestrial outages.

Key Strengths and Differentiators. The proposed Intrado-based solution delivers modernization while preserving uninterrupted 911 operations, sustaining **99.999%** availability for call-path services, and providing the State with transparent oversight and control throughout the contract term. Our proposal is built around five key strengths and differentiators, including a disciplined NG911 architecture, proven operational practices, and an execution model aligned with NENA i3 requirements and Nebraska’s objectives for continuity, resiliency, cost efficiency, operational governance, and standards compliance:

- 1. Mission Continuity Through Proven, Integrated Operations.** Lumen's solution preserves uninterrupted NG911 operations by leveraging an Intrado-based operating model that is already deployed, proven, and integrated across multiple NG911 environments, including Nebraska. Transition activities are executed using parallel operation, controlled cutover sequencing, and predefined rollback paths to avoid service resets, retraining cycles, or disruption to live call routing.

Benefit to the State of Nebraska: Public safety operations remain continuous during transition, protecting callers, PSAP operations, and statewide emergency response capabilities while reducing transition-related risk.
- 2. Modernized Architecture Delivering Resiliency, Availability, and Accountability.** Lumen delivers a fully Internet Protocol (IP)-based ESInet architecture enhanced with Software Defined - Wide Area Network (SD-WAN) technologies to eliminate single points of failure and improve network management and orchestration. Policy-based routing, path diversity, and real-time performance monitoring enable intelligent traffic steering and automated failover while providing auditable visibility into network behavior across the NG911 environment.

Benefit to the State of Nebraska: Improved resiliency against localized and systemic failures, enhanced operational visibility, faster fault isolation, and greater assurance that NG911 traffic is continuously routed over optimal and available paths.
- 3. Efficient Transition With Cost and Operational Discipline.** Nebraska receives a transition approach informed by Lumen's extensive NG911 deployment experience, enabling parallel execution, staged cutovers, and coordinated training aligned to PSAP readiness. This approach avoids dual billing, limits overlap periods, minimizes repeated testing cycles, and reduces the operational burden placed on PSAP and State personnel.

Benefit to the State of Nebraska: Modernization proceeds on a predictable timeline without unnecessary expense or disruption to PSAP operations or other NG911 stakeholders.
- 4. Experienced NG911 Leadership and Governance Alignment.** Lumen provides an experienced NG911 delivery and operations team (**current program management personnel**) with established familiarity with Nebraska's regulatory environment, operational workflows, and oversight expectations. Governance, reporting, risk management, and service management are aligned from day one through structured monthly reviews, SLA and KPI reporting, risk register updates, and defined escalation ownership.

Benefit to the State of Nebraska: Reduced learning curve, improved responsiveness, consistent performance, and transparent oversight throughout the contract term.
- 5. Standards-Aligned NG911 Modernization Without Operational Disruption.** Nebraska transitions to a fully standards-compliant i3 NG911 architecture without wholesale replacement of existing operational infrastructure. Lumen delivers NGCS, ESInet, and supporting services aligned with NENA-STA-010.3, with documented gap identification, remediation planning, and ongoing conformance management to support standards evolution without increasing operational risk.

Benefit to the State of Nebraska: The State achieves NG911 modernization while preserving service stability, minimizing transition risk, and maintaining continuous call handling for PSAPs.

State of Nebraska Modernization, Implementation, and Transition Strategy. Lumen executes NGCS implementation and transition as a disciplined modernization program that advances an already operational statewide ESInet and NGCS environment rather than replacing it. As reflected in the Microsoft Project schedule provided in **Attachment 6**, Lumen applies a phased execution model that modernizes ESInet transport, expands NGCS resiliency, and upgrades regional connectivity while maintaining uninterrupted NG911 operations statewide. Modernization proceeds through seven regional deployments; each staggered in approximately four month cycles with planned overlap. This approach allows Lumen to initiate provisioning and validation activities for upcoming regions while cutover preparation and stabilization activities are underway in the current region, accelerating statewide delivery while preserving operational continuity and minimizing risk.

Operational Continuity and Performance Assurance

Lumen delivers operational continuity for Nebraska's NG911 environment through a carrier grade management framework that includes 24x7 NOC monitoring, predictive performance analytics, automated SLA and KPI reporting, and documented escalation and restoration procedures. This framework provides continuous verification of ESInet and NGCS performance, proactive fault detection and resolution, and enforcement of availability and recovery objectives for mission critical 911 call delivery and routing services.

Modernized - Third Core Deployment. The schedule incorporates deployment of a third NGCS core as a parallel workstream coordinated with our subcontractor partner Intrado. Core connectivity, transport updates, provisioning, and closed user group activities proceed concurrently with regional ESInet circuit modernization, allowing NGCS resiliency enhancements to advance without delaying regional milestones. IP Point of Interconnect (POI) integration across the ESInet is already complete via nationwide connectivity with the largest OSPs statewide. This dependency is isolated and does not affect modernization activities in the remaining regions, all of which receive new ESInet circuits upgraded with the SD-WAN solution.

The schedule preserves TDM points of interconnection as an ongoing option for originating service providers, with migration to IP POIs performed only at an OSP's request with continuous communications with the State of NE on OSP migration status to IP POI's, ensuring that OSP interconnection does not introduce external dependencies or delay implementation. **Attachment 6** serves as the authoritative Integrated Master Schedule governing NGCS implementation and transition, and all transition schedules remain living documents throughout the contract term to ensure continued alignment with the State, PSAPs, and all participating service providers.

Summary: Lumen has designed the entire ESInet and NGCS as a cohesive NG911 platform that directly addresses the State of Nebraska's justification for modernizing the current system. The architecture was engineered from the outset to resolve legacy limitations, eliminate known NG911 failure modes, and provide the State with a secure, resilient, and operationally mature foundation for statewide emergency communications. Specifically, the proposed solution addresses each State of Nebraska justification as follows:

- **Regulatory Compliance.** The ESInet and NGCS are built to align with the FCC's 2025 NG911 rules for reliability and location accuracy. Standards-based call processing, authoritative GIS-driven routing, and measurable performance controls ensure regulatory expectations are met across the end-to-end call path.
- **Operational Improvements.** GIS-based validation and routing reduce call-handling errors, including boundary and edge-case conditions, while native multimedia support

enables voice, text, and real-time video services. This design directly supports expanded NG911 capabilities, including VRS for Deaf, hard of hearing, and speech-disabled callers.

- **Resiliency and Scalability.** Geographically diverse ESInet and NGCS core deployments (CO, FL, and NE) mitigate weather-related and regional outage risks and are engineered to sustain at least **150%** of projected peak call volumes. Redundant paths, components, and data centers eliminate single points of failure and support continuous operations.
- **Security Enhancements.** Zero-Trust principles, strong identity and encryption controls, and layered boundary protections are embedded across the architecture. These controls mitigate modern cyber threats, including Terabit-scale DDoS and TDoS attacks, without compromising call handling performance or availability.
- **Cost Efficiency.** A phased migration strategy minimizes operational disruption and transition risk while preserving continuity of service. Shared but logically isolated data center resources optimize cost efficiency without sacrificing resiliency, security, or accountability.
- **Future-Proofing.** The ESInet and NGCS support emerging NG911 capabilities, including IoT-initiated calls, NG-AACN, and Emergency Incident Data Objects. Full NENA i3 conformance, including REST and JSON interfaces, ensures interoperability with legacy environments and positions Nebraska to adopt future NENA standards as they evolve.

Collectively, this design delivers a secure, resilient, and standards-compliant NG911 system that modernizes Nebraska's emergency communications while sustaining **99.999%** availability, reducing operational and transition risk, and providing long-term operational confidence aligned with State governance and oversight expectations.

Sincerely,

Kim VanDenTop, Account Director

Lumen

605-496-5800 | kim.vandentop@lumen.com

1. CORPORATE OVERVIEW

The Corporate Overview section of the solicitation response should consist of the following subdivisions:

LUMEN RESPONSE:

Lumen has decades of experience supporting Public Safety and 9-1-1, delivering mission-critical emergency communications infrastructure for states, counties, and service providers nationwide. Internally documented references show Lumen supporting over 300 million 9-1-1 calls annually, partnering with 1,100+ PSAPs across 34 states, and deploying NG911 solutions for more than 11 years through NENA i3-aligned architectures, ESInets, and Next Generation Core Services, while continuing to operate and interwork with legacy E9-1-1 environments. As a Fortune 100 company, Lumen combines financial strength, nationwide network scale, and dedicated Public Safety expertise to support long-term 9-1-1 modernization with proven reliability and continuity of operations.

1.1. 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.

LUMEN RESPONSE:

CenturyLink Communications, LLC d/b/a Lumen Technologies Inc. (Lumen)

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.

Attachment 1a shows the Name Change Certificate of Amendment that became effective on April 1, 2014.

1.2. 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 solicitation 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.

LUMEN RESPONSE:

Lumen is providing the most recent 10K financial report as **Attachment 1b** to our proposal.

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

Wells Fargo

Stephanee Taylor, CTP

Director, Lead Treasury Management Sales Consultant

Corporate Banking & Specialized Industries | Technology, Media, & Telecom

Wells Fargo Bank N.A.

Office: 303-863-6403

Cell: 720-916-4651

eFax: 855-699-2871

stephanee.n.taylor@wellsfargo.com

US Bank

Andrew J Stredde

Vice President

Technology, Media & Telecom (TMT), Corporate Banking

U.S. Bank

p: 630.637.2704

m: 312.515.0633

andrew.stredde@usbank.com

JPMorgan

Mariel Doyle

Vice President, Media and Communications

J.P. Morgan Payments

646.797.7003

mariel.doyle@jpmorgan.com

Due to size of Lumen, various suits, proceedings, and claims typical for an enterprise business can be pending against Lumen 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 Lumen's position, Lumen expects the outcome of such proceedings, individually or in aggregate, will not have a materially adverse effect on the financial condition or results of Lumen operations or its business segments; nor negatively affect its ability to provide the services proposed.

As a public corporation, Lumen is required to fully disclose material data and relevant information that may influence investment decisions to all investors at the same time. Lumen does not provide detailed information on litigation except through its securities filings. Please refer to Lumen's Annual Report on Form 10-K.

1.3. Change of Ownership

If any change in ownership or control of the company is anticipated during the twelve (12) months following the solicitation response 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 Commission.

LUMEN RESPONSE:

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

1.4. 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.

LUMEN RESPONSE:

Lumen

118 S 19th St.

Omaha, NE 68105

1.5. Relationships with the State

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's solicitation 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.

LUMEN RESPONSE:

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

In the last five years, Lumen has extensively participated in the development and support of the Nebraska Public Service Commission "9-1-1 Service System Plan" with the implementation of the NG911 Statewide ESInet delivered to all regions in the State. The Lumen local support team has acted in one capacity or another as the consultant, design engineers, support technicians, and project managers with the South Central, Panhandle,

North Central, East Central, Northeast, Southeast, Metro, and Mid-West 911 regions. We helped upgrade multiple regions' call handling and networks in preparation for the NG911 ESInet prior to deployment and have completed several upgrades since completion.

In parallel with the ESInet migration, Lumen deployed NG911 Points of Interface (POIs) for direct Carrier connectivity to each Local Access Transport Area (LATA) as well as two out-of-State SIP POIs that are used nationally with larger carriers. By the end of 2025, Lumen had worked with all 38 Carriers in the State to gain agreement and ensure a plan for full migration off of the legacy Selective Routers. The migrations to date are at 99% completion with all non-deployed Carriers gaining the necessary extensions upon Nebraska State Board approval.

Lumen has previously had a member appointed to the Nebraska Public Service Commission 911 Service System Advisory Committee. As a member of this committee, Lumen was able to support at the PSAP level but also support the Public Service Commission 911 initiatives.

We have 93 active Public Safety specific contracts with 29 PSAPs. These contracts support network and call handling equipment. Lumen is the predominate Local Exchange Carrier (LEC) in the state and provides an extensive network of voice and data circuits. Lumen owns four of the five 911 selective routers which were used as aggregation points for Legacy OSPs until such a time they can migrate to the Lumen IP POIs. Lumen 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, Lumen 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 State of Nebraska Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) contracts with Lumen. 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_gc_ens_c.pdf

1.6. Bidder's Employee Relations to State

If any Party named in the bidder's solicitation response is or was an employee of the State of Nebraska within the past six (6) 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 is employed by the bidder or is a subcontractor to the bidder, as of the due date for solicitation response 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 solicitation. If no such relationship exists, so declare.

LUMEN RESPONSE:

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

1.7. Contract Performance

If the bidder or any proposed subcontractor has had a contract terminated for default during the past ten (10) 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 ten (10) 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 solicitation response accordingly. If no such termination for default has been experienced by the bidder in the past ten (10) 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.

LUMEN 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 Lumen's reasonable efforts to avoid disputes, the sheer volume of contracts entered into by Lumen dictates that Lumen is occasionally involved in contract disputes. Lumen 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.

1.8. Summary of Bidder's Corporate Experience

The bidder should provide a summary matrix listing the bidder's 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 solicitation response.

The bidder should address the following:

- i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this Solicitation. 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, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and
- e) Each project description should identify whether the work was performed as the prime vendor or as a subcontractor. If a bidder performed as the prime vendor, 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.
- ii. Bidder and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as subcontractor projects.
- iii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the bidders above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

LUMEN RESPONSE:

As a recipient of the Frost & Sullivan NG9-1-1 Enabling Platform Leader award, Lumen has installed and maintains a variety of 9-1-1 equipment and services in 35 states. Lumen has successfully implemented or is currently implementing:

- Statewide/regional ESInets and NG9-1-1 services in Arizona, California, Minnesota, Montana, New Jersey, Nebraska, North Dakota, South Dakota, Utah, and Washington.
- County and individual PSAP ESInets with NG9-1-1 services in Florida including Lake County, Sumter County and Osceola County.

Table 1.8-1 provides the summary matrix of Lumen's previous projects similar to this Solicitation in size, scope, and complexity.

Table 1.8-1. Corporate Experience Summary Matrix.

Attribute	Project 1	Project 2	Project 3
Project Name	Nebraska NG911 ESInet (Incumbent)	North Dakota	South Dakota
Customer	State of Nebraska Public Service Commission	State of North Dakota	State of South Dakota
Role (Prime / Subcontractor)	Prime Vendor	Prime Vendor	Prime Vendor
Time Period	2020 - 2026	2021 - 2026	2024 - 2029
Originally Scheduled Completion Date	2026	11/2026	10/2029
Actual / Planned Completion Date	Ongoing	Ongoing	Ongoing
Original Budget	\$12M	\$3,256,000	\$442,000

Attribute	Project 1	Project 2	Project 3
Actual / Planned Budget	\$12M	\$3,256,000	\$442,000
Bidder Responsibilities	Statewide ESInet design, IP routing, NGCS integration, operations, and governance	Statewide ESInet design, IP routing, NGCS integration, operations, and governance	Statewide ESInet design, IP routing, NGCS integration, operations, and governance
Similarity in Size	Statewide, multi-PSAP	Statewide, multi-PSAP	Statewide, multi-PSAP
Similarity in Scope	ESInet, NGCS, IP routing, operations	ESInet, NGCS, IP routing, operations	ESInet, NGCS, IP routing, operations
Similarity in Complexity	Live NG911 traffic, incumbent operations	Live NG911 traffic, incumbent operations	Live NG911 traffic, incumbent operations
Customer Reference	David Sankey - State 911 Director Agency: Nebraska Public Service Commission dave.sankey@nebraska.gov P: 402-471-3101	Jason Horning, ENP NG9-1-1 Program Manager North Dakota Association of Counties jason.horning@ndaco.org P: 701-425-0816	Jason Husby STATE 9-1-1 COORDINATOR SD DEPARTMENT OF PUBLIC SAFETY Jason.husby@state.sd.us P: 605.773.3264
Subcontractor Share of Costs (if applicable)	Intrado = ~40%	Intrado = ~40%	Intrado = ~40%
Subcontractor Scope & Time Period (if applicable)	Intrado - NGCS and GIS services, implementation and ongoing management and operational support.	Intrado - NGCS and GIS services, implementation and ongoing management and operational support.	Intrado - NGCS and GIS services, implementation and ongoing management and operational support.

1.9. 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 Commission'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 Commission 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.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The Commission 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 Commission.

LUMEN RESPONSE:

Lumen proposes a dual-team management structure that separates program and project execution responsibilities from ongoing account and service management, ensuring clear accountability throughout implementation and the full contract term. Following contract award, Lumen will conduct an initial coordination meeting with the State at which both teams are represented to explain roles, interfaces, reporting relationships, and the overall management approach.

Lumen's Program Management Office (PMO) is responsible for planning, coordinating, and delivering all project activities through service implementation acceptance and formal project completion. The PMO

applies a documented project management methodology aligned with Project Management Institute principles and ITIL v5 practices, supporting controlled execution, risk management, and compliance with contract requirements. The PMO's charter emphasizes structured planning, adherence to contractual terms, coordinated execution across technical and operational teams, and sustained customer engagement throughout the project lifecycle. This approach is designed to support predictable milestone achievement and minimize implementation risk.

The PMO is staffed with experienced project managers who have demonstrated expertise in telecommunications and NG911 system delivery. Project managers are authorized to manage project resources, direct internal teams, and coordinate external suppliers, vendors, and third-party contributors as required to meet project objectives. Project management is a formal functional role within Lumen, supported by established governance, escalation paths, and change and configuration management processes.

Key Personnel - Operational Structure. Upon completion of contract negotiations, **Ms. Angela Schrawyer** will serve as Lumen's Senior Program Manager (PgM) for the State of Nebraska NG911 program, providing a single, consistent primary point of contact for the State throughout the full contract lifecycle. In this role, she is accountable for end-to-end program governance, including oversight of all implementation and maintenance activities, project scope, schedule, budget, resources, stakeholder communications, governance cadence, risk and issue management, change control, and delivery of all contractual project deliverables, while ensuring continuity of 911 operations is protected. During the implementation phase, **Ms. Schrawyer will also perform the role of the dedicated Project Manager (PM)**, managing day-to-day execution activities, coordinating with the State and Lumen account team, confirming compliance with contract requirements, and facilitating timely resolution of technical and operational issues. She will coordinate closely with Lumen operations, network, and support organizations to ensure alignment between implementation activities and long-term operational readiness. Lumen's key personnel in support of this contract include:

Experienced NG911 Leadership & Governance Alignment

Lumen provides an experienced NG911 delivery and operations team with established familiarity with Nebraska's regulatory environment, operational workflows, and oversight expectations. Governance, reporting, risk management, and service management are aligned to State needs from day one of award.

Benefit to the State of Nebraska: Reduced learning curve, improved responsiveness, consistent performance, and transparent oversight throughout the contract.

- Angela Schrawyer – Program/Project Manager (PgM, PM)
- Shelly Guenther – Deputy Program/Project Manager (DPgM, DPM)
- Charlie Knox – Technical Lead (TL)
- Doug Cunningham – Solution Architect (SA)
- Mia Blake – Customer Engagement Manager (CEM)
- Michelle Devlin – Operations Service Manager (OSM)
- Kim VanDenTop – Account Director (AD)
- John Sintim – Security Lead

Lumen provides a Draft Program Management Plan (PMP) with this submission and a final PMP will be developed after contract award and will be tailored to the specific scope, requirements, and sequencing defined in the contract and statement of work. The plan will include, at a minimum, a communications plan, testing plan, cutover plan, and detailed project schedule with task sequencing and dependencies. Development of this plan will be based on a comprehensive review of contract requirements and collaborative discussions with the State's designated representatives and Lumen's technical and operational teams. Our draft PMP is provided in **Attachment 3**.

The proposed organizational structure for the Nebraska account, including account management, program leadership, and supporting roles, is illustrated in **Figure 1.9-1**.

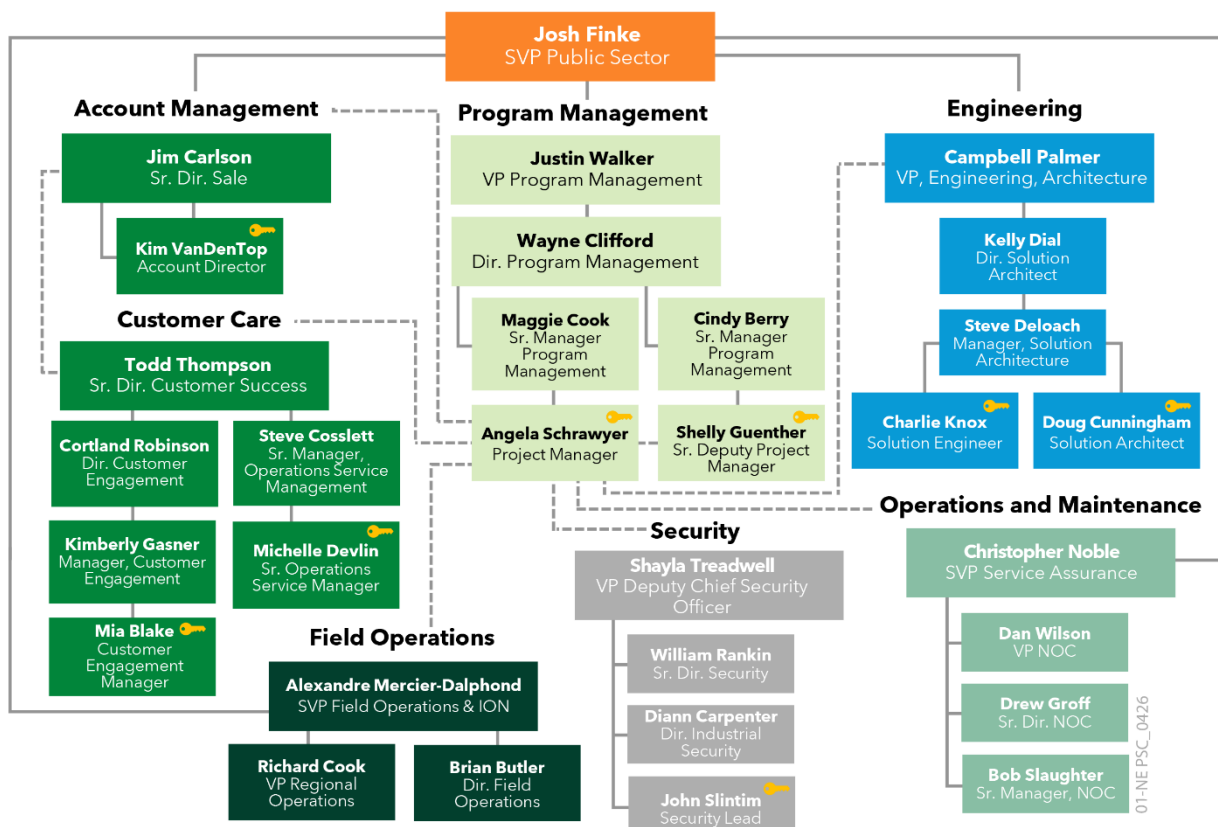


Figure 1.9-1. Lumen's Proposed Organization Structure

Lumen's account management team is assigned during the proposal process and remains engaged throughout the full term of the contract. The account team is responsible for ongoing coordination with the State, service oversight, issue resolution, and support of operational and governance activities after implementation is complete. This team operates

within Lumen's global sales and support model, which is structured to align customer engagement with network operations and service delivery functions.

A detailed account team profile is provided in **Table 1.9-1**, identifying the proposed personnel by name and title, describing their responsibilities, experience, contact information, and primary work assignments related to the NG911 project.

Table 1.9-1. Lumen Account Team

Title	Responsibility	Name and Contact Information	Experience
Account Director	Serves as the primary Account Director and executive point of contact for the State. Leads customer governance and executive communications; manages escalations; coordinates with program management, engineering, operations, and vendors to ensure continuity of NG911 operations and alignment with contractual and performance requirements.	Kim VanDenTop Phone: 605-496-5800 Email: kim.vandentop@lumen.com	Public-sector account leader with more than 20 years of experience supporting mission-critical telecommunications and NG911 programs. Currently serving as the incumbent Account Director for Nebraska NG911 with extensive experience in executive engagement, escalation management, vendor coordination, and service continuity.
Project Manager	Sr. Program Manager with lifecycle management responsibility for the NE NG911 program. Serves as the primary customer liaison between Lumen and State of Nebraska stakeholders. Accountable for overseeing project scope, schedule, budget, resources, stakeholder communications, governance cadence, risk and issue management, change	Angela Schrawyer Phone: 970-690-6329 Email: angela.schrawyer@lumen.com	Senior program manager with over 20 years of experience delivering large-scale NG9-1-1 and public safety telecommunications programs. PMP and PgMP certified with deep expertise in program governance, stakeholder communications, vendor coordination, risk management, and post-implementation operational oversight.

Title	Responsibility	Name and Contact Information	Experience
	control, and the delivery of all contractual project deliverables, while ensuring the continuity of 911 operations is protected.		
Deputy Project Manager	Supports day-to-day project execution and assists the Project Manager. Coordinates NGCS and ESInet activities, manages multi-OSP lab and end-to-end testing, supports cutover readiness and migration sequencing, tracks risks and issues, and coordinates communications with PSAPs and State stakeholders.	Shelly R. Guenther Phone: 720-879-8089 Email: shelly.guenther@lumen.com	Public safety and 9-1-1 industry leader with more than 25 years of experience spanning NGCS and ESInet integration, multi-provider migration of live 9-1-1 traffic, requirements documentation, interface control documentation, and statewide NG911 testing and acceptance activities.
Technical Lead	Provides technical leadership for ESInet, NGCS, and Call Handling Equipment design and implementation. Develops technical ordering documents and network diagrams, supports requirements discovery and solution design, enables operational monitoring, and supports testing, cutover planning, and steady-state technical operations.	Charlie Knox Phone: 720-888-3573 Email: Charlie.knox@lumen.com	NG911 Solution Engineer with direct experience supporting statewide ESInet and NGCS environments. Lead engineer for Call Handling Equipment projects across a wide range of PSAP sizes, supporting both implementation and post-sales technical execution for statewide NG911 programs.
Solution Architect	Provides technical leadership for ESInet, NGCS, and Call	Doug Cunningham Phone: 352 414 3392	Veteran public-safety Solution Architect with more than 20 years of

Title	Responsibility	Name and Contact Information	Experience
	Handling Equipment (CHE) design and implementation. Leads technical discovery, develops solution architectures and network diagrams, and produces technical documentation supporting NG911 implementations. Works closely with program management, engineering, operations, OSPs, and vendors to ensure standards-aligned designs, implementation readiness, testing support, cutover planning, and steady-state technical operations.	Email: Douglas.C.Cunningham@lumen.com	experience supporting NG911, ESInet, and NGCS architectures for state and local government customers. Long-standing member of Lumen's Public Safety team with deep expertise in NENA i3 design, ESInet architecture, and CHE integration for hosted and standalone environments. Provides hands-on technical leadership supporting statewide NG911 programs, including solution design, customer workshops, RFP responses, standards alignment, and post-implementation technical support.
Customer Engagement Manager	Acts as the primary day-to-day customer engagement point for the State. Coordinates communications related to service performance, issue resolution, billing inquiries, and change notifications. Supports escalation management, cross-functional coordination, and long-term relationship management to maintain customer confidence and service continuity.	Mia Blake Phone: 206-652-5663 Email: Mialisa.B.Blake@Lumen.com	Customer engagement and account support professional with more than 20 years of experience in telecommunications environments. Extensive background in customer advocacy, post-sales support, issue resolution, contract lifecycle management, and maintaining service stability during complex system transitions.

Title	Responsibility	Name and Contact Information	Experience
Operations Service Manager	Responsible for day-to-day operational performance of the NG911 network. Provides real-time incident, event, and escalation management; conducts network hardening and diversity reviews; ensures operational documentation remains current; and coordinates with engineering and field operations to protect continuity of emergency communications.	Michelle Devlin Phone: 505 250 1133 Email: michelle.devlin@lumen.com	Operations and service management professional with more than 22 years of experience supporting mission-critical telecommunications networks, including public safety and NG911 environments. Extensive experience in network monitoring, escalation management, resiliency planning, and service assurance.
Security Lead	Responsible for cybersecurity governance, risk management, and compliance oversight for the NG911 environment. Oversees security architecture, monitoring, vulnerability management, incident response, audit coordination, and compliance with NG911, federal, and State security standards.	John Sintim Phone: 908 720 1909 Email: John.Sintim@lumen.com	Cybersecurity leader with more than 10 years of experience supporting public-sector and service-provider environments. Brings deep expertise in NG911-aligned security architecture, continuous monitoring, risk management, vulnerability remediation, and regulatory compliance.

Lumen understands the importance of personnel continuity for a mission-critical public safety system. While Lumen retains responsibility for staffing decisions, any changes to proposed personnel will be communicated to the State and implemented only after written approval by the Commission. Resumes for all proposed personnel are provided in **Attachment 2, "Key Personnel Resumes."** Each resume includes academic background, professional certifications, relevant experience, and at least three references who can attest to the individual's competence and skill level. Resumes are limited to three pages in length in accordance with the solicitation requirements.

This management approach provides the State with a clearly defined project execution structure, identified leadership and support resources, transparent reporting relationships, and assurance that qualified personnel with appropriate experience and credentials will be assigned to deliver and support the NG911 solution.

1.10. Subcontractors

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

1.10.1 Subcontractor(s) Information

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

LUMEN RESPONSE:

Intrado Life & Safety, Inc.

1601 Dry Creek Drive

Longmont, CO 80504

720-494-5800

1.10.2 Specific Subcontractor's Tasks

- ii. specific tasks for each subcontractor(s),*

LUMEN RESPONSE:

Intrado will support Lumen as a specialized NG911 subcontractor for the expansion of the State's IP based NG911 architecture through the addition of a third Next Generation Core Services (NGCS) instance. All PSAPs are currently installed and operational; therefore, Intrado's scope is focused on IP based core integration, testing, cutover support, and ongoing data management rather than PSAP deployment.

Intrado's responsibilities include provisioning, configuration, and turn up of IP based NGCS components supporting the third core, including IP Selective Routing and associated call processing functions. Intrado will perform hardware and software provisioning activities as required to support the additional core and will validate connectivity and interoperability with the existing NG911 cores and Lumen managed ESInet.

Intrado will support Lumen in the coordinate and execute interoperability, redundancy, and failover testing with Lumen, PSAPs, and connected customer premises equipment (CPE) to ensure seamless call routing, load balancing, and resiliency across all NGCS instances. Testing activities will confirm that the third core integrates transparently into the existing operational environment without disruption to live 911 services.

During implementation, Intrado will support Lumen with project planning and scheduling related to third core integration, including coordination with Lumen and any additional vendors or stakeholders required for testing and cutover activities. Intrado will assist Lumen, as needed, in planning and executing cutover events to ensure a controlled, low risk transition that maintains uninterrupted emergency communications.

Following implementation, Intrado will continue to support Lumen's Operational teams, as needed, and will provide ongoing Geographic Information System (GIS) and Location Database management services. These services ensure accurate location data, routing

integrity, and continued operational readiness across the expanded multi core NG911 environment.

1.10.3 Percentage of Performance for Each Subcontract

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

LUMEN RESPONSE:

Intrado will have approximately 40% of the contract hours.

1.10.4 Total Percentage of Subcontractor(s) Performance

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

LUMEN RESPONSE:

Intrado will have approximately 40% of the contract hours.

1.10.5 Subcontractor Affiliation

v. *whether the subcontractor is affiliated with the bidder or has common ownership.*

LUMEN RESPONSE:

Intrado has no affiliation with Lumen other than as a subcontractor for NG911 services under a Master Services Agreement.

2. FACTORS USED TO EVALUATE CORPORATE OVERVIEW

Corporate Overview will be evaluated as follows:

- i. the ability, capacity, and skill of the bidder to deliver and implement the system or project that meets the requirements of the Solicitation;
- ii. the character, integrity, reputation, judgment, experience, and efficiency of the bidder;
- iii. whether the bidder can perform the contract within the specified time frame;
- iv. the bidder's historical or current performance; and
- v. such other information that may be secured and that has a bearing on the decision to award the contract.

In evaluating the corporate overview, the Commission may consider: past experiences with the vendor; references; the Department of Administrative Services' record of the vendor, which may include, but is not limited to Vendor Compliance Request, Contract Non-Compliance Notice, or vendor performance reports; and any information related to the vendor's historical or current character, integrity, reputation, capability, or performance with the Commission, State or a third-party. Information obtained from any Contract Compliance Request or any Contract Non-Compliance Notice may be used in evaluating responses to determine the best value for the State.

LUMEN RESPONSE:

Lumen is a national telecommunications provider with the scale, operational maturity, and technical expertise required to deliver and operate mission-critical public safety systems such as Nebraska's NG911 ESInet and NGCS. Our organization has the capacity and skill to implement complex, standards-based emergency communications architectures, integrate with public safety and originating service providers, and operate those systems with the reliability and accountability required for statewide 9-1-1 services.

Corporate Capability, Integrity, and Proven Performance

Lumen demonstrates the ability, capacity, and operational maturity to deliver and operate Nebraska's NG911 ESInet and NGCS through a carrier-grade network, disciplined program management, and proven public-safety operations. Our reputation for integrity, accountability, and consistent performance is reflected in our ability to meet contractual obligations, operate within defined timelines, and support mission-critical NG911 services.

Benefit to the State of Nebraska: Confidence that the selected vendor has the scale, experience, and operational discipline to deliver NG911 services reliably, meet contractual timeframes, and perform with the character, judgment, and accountability required for statewide public safety operations.

Lumen's Ability, Capacity, and Skill.

We bring demonstrated ability to deliver systems that meet the technical and operational requirements of this Solicitation. Lumen operates a carrier-grade IP and fiber network designed for high availability, geographic diversity, and secure interconnection, which provides the foundation for NG911 ESInet services. Our NG911 delivery model integrates network engineering, security, program management, and operations to support end-to-end call routing, data transport, monitoring, and recovery. This capability is supported by formal program management disciplines, structured change and risk management processes, and 24x7x365 operational support functions that are essential for public safety environments.

Nebraska's NG911 Trusted Provider. Lumen's character, integrity, and reputation are reflected in our long-standing role as a trusted provider of critical communications services to government, public safety, and enterprise customers. We operate under established corporate governance, compliance, and security frameworks and maintain disciplined operational controls to ensure contractual adherence and service accountability. Our approach emphasizes transparency, documented processes, and clear ownership of outcomes, which are fundamental to maintaining trust with public sector customers and oversight bodies.

Contract Performance. We have the capacity to fulfil this contract within the required time frame. Lumen maintains dedicated resources for NG911 program delivery, including experienced project managers, network engineers, security professionals, and operations staff who are familiar with NG911 standards and deployment models. Our implementation approach is structured to support parallel execution, controlled cutovers, and coordinated testing and training, allowing the State to transition services without disruption while meeting project milestones defined by the Commission.

Historical and Current Performance. As the State's current E911 provider, Lumen's offers demonstrated historical and current performance proving our ability to deliver and operate high-availability, large-scale communications services. Our network operations and service management practices support stringent availability targets, proactive monitoring, rapid fault isolation, and documented incident and root-cause analysis. These practices are supported by integrated NOC functions, automated performance reporting, and escalation processes that align operational response with contractual service levels. Where we have existing or prior relationships with public sector entities, our performance history reflects adherence to contractual obligations and responsiveness to operational and governance requirements.

Evaluation Factors. In evaluating Lumen's corporate overview, the Commission may consider past experience with Lumen, vendor performance records, and any compliance or performance information available through State systems or third-party references. Lumen understands the importance of these factors and approaches this engagement with a commitment to meeting the State's expectations for reliability, transparency, and accountability. We recognize that NG911 services carry heightened public trust obligations, and we structure our delivery and operations accordingly.

Taken together, Lumen's technical capability, operational capacity, experienced workforce, and disciplined governance model position us to deliver best value to the State of Nebraska. Our corporate strength lies not only in network scale, but in our ability to apply that scale responsibly to public safety systems, ensuring that Nebraska's NG911 services are delivered securely, reliably, and in full alignment with the Commission's requirements and oversight expectations.

3. RESPONSE TO SCOPE OF WORK

B. SCOPE OF WORK

Services to be Provided

The scope of this RFP encompasses the full lifecycle of the NG911 system, from design and implementation to operations and decommissioning. A comprehensive listing of the minimum technical requirements needed to operationalize a proposed solution is located in §E (Technical Requirements) of this document.

LUMEN RESPONSE:

Lumen Technologies is a global leader in network infrastructure and communications services, with a legacy spanning nearly a century. Lumen brings more than 30-years of experience delivering mission-critical solutions for public safety agencies nationwide, including Next Generation 911 (NG911), Emergency Services IP Networks (ESInet), and Next Generation Core Services (NGCS).

Full Lifecycle Support. In alignment with the State of Nebraska's NG911 vision, Lumen offers comprehensive ESInet and NGCS solutions that

support the full lifecycle of the NG911 system, from architecture and design through implementation, ongoing operations, continuous optimization, and eventual system transition or decommissioning, as defined in the Scope of Work (SOW) and the minimum technical requirements outlined in this RFP. Our approach ensures that Nebraska's ESInet and NGCS environment is resilient, scalable, secure, and capable of evolving as NG911 standards, technologies, and operational needs mature.

Adherence to Standards. Lumen's ESInet and NGCS solutions are designed to support NENA i3 functional requirements, including interoperability, IP-based call handling, geospatial call routing, and end-to-end IP connectivity. Lumen or its affiliated companies have actively participated in key industry standards organizations, including NENA, APCO, NIOC, ATIS, IETF, and MEF, reinforcing our commitment to standards-based solutions that protect Nebraska's investment and reduce vendor lock-in.

Supporting the State of Nebraska's operational objectives, Lumen delivers managed services, 24x7x365 network monitoring and operations, integrated cybersecurity capabilities, and seamless coexistence with legacy systems during transition periods. These capabilities ensure continuity of emergency services while enabling a controlled, standards-compliant evolution to a fully realized NG911 environment.

Modernized Architecture Delivering Resiliency, Availability, and Accountability.

Lumen proposes a fully IP-based ESInet architecture enhanced with Software Defined - Wide Area Network (SD-WAN) technologies to eliminate single points of failure and improve network management and orchestration. Policy-based routing, path diversity, and real-time performance monitoring enable intelligent traffic steering and automated failover while providing auditable visibility into network behavior across the NG911 environment.

Benefit to the State of Nebraska: Improved resiliency against localized and systemic failures, enhanced operational visibility, faster fault isolation, and greater assurance that NG911 traffic is continuously routed over optimal and available paths.

3.1. ESInet Architecture and Design

- a. Contractor shall provide an ESInet design and implementation conforming to the NENA i3 ESInet architecture and functional requirements, including multi-site, geographically diverse redundant

cores, session border control at boundaries, and tenant isolation. (This includes bandwidth provisioning, diagrams, availability, and reliability features).

LUMEN RESPONSE:

Lumen provides an Emergency Services IP Network (ESInet) design and implementation that conforms to the NENA i3 ESInet architecture and functional requirements, including compliance with NENA-STA-010.3 (i3 Standard) and the NENA Emergency Services IP Network Design (ESIND) guidance. The proposed ESInet establishes a secure, resilient, and standards-based IP infrastructure supporting statewide NG911 and NGCS operations.

Lumen delivers a multi-site, geographically diverse ESInet core architecture engineered to eliminate single points of failure and ensure continuity of emergency services. Redundant core locations are physically and geographically separated and interconnected using diverse network paths. Each core incorporates redundant routing, switching, and security components to support automatic failover and sustained operations during outages, maintenance activities, or disaster events.

Transformative ESInet - NG911 Solution Architecture and Design. Lumen is committed to enhancing the digital capabilities of the State of Nebraska. By leveraging one of the largest fiber networks in the country, Lumen ensures rapid, secure, and seamless connection among people, data, and applications. As artificial intelligence and digital transformation evolve, public sector organizations such as the State of Nebraska require increasingly sophisticated access to data, adaptable to their dynamic needs. Lumen employs digital services, data, and analytics to drive the success of our clients in Nebraska, enabling them to achieve their objectives more efficiently. Lumen remains dedicated to investing in Nebraska, fostering innovation and growth while prioritizing the human experience.

What's New for 2026?

Lumen modernizes Nebraska's existing ESInet by introducing a managed, policy driven SD-WAN transport fabric engineered specifically for NG911 and mission critical public safety operations. Lumen deploys high availability Versa SD-WAN appliances in redundant pairs at every PSAP and NGCS hub site, creating an active, continuously monitored overlay that operates across multiple diverse underlay transports. This architecture adds real time path intelligence, application aware traffic steering, automated failover, continuous telemetry, and integrated security enforcement to the ESInet.

Benefit to the State of Nebraska: Unlike traditional static IP routing or legacy VPN designs, the SD-WAN fabric continuously evaluates latency, jitter, loss, and availability and dynamically selects the optimal path for NG911 signaling, media, and data flows. The result is an ESInet that adapts in real-time to network conditions rather than reacting after degradation occurs.

Proven NG911 Experience. Lumen is uniquely positioned to deliver a transformative Next Generation 911 (NG911) solution for the State of Nebraska, backed by a proven record of successful statewide deployments across the United States. Our experience in implementing NG911 and ESInet solutions for the States of North Dakota, South Dakota, and previously for Nebraska demonstrates our ability to deliver resilient, standards-compliant, and future-ready emergency communications platforms at scale. Lumen has extensive experience designing and implementing NG911/NGSC and ESInet solutions for multiple state partners including:

- **North Dakota:** In North Dakota, Lumen transitioned 22 PSAPs to a NENA i2-compliant NGCS and ESInet solution, integrating GIS and supporting statewide call handling enhancements. This project improved call routing accuracy, increased system reliability, and provided a more resilient emergency communications network, handling over 270,000 calls annually. Our proactive project management and collaborative approach

enabled North Dakota to exceed public safety goals and set a benchmark for regional NG911 deployments.

- **South Dakota:** In South Dakota, Lumen implemented a NENA i3 NGCS and ESInet solution across 37 PSAPs, replacing outdated infrastructure with a modern, interoperable platform. The deployment included Intrado VIPER (MECH) solutions, supporting over 340,000 calls per year. Lumen's solution enabled South Dakota to streamline emergency call processing, reduce downtime, and enhance disaster recovery capabilities—delivering a measurable increase in service reliability and operational efficiency.
- **Nebraska:** In Nebraska, Lumen's work encompassed 68 PSAPs across seven regions, deploying a NENA i3 NGCS and ESInet solution with 28 ESInet circuits. By migrating nearly one million annual emergency calls to a unified, standards-based platform, Lumen enabled Nebraska to achieve statewide interoperability, improved GIS integration, and future scalability. Our team's expertise in managing large-scale transitions ensured minimal disruption and rapid realization of benefits for public safety agencies and citizens alike.

By leveraging our experience and lessons learned from these statewide NG911 implementations, Lumen is uniquely positioned to deliver a solution for Nebraska that is resilient, scalable, and fully aligned with NENA standards. Our track record demonstrates our commitment to exceeding customer expectations, driving innovation, and delivering tangible value to public safety agencies and the communities they serve.

The Lumen Next Generation functional element architecture is depicted in **Figure 3.1-1**.

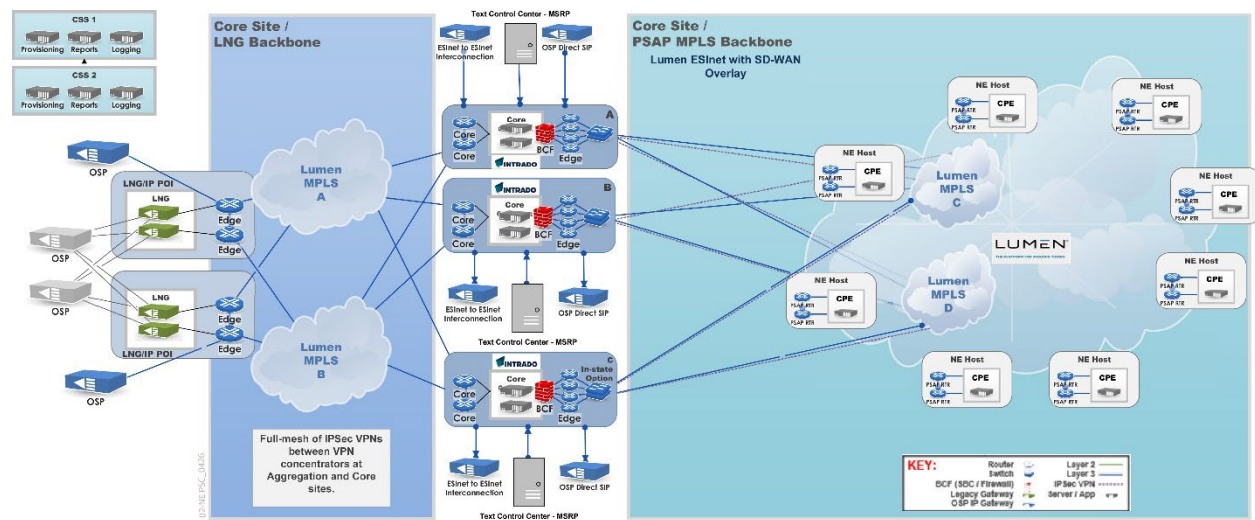


Figure 3.1-1. Lumen System Diagram.

Lumen's solution includes an architecture that is segmented into multiple areas that include Ingress (SIP), NGCS, and ESInet (Egress). This allows Lumen to create separate security zones to support each of these segments that feed into our overall management and protection policy of the NG911 solution.

Legacy Network Gateway (LNG). Lumen provides as part of its service experienced Originating Service Provider (OSP) coordinators that work with the 911 authority to manage the delivery of SIP traffic to prescribed IP Points of Interconnection (POIs) locations (NG911 Delivery Points). Where this capability cannot be met via the OSP, Lumen provides LNG

services that provide the interworking functionality Protocol (PIF), Location (LIF) and Next-Gen911 (NIF) to route emergency calls from Legacy systems to the ESInet.

Our LNG enables immediate connectivity to systems, allowing Nebraska (PSAP) connectivity to the NG911 system. The LNG is a standard component of our NG911 solution for legacy origination networks requiring TDM access.

Lumen's goal is to implement all interconnections, whether they are ingress from the OSP or egress to the PSAP's T-ESRP/CPE, to SIP/i3 as soon as possible. In support of this plan, both Lumen and our partner, Intrado, have already interconnected to multiple OSPs via IP technology and have successfully tested full i3 functionality with multiple OSPs in either Phase 1 or Phase 2 of the proposed FCC order 24-78. While it is preferable for the entire infrastructure to be deployed to IP/i3 as soon as possible, Lumen understands the migration may need to follow a phased timeline based on individual OSPs capabilities.

What's New for 2026?

Lumen transitions the ESInet underlay from legacy MPLS constructs to Lumen IP VPN, a modern, cloud ready evolution of MPLS that operates on Lumen's private backbone while supporting hybrid underlays and automation. While legacy iQ MPLS functioned primarily as a transport technology, IP VPN is delivered as an intelligent service layer that supports dynamic provisioning, elastic bandwidth scaling, and native integration with public cloud platforms. IP VPN enables scalable bandwidth options from low-capacity access links through high-capacity core connectivity while preserving deterministic performance characteristics required for NG911.

Benefit to the State of Nebraska: This underlay provides the foundation that allows the SD-WAN overlay to operate with greater flexibility, resilience, and operational efficiency than legacy MPLS only design.

NGCS Architecture. The Lumen provided NGCS components are housed together in diverse Emergency Call Processing Centers (ECMC). The reference architecture supports a minimum of two ECMCs for any given NGCS deployment; however, based on requirements Lumen has provided an in-state option with this bid. The ECMCs will interconnect with:

- Border Control Function (BCF), Session Border Controller (SBC) receives emergency voice calls, Real Time Text (RTT), MSRP, and/or requests for assistance (RFA) from Internet of Things (IoT) devices.
- This also includes NNI points of presence for ESInet-to-ESInet call exchange for hand-offs, transfers, and conferences
- Legacy Selective Router Gateway for ESInet to legacy PSTN emergency networks
- Egress ESInet connections via SD-WAN over private MPLS underlay for layer 3 IP endpoint delivery to the Call Handling equipment for the PSAP or Emergency Communications Center (ECC) within the customers covered jurisdiction. Note optional if required that we will deploy an i3-compliant Legacy PSAP Gateway (LPG) for each legacy PSAP.

The ECMCs also support:

- LIS and ADR interface to Location Databases and Additional Data Repositories for caller location and additional data about the caller and/or incident.
- DNS function to de-reference Location by Reference uniform resource locator (URL) for Held queries to the third-party location and additional data services

Figure 3.1-2 depicts an expanded view of an NGCS single core architecture.

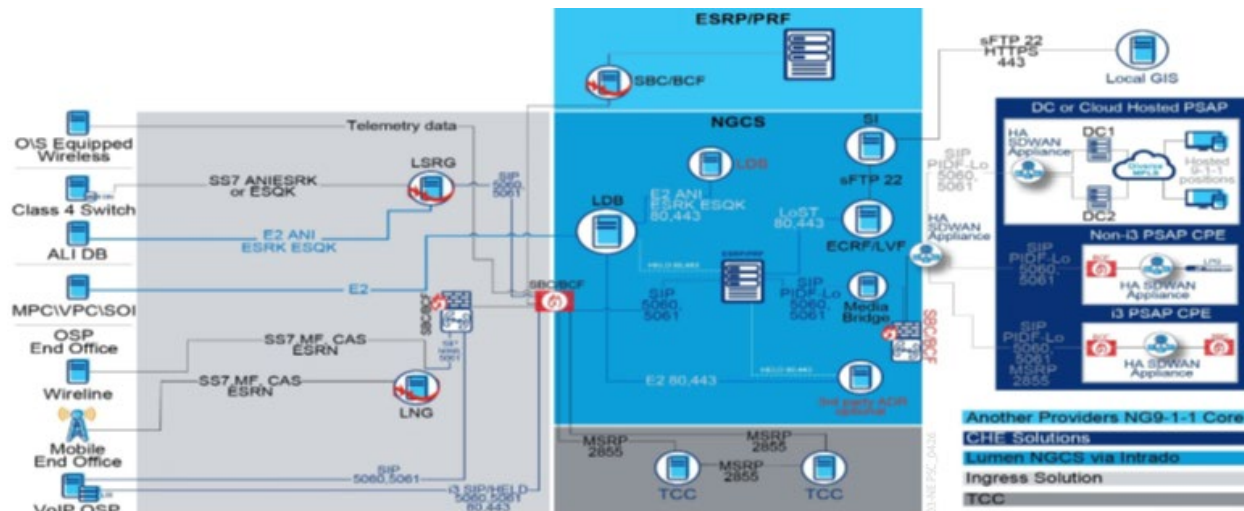


Figure 3.1-2. Lumen NGCS Single Core Architecture

Each of the geo-redundant NGCS ECMCs contains:

- Border Control Function (BCF)
- Emergency Services Routing Proxy (ESRP)
- Policy Routing Function (PRF)
- Emergency Call Routing Function (ECRF)
- Location Database (LDB) for Legacy/Transitional OSPs
- Common Support Services such as logging, reporting, database back-ups, management functions, Spatial Interface, and Location Validation Function (A minimum of two CSS sites) support each NGCS deployment.

Lumen's ESInet solution is designed with diverse entrances into each core call processing facility, e.g., data centers. PSAP connections to the ESInet are redundant, resilient, and physically diverse where possible. Primary and redundant links do not share common routes or trenches. Lumen also allows media diversity, at a minimum, to logically separate for delivery of NG911 related traffic.

Our solution is architected for multiple paths using different backbone topologies to ensure separate NNI's and core switching. Our standards-driven design and implementation involve a high degree of diversity, including independent transport networks (MPLS) and optional OTA transport, all realized through our application of SD-WAN technology.

What's New for 2026?

Lumen's NG911 ingress architecture provides a managed, scalable IP Point of Interconnection framework that supports both the State's operational requirements and the national transition to IP based 911 delivery. By transitioning OSPs from TDM to IP POIs Lumen eliminates the risk of statewide outages unless all IP POIs fail simultaneously. Lumen delivers pre-engineered, standards compliant ingress points with geographic redundancy across its nationwide backbone, secure SIP and i3 interfaces, traffic segmentation, encryption, and firewall enforcement at the ESInet boundary. This design simplifies OSP onboarding, reduces operational complexity, and ensures consistent handling of call signaling, location, and associated data.

Benefit to the State of Nebraska: The architecture supports both in state and national ingress options and preserves TDM Points of Interconnection as required by the State, while enabling OSPs to migrate to IP delivery at their discretion. By migrating OSPs to IP POIs Lumen eliminates the risk of statewide outages unless all IP POIs fail simultaneously. By decoupling ESInet modernization from OSP migration timelines, Lumen eliminates a common source of schedule risk while remaining fully aligned with FCC requirements for NG911 delivery points and NENA i3 principles.

Each core site uses redundant components of each element to allow for highly available core sites. The core architecture of the Lumen 911 solution is depicted in **Figure 3.1-3**.

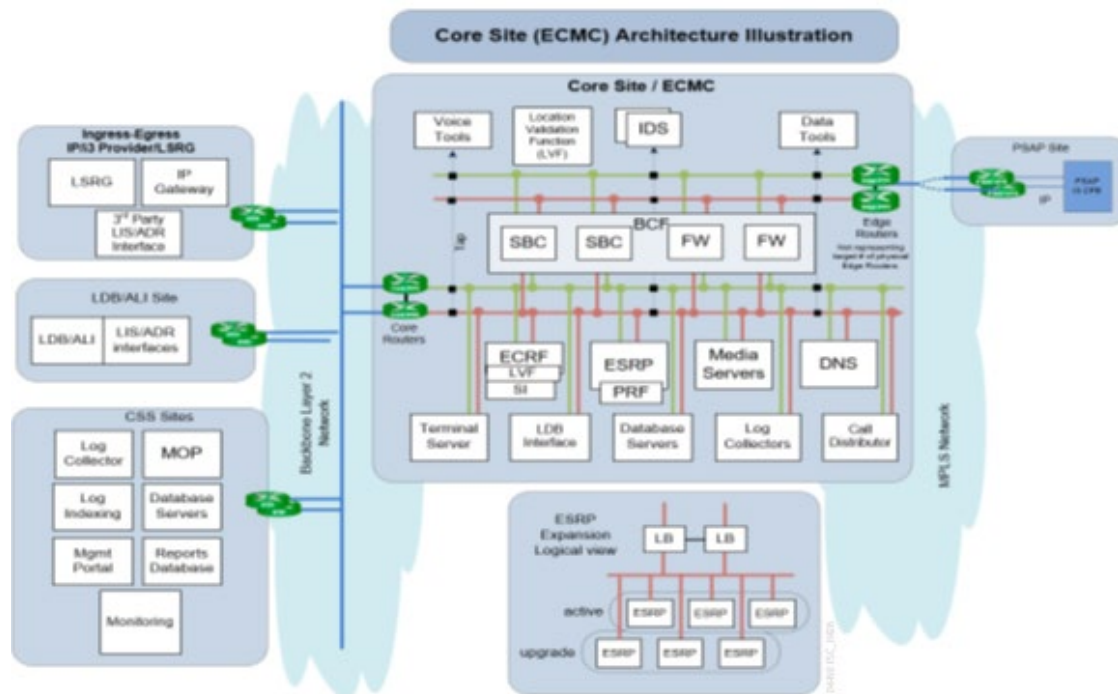


Figure 3.1-3. Core Site (ECMC) Architecture Illustration

We provide an optional Over the Air (OTA) capability that supports enabling Smart Blending technology to deliver multiple carrier 5G/LTE solutions as well as a Low Earth Orbit satellite option for hard-to-reach locations.

The proposed solutions use both bare metal appliances and virtual servers in its environment; all deployed regardless of the manner support a redundant or high-availability deployment. For example, within the NGCS all elements are not only geo-redundant via location, but these components are also deployed as pairs per ECMC. For elements that do not support this manner are dual powered, dual network interface cards (NIC) and are split over geo-redundant virtual servers. For network diversity Lumen protects each Core location for both NGCS and public safety endpoint via path diverse solutions and hardware redundancy via termination device with either SD-WAN or BCF components in a high availability (HA) configuration. In the event of not being able to provide diverse path to the

What's New for 2026?

Enabled by the SD-WAN architecture, Lumen offers optional Over The Air (OTA) connectivity to protect PSAP operations during events that impact terrestrial infrastructure. These options bypass fiber, copper, and traditional last mile dependencies and provide continuity during fiber cuts, carrier outages, severe weather, power loss, wildfires, floods, or physical damage. Over the air paths operate as fully integrated tertiary or quaternary underlays within the SD-WAN fabric and participate in the same real time path scoring and traffic steering logic as terrestrial circuits.

Benefit to the State of Nebraska:

Wireless Continuity Without Carrier Dependency. Lumen Managed Multi-Connect aggregates multiple LTE and 5G wireless providers to sustain NG911 signaling and PSAP operations during wireless outages or congestion.

Regional Resilience Beyond Terrestrial Networks. Starlink Low Earth Orbit (LEO) connectivity enables NG911 continuity during large-scale infrastructure failures and operates as a managed SD-WAN path with automatic failover.

PSAP or public safety endpoint, Lumen recommends using a common access provider to diverse network POP locations as well as adding a tertiary over-the-air solution such as Low Earth Orbit (LEO) Satellite or 5G/LTE solution.

Figure 3.1-4 depicts the proposed ESInet architecture.

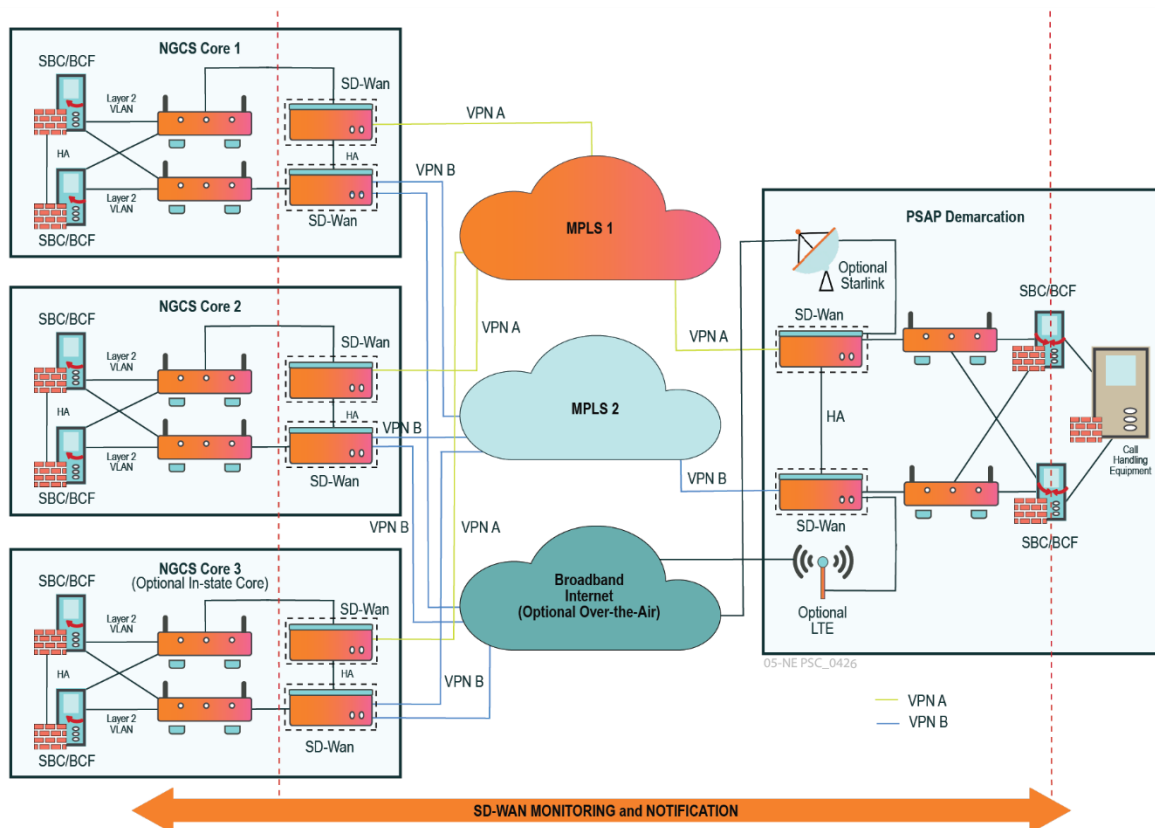


Figure 3.1-4. Lumen ESInet Architecture Design

Open Standards Interoperability. Lumen employs a forward-thinking strategy in developing NG911 solutions, emphasizing the use of published and open standards for all application interfaces. This commitment to open standards ensures Lumen solutions are interoperable, adaptable, and future-ready, allowing seamless integration with various systems and technologies prevalent in NG911 environments.

Interoperability is vital for NG911 systems, facilitating effective communication among different components and entities within the emergency communication ecosystem. By leveraging open standards, Lumen solutions effortlessly exchange data and interact with other systems, such as CAD (Computer-Aided Dispatch) systems, GIS (Geographic Information System) platforms, and other emergency response tools. By utilizing published and open standards Lumen enables interoperability with neighboring ESInets for ESInet to ESInet transfers to other states.

Flexibility is another key aspect of NG911, as emergency response systems must adapt to evolving technological landscapes and changing requirements. Open standards enable our software to be easily customized and tailored to specific customer needs, ensuring it meets the unique demands of various emergency response agencies. Lumen utilizes universal CPE (uCPE) appliances where it is possible to provide a scalable approach to software defined networking applications throughout the ESInet.

Furthermore, Lumen's adherence to open standards in software development guarantees that our solutions are future proof. This approach ensures our solutions remain relevant and functional as technology advances and new standards emerge, minimizing the risk of obsolescence and maximizing the long-term value of our NG911 solutions.

The proposed system is designed for seamless scalability, capable of handling increasing data volumes without sacrificing performance. It is engineered to withstand component failures without causing system-wide disruptions.

Lumen SD-WAN appliances for this implementation will support two configurations based on throughput requirements at each location. These will be segmented into Medium and Large appliances; large appliances will be reserved for hub sites and or larger public-safety endpoints. These appliances have two hardware profiles that are considered uCPE for the Versa software deployments, focusing on Advantech FWA-2320 for medium appliance and Advantech FWA-3260 for the large appliances.

The proposed design meets all applicable standards for i3 emergency call routing. Certain items such as OCIF EIDO and Forest Guide are supported but may be used in limited scope based on update requirements in the applicable standard.

The solution provides a secure IP-based network with no single point of failure. The proposed core solution is deployed across data centers located at highly secured facilities throughout the country. Each i3 element has multiple instances within a single core to provide redundancy for that core. The same redundant configuration is replicated at each of the six geo-diverse core sites.

The Lumen solution and NGCS core aggregation sites use the same design approach of redundancy within each individual site mirrored at the other sites. All vital system components are protected using redundant modules to eliminate any single point of failure. Transactions or call traffic are diverted 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 solution 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.

High-Availability Configuration. 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.

High-Availability - No Single Point of Failure

Our solution delivers a highly reliable emergency services IP network with **99.999%** uptime, ensuring uninterrupted call processing and eliminating any single point of failure.

Our networks are known for reliability, security, and redundancy. We use a private, high-speed, MPLS IP backbone, not the public Internet, for transmission; 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. The core routing and intelligence of the solution provides the State with immediate scalability in call routing and data delivery. The Core network and NG911 services are designed to support very large volumes with geographic diversity of the core processing centers.

Proactive 24x7x365 Monitoring. Lumen provides 24x7x365 monitoring of the 911 network and equipment. For security purposes, we do not allow outside vendor/customer access to monitoring equipment; however, we provide real-time reporting capabilities as well as access to the NOC for real-time updates on network and equipment health, including 24x7x365 monitoring and Denial of Service mitigation tools. monitoring of the core network for traffic anomalies and shared resource consumption thresholds is performed to protect the core network and assure that traffic storms do not impact the performance of other customers.

Proactive 24x7x365 Monitoring and Real-Time Reporting

The State will benefit from real-time reporting capabilities as well as access to the NOC for real-time updates on network and equipment health, including 24x7x365 monitoring and Denial of Service mitigation tools.

OSP Interconnections. Lumen implements session border control at all ESInet boundaries, including interconnections with Originating Service Providers (OSPs), PSAPs, NGCS platforms, and inter-ESInet peers. Session Border Control Functions (SBCFs) enforce security policies, protocol normalization, and traffic protection consistent with NENA i3 functional requirements, supporting secure SIP signaling and media transport across all interfaces.

Lumen supports tenant isolation and traffic segregation through virtual routing, logical segmentation, or equivalent technologies to ensure emergency services traffic is isolated from non-emergency or non-NG911 traffic. This design enables secure multi-tenant operations while preserving interoperability and compliance with NENA i3 standards.

Lumen engineers scalable bandwidth provisioning across ESInet access, aggregation, core, and interconnection points. Bandwidth capacity is designed to support current and forecasted NG911 call volumes, peak traffic conditions, and future multimedia services. Quality of Service (QoS) mechanisms prioritize emergency communications to maintain consistent performance under all operating conditions.

Lumen designs the ESInet with a focus on high availability and reliability, incorporating carrier-diverse access paths, redundant power and environmental controls, fault-tolerant network components, and continuous monitoring. These features enable rapid fault detection, isolation, and restoration to maintain uninterrupted NG911 service delivery.

Lumen produces comprehensive ESInet documentation, including detailed architecture diagrams depicting bandwidth provisioning, core redundancy, boundary elements, tenant isolation, and availability and reliability features. Transitional and end-state diagrams, along with as-built documentation, are delivered in accordance with project milestones and acceptance requirements to clearly demonstrate conformance with NENA i3 architecture and functional requirements.

Extensive Public Safety Experience. Lumen's portfolio includes secure, highly available, IP-based voice and data services delivered over one of the world's largest and most deeply peered fiber networks. This network foundation enables the reliable transport of emergency services traffic while supporting geographic redundancy, diversity, and interoperability across PSAPs, originating service providers, and interconnecting ESInets.

Through decades of service to public safety customers, Lumen has established physical and operational interconnections with the majority of carriers, vendors, and NG911 ecosystem partners across the United States. This broad interconnection experience allows Lumen to support multi-vendor, standards-based environments consistent with NENA i3 architecture, while facilitating coordinated testing, system turn-up, and integration activities required to operationalize Nebraska's NG911 solution.

Architecture Design Summary: Lumen's approach does not replace Nebraska's NG911 system. It modernizes an already operational ESInet and NGCS environment by layering SD-WAN intelligence, IP VPN flexibility, over the air resilience, and a mature national ingress framework onto an incumbent, proven foundation. This combination delivers measurable improvements in resiliency, visibility, and operational control while avoiding the disruption, risk, and extended timelines associated with greenfield NG911 deployments.

- b. *Contractor shall support IPv4 and IPv6 addressing, implement Quality of Service (QoS) (DiffServ or equivalent) to prioritize emergency signaling and media, and document bandwidth and capacity needs for all services. (This includes referenced 99.999 requirements that will be included in the Service Level Agreement (SLA)).*

LUMEN RESPONSE:

Lumen supports both IPv4 and IPv6 addressing throughout the ESInet, enabling seamless interconnection with Originating Service Providers (OSPs), PSAPs, NGCS platforms, and inter-ESInet peers. Dual-stack capability ensures compatibility with legacy environments while supporting the State's long-term transition to IPv6 in accordance with NENA i3 architectural guidance.

Lumen implements Quality of Service (QoS) mechanisms, including Differentiated Service Code Point (DSCP/DiffServ) or equivalent technologies, to prioritize NG911 signaling and media traffic across the ESInet. Emergency call signaling, media streams, and associated control traffic are classified and prioritized to ensure predictable performance, low latency, and minimal packet loss during normal operations and peak traffic conditions.

Lumen engineers the ESInet to support consistent traffic prioritization end-to-end, including access, aggregation, core, and interconnection segments. QoS policies are designed to preserve emergency communications integrity even during periods of network congestion or abnormal traffic patterns.

Lumen documents bandwidth and capacity requirements for all ESInet-supported services, including core connectivity, PSAP access, NGCS interconnections, and external peering points. Capacity planning accounts for current call volumes, peak load scenarios, geographic diversity, and projected growth, including support for future NG911 multimedia services. This documentation is provided as part of the ESInet design and maintained throughout the system lifecycle.

Lumen aligns ESInet performance objectives with the availability and reliability requirements referenced in the Service Level Agreement (SLA), including **99.999%** service availability for applicable core network components. The ESInet design incorporates redundancy, traffic prioritization, proactive monitoring, and fault-tolerant architectures to support these availability targets.

Lumen commits to measuring, monitoring, and reporting performance metrics associated with QoS, bandwidth utilization, and availability in accordance with SLA requirements. These

capabilities ensure transparency, accountability, and continuous service assurance for Nebraska's NG911 operations.

- c. *Contractor shall support SIP signaling per RFC 3261 and required NG911 SIP extensions (SIP over TLS for signaling, and SRTP for media, where used), and demonstrate SIP interconnects with external peers. (This includes SIP call flow across the ESInet, no calls "lost," and conversion where necessary).*

LUMEN RESPONSE:

Lumen supports Session Initiation Protocol (SIP) signaling in accordance with RFC 3261 and all required NG911 SIP extensions as defined by NENA i3 standards. The ESInet is engineered to support SIP-based call setup, control, and teardown for NG911 services across all core, access, and interconnection segments.

Lumen implements SIP over Transport Layer Security (TLS) for signaling and Secure Real-Time Transport Protocol (SRTP) for media, where used, to protect NG911 communications from unauthorized access, interception, or tampering. These security mechanisms are applied consistently across ESInet boundaries and interconnection points in alignment with NG911 security best practices and standards.

Our personnel enable SIP interconnects with external peers, including Originating Service Providers (OSPs), NGCS platforms, PSAPs, and inter-ESInet partners. Interconnections are established using standards-based SIP interfaces and boundary controls to support multi-vendor interoperability and seamless call delivery across organizational and network domains.

We validate end-to-end SIP call flows across the ESInet, ensuring that emergency calls traverse the network reliably without call loss. Call processing is designed to maintain session integrity across redundant paths, boundary elements, and failover scenarios so that no calls are dropped or misrouted during normal operations or fault conditions.

Our team performs protocol normalization and conversion where necessary to support interoperability between legacy systems and NG911-compliant SIP environments. These capabilities ensure that calls originating from non-IP or transitional networks are properly converted and delivered into the ESInet without disruption to emergency services.

Lumen documents SIP call flows, interconnection architectures, and boundary control functions as part of the ESInet design and implementation deliverables. Documentation demonstrates compliance with RFC 3261, required NG911 SIP extensions, and secure call handling requirements, providing transparency and assurance of standards-based operation.

- d. *Contractor shall provide documented peering and interconnect interfaces (LNG, LSRG, LPG, SBCs and other edge elements, Points of Interconnection) and APIs and procedures for peering with other ESInets and third-party providers. (Configuration management database, diagrams, IP-schema).*

LUMEN RESPONSE:

Lumen provides documented peering and interconnect interfaces that support connectivity across the full NG911 ecosystem, including Legacy Network Gateways (LNG), Legacy Selective Router Gateways (LSRG), Legacy PSAP Gateways (LPG), SBCs, other edge elements, and designated Points of Interconnection (POIs). These interfaces are designed and implemented in accordance with NENA i3 architecture to support interoperable, multi-vendor ESInet and NGCS environments.

We deliver standards-based interconnection architectures that enable peering with neighboring ESInets, Originating Service Providers (OSPs), and third-party service providers.

Our interconnect designs support SIP-based signaling and media transport, boundary security enforcement, and traffic normalization to ensure seamless and secure exchange of NG911 traffic across organizational and network boundaries.

We support ESInet-to-ESInet peering through clearly defined technical interfaces, operational procedures, and governance controls. These peering arrangements enable call routing, transfer, conferencing, and data exchange across ESInets while maintaining session integrity, routing accuracy, and compliance with NENA i3 functional requirements.

Lumen documents all peering and interconnect configurations as part of the ESInet design and implementation deliverables. Documentation includes detailed network diagrams, logical and physical topology representations, boundary element placement, and Points of Interconnection to clearly illustrate how traffic enters, exits, and traverses the ESInet.

We maintain a configuration management database (CMDB) that records ESInet interconnect components, interfaces, IP addressing schemas, routing relationships, and dependency mappings. This information supports operational visibility, change management, troubleshooting, and auditability throughout the NG911 system lifecycle.

We define and publish IP addressing schemas and interface specifications for all ESInet peering and interconnection points, including internal segmentation and external peer connectivity. Addressing plans are designed to support scalability, tenant isolation, and interoperability while aligning with IPv4 and IPv6 requirements.

Lumen establishes documented APIs and operational procedures to support peering with other ESInets and third-party providers. These procedures define onboarding, testing, validation, change control, and operational coordination processes to ensure consistent, repeatable, and secure interconnection activities.

We ensure that all peering and interconnect documentation remains current and reflects both transitional and end-state architectures, providing the State with a clear, authoritative reference for operational management, future expansion, and inter-jurisdictional collaboration.

Please see **Attachment 5** for our interface documents.

3.2. NG911 Core Services (NGCS)

- a. Contractor shall provide or interoperate with NGCS functional elements (BCF, ESRP, ECRF, LVF/LIS, MSAG/ALI-equivalent services, ESRP/ESRP-like routing proxy, etc.) as defined in the NENA i3 Standard and shall map which product components implement each NGCS function.
- b. Contractor shall implement NGCS interfaces per the NGCS Interface Standard (SIP and REST interfaces, expected message formats including PIDF-LO where applicable) and shall provide interface documentation, schemas, and test harness endpoints.
- c. Contractor shall meet stated latency and throughput SLAs for NGCS lookups and routing decisions. (99.999 from caller to call-taker unless specified in writing between the PSC and Contractor.)

LUMEN RESPONSE:

a. NGCS Functional Elements and Component Mapping. Lumen provides and interoperates with all required NGCS functional elements as defined in the NENA i3 Standard and supports both end-state and transitional NG911 environments for the State of Nebraska. Our NGCS architecture replaces legacy selective routing and ALI functions with standards-based, IP-native services while maintaining interoperability with

originating service providers, neighboring NGCS domains, and PSAP call-handling systems.

The Border Control Function (BCF) is implemented using NG911-grade session border control components that enforce SIP protocol normalization, topology hiding, admission control, and media security at all ESInet, OSP, and inter-NGCS boundaries. These components provide protection against malformed signaling, denial-of-service conditions, and unauthorized access while preserving emergency call priority handling consistent with NENA i3 requirements.

Emergency Services Routing Proxy (ESRP) functionality is implemented through policy-driven routing proxies that form the NGCS call path. These proxies are responsible for emergency call intake, policy evaluation, controlled call forwarding, and automatic failover to alternate routing paths or PSAP destinations. ESRP behavior is fully aligned with NENA i3 call flow models and supports both primary and secondary routing scenarios.

The Emergency Call Routing Function (ECRF) is implemented as a LoST-based routing engine that uses authoritative Nebraska GIS data to determine the appropriate PSAP or agency destination based on the caller's civic or geodetic location. Routing decisions are derived exclusively from authoritative data and policy, ensuring deterministic and auditable call delivery.

Location validation is provided through an independently implemented Location Validation Function (LVF) that shares a common GIS provisioning pipeline with the ECRF while remaining isolated from the live call-routing path. This design allows location objects to be validated without introducing latency or risk to active emergency call processing.

Location Information Server (LIS) functionality supports both location-by-value and location-by-reference workflows and provides standards-compliant PIDF-LO objects for use by originating networks, NGCS elements, and PSAP systems. Legacy MSAG and ALL-equivalent services are implemented through NGCS location database services that support traditional query mechanisms (such as ANI, ESRK, and ESQK) while remaining fully aligned with NENA i3 data models and GIS-based routing.

Each NGCS functional element is explicitly mapped to a deployed product or service component within Lumen's Nebraska NG911 solution. This functional mapping is documented and provided to the Nebraska Public Service Commission as part of the NGCS design and implementation documentation.

b. NGCS Interfaces, Message Formats, and Test Support. Lumen implements NGCS interfaces in accordance with the NGCS Interface Standard and supports the full range of SIP-based and REST-based interactions required for NG911 call processing, routing, and location services within Nebraska.

SIP interfaces are used for emergency call setup, routing, transfer, and termination between originating service providers, NGCS functional elements, and PSAP call-handling systems. These interfaces support emergency service URNs, priority handling, and standards-based media negotiation consistent with NENA i3 call flows.

REST-based interfaces are implemented where defined by NGCS interface specifications, including LoST interfaces for ECRF and LVF queries and HELD-based interfaces for LIS

interactions. All location exchange uses PIDF-LO objects, supporting both civic and geodetic representations and conforming to applicable NENA schemas.

Lumen provides comprehensive NGCS interface documentation to the State of Nebraska and authorized interconnecting parties. This documentation includes interface descriptions, message schemas, request and response examples, call flow diagrams, and error handling expectations. To support onboarding, interoperability validation, and regression testing, Lumen also provides controlled test harness endpoints that allow originating networks and neighboring NGCS operators to validate SIP signaling, LoST queries, location handling, and failover behavior prior to the introduction of live emergency traffic.

c. NGCS Latency, Throughput, and Availability SLAs. Lumen meets the State of Nebraska's stated performance and availability requirements for NGCS operations. The NGCS is engineered to support end-to-end emergency call processing with **99.999%** availability from caller to call-taker, unless otherwise specified in writing between the Nebraska Public Service Commission and Lumen.

NGCS lookup and routing functions, including ECRF, LVF, and LIS services, are designed for low-latency response and high throughput through the use of redundant, geographically diverse service instances, load-balanced query handling, and optimized spatial indexing for GIS-based routing decisions. Routing and validation services operate in an active/active configuration, enabling automatic failover without manual intervention or service interruption.

Performance metrics for NGCS transactions, including lookup latency, routing success rates, and availability, are continuously monitored and logged. SLA adherence is measured and reported in accordance with Nebraska NG911 operational oversight requirements, providing transparency and auditability for both operational and governance purposes.

3.3. GIS and Location-Based Routing

- a. Contractor shall accept, store, and use GIS data in the NENA GIS data model/schema and SHALL maintain the required NENA layers (PSAP boundaries, ESN/service boundaries, address points, civic addressing, emergency routing attributes). GIS data shall conform to normative language identified in NENA-STA-006.2-2022. The Contractor may utilize NENA-REF-006.2-2023 (NENA NG9-1-1 GIS Data Model Templates) to assist in conformance to the Standard.
- b. Contractor shall use authoritative GIS data for routing decisions (ECRF) and shall accept location in PIDF-LO format (and convert civic/geodetic input) for routing and display.
- c. Contractor shall provide GIS data versioning, change tracking, import/export in NENA formats (e.g., GML/GeoJSON or NENA schema), and support automated incremental updates.

LUMEN RESPONSE:

a. GIS Data Model, Required Layers, and Standards Conformance. Lumen accepts, stores, and uses GIS data that conforms to the NENA GIS Data Model and Schema as defined in NENA-STA-006.2-2022, and maintains all required NG911 GIS layers necessary to support location-based routing for the State of Nebraska. The NG911 GIS repository is implemented as a managed, standards-based geospatial environment designed specifically to support ECRF and LVF operations within an i3 architecture.

The maintained GIS layers include, at a minimum, PSAP boundaries, ESN or emergency service boundaries, address points, civic addressing elements, and emergency routing attributes. These layers are stored and managed in a manner consistent with the normative

language of NENA-STA-006.2-2022 and are provisioned for direct use by NGCS functional elements without manual translation or proprietary transformation. Where appropriate, Lumen utilizes the NENA-REF-006.2-2023 NG9-1-1 GIS Data Model Templates as an implementation aid to support schema alignment and data consistency while preserving Nebraska's authoritative data governance.

GIS data quality and integrity checks are applied as part of the provisioning process to ensure that submitted data complies with applicable NENA standards and is suitable for use in live emergency call routing. The solution is designed to integrate Nebraska-provided and PSAP-provided GIS data without interfering with existing local GIS management responsibilities or vendor relationships.

b. Authoritative GIS Use and Location Handling for Routing and Display. Lumen uses authoritative GIS data as the sole basis for emergency call routing decisions performed by the Emergency Call Routing Function (ECRF). Routing outcomes are derived from spatial analysis of authoritative Nebraska GIS layers, ensuring that calls are delivered to the correct PSAP or emergency service agency based on the caller's validated location.

The NGCS solution accepts location information conveyed in PIDF-LO format, including both civic and geodetic representations, and supports the conversion of civic and geodetic inputs as required for routing and display. Location objects may be validated through the Location Validation Function (LVF) prior to routing, and validated location information is made available to downstream NGCS elements and PSAP systems using standardized NG911 interfaces.

Location information is delivered to PSAP call-handling equipment and mapping clients using NENA-compliant interfaces and formats, supporting both push and pull mechanisms consistent with the NENA i3 architecture. This approach ensures consistent and accurate location presentation across call processing, mapping, and dispatch workflows within Nebraska's NG911 environment.

c. GIS Versioning, Change Tracking, and Data Exchange. Lumen provides comprehensive GIS data lifecycle management through its Enterprise Geospatial Database Management System (EGDMS), which serves as the centralized intake, validation, and provisioning platform for NG911 GIS data. EGDMS supports version control, change tracking, and full auditability of GIS updates, including time stamped data submissions, historical snapshots, and rollback capabilities to maintain operational integrity and governance.

EGDMS consumes GIS data directly from authoritative state, regional, and local GIS data sources via a secure, web-based data submission interface. Authoritative entities upload GIS datasets in supported NENA formats and schemas, after which EGDMS performs automated QA/QC validation, schema and field mapping, and consistency checks to identify attribute errors, formatting issues, and spatial conflicts (e.g., gaps or overlaps). Validated datasets are versioned and staged prior to activation to ensure routing stability and prevent service impacts.

The solution supports import and export of GIS data using NENA supported formats, including GML, GeoJSON, and NENA defined schemas, enabling standardized data exchange across jurisdictions. EGDMS also supports automated incremental updates, allowing authoritative data sources to submit routine or event driven changes without requiring full dataset replacement. Once validated, updates are automatically

provisioned to NG911 functional elements (e.g., ECRF/LVF) while preserving prior production versions for rollback if required.

3.4. Call Flow and Media Session Handling

- a. Contractor shall implement NENA i3 call flows (incoming SIP INVITE → ESRP/ECRF lookup → PSAP routing) preserving required SIP headers (P-Asserted Identity, Diversion, History Info, etc.) and shall deliver PIDF-LO location payloads with calls where required.
- b. Contractor shall support real-time multimedia as defined by NENA (voice, IP text-to-911, real-time video, and supplemental data) with media negotiation, fallback behaviors, and preservation of metadata across transfers.
- c. Contractor shall support PSAP call transfer (warm or attended and blind transfers) while preserving call metadata and location.

LUMEN RESPONSE:

a. NENA i3 Call Flow Implementation and SIP/Location Handling. Lumen implements NENA i3-compliant call flows for emergency calls entering the Nebraska ESInet, including the standardized progression from receipt of an incoming SIP INVITE, through ESRP policy handling and ECRF routing lookup, to final delivery at the appropriate PSAP. Call processing follows the normative i3 sequencing and decision points to ensure deterministic routing behavior and interoperability with originating service providers and PSAP call-handling systems.

SIP signaling is processed and forwarded in a manner that preserves all required SIP headers, including but not limited to P-Asserted-Identity, Diversion, and History-Info headers, as calls traverse NGCS functional elements. Header integrity is maintained across routing decisions, transfers, and failover scenarios to ensure continuity of call identity, routing context, and auditability.

Where required by call type or originating network, PIDF-LO location payloads are delivered with the call and conveyed through the NGCS to the PSAP. Location information (P-Asserted Identity, Diversion, History Info, and other applicable NENA i3 signaling elements) is preserved end-to-end and made available to downstream elements without loss, truncation, or proprietary alteration, consistent with NENA i3 location conveyance expectations.

b. Real-Time Multimedia and Supplemental Data Support. Lumen supports real-time multimedia communications as defined by NENA, enabling voice, IP-based text-to-911, real-time video, and supplemental data to be conveyed through the Nebraska NG911 environment. Media sessions are established using standards-based negotiation mechanisms to ensure compatibility between originating networks, NGCS elements, and PSAP systems.

Media negotiation includes defined fallback behaviors to allow calls to continue in an alternate supported media mode if a requested media type cannot be sustained end-to-end. Throughout call processing and any subsequent transfers, associated metadata—including call identifiers, location information, and supplemental data—is preserved and conveyed alongside the media streams.

Supplemental data associated with the emergency call is maintained in context with the call session and remains accessible to PSAP personnel as the call progresses, transfers,

or is conferenced, ensuring that critical information is not lost or disassociated during NG911 call handling.

c. PSAP Call Transfer with Metadata and Location Preservation. Lumen supports PSAP call transfer operations, including both attended (warm) transfers and blind transfers, in accordance with NENA i3 call handling models. Transfers are executed in a manner that preserves the integrity of the original call session while enabling the receiving PSAP or agency to obtain full situational context.

During transfer, call metadata and location information are preserved and conveyed to the receiving party, including original caller identity, call history, and validated PIDF-LO location data. This ensures that transferred calls arrive with complete context and do not require re-querying or revalidation to continue effective call handling.

Transfer behavior is designed to support both routine inter-PSAP coordination and exceptional routing scenarios, while maintaining continuity of call data and adherence to Nebraska's NG911 operational expectations.

3.5. Security, Privacy, and Trust

- a. *Contractor shall implement the NENA ESInet security and trust model including mutual TLS between NG911 elements, strong authentication and RBAC for administrative interfaces, and secure boundary elements (SBCs).*
- b. *Contractor shall encrypt sensitive data in transit (TLS 1.2+ / TLS 1.3) and at rest (AES-256 or equivalent), provide PKI/certificate lifecycle management, and protect cryptographic keys using a hardware security module or equivalent. Contractor shall support certificate revocation.*
- c. *Contractor shall provide incident response and vulnerability management processes and supply recent third-party penetration test reports and remediation plans.*
- d. *Contractor shall satisfy Neb. Rev. Stat. 86-125 by completing the affidavit provided by the State regarding the use of prohibited communications equipment by communications providers.*

LUMEN RESPONSE:

a. ESInet Security and Trust Model. Lumen's ESInet is aligned with the NENA ESInet security and trust model and applies a layered security architecture to protect NG911 services. Secure boundary elements, including Session Border Controllers (SBCs), are deployed to enforce trust boundaries, control access, and protect SIP signaling and media flows between interconnected NG911 systems and external networks.

Mutual TLS is used at ESInet trust boundaries and external interconnection points, where required to establish trust with interconnected NG911 systems, service providers, and external entities. Within the internal ESInet environment, Lumen employs alternative compensating security controls consistent with NENA guidance, including network isolation, strict access controls, strong authentication, and continuous monitoring to protect communications between functional elements.

Administrative access to ESInet and NG911 components is secured using strong authentication mechanisms and role based access control (RBAC), ensuring that only authorized personnel can access system resources. These controls collectively provide confidentiality, integrity, and availability protections consistent with the intent of the NENA ESInet security and trust framework.

b. Encryption, PKI, and Key Management. Lumen encrypts sensitive data in transit using industry-standard cryptographic protocols, including TLS 1.2 or higher (including

TLS 1.3), to protect SIP signaling, APIs, and data exchanges between NG911 elements. Sensitive data at rest is protected using strong encryption mechanisms such as AES-256 or equivalent, ensuring confidentiality of stored call data, location information, and system records.

A managed public key infrastructure (PKI) is used to support certificate issuance, renewal, expiration, and revocation for NG911 components. Certificate lifecycle management processes are in place to maintain trust continuity and support rapid response to compromise scenarios. Cryptographic keys are protected using hardware security modules (HSMs) or equivalent secure key management technologies, preventing unauthorized access or extraction of private key material. Certificate revocation mechanisms are supported to invalidate credentials promptly when required.

c. Incident Response and Vulnerability Management. Lumen maintains formal incident response and incident response processes applicable to NG911 systems supporting Nebraska. These processes include continuous monitoring for security events, defined escalation and containment procedures, and coordinated response actions to mitigate operational or data security risks.

Vulnerability management activities include routine assessment, prioritization, and remediation of identified weaknesses. Lumen supports independent security validation by conducting third-party penetration testing and provides the State with recent penetration test reports and associated remediation plans, demonstrating both identified findings and corrective actions taken to address them.

Please see **Section 5.8.3.2** for further details of our incident response and vulnerability management capabilities and approach.

d. Nebraska Statutory Compliance (Neb. Rev. Stat. § 86-125). Lumen complies with Neb. Rev. Stat. § 86-125 regarding the use of prohibited communications equipment by communications providers. When provided, Lumen will complete and submit the State's affidavit affirming compliance with the statute and attesting that prohibited communications equipment is not used in the provision of services to the State of Nebraska's NG911 environment.

This statutory compliance is treated as a mandatory contractual obligation and is maintained throughout the term of service delivery.

3.6. Logging, Reporting, and Call Detail Records

- a. Contractor shall produce end-to-end logs and Call Detail Records (CDRs) for every emergency transaction containing timestamps and share with the data analytics engine, correlation IDs, call identifiers, caller identity (if available), location used for routing, PSAP destination, media-types, and call disposition.
- b. Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats.
- c. Contractor shall provide operational reports (call volume, answer times, transfers, location failure rates, outage reports) and support ad-hoc queries.

LUMEN RESPONSE:

a. End-to-End Logging and Call Detail Records. Lumen produces end-to-end logs and Call Detail Records (CDRs) for every emergency transaction processed within the Nebraska NG911 environment. Logging and CDR generation span the full lifecycle of the

call, from ingress at the ESInet boundary through routing, delivery, transfer, and termination, ensuring complete transactional visibility.

Each log record and CDR includes the required operational and analytic elements necessary for correlation, auditing, and performance analysis, including timestamps, correlation identifiers, call identifiers, caller identity when available, the location object used for routing, PSAP destination, media types involved, and final call disposition. These records are structured to support ingestion by the State's designated data analytics engine and to enable cross-system correlation across NGCS functional elements. **Figure 3.6-1** provides an example of our NGCS CDR capabilities.

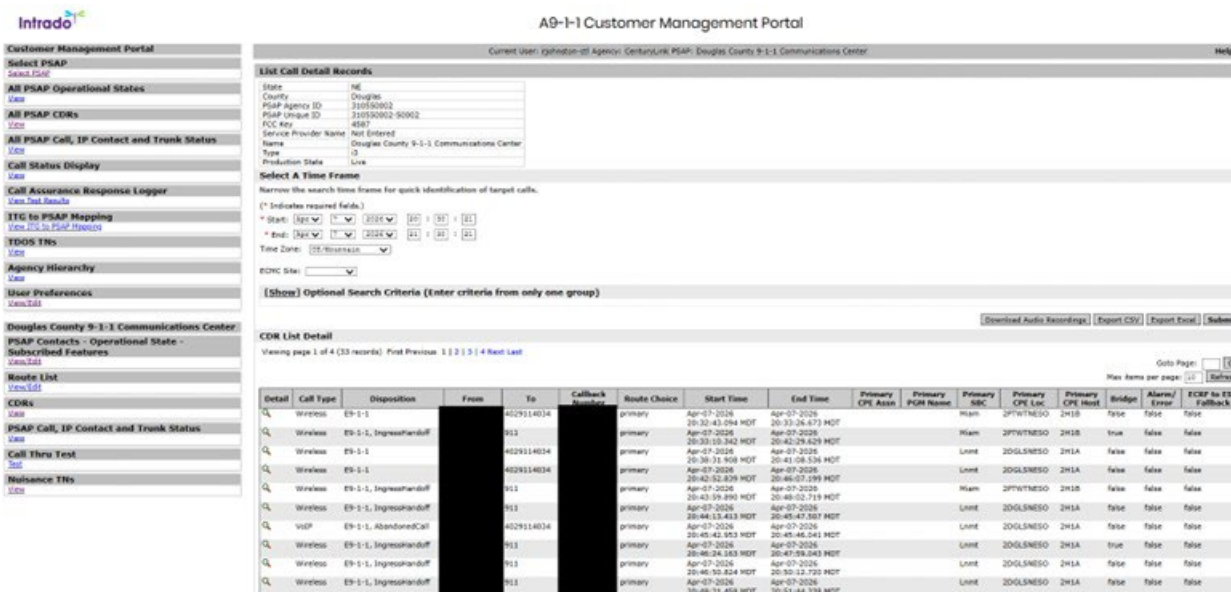


Figure 3.6-1. Individual CDRs by Date/Time

b. Secure Storage, Access Control, and Export of Logs and CDRs. Lumen provides secure storage for logs and CDRs generated by NG911 systems supporting Nebraska. Stored records are protected through role-based access controls that restrict visibility and administrative actions to authorized personnel based on assigned roles and responsibilities.

Access to log and CDR data is governed by least-privilege principles and supports separation of operational, administrative, and audit functions. Logs and CDRs may be exported in open, non-proprietary formats, enabling independent analysis, regulatory review, and integration with external reporting or analytics tools without vendor lock-in.

c. Operational Reporting and Ad-Hoc Query Support. Lumen provides operational reporting capabilities that enable visibility into NG911 service performance and operational health for the State of Nebraska. Standard reports support key operational metrics such as call volume, answer times, call transfers, location validation or routing failure rates, and outage or degradation events.

In addition to standard reports, the solution supports ad-hoc query capabilities, allowing authorized users to analyze logs and CDRs dynamically to investigate specific incidents, trends, or performance questions. This reporting and query framework supports both routine operational oversight and exception-based analysis, ensuring that Nebraska stakeholders have timely and actionable insight into NG911 system behavior. **Figure**

3.6-2 provides an example of our incident CDR reports available through the Intrado NGCS management portal.

The screenshot displays the Intrado A9-1-1 Customer Management Portal. The left sidebar contains navigation links such as 'Select PSAP', 'All PSAP Operational States', 'All PSAP CDRs', 'All PSAP Call, IP Contact and Trunk Status', 'Call Status Display', 'Call Assurance Response Logger', 'ITG to PSAP Mapping', 'TDOS TNS', 'Agency Hierarchy', 'User Preferences', 'Route List', 'CDRs', 'PSAP Call, IP Contact and Trunk Status', 'Call Thru Test', and 'Nuisance TNS'. The main content area is titled 'A9-1-1 Customer Management Portal' and shows details for a PSAP in Nebraska. The 'Operational State' tab is active, displaying fields for State (NE), County (Douglas), PSAP Agency ID (310550002), PSAP Unique ID (310550002-50002), FCC Key (4587), Service Provider Name (Not Entered), Name (Douglas County 9-1-1 Communications Center), Type (3), and Production State (Live). The 'Subscribed Features' tab is also visible, showing options for Normal, Abandoned, and Backup Routing. The 'No Answer Disconnect Timeout' is set to 45 seconds. The 'Call Processing Feature Subscriptions' are listed as None.

Figure 3.6-2. PSAP State Configurable CDR Options

3.7. Interoperability, Testing, Conformance, and System Acceptance

- Contractor shall participate in jurisdiction-specified interoperability and conformance testing, independent third-party validation and verification, demonstrate NGCS and ESInet interfaces in a test harness, and provide test results and logs.
- Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals.

LUMEN RESPONSE:

a. Interoperability, Conformance, and Validation Testing. Lumen participates in jurisdiction-specified interoperability and conformance testing as required by the State of Nebraska to validate NG911 service readiness and standards compliance. This participation includes coordinated testing with originating service providers, PSAPs, neighboring NGCS domains, and other designated stakeholders to verify proper operation of NGCS and ESInet interfaces.

Lumen supports independent third-party validation and verification activities and demonstrates NGCS and ESInet functionality using a controlled test harness environment. This environment is used to exercise call flows, interfaces, routing behavior, security controls, and failover scenarios in a non-production setting. Test execution results, including logs and supporting artifacts, are provided to the State or its designated representatives to document conformance, identify issues, and confirm remediation prior to production use.

Testing activities are conducted in alignment with Nebraska-defined objectives and acceptance criteria and are intended to demonstrate operational readiness without introducing unapproved production risk.

b. Documentation, APIs, Training, and Operational Materials. Lumen provides complete product and operational documentation for NG911 services supporting the State of Nebraska. Documentation includes system descriptions, architectural overviews,

and interface details sufficient to support operational oversight, interoperability, and lifecycle management.

API specifications are provided for applicable interfaces to support integration, testing, and analytics activities. In addition, Lumen delivers training and operational materials appropriate to the roles involved in NG911 service delivery, including runbooks and operator and administrator manuals. These materials are designed to support day-to-day operations, incident response, maintenance activities, and administrative functions within the Nebraska NG911 environment.

Documentation and training artifacts are maintained to reflect the deployed configuration and are updated as necessary to remain aligned with system changes and operational practices.

3.8. Operational Support and Service Level Agreements (SLAs)

- a. *Contractor shall negotiate with the PSC to establish firm SLAs for availability, incident response, escalation, mean time to repair (MTTR), change management procedures, and maintenance windows.*
- b. *Contractor shall produce a rollback and contingency plan for major updates that affect routing/GIS or call handling.*

LUMEN RESPONSE:

a. Service Level Agreements, Incident Response, and Change Management. Lumen will negotiate with the Nebraska Public Service Commission (PSC) to establish firm, contractually binding Service Level Agreements (SLAs) governing the delivery and operation of NG911 services. These SLAs will address system availability, incident response and escalation procedures, mean time to repair (MTTR), change management processes, and defined maintenance windows, and will reflect Nebraska's operational priorities and governance expectations.

Availability and performance commitments will be clearly defined and measurable, with incident severity classifications and associated response and restoration objectives agreed upon with the PSC. Escalation procedures will be documented to ensure timely engagement of appropriate technical and management resources, and MTTR metrics will be established to support rapid service restoration for events affecting call handling, routing, or GIS functionality.

Change management procedures will be formally documented and jointly reviewed with the PSC. These procedures will define how planned and emergency changes are requested, evaluated, approved, communicated, and executed. Maintenance windows will be scheduled in coordination with the PSC to minimize operational impact, with advance notice provided for changes that may affect routing, GIS data, or call handling behavior.

b. Rollback and Contingency Planning for Major Updates. Lumen provides a rollback and contingency plan for major updates that may affect NG911 routing, GIS data, or call handling functions. This plan is designed to ensure service continuity and rapid recovery in the event that an update produces unintended operational impacts.

For major changes, rollback procedures are defined in advance and include pre-change validation, impact assessment, and clearly documented back-out steps that can be executed without compromising emergency service availability. Contingency measures

are designed to preserve existing routing and call handling behavior until updates are fully validated and accepted.

Rollback and contingency planning is integrated into Lumen's overall change management framework and is applied consistently to system upgrades, configuration changes, and data updates that could affect live NG911 operations within the State of Nebraska.

3.9. Applicable Standards

Respondents must demonstrate their industry knowledge and describe their commitment to proposing standards-based NG911 solutions and services.

The State may disqualify or reject non-standard or proprietary systems that may hinder NG911 implementation, limit interoperability, or that might restrict the State from interconnecting to a regional or national 911 system in the future.

Throughout the duration of this contract, Respondents SHALL maintain conformance with all standards listed in this Scope of Work and ensure that the products, solutions, and services provided for the State of Nebraska evolve and adapt as the standards evolve. A listing of currently approved NENA standards can be found at <https://www.nena.org/page/standards>.

In their response, Respondents must explain in detail how their proposed solution conforms to the requirements of the referenced standards.

Federal Communications Commission Rules

*The Federal Communications Commission (FCC) regulates 911 services through various rules and requirements, primarily found in **47 CFR Part 9**, covering Enhanced 911 (E911), Text-to-911, Next Generation 911 (NG911), and location-based routing. Key requirements include transmitting all 911 calls, providing call-back numbers and precise location data, ensuring service for text and multimedia, and meeting standards for digital, IP-based systems and network reliability.*

Other Industry Standards

All equipment proposed to support or operate within the State of Nebraska NG911 System must comply with relevant industry standards and reference models, including, but not limited to:

- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- Open Systems Interconnection (OSI)
- Telecommunications Industry Association (TIA)
- Underwriters Laboratories (UL)

Respondents must propose a system that utilizes an Open Standards Methodology:

- *The proposed system shall be subject to standards that enhance open standards and increase interoperability such as ITU, IEEE 802 at OSI Layer 2, and IP and TCP, as defined by the IETF in the applicable RFCs, at OSI Layer 3 and above.*

- *If proprietary standards or protocols are used within a proposed solution, Respondents shall disclose the proprietary nature and discuss any limitations that may result.*

Conformance to Standards Baseline Conformance

*The State prefers full conformance with **NENA-STA-010.3** at System Acceptance. The solution must remain current with NENA standards as they evolve. The State understands some limitations may require additional development.*

Gap Identification (Proposal Requirement)

*Respondents shall identify any gaps to full **NENA-STA-010.3** conformance in their proposals. Respondents are solely responsible for disclosing such gaps and providing a plan and timeline to close them.*

LUMEN RESPONSE:

Commitment to Standards-Based NG911 Solutions and Industry Knowledge. Lumen demonstrates deep industry knowledge of Next Generation 911 (NG911) architectures and a longstanding commitment to delivering standards-based, interoperable solutions that align with national, regional, and statewide NG911 objectives. Our proposed solution for the State of Nebraska is grounded in the NENA i3 framework and is designed to support the State's current and future NG911 operational, interoperability, and governance needs without introducing proprietary constraints.

Standards-Aligned NG911 Modernization Without Operational Disruption.

Nebraska transitions to a fully standards-compliant i3 NG911 architecture without wholesale replacement of existing operational infrastructure. Lumen delivers NGCS, ESInet, and supporting services aligned with NENA-STA-010.3, with documented gap identification, remediation planning, and ongoing conformance management to support standards evolution without increasing operational risk.

Benefit to the State of Nebraska: The State achieves NG911 modernization while preserving service stability, minimizing transition risk, and maintaining continuous call handling for PSAPs.

The NG911 solution is architected to support seamless interconnection with regional and national 911 systems and to avoid reliance on non-standard or closed technologies that could hinder Nebraska's ability to evolve, interconnect, or adopt future capabilities. Lumen does not require the State to deploy proprietary signaling, routing, or data exchange mechanisms that would limit interoperability or create vendor lock-in. This approach ensures that Nebraska retains flexibility and long-term control over its NG911 ecosystem.

Ongoing Conformance with NENA Standards. Lumen maintains continuous conformance with all NENA standards identified in the Scope of Work, including those referenced by the State as currently approved. The proposed solution is designed to remain aligned with NENA i3 and related NG911 standards as they evolve over the duration of the contract, ensuring that Nebraska benefits from advancements in NG911 functionality, security, and interoperability.

Standards conformance is treated as an operational requirement rather than a one-time implementation milestone. As NENA standards are updated or extended, Lumen evaluates impacts, incorporates changes where applicable, and works collaboratively with the Nebraska Public Service Commission to ensure continued alignment without service disruption. This approach supports long-term sustainability and protects the State's investment in NG911 infrastructure.

Federal Communications Commission (FCC) Rules Compliance. Lumen's proposed solution complies with applicable Federal Communications Commission (FCC) rules, including those codified in 47 CFR Part 9, governing E911, Text-to-911, NG911, and location-based routing. The solution supports the transmission of all emergency calls, delivery of call-back numbers, conveyance of accurate and actionable location information, and support for text and multimedia communications using digital, IP-based technologies.

Network design and operational practices emphasize reliability, resiliency, and standards-based interoperability consistent with FCC expectations for NG911 systems. This ensures that Nebraska's NG911 environment remains compliant with federal regulatory requirements while supporting next-generation emergency communications.

Conformance with Other Industry Standards. All equipment and systems proposed for use within the Nebraska NG911 System comply with relevant industry standards and reference models, including those promulgated by ANSI, EIA, IEEE, ISO, OSI, TIA, and UL, as applicable. These standards inform hardware design, network interfaces, electrical safety, interoperability, and operational reliability across the NG911 environment.

By adhering to widely recognized industry standards, Lumen ensures that the Nebraska NG911 System is compatible with third-party components, future technologies, and multi-vendor environments.

Open Standards Methodology and Disclosure of Proprietary Elements. Lumen proposes an NG911 solution that utilizes an open standards methodology across network, transport, and application layers. This includes the use of Layer 2, IP and TCP, as defined by applicable IETF RFCs and OSI Layer 3 and above, and adherence to recognized standards at lower layers where applicable, including IEEE 802 standards. The system complies with SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), NENA STA-010.2, IETF ECRIT best practices, and ANSI standards.

Lumen is committed to supporting the NENA STA-010.3 standards for all external interfaces included in our solution that require interoperability with other vendors' systems. Lumen adheres to the various required interoperability protocols specified for use in the NENA i3 standards, such as HELD, LoST, Additional Data, MSRP, and others.

The Lumen ESInet system does not use proprietary software or hardware. If any proprietary components or protocols are used internally within the solution, their proprietary nature is disclosed, and their scope is limited so as not to impede interoperability, data portability, or the State's ability to interconnect with other NG911 systems. Any such proprietary elements are not required for external interfaces and do not restrict Nebraska's future system evolution.

Table 3.9.1 illustrates how Lumen uses open, non-proprietary standards across the physical, data link, network, and transport layers to ensure consistent, interoperable connectivity throughout Nebraska's ESInet architecture.

Table 3.9-1. OSI Layer Mapping for Nebraska ESInet Network Segments

Network Segment	OSI Layer 1 - Physical	OSI Layer 2 - Data Link	OSI Layer 3 - Network	OSI Layer 4 - Transport
Backbone Network	Fiber	IEEE 802.3 Ethernet	IP	UDP, TCP, BGP
PSAP WAN Network	Fiber, T1	IEEE 802.3 Ethernet	IP	UDP, TCP, BGP

Aggregation Sites	Fiber, DS3	IEEE 802.3 Ethernet	IP	UDP, TCP, BGP
Core Sites	Fiber, Copper	IEEE 802.3 Ethernet	IP	UDP, TCP, BGP
PSAP Sites	Copper	IEEE 802.3 Ethernet	IP	UDP, TCP, BGP

Lumen's ESInet complies with applicable rules and standards from the Federal Communications Commission (FCC), including Part 15, Class A, Commercial, Non-Residential Radiation and Conduction Limits for Electromagnetic Interference (EMI), and FCC Rules, Part 68, Connection of Terminal Equipment to the Telephone Network.

Lumen's solution complies with the FCC 911 Reliability rules and requirements (FCC Report and Order FCC 13-158), including the audit requirements and submitting an annual report to the customer.

Lumen's ESInet also complies with the following:

- Underwriters Laboratories (UL)
- International Organization of Standards (ISO)
- Open Systems Interconnection (OSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- Telecommunications Industry Association (TIA), including ANSI/EIA/TIA-568 Commercial Building Telecommunications Wiring Standards

Baseline Conformance to NENA-STA-010.3 and Gap Identification. Lumen's solution is designed to achieve full conformance with NENA-STA-010.3 as the preferred baseline at System Acceptance, recognizing that certain capabilities may require additional development as standards evolve or as implementation contexts change. Where full conformance is not immediately achievable, Lumen explicitly identifies any gaps to NENA-STA-010.3 compliance within the proposal.

For each identified gap, Lumen provides a clear explanation, along with a plan and timeline to close the gap, ensuring transparency and accountability. Responsibility for identifying and addressing such gaps rests solely with Lumen, and remediation planning is coordinated with the Nebraska Public Service Commission to align with State priorities and operational constraints.

Note:

The State recognizes that no existing implementation fully conforms to NENA-STA-010.3 (and many still have gaps against NENA-STA-010.2). Proposals must explicitly state all areas where the delivered system will not conform at time of delivery.

Standards Updates (Post-Award)

*Contractors shall implement any new or changed feature required by an upgraded or revised NENA standard **within nine (9) months** of the standard's ratification for public use. The Contractor must supply regular progress reports for features and functions that are in revision. If at any point in the 9 month window the Contractor becomes aware that they will not meet the deadline they must inform the State in writing with an adjusted timeline for when the new features or functions will be delivered. If the Contractor cannot*

meet this timeline, it must request a **waiver**, including an alternative plan and schedule to achieve conformance.

Non-Disclosure and Breach

Exceptions to conformance must be explicit. Notwithstanding any other provision in the contractual terms, if the system is delivered with a **material deviation** from **NENA-STA-010.3** that was **not** disclosed in the proposal, and the State determines (in its sole discretion) the omission was **not** accidental, the Contractor will be deemed **in breach** of contract. If the State determines the omission was accidental, the State and Contractor will negotiate in good faith a deadline by which conformance must be achieved.

Deviation Classification (Proposal Requirement)

Each deviation must be classified as one of the following:

- **NENA-STA-010.3 upgrade, proposed date:** The delivered system conforms for the feature, and the proposal includes an estimated date for providing the **NENA-STA-010.3** upgrade to the State (no later than **Contract Year 2**).
- **Missing capability, proposed date:** The delivered system does **not** conform to NENA-STA-010.3 for the feature; the proposal includes an estimated upgrade date (no later than **Contract Year 2**).
- **Missing capability, no proposed date (will be provided):** The delivered system does not conform to **NENA-STA-**
- **010.2 or NENA-STA-010.3** for the feature; the proposal commits to provide the capability but does not specify a date.

Missing capability, no plans: The delivered system does not conform and there is no intention to conform. An alternative to the **NENA-STA-010.3** feature may be proposed for State consideration.

Remediation Plan and Progress

Non-conforming features shall be listed in a **Remediation Plan** included with the proposal, identifying each feature and the estimated schedule. The Contractor shall update the Remediation Plan **at least quarterly**. The State expects reasonable, continuous progress. If any features remain non-conforming to **NENA-STA-010.3** by the end of **Contract Year 2**, the Contractor will be deemed **in breach** of contract.

Interoperability

The system must interoperate with any system conforming to **NENA-STA-010.3** that must interwork with the State's system. The State understands interoperability issues can arise from either party's non-conformance or from ambiguities in the standard. In such cases, the Contractor, the other vendor, and (as appropriate) the State's consultants shall work cooperatively to determine the non-conformance and corrective actions, using the **intent of NENA-STA-010.3** as the guiding objective.

- If the Contractor is required to make changes, it shall propose a completion date acceptable to the State.
- If the issue lies with the other vendor, the Contractor shall cooperate in testing but has no further responsibility.

- If the other vendor conforms to **NENA-STA-010.2**, the State's system conforms to **NENA-STA-010.3**, and the issue falls outside the **010.3** backward-compatibility statements for **010.2**, the Contractor is **not** required to make changes.

NENA NG911 i3 Standard Conformance

The following section includes references to conformance with **NENA-STA-010.3**. The absence of an explicit reference **DOES NOT** imply the State does not require conformance to that portion of the Standard. The State requires conformance to the full standard, while recognizing the practicalities of achieving conformance within the contract period as described above.

If the proposed system does not apply NENA Standards throughout the ESInet, the proposal must identify each deviation, explain why the Standard is not met, and propose an alternative.

Additional explicit Standards-conformance requirements appear in other sections of this RFP. **RESPONDENTS MUST COMPLETE THE STATUS TABLE (Table 1) BELOW.**

Status must be presented with one of the following options:

- Implemented
 - The requirement is tested, approved, and in production.
- Roadmap – with timeframe in months
 - The requirement is not in production for any reason.
 - **Timeline for implementation MUST be within 12 months of RFP Response.**
- Future Planned
 - The requirement is not in production for any reason, and the planned implementation is **longer than 12 months**.
- Not implemented
 - The requirement is not in production, and no plans have been developed for deployment/implementation of the requirement.

LUMEN RESPONSE:

Disclosure of Non-Conformance at Time of Delivery. Lumen acknowledges the State's recognition that no existing NG911 implementation fully conforms to NENA-STA-010.3 at this time and that gaps may also exist relative to NENA-STA-010.2. Consistent with this understanding, Lumen explicitly identifies all areas of non-conformance at the time of system delivery within the proposal. Any deviations from NENA-STA-010.3 or NENA-STA-010.2 are disclosed transparently, described in technical detail, and documented as part of the proposal's standards conformance and remediation materials.

This disclosure obligation is treated as a mandatory requirement, and Lumen does not rely on implied conformance or omission. All known limitations, dependencies, or partial implementations are clearly stated to enable informed evaluation by the State.

Post-Award Standards Updates and Upgrade Obligations. Lumen acknowledges that NENA standards continue to evolve and recognizes the importance of timely adoption of newly ratified or revised requirements. Consistent with the approach outlined in the Nebraska NG911 RFP, Lumen treats NENA STA 010.3 conformance as an ongoing obligation throughout the life of the contract.

Following ratification of a new or revised NENA standard for public use, Lumen will evaluate the impact to the proposed ESInet and NGCS solution and implement any required new or changed features within the required timeframe. For features or functions that are under revision, Lumen will provide the State with regular progress updates describing development status and anticipated availability.

If at any point Lumen determines that a specific update cannot be delivered within the required window, we will notify the State in writing and provide an adjusted delivery schedule for State review. In the event that the revised schedule cannot be met, Lumen will formally request a waiver and will submit an alternative plan and timeline to achieve conformance.

Non-Disclosure, Breach, and Good-Faith Resolution. Lumen understands that exceptions to conformance must be explicit and that undisclosed material deviations from NENA-STA-010.3 may constitute a breach of contract. Lumen treats accurate and complete disclosure as a core contractual obligation.

If a material deviation was not disclosed and the State determines the omission was not accidental, Lumen acknowledges that such a finding may constitute a breach of contract. If the State determines an omission was accidental, Lumen commits to negotiating in good faith a mutually acceptable deadline by which conformance will be achieved, consistent with the State's governance authority and operational priorities.

Deviation Classification and Proposal Transparency. Each deviation from NENA-STA-010.3 or NENA-STA-010.2 identified in the proposal is explicitly classified into one of the State-defined deviation categories. These classifications clearly distinguish between features that are already implemented, those requiring upgrades, and those not currently supported, and they identify whether a proposed delivery date is provided.

Where a delivery date is proposed, it is no later than Contract Year 2, unless otherwise stated. Where no date is proposed, Lumen explicitly commits to future provision or discloses that no conformance is planned, including any alternative approach offered for State consideration. This classification framework ensures clarity, traceability, and enforceability of standards commitments.

Remediation Plan and Ongoing Progress Reporting. All non-conforming features are listed in a Remediation Plan included with the proposal, identifying the affected feature, the applicable standard reference, and the estimated schedule for achieving conformance. Lumen updates the Remediation Plan at least quarterly throughout the contract term and provides these updates to the State for review.

Lumen acknowledges the State's expectation of reasonable, continuous progress toward full conformance. Any feature that remains non-conforming to NENA-STA-010.3 by the end of Contract Year 2 is understood to constitute a breach of contract unless otherwise waived or amended by the State.

Interoperability Commitments. Lumen's NG911 solution is designed to interoperate with any system compliant with NENA STA 010.3 that must interface with the State's system. Lumen acknowledges that interoperability issues may result from differences in conformance or from interpretation of the standard and commits to working jointly with the affected vendor and the State's consultants, when applicable, to assess non-conformance and define appropriate remediation consistent with the intent of NENA STA 010.3.

When remediation requires changes by Lumen, a proposed schedule acceptable to the State will be provided. If the interoperability issue originates with another vendor, Lumen will support cooperative testing efforts without assuming responsibility for corrective action. In cases where the other vendor conforms to NENA STA 010.2, the State's system conforms to NENA STA 010.3, and the issue is outside the defined backward compatibility scope, Lumen will not be obligated to modify its solution.

System-Wide Application of NENA Standards. Lumen affirms that the State requires conformance to the full NENA-STA-010.3 standard, regardless of whether individual requirements are explicitly referenced within the RFP. Where NENA standards are not applied uniformly across the ESInet or NGCS, each deviation is identified, the reason for non-conformance is explained, and an alternative approach is proposed for the State's consideration.

Additional standards-conformance requirements appearing elsewhere in the RFP are addressed consistently with this disclosure and remediation framework.

Status Table Completion. Lumen completes the required status, **Table 3.9-2**, using only the State-defined status options:

- Implemented
- Roadmap - with timeframe in months (within 12 months of RFP response)
- Future Planned
- Not implemented

Each status entry accurately reflects the delivered or planned state of the feature and aligns with the Remediation Plan and deviation classifications provided in the proposal.

Table 3.9-2. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ElementState and ServiceState	Allows a PSAP/State management app to see the status of each service (ESRP, ECRF (Emergency Call Routing Function)) and each "box" in a non-proprietary way	Implemented
All i3v3 interfaces plus i3v2 for backwards compatibility	REST/JSON interfaces conforming to i3v3 standard YAML with backwards compatibility to the i3v2 SOAP/XML interfaces	Implemented
Security Posture	Allows routing rules to take security state (green/yellow/orange/red) into account	Implemented
IPv6	Allows every element to have a public address and get calls/data from modern nets (wireless) without translation	Implemented
DNS based redundancy model	All services implement a redundancy model where more than one IP address is returned for the service URI, and any address can be used for a transaction	Implemented
History Info/Reason	Provides a logged reason why a call was not delivered the "normal" way	Implemented
Video	Supports video calls to 911. Most	Future Planned

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
	importantly, allows deaf callers using VRS to be seen by call takers. Includes BCF, Bridge and logging service support	
MSRP	Instant Messaging Service	Implemented
Non-Human Initiated Calls	Support for IoT devices, alarms, etc.	Implemented
TLS (Transport Layer Security) transport of SIP	Provides secure call signaling	Implemented
SRTP	Provides secure media (voice, video, text) for calls	Implemented
RTCP support on all SIP entities	Provides secure control of RTP (Real Time Transport Protocol) streams	Implemented
RTCP Extended Reports	Provides diagnostic information on media streams	Implemented

This status assignment reflects a transparent, standards-disciplined approach consistent with the State's expectations for disclosure, remediation, and evolution toward full NENA-STA-010.3 conformance. All roadmap and future-planned items are tracked in the proposal Remediation Plan and are subject to quarterly progress reporting.

Table 3.9-3. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
PSAP detection of loss of RTP vs silence	Differentiates silent calls from mechanical loss of audio media stream	Implemented
Element Overload (RFC 7339)	Graceful coping with too many SIP calls	Implemented
STUN/TURN/ICE	Standards based mechanisms for NAT Traversal	Implemented
NG-AACN Support	Update to Automatic Car Crash Notification standards	Implemented
SIP Presence for location	Allows OSPs to send location updates for mobile devices without manual rebid (requires OSP to implement also).	Implemented
Policy Store i3v3 interface	Interoperable policy repository that allows 3 rd party editors/verifiers/etc.	Implemented
Multiple Geolocation	Accepts more than one location reported in a 911 call	Implemented

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Discrepancy Reporting mechanism + i3v3 defined DRs (Discrepancy Report)	Standardized way to report discrepancies with standardized responses	Implemented
Bad Actor mechanism	Allows PSAP to stop repeated bad calls from a source	Implemented
Call Suspicion mechanism	Allows the system to mark calls that MAY be bad, and then treat them specially at the PSAP (warnings, special queues, etc.)	Implemented
QueueState	Allows Policy routing based on queue congestion	Implemented
DequeueRegistration	Allows multiple PSAPs and other entities to dequeue from a queue	Implemented
ESRPnotify	Allows policy routing rule to notify some entity that a condition was encountered	Implemented
AbandonedCall	Standardized way to report a call that was hung up before PSAP got the call	Implemented

These status assignments maintain internal consistency with the earlier i3 v3 status table, align with the Contract Year 2 conformance threshold, and support transparent tracking through the proposal Remediation Plan and quarterly updates.

Table 3.9-4. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Service/Agency Locator	Service that allows discovery of things on any ESInet rather than provisioning it.	Implemented
XACML based data rights management	Standardized way to control who has access to what data	Implemented
EIDO on Transfer	Mechanism to transfer call state to a PSAP along with the call	Implemented
3rd Party Origination	Allows a 3 rd party, like Video Relay Interpreter, to be automatically added to a call as a 3 way	Implemented
RTT	Real Time Text support, includes multiparty RTT (Real Time Text) support (RFC 9071) and mixer support for non-aware devices	Implemented

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Resource Priority header	Allows SIP Resource Priority handling of SIP messages. All SIP entities support it, BCF polices/inserts it.	Implemented
Incoming Baudot is converted to RTT	TTY to/from OSP converted to Real Time Text by LNG (Legacy Network Gateway) (Baudot to RFC 4103)	Not Implemented
Outgoing Baudot is converted to RTT	TTY to/from PSAP converted to Real Time Text by LPG (Legacy PSAP Gateway) (Baudot to RFC 4103)	Implemented
Multipart MIME (BCF, bridge, media server)	Allows multiple SIP bodies. Typically, this is Location by Value plus SDP.	Implemented
SRV records for SIP interface resolution (BCF/ESRP and PSAP)	Standard mechanism to derive SIP connection address from a domain name	Implemented
Support for Outbound (RFC 5626)	SIP Protocol fixes for outbound calls	Implemented
i3v3 Syntax and Semantics for Policy Routing Rules	Standardized Syntax and Semantics for Policy Routing Rules	Implemented
SBC inserts NENA-Source parameter	Allows PSAP to identify which SBC (BCF component) handled a call. Used with Bad Actor	Implemented
ESRP supports AdditionalData dereference for PRR	Allows policy routing based on additional data	Implemented

The information presented reflects the proposed solution's alignment with NENA i3 v3 requirements and clearly distinguishes between capabilities that are fully implemented today and those planned through defined, time-bound roadmap commitments. All roadmap items are intentionally sequenced to achieve full conformance within the contract term while minimizing operational risk and avoiding disruption to live 9-1-1 services. This approach ensures immediate delivery of core NG911 functionality while providing a transparent, standards-aligned path to complete i3 v3 capability maturity as adoption, policy, and interoperability considerations evolve.

Table 3.9-5. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ESRP handles incoming admin calls	Allows policy routing of admin calls	Implemented

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ESRP policy routes calls to other agencies	Allows calls to other PSAPs, responders, to be policy routed. Includes extraction of location from an EIDO	Implemented
Support for incoming identity validation	STI-VS implemented to return STIR/SHAKEN validation on incoming calls.	Implemented
Gap/Overlap	Tells agencies about gap or overlap discovered by ECRF/LVF in GIS data	Implemented
ECRF handles any standard shape	Location can be specified by polygon, circle, ellipse, or arc band, in addition to point	Implemented
ECRF returns service boundary	ECRF can return a polygon, within which, the response will still be valid	Implemented
ECRF Supports lost-planned-changes	allows planned changes in GIS to occur on a schedule	Roadmap - Within 12 months
matchType and degradedMatch implemented	Allows querier to know how validation was determined and receive a warning that validation was not necessarily as good as intended	Implemented
i3v3 Appendix B/NG GIS implemented	Updated GIS provisioning data model	Implemented
Support CLDXF location	US profile of PIDF-LO, FGDC conformant.	Implemented
Internal and External ECRF/LVF supplied	ECRF and LVF (Location Validation Function) for public and OSP support available on the Internet, separate from internal ECRF/LVF available on ESInet	Implemented
ECRF/LVF replica support	Interface that allows an OSP or other entity to maintain a local copy of the ECRF/LVF	Implemented
Interconnected ESInet support	Allows neighboring ESInets to connect to the State ESInet. Supports bidirectional ECRF/LVF query, call transfer, etc.	Implemented
Forest Guide Support	Entry in FG for State ECRF/LVF, and recursive resolution of out of area queries via the FG	Implemented

The status assignments in the previous table reflect a standards-aligned and operationally responsible approach to NENA i3 v3 core routing and GIS-related capabilities. Functions identified as implemented are in active use and support reliable, interoperable NG911 operations today, while roadmap items are deliberately sequenced to reach full conformance

within the contract term without introducing risk to live call handling. This phased approach ensures immediate operational integrity, transparent disclosure of planned enhancements, and a clear, auditable path toward complete i3 v3 capability maturity as standards adoption and inter-jurisdictional interoperability continue to evolve.

Table 3.9-6. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
MCS (MSAG Conversion Service) and GCS (Geocode Conversion Service) are implemented	MCS = MSAG (Master Street Address Guide) Conversion Service, converts between MSAG form of address and PIDF-LO. GCS=Geocode conversion service, provides civic to geo, or geo to civic conversion for any system	Implemented
Change in GIS results in routing change in minutes	A change in the GIS data can affect routing within minutes of the GIS authority releasing the change	Implemented
MDS implemented	Map Database Service returns maps (as images) or features to support both local and out of area maps	Roadmap - Within 12 months
Spatial Interface is implemented	Standard was to provision ECRF/LVF/MDS/GCS/MCS	Implemented
Changes to PRR effective on next call	Update of PRR policy in Policy Store causes changes in routing immediately	Implemented
i3v3 DR interface and all defined DRs implemented	Automated Discrepancy Reporting mechanism and several standard DR formats	Implemented
i3v3 Test call is supported	Automated mechanism to test the call path. No human required. Includes media check (loopback)	Implemented
i3v3 Test Call Generator supported	Automated mechanism to generate test calls (can text PRR sets)	Implemented
IS-ADR search supported at PSAP	Standardized way to check outside sources to see if they have additional data for a telephone number (like RapidSOS)	Implemented
humintlang tag supported	Signals request for language used on a call	Implemented
Call Transfer follows i3v3 call flows	Either Ad hoc or Route All Calls Via a Conference Aware UA (User Agent) model is followed for bridge based attended transfer	Implemented
Transfers between ESInets with different bridge models supported	Transfer of calls between ESInets that have different bridge models work as defined in the i3V3 standard	Implemented

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Media server supports i3v2 IMR	Standardized multimedia "Interactive Voice Response" unit (auto answer with menus). Includes audio, video, text, RTT. Includes VXML for control.	Implemented

The status designations in the previous table reflect a balanced and standards-aligned approach to NG911 data services, GIS integration, testing, and media handling capabilities. Implemented functions are actively supporting operational NG911 environments today, while roadmap and future-planned items are sequenced to achieve full conformance without disrupting live call processing. This phased delivery model provides transparency, supports continuous improvement, and establishes a clear, auditable path toward complete NENA i3 v3 capability maturity as supporting standards, tooling, and operational adoption continue to advance.

Table 3.9-7. NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Logging service supports all i3v3 LogEvents	Logging Service supports all i3 defined log events	Implemented
NGCS elements create the specified LogEvents	All NGCS elements generate all V3 standardized log events they should implement	Implemented
Logger logs media per the standard	Logging service logs all media per the standard	Implemented
Logger retrieval interface follows standard	Logging Service implements i3 standardized log retrieval interface	Implemented
Logger can be used as IRR (Instant Recall Recorder)	Logging Service implements the Instant Recall Recorder function	Implemented
LNG supports P-Preferred-Identity + ESN/IMEI for non-initialized mobile	LNG retrieves IMEI for non-initialized phones and passes it in SIP P-Preferred Identify header	Implemented
Outgoing Call Interface Function	Supports call backs and other outgoing calls with all media supported on the incoming emergency call. Includes support for STIR/SHAKEN signing of Identity.	Roadmap - Within 12 months

The capabilities summarized in this table demonstrate a mature, standards-aligned approach to NG911 logging, identification, and outbound call handling. Implemented functions provide immediate operational support for accountability, quality assurance, and incident review, while the defined roadmap item is scheduled to reach full conformance within the contract term without introducing risk to live 911 operations. This approach ensures transparency, operational continuity, and a clear, auditable path to complete NENA i3 v3 compliance across logging and call control functions.

4. RESPONSE TO WORK PLAN AND PROJECT PLANNING

C. WORK PLAN AND PROJECT PLANNING

This section defines the required plans, methods, staffing, testing, and governance for implementing, accepting, and operating the NG911 solution. In this section and throughout this document (and as noted in the Glossary), ‘Respondent’ refers to the proposing entity pre-award, and ‘Contractor’ refers to the awarded entity post-negotiation and post-award. Any references to ‘Vendor’ identify any third party from whom the Respondent or Contractor (as applicable) procures goods or services to fulfill the requirements of this RFP and subsequent contract, including hardware, software, connectivity services, and external personnel.

4.1. Project Management

4.1.1. Project Management Approach

The Respondent shall describe a project management approach aligned with Project Management Institute (PMI) best practices and informed by the Information Technology Infrastructure Library (ITIL) for service transition and operations. The approach must cover governance, control of scope, schedule, and budget, risk and issue management, stakeholder communications, and status reporting. Post-award, the Contractor shall execute this approach.

LUMEN RESPONSE:

Lumen will execute the Nebraska statewide NG911 ESInet and Next Generation Core Services (NGCS) implementation using a disciplined, phased project management approach that spans from Notice of Award through Final System Acceptance and transition to steady-state operations. This approach is designed to ensure predictable delivery, transparent governance, and minimal risk to live 9-1-1 operations across Nebraska’s regions and PSAPs. Post-award, Lumen assumes full responsibility for executing this approach, coordinating all subcontractors and vendors, and meeting the State’s requirements for scope control, schedule adherence, budget management, risk mitigation, testing, and acceptance.

Immediately upon receipt of the Notice of Award from the Nebraska Public Service Commission, Lumen initiates the project by establishing formal governance and mobilizing the project team. A dedicated Lumen PM is assigned as the single point of accountability and will convene a project kickoff meeting with the State, regional representatives as appropriate and key vendors. During initiation, Lumen confirms project objectives, success criteria, communication protocols, escalation paths, and decision-making authority, establishing a governance framework consistent with Project Management Institute (PMI) best practices and standards and Nebraska’s oversight expectations.

Following initiation, the Lumen PM leads a comprehensive planning phase focused on developing and baselining a detailed Project Management Plan (PMP). The PMP defines the work breakdown structure, milestones, dependencies, resource assignments, and integrated schedule for the statewide ESInet and NGCS deployment, including regional onboarding and interconnection sequencing. The plan also documents formal processes for scope control, change management, risk and issue management, quality assurance, and status reporting. Consistent with ITIL principles, the PMP explicitly addresses service transition activities to ensure that new or modified services are introduced into the production environment in a

controlled and operationally sound manner. The PMP is reviewed with the State and updated as needed prior to execution.

During the design phase, Lumen produces detailed technical designs for the Nebraska ESInet and its integration with NGCS, PSAP call handling systems, Originating Service Providers, and ancillary systems. This phase will include definition of network architecture, redundancy and resiliency models, security controls, interconnection points, and operational boundaries. Lumen works closely to ensure alignment between the ESInet design and NGCS functional elements, including ESRP, ECRF/LVF, logging, and associated data services. Design artifacts are reviewed with the State to confirm conformance with NENA i3 requirements and Nebraska-specific operational needs before implementation begins.

Implementation proceeds in a controlled and coordinated manner to avoid disruption to live 9-1-1 services. Lumen installs, configures, and validates ESInet components, establishes interconnections with Originating Service Providers, integrates required ancillary systems, and coordinates connectivity with PSAP call handling equipment across Nebraska's regions. Gateway and network interfaces are configured to securely interconnect legacy and IP-based environments, translating protocols as required while maintaining end-to-end call integrity. Throughout implementation, Lumen will maintain strict change control and configuration management to ensure traceability and stability.

Testing and acceptance activities are tightly integrated into the implementation phase and executed in accordance with State-approved plans. Lumen develops comprehensive test and acceptance plans covering all network connections, NGCS interfaces, and PSAP integrations. Testing will include functional validation against requirements, performance and resilience testing, security verification, and end-to-end call flow testing. Final acceptance activities include formal acceptance testing and a sustained reliability period to demonstrate system stability under operational conditions. Any defects or deficiencies identified during testing are tracked, prioritized, and resolved through Lumen's issue management process prior to acceptance.

In parallel with technical deployment, Lumen delivers training and documentation to support a smooth transition to operations. Training is provided for appropriate State and PSAP personnel, focusing on system awareness, operational interfaces, and escalation procedures rather than altering local call-taking workflows. Comprehensive documentation is delivered to support ongoing operations, maintenance, and governance, consistent with ITIL service operation practices.

The final system acceptance phase concludes the implementation effort and formally transitions the Nebraska NG911 solution into steady-state operations. Lumen conducts a final review with the State to confirm that contractual requirements have been met, acceptance criteria satisfied, and operational readiness achieved. Upon State approval, formal sign-off will be completed, and the solution enters operational service under established service management and support processes.

Lumen's PM will retain overall accountability and coordinates all subcontractor activities, manages interdependencies, and ensures consistent communication with the State. Throughout the project lifecycle, Lumen provides regular status reporting, maintain active risk and issue registers, and support State oversight, ensuring a transparent, controlled, and successful delivery of Nebraska's statewide NG911 solution.

4.1.2. Project Manager

The Respondent shall assign a dedicated Project Manager (PM) as the single point of contact. The PM is responsible for scope, schedule, budget, resources, risks, and stakeholder communications; must hold the Project Management Professional® (PMP) certification; and have ≥5 years' experience leading projects of comparable size and complexity, preferably in public safety or telecommunications.

LUMEN RESPONSE:

Lumen assigns a dedicated, highly qualified Program/Project Manager (PM), **Ms. Angela Schrawyer**, as the single point of contact for the State of Nebraska throughout the life of the contract. The assigned PM holds an active Project Management Professional (PMP) certification and brings more than **five years of experience** leading large-scale, complex telecommunications and public safety projects comparable in size and scope to Nebraska's statewide NG911 ESInet and NGCS implementation. The PM assumes full responsibility for managing scope, schedule, budget, resources, risks, issues, and stakeholder communications, ensuring disciplined execution and accountability from project initiation through final system acceptance and ongoing operations.

The PM operates within Lumen's Federal and Public Safety Program Management organization and leads a dedicated public safety delivery team with deep expertise in NG911 networks, GIS, NGCS, text services, call handling integration, and legacy system interworking. This multidisciplinary team includes specialists in network design and implementation, public safety system integration, cybersecurity, and NG911 standards compliance. Lumen structures the team to ensure that technical decisions remain aligned with operational realities at Nebraska PSAPs while maintaining statewide consistency and standards conformance. This collaborative model enables rapid issue resolution, informed decision-making, and predictable delivery.

Lumen reinforces project governance by providing senior-level oversight from a Senior Manager of Program and Project Management, who supplies strategic guidance, escalation support, and independent assurance of project performance. This oversight role strengthens executive visibility, reinforces accountability, and ensures alignment with contractual commitments and State priorities. Together, the PM and senior leadership apply PMI best practices for project governance and control, while incorporating ITIL principles to manage service transition and readiness for operational support.

The PM coordinates all project activities and serves as the State's primary interface, ensuring consistent communication and clear lines of authority. Lumen assigns dedicated project managers or technical leads for each major solution segment—GIS, text, customer premises equipment, network, NGCS, and LDB/ALI—while the primary PM integrates these workstreams into a single, coherent delivery effort. This structure ensures that specialized work progresses efficiently while maintaining alignment to the overall Project Schedule and Milestones approved by the State. The PM actively manages dependencies, validates deliverables, and enforces change control to protect scope, schedule, and budget throughout the contract lifecycle.

Lumen executes project coordination activities in close partnership with the State and participating PSAPs. The PM leads site readiness assessments, coordinates site surveys, finalizes configuration requirements for equipment staging, and oversees logistics for equipment staging, shipping, delivery, and inventory validation, as applicable. The PM

reviews and finalizes system designs, ensures completion of required site and network diagrams, manages third-party contractors included in the solution, and maintains comprehensive risk and issue registers. Lumen applies lessons learned from prior statewide NG911 deployments to proactively mitigate risk and reinforce reliability, security, and standards compliance.

The PM establishes a structured meeting cadence and reporting framework to maintain transparency and stakeholder engagement. Lumen conducts a formal project kickoff meeting followed by regularly scheduled status meetings, led and documented by the PM. The PM maintains all project documentation, tracks schedule progress, manages internal and external resources, and coordinates on-site activities with the State, PSAPs, and third-party providers. Regular status reports present progress, upcoming activities, risks, issues, and required decisions, enabling informed oversight and timely resolution.

Lumen maintains an active on-site presence during critical project events, including core system installation, optional capability deployment, testing milestones, cutover activities, and go-live. This presence supports real-time coordination, accelerates problem resolution, and reinforces collaboration with State personnel. During and after implementation, the PM oversees post-implementation support, serves as the escalation point for issue resolution, and coordinates continuous improvement activities informed by performance data and operational feedback. Lumen also delivers a complete site book at handover to support ongoing operations and knowledge transfer.

This structured project management approach provides the foundation for disciplined execution, predictable outcomes, and a successful statewide NG911 deployment for the State of Nebraska. The following section describes the Project Management Plan (PMP) in detail, including governance structure, control processes, schedules, reporting mechanisms, and tools used to execute this approach in a transparent and auditable manner.

4.1.3. Preliminary Plan (Project Management Plan [PMP])

The Contractor shall develop and maintain a living PMP consistent with PMI. The PMP will be used to monitor and control installation and deployment and must be kept current with State visibility and approval of changes via the Change Management process.

Minimum PMP contents:

- **Work Breakdown Structure (WBS), scope, deliverables, and schedule** (with milestones and the explicit handoff from implementation to service management).
- **Quality Assurance and Quality Control (QA/QC)** processes and acceptance criteria.
- **Risk and issue management** (registers, mitigation strategies).
- **Change Management Plan** and **Configuration Management Plan**.
- **Communications and Status Reporting Plan** (cadence, formats, dashboards, programmatic notifications).
- **Deployment and transition plan and schedule**, including a PSAP-by-PSAP work plan.

Notes:

- The PMP will be referenced regularly during implementation to ensure timely completion. -

- Any schedule or work-plan changes require prior State approval through the Change Management process. -

LUMEN RESPONSE:

This section describes Lumen's project management approach and demonstrates how Lumen satisfies all Project Management requirements identified by the State of Nebraska. Lumen provides the required information within this technical volume to clearly explain governance, controls, and execution methodology, and also delivers a comprehensive Project Management Plan (PMP) as an appendix to this volume to support detailed execution and ongoing program governance.

The PMP establishes the processes, controls, roles, and responsibilities including NENA, ITIL and PMI standards that guide project execution from Notice of Award through final system acceptance and transition to steady-state operations.

The PMP serves as the controlling project document for installation, deployment, testing, acceptance, and service transition activities. Lumen maintains the PMP as a living document throughout the contract term and uses it to monitor and control implementation and deployment activities. Lumen updates the PMP to reflect approved changes, evolving conditions, and current execution status through the formal Change Management process, with full visibility and approval by the State of Nebraska.

The PMP aligns with Project Management Institute (PMI) best practices and incorporates ITIL-informed service transition principles to ensure that new and modified services enter the production environment in a controlled, operationally sound manner. The PMP supports transparent governance, disciplined execution, and protection of live 9-1-1 operations across all Nebraska PSAPs.

As required, the PMP includes a detailed Work Breakdown Structure (WBS) defining scope, deliverables, schedules, milestones, and the explicit handoff from implementation to service management; Quality Assurance and Quality Control (QA/QC) processes with defined acceptance criteria; risk and issue management registers with mitigation strategies; formal Change Management and Configuration Management plans; a Communications and Status Reporting plan defining cadence, formats, dashboards, and notifications; and a deployment and transition plan that includes a PSAP-by-PSAP work plan. Lumen provides this comprehensive PMP as **Attachment 3** to this technical volume to support execution, State oversight, and long-term program governance.

4.1.3.1 WORK BREAKDOWN STRUCTURE (WBS)

Lumen uses a hierarchical WBS to organize, plan, and control all project activities. The WBS decomposes the statewide NG911 implementation into manageable phases, deliverables, and tasks, providing clear traceability between contractual requirements and execution activities.

The WBS aligns directly to the approved Statement of Work and serves as the foundation for scheduling, resource planning, cost control, and progress tracking. Major WBS elements include project initiation and planning, system design, ESInet and NGCS implementation, PSAP onboarding, testing and acceptance, cutover, and transition to service management.

Lumen maintains the WBS throughout the project lifecycle and updates it as needed through approved changes. The WBS enables the Lumen PM and the State of Nebraska to monitor progress at both a high level and a detailed task level, ensuring transparency and control

across the full scope of the project. **Table 4.1.3.1-1** provides the high-level details and major milestones of our proposed WBS.

Table 4.1.3.1-1. Lumen's High-Level Work Breakdown Structure

WBS ID	Phase	Deliverable	Description
1.0	Project Initiation & Planning	Kickoff & PMP Baseline	Project kickoff, governance establishment, PMP approval
2.0	Design	ESInet & NGCS Design	Detailed network, NGCS, GIS, and security design
3.0	Implementation	ESInet & NGCS Build	Deployment and configuration of ESInet and NGCS
4.0	PSAP Onboarding	PSAP Connectivity	Circuit delivery, configuration, and readiness validation
5.0	Testing	System & PSAP Testing	Functional, performance, security, and call flow testing
6.0	Cutover	PSAP Cutover	Controlled PSAP-by-PSAP migration to NG911
7.0	Acceptance	System Acceptance	Final acceptance and reliability observation
8.0	Transition	Service Handoff	Transition to steady-state service management

A complete implementation schedule and detailed WBS is provided as **Attachment 6**.

4.1.3.2 QUALITY ASSURANCE AND QUALITY CONTROL (QA/QC)

Program-Level Quality Framework. Lumen applies a structured Quality Assurance (QA) and Quality Control (QC) program to ensure that all NGCS components are standards-conformant, resilient, secure, and operationally ready prior to deployment and throughout the service lifecycle. QA focuses on adherence to approved processes, standards, and governance controls, while QC validates that implemented components perform as designed through inspection, review, and testing. Together, these controls ensure that contractual, technical, and operational requirements are met without introducing risk to live NG911 services.

Standards-Based Design and Validation. NGCS architecture and implementation are validated against applicable NENA i3, IETF, and industry standards, with emphasis on functional interoperability, resiliency, and NG911 operational requirements. Validation activities confirm how required functions are implemented and operate in practice, rather than relying solely on standards declarations. This approach ensures real-world operability across the ESInet, PSAPs, and third-party integrations.

Lifecycle Quality Controls. Quality enforcement is embedded across the full NGCS lifecycle, including planning, design, implementation, testing, cutover, and acceptance. QA/QC activities include structured design and architecture reviews for redundancy, geographic diversity, and failover; configuration and integration validation for NGCS core functions such as ESRP processing, ECRF/LVF interaction, routing logic, and policy enforcement; and security and resilience validation using defense-in-depth principles and layered controls across NGCS platforms and supporting infrastructure.

Continuous Monitoring and Operational Quality. Operational quality is continuously measured using defined service and performance metrics. Media quality is validated using MOS-equivalent POLQA scoring and monitored across active call paths to confirm PSAP-grade voice quality during steady-state operations and failover conditions. Monitoring data supports early detection of degradation and verification that service levels remain within acceptable thresholds.

NGCS Quality Control Activities

Controlled Configuration and Change Management. All NGCS changes, including software releases, configuration updates, cloud region modifications, and interconnection changes, are subject to formal review, testing, and approval prior to production deployment. QC gates prevent unvalidated changes from impacting live NG911 operations and ensure traceability from change request through implementation and verification.

Testing and Verification. QC verification includes functional testing of NGCS call flows, routing behavior, and inter-NGCS and ESInet interoperability; performance and load testing to validate response times, transaction handling, and scalability targets; and verification of logging, monitoring, and audit capabilities to support end-to-end traceability of NGCS transactions.

Defect Tracking and Corrective Action. Identified defects, non-conformances, or performance gaps are documented, prioritized, and tracked to resolution using a centralized defect management process. Corrective actions are linked to risk management, retesting, or acceptance activities as required, ensuring transparency, accountability, and closure before acceptance.

NGCS Acceptance and Readiness

Pre-Cutover Acceptance Criteria. NGCS acceptance is a structured, evidence-based process defined by predefined criteria. Acceptance typically includes successful completion of functional and interoperability testing; verification of redundancy, failover, and geographically diverse operations; confirmation that logging, monitoring, and reporting meet operational and audit requirements; and validation that security, identity management, and access controls are fully operational.

Documentation and Stakeholder Review. Acceptance artifacts, including test results, configuration baselines, and readiness reports, are documented and reviewed with the State or designated stakeholders prior to authorization to proceed. This ensures shared understanding of NGCS readiness and operational expectations before cutover.

Ongoing Acceptance and Governance. Following initial acceptance, NGCS services remain subject to periodic review through established governance forums, such as monthly project or operational reviews, to confirm continued compliance, performance, and service quality over time.

QA/QC Oversight and Enforcement. The PM oversees QA/QC execution and ensures that deficiencies are documented, tracked, and resolved. Lumen does not advance to cutover or acceptance activities until all quality requirements are met and validated. This disciplined approach ensures predictable outcomes and protects the reliability and continuity of Nebraska's NG911 services.

QA/QC Objectives:

- Ensure the system meets all functional and performance requirements.
- Identify and resolve any defects or issues before deployment.
- Maintain high standards of quality throughout the project lifecycle.

QA/QC Process:

1. Planning and Documentation:

- Develop a comprehensive QA/QC plan that outlines the testing strategy, methodologies, and tools to be used.
- Create detailed test cases and scenarios based on the system requirements and specifications.

2. Testing Phases:

- **Unit Testing:** Each component of the system will undergo rigorous unit testing to ensure it functions correctly in isolation.
- **Integration Testing:** Components will be integrated and tested together to verify that they work seamlessly as a whole.
- **System Testing:** The entire system will be tested in a controlled environment to validate its overall functionality and performance.
- **User Acceptance Testing (UAT):** End-users will test the system to ensure it meets their needs and expectations.

3. Defect Management:

- Implement a defect tracking system to log, prioritize, and resolve any issues identified during testing.
- Conduct regular reviews and status meetings to monitor progress and address any challenges.

4. Continuous Improvement:

- Gather feedback from stakeholders and end-users to identify areas for improvement.
- Update the QA/QC plan and processes as needed to enhance quality and efficiency.

Quality activities occur throughout the project lifecycle and are integrated into planning, design, implementation, and acceptance phases. Lumen defines acceptance criteria for each major deliverable in advance and validates completion against those criteria before authorizing progression to the next phase. Deliverables subject to QA/QC include design artifacts, network configurations, NGCS provisioning, PSAP connectivity, test plans, test results, and acceptance documentation.

Please see our Project Management Plan (PMP) **Attachment 3** for our detailed Quality Management Plan (QMP).

4.1.3.3 RISK AND ISSUE MANAGEMENT

Lumen implements a mission critical risk and issue management program designed to protect end-to-end NG911 call delivery, routing integrity, security, and operational continuity in alignment with the RFP's requirements for risk and issue management within the Project Management Plan (PMP) and related governance processes.

Incumbent Risk Context. As the State's incumbent NG911 ESInet and NGCS provider, Lumen enters this engagement with a mature, operational environment already deployed and actively supporting statewide NG911 operations. Accordingly, the risk profile associated with Lumen's proposal is materially different than a net new or replacement deployment. Many risks typically associated with NG911 programs—such as initial core activation, statewide cutover, parallel operations ramp up, major SAP retraining, and largescale integration revalidation—have already been successfully mitigated through prior deployment, acceptance activities, and sustained operations. Lumen's risk program therefore focuses on (1) **residual operational risks**, (2) **change driven risks**, and (3) **external dependency risks**,

while still documenting transition and cutover risks for completeness and contingency planning.

Risk Management Objectives. The objectives of Lumen's risk and issue management approach are to:

- Proactively identify administrative, operational, technical, and security risks that could impact NG911 services
- Protect the entire call path (Ingress, Core, and Egress) from single points of failure
- Identify and manage risks outside Lumen's direct span of control, including OSP interconnect diversity and PSAP access constraints
- Ensure high-impact risks are mitigated, escalated, or formally accepted with State visibility
- Maintain continuous alignment with **99.999%** availability and public safety operational priorities

Risk Management Methodology. Lumen maintains a living Risk and Issue Register throughout implementation and operations. Risks are identified through architecture reviews, transition planning, security assessments, operational monitoring, change reviews, maintenance planning, and stakeholder input.

Each risk is documented with, at a minimum, the following attributes:

- Risk ID and Risk Category (Architecture, Operations, Security, OSP Interconnect, PSAP Access, GIS, Change, Maintenance, Vendor, Compliance)
- Impacted Asset or Service (Ingress, Core, Egress, NGCS Functional Element, GIS, Logging, DNS/NTP, Policy Store)
- Threat and Vulnerability Description
- Likelihood and Impact Scoring (Inherent Risk)
- Risk Treatment Strategy (Reduce, Avoid, Transfer, Accept)
- Integrated Mitigation Strategy (Prevent, Detect, Respond, Recover)
- Residual Risk Rating
- Trigger Conditions and Early Warning Indicators
- Risk Owner and Target Resolution Date
- Verification Method and Closure Criteria
- Identification of State Decision Required where risks fall outside Lumen's span of control

Risks that cannot be fully mitigated due to external dependencies are explicitly flagged and managed through compensating controls, escalation procedures, and formal State coordination and acceptance processes.

Risk Mitigation Strategy. Lumen applies a defense in-depth mitigation strategy to every identified risk. Each mitigation strategy is structured across four mandatory layers:

- **Preventive Controls.** Architectural, procedural, and governance controls are designed to reduce the likelihood of risk realization (e.g., physical diversity, active-active NGCS cores, configuration baselines, security hardening).
- **Detection and Early Warning.** Continuous monitoring, thresholds, alarms, and analytics designed to detect degradation before service impact (e.g., congestion alerts, replication lag thresholds, certificate expiry notifications).
- **Corrective / Containment Actions.** Immediate actions taken to isolate or contain the risk if it materializes (e.g., rerouting traffic, invoking policy overrides, isolating compromised ingress).

- **Recovery and Rollback.** Predefined rollback and recovery procedures that restore service without call loss (e.g., failover to alternate sites, rollback to last known good configurations, contingency routing).

This layered mitigation model directly supports the RFP's requirements for 99.999% availability, change control, and maintenance risk management.

Governance, Cadence, and Reporting

- Weekly internal risk triage involving the Project Manager, Technical Lead, Operations Service Manager, and Security Lead
- Bi-weekly risk reviews with the State during implementation, transitioning to monthly reviews during steady-state operations
- Monthly Risk Management Report delivered to the State summarizing:
 - Top risks and emerging trends
 - Changes in risk posture
 - Mitigation progress and aging actions
 - Decisions or approvals required
- Immediate risk reassessment following major configuration changes, OSP migrations, GIS updates, security findings, or failover testing

Escalation and Issue Management. Risks and issues are categorized by severity and escalated as follows:

- **Severity 1 (Critical):** Risks or issues that threaten call delivery, routing integrity, security posture, or five-nines availability are escalated to executive leadership and State oversight within **one hour**, with an initial mitigation or containment plan provided within **24-hours**.
- **Severity 2 (High):** Escalated within **one business day**, with a corrective action plan provided within **three business days**.
- **Severity 3 (Moderate/Low):** Managed through standard governance with defined resolution timelines.

Root Cause Analysis (RCA) is performed for all Severity 1 and Severity 2 issues, and lessons learned are incorporated into preventive controls and future risk planning.

Maintenance and Change Risk Controls. Consistent with the requirement for no scheduled downtime, any maintenance activity that could affect availability is executed only under approved change control and includes:

- A Pre-Maintenance Risk Register specific to the maintenance activity
- A Maintenance Operation Plan (MOP) delivered at least 14 days in advance, documenting:
 - Identified risks and mitigations
 - Provisional operating configurations to maintain availability
 - Rollback procedures
 - Post-maintenance validation testing (routing, failover, QoS, and security)

All major changes include documented risk and impact assessments, security review, rollback planning, and State participation in governance.

Risk Register (Baseline). Below are the known risks that may affect the execution and schedule of the project. Each risk identified is associated with the following class designation.

- **Class A (Residual Ops):** Real risks Lumen must manage as the operating provider

- **Class B (Change-Driven):** Risks introduced by upgrades, expansions, new interconnects, standards updates
- **Class C (Transition/Cutover):** Higher for a replacement vendor; reduced for the incumbent but documented for completeness/contingency

As the State's incumbent NG911 ESInet and NGCS provider, Lumen's risk profile differs materially from that of a replacement or greenfield deployment. The risks identified below are therefore categorized to distinguish industry-wide operational risks that exist for all NG911 providers from transition-driven risks that are materially higher for a non-incumbent bidder.

Where risks are identified as applicable to all bidders, Lumen further identifies whether residual exposure is reduced in the incumbent operating environment due to existing deployment, acceptance testing, operational maturity, and established interconnections. Transition specific risks are documented for completeness and contingency planning but are significantly mitigated by continuity of operations under Lumen's incumbent solution.

Table 4.1.3.3-1 provides Lumen identified risks, descriptions, and mitigation activities to ensure seamless and continuous NG911 operations.

Table 4.1.3.3-1. Lumen Risk Register

Risk ID	Risk Class	Applicability	Risk Description	Impacted Area	Inherent Risk	Integrated Mitigation Strategy (Prevent / Detect / Respond / Recover)	Residual Risk	Owner	State Decision Required
R-01	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	OSP lacks diverse connectivity to POI	ESInet Ingress	High	Prevent: Dual POIs where feasible; document non-diverse OSPs; alternate routing design. Detect: Ingress health and call-success monitoring. Respond: Reroute to alternate POI; emergency routing updates. Recover: Coordinate OSP remediation and long-term diversity plan.	Medium	PM / Network Lead	Yes
R-02	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	PSAP last-mile diversity limitations	ESInet Egress	High	Prevent: Dual access circuits where feasible; tertiary OTA/LEO option. Detect: Packet-loss, jitter, latency thresholds. Respond: Degraded routing profile; backup PSAP routing. Recover: Restore primary path and validate QoS.	Medium	Ops Manager	Yes
R-03	B	Change-Driven Risk; Controlled Through Existing Governance	SD-WAN / routing policy misconfiguration during approved change	Core Network	Medium	Prevent: CAB-governed changes; configuration baselines; peer review. Detect: Compliance checks and telemetry alarms. Respond: Immediate rollback to golden config. Recover: Post-change validation and controlled re-release.	Low	Network Lead	No
R-04	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	Underlay congestion degrades QoS	Transport	Medium	Prevent: DSCP enforcement; proactive capacity planning. Detect: Congestion and QoS KPI thresholds. Respond: Traffic shaping; reroute. Recover:	Low	Ops Manager	No

Risk ID	Risk Class	Applicability	Risk Description	Impacted Area	Inherent Risk	Integrated Mitigation Strategy (Prevent / Detect / Respond / Recover)	Residual Risk	Owner	State Decision Required
						Permanent bandwidth augmentation.			
R-05	A	Residual Operational Risk in Mature Production Environment	NGCS site/component failure despite geo-redundancy	NGCS Core	Medium	Prevent: Active-active multi-site redundancy; fault isolation. Detect: Service/element health monitoring. Respond: Automatic failover. Recover: Restore failed site and rebalance traffic.	Low	NGCS Lead	No
R-06	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	GIS data gaps or overlaps cause routing errors	GIS / ECRF	High	Prevent: Automated GIS QA/QC; staged activation. Detect: Discrepancy reporting and validation failures. Respond: Policy override or routing fallback. Recover: Revert to last known good GIS dataset.	Medium	GIS Lead	No
R-07	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	Certificate lifecycle failure impacts SIP/TLS/mTLS	Security	Medium	Prevent: PKI lifecycle automation; renewal SLAs. Detect: Expiry alerts and trust health checks. Respond: Emergency certificate rollover. Recover: Resume standard rotation and validate trust paths.	Low	Security Lead	No
R-08	B	Change-Driven Risk; Controlled Through Maintenance Governance	Maintenance activity could impact availability	Operations	Medium	Prevent: Pre-maintenance risk register and MOP (≥14 days); lab validation. Detect: Live monitoring during maintenance. Respond: Immediate rollback. Recover: Post-maintenance validation testing.	Low	Ops Manager	No

Risk ID	Risk Class	Applicability	Risk Description	Impacted Area	Inherent Risk	Integrated Mitigation Strategy (Prevent / Detect / Respond / Recover)	Residual Risk	Owner	State Decision Required
R-09	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	DDoS/TDoS or SIP signaling attack saturates ingress	Security / Ingress	High	Prevent: Rate limiting; anomaly detection; upstream scrubbing; bad-actor controls. Detect: SOC alerts and traffic anomalies. Respond: Isolate impacted ingress; reroute. Recover: Restore service with tuned controls and post-incident RCA.	Medium	Security Lead	No
R-10	A	Industry-Wide Risk; Residual Exposure Reduced for Incumbent	Logging/CDR correlation gaps impact analytics or IV&V	Logging / Analytics	Low	Prevent: Correlation-ID enforcement; schema validation. Detect: Completeness checks. Respond: Manual reconciliation runbook. Recover: Automated backfill and verification.	Low	Reporting Lead	No
R-11	C	Primarily Non-Incumbent Transition Risk; Minimized by Continuity	Parallel operations and statewide cutover risk	Transition	High	Lumen Advantage: Existing production environment avoids wholesale cutover. Prevent: Staged changes only. Detect: Routing KPIs. Respond: Rollback to steady-state routing. Recover: Re-validate incremental change.	Low (Incumbent)	PM	Yes
R-12	C	Primarily Non-Incumbent Transition Risk; Minimized by Continuity	OSP re-interop and re-turn-up risk during provider change	Interconnect	High	Lumen Advantage: Existing OSP interconnects already active. Prevent: Limited change scope. Detect: Call completion monitoring. Respond: Fall back to established POIs. Recover: Remediate and retest.	Low (Incumbent)	OSP Coord Lead	Yes
R-13	C	Primarily Non-Incumbent Transition Risk; Minimized by Continuity	PSAP retraining and operational disruption	PSAP Ops	Medium	Lumen Advantage: No wholesale workflow replacement. Prevent: Delta training only. Detect: Acceptance metrics. Respond:	Low (Incumbent)	Training Lead	Yes

Risk ID	Risk Class	Applicability	Risk Description	Impacted Area	Inherent Risk	Integrated Mitigation Strategy (Prevent / Detect / Respond / Recover)	Residual Risk	Owner	State Decision Required
						Pause change. Recover: Incremental adoption.			

A detailed risk management approach is provided in **Section 4.4.1.5, Risk, Dependencies, and Interdependencies.**

4.1.3.4 CHANGE AND CONFIGURATION MANAGEMENT PLAN

Lumen enforces formal Change Management and Configuration Management processes to control modifications to scope, schedule, budget, and technical baselines. All changes are documented, assessed for impact, reviewed internally, and submitted to the State of Nebraska for approval prior to implementation.

The established Change Management Plan (CMP) process is one of the many tools used to assist the PM 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 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 team. 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.

Change Management Processes. Lumen is committed to maintaining a robust and reliable network infrastructure for the NG911 project. Our standard operating procedures for network configuration management and change management policies are designed to ensure the highest levels of performance, security, and compliance.

Network Configuration Management. Lumen employs a comprehensive network configuration management process to ensure that all network devices and systems are configured correctly and consistently. Lumen employs NIST publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, as its model with procedures articulated in Lumen's Information assurance program manual.

This process includes:

1. **Configuration Standards:** We adhere to industry best practices and standards, such as those defined by NENA and ITIL, to ensure that all network configurations meet the required specifications and performance criteria.
2. **Automated Configuration Management Tools:** We utilize automated tools to manage and monitor network configurations. These tools help us to detect and correct configuration errors, enforce configuration policies, and maintain an accurate inventory of network devices.
3. **Regular Audits and Reviews:** We conduct regular audits and reviews of network configurations to ensure compliance with established standards and policies. Any deviations are promptly addressed to maintain the integrity and reliability of the network.

Change Management Policies. Lumen's change management policies are designed to minimize the risk of disruptions and ensure that all changes to the network are implemented in a controlled and systematic manner. Our change management process includes:

1. **Change Request and Approval:** All changes to the network must be requested and approved through a formal change management process. This includes a thorough review of the proposed change, its impact on the network, and any potential risks.
2. **Change Implementation:** Approved changes are implemented by qualified personnel following a detailed change plan. This plan includes step-by-step instructions, rollback procedures, and contingency plans to ensure a smooth and successful implementation.
3. **Testing and Validation:** All changes are tested and validated in a controlled environment before being deployed to the production network. This helps to identify and resolve any issues before they can impact the live network.
4. **Documentation and Reporting:** All changes are documented and reported to ensure transparency and accountability. This includes detailed records of the change request, approval, implementation, testing, and validation.
5. **Post-Implementation Review:** After a change has been implemented, a post-implementation review is conducted to assess its impact and identify any lessons learned. This helps to continuously improve our change management process and ensure the ongoing reliability of the network.

By adhering to these standard operating procedures for network configuration management and change management policies, Lumen ensures that the NG911 network is maintained at the highest levels of performance, security, and compliance.

Note: Configuration baselines are maintained for ESInet infrastructure, NGCS elements, PSAP connectivity, and supporting systems. Lumen tracks approved changes to ensure traceability, auditability, and operational stability.

4.1.3.5 COMMUNICATIONS AND STATUS REPORTING PLAN

Lumen executes a structured Communications and Status Reporting Plan designed to support real-time coordination, rapid issue resolution, and informed decision-making across all phases of the State of Nebraska's NG911 implementation. Because statewide NG911 deployment involves multiple interdependent workstreams, including ESInet buildout, NGCS integration, Originating Service Provider coordination, and PSAP-by-PSAP onboarding, clear, timely, and technically precise communications are essential to maintaining schedule integrity and protecting live 9-1-1 operations.

The designated Lumen PM, **Ms. Angela Schrawyer**, serves as the single authoritative point of contact for all project communications and is accountable for synchronizing information flow between the Lumen project team, the Lumen PMO, State of Nebraska stakeholders, PSAP representatives, and third-party providers. During the project planning phase, the PM establishes communication protocols, reporting formats, escalation thresholds, and issue-tracking mechanisms. The PM also reviews the risk and issue registers with stakeholders to ensure shared understanding of dependencies, constraints, and mitigation strategies before implementation activities begin.

Lumen maintains a defined weekly communications cadence, supplemented by ad-hoc technical coordination sessions as required for design reviews, testing readiness, cutover planning, or issue resolution. This cadence enables rapid identification and escalation of issues affecting routing, connectivity, GIS readiness, or PSAP operations. Lumen provides a formal escalation matrix covering both implementation and service-related concerns to

ensure that the State of Nebraska can immediately engage appropriate technical or executive resources when additional focus is required.

The PM provides detailed written status reports and leads scheduled status meetings with the State and key stakeholders. Status reporting includes progress against milestones, upcoming technical activities, cross-workstream dependencies, identified risks and issues, approved and pending change requests, and decisions required to maintain forward progress. Reporting is structured to provide both executive-level visibility and sufficient technical detail to support operational decision-making. This disciplined communications approach ensures continuous State visibility, maintains alignment across all parties, and enables proactive governance throughout implementation of Nebraska's statewide NG911 solution.

4.1.3.6 DEPLOYMENT AND TRANSITION PLAN AND SCHEDULE

PSAP-by-PSAP Deployment, Testing, and Transition Work Plan. Prior to the start of deployment activities, the Lumen PM conducts structured internal Project Kickoff meetings with all delivery teams to confirm understanding of project objectives, contractual outcomes, dependencies, and transition sequencing. These sessions establish the detailed PSAP-by-PSAP work plan, including readiness gates, schedule alignment, and acceptance criteria. Lumen then conducts a formal Project Kickoff with the State of Nebraska to review the deployment and transition approach, confirm sequencing assumptions, and reach agreement on milestone expectations, communications cadence, and escalation paths.

Lumen executes deployment and transition using a PSAP-by-PSAP work plan that treats each PSAP migration as a discrete, fully governed work package within a single statewide program baseline. This approach reduces operational risk, protects live 911 services, and enables repeatable execution across Nebraska's diverse PSAP environments. Lumen sequences deployment based on objective readiness, dependency resolution, and operational risk rather than enforcing uniform timing across all PSAPs.

The PSAP-by-PSAP work plan aligns ESInet readiness, NGCS availability, Originating Service Provider (OSP) interconnection, PSAP connectivity, testing, and acceptance into a single, sequenced workflow with defined entry and exit criteria. Each PSAP advances through the workflow only after meeting documented readiness conditions, ensuring that cutover and acceptance occur under stable and supportable conditions.

For each PSAP, Lumen begins with readiness validation and site assessment. Lumen confirms facility readiness, validates power, space, environmental conditions, network demarcation, and interface requirements, and documents any constraints that could affect installation or cutover. Lumen uses site survey results to actively manage sequencing by reordering PSAPs that require remediation, such as fiber extension to demarcation, power upgrades, or rack readiness, without delaying other PSAP deployments.

Lumen delivers infrastructure and connectivity using a staged, turnkey approach. Lumen finalizes the PSAP site list, determines on-net and off-net locations, establishes logical network addressing, and orders, installs, and tests circuits in alignment with the master project schedule. Lumen validates Layer 1 connectivity, routing, and throughput prior to scheduling PSAP cutover. Each PSAP must reach a documented "connectivity ready" state before advancing to integrated testing and cutover activities.

System testing and acceptance serve as the formal gate between implementation and operational cutover. Although acceptance occurs in phases aligned to statewide milestones,

Lumen designs testing to validate the NG911 solution as an integrated system. Network infrastructure, NGCS components, PSAP connectivity, and call routing behaviors are tested together to confirm true end-to-end functionality. This approach avoids partial validation and ensures acceptance reflects real operational conditions.

Lumen executes PSAP cutover using a controlled, checklist-driven process coordinated with the State and PSAP staff. Cutover occurs only after all prerequisites are met and testing demonstrates readiness. Lumen pre-tests circuits, validates live call paths, and monitors system behavior throughout cutover. Lumen maintains rollback and contingency procedures to ensure uninterrupted 911 service.

Following cutover, Lumen supports a defined 30-day operational burn-in period to confirm system stability under live conditions. During this period, Lumen monitors performance, resolves issues, and confirms operational readiness. Upon successful completion, Lumen completes formal acceptance documentation and transitions the PSAP and statewide solution to steady-state service management with full monitoring, escalation, and support enabled.

Lumen maintains the PSAP-by-PSAP work plan (**Table 4.1.3.6-1**) as a living deployment instrument synchronized to the project schedule and controlled through change management. Lumen updates sequencing when readiness conditions, third-party dependencies, or State priorities change and documents those updates for State visibility. This disciplined, PSAP-centric deployment model provides Nebraska a controlled, low-risk path to statewide NG911 implementation while maintaining accountability, transparency, and public-safety-grade operational rigor.

Table 4.1.3.6-1. PSAP-by-PSAP Work Plan Phased Activities

Phase	Inputs / Prerequisite Tasks	Primary Lumen Tasks	Outputs / Deliverables	Acceptance Criteria	Completion Target
PSAP Readiness & Site Assessment	PSAP site data, facility access, State coordination	Conduct site survey, validate power/space/demarcation, document constraints	Approved site readiness report	State approval of readiness; remediation plan (if needed)	PSAP-specific, Date XXX
Infrastructure & Connectivity	Approved site readiness, design baseline	Order/install circuits, configure network, validate Layer 1-3 connectivity	Connectivity-ready PSAP	Successful connectivity tests; routing validated	PSAP-specific, Date XXX
System Staging & Pre-Deployment	Final configurations, software/firmware are baseline	Stage equipment, execute SATP, resolve defects	Staging acceptance results	SATP pass; no critical defects	PSAP-specific, Date XXX
Integration & Interconnection	OSP readiness, NGCS availability	Integrate PSAP with ESInet/NGCS, validate trunking and routing	Integrated PSAP environment	End-to-end integration validated	PSAP-specific, Date XXX
Testing & Acceptance	Integrated PSAP, test plans	Execute functional, stability, and integration testing	Acceptance test results, punch list	All acceptance tests passed; punch list closed	PSAP-specific, Date XXX

PSAP Cutover	Acceptance approval, cutover window	Execute cutover, validate live call handling	Live NG911 PSAP	Successful live call validation	PSAP-specific, Date XXX
Burn-In & Transition	Completed cutover	Monitor operations, resolve issues, finalize documentation	Final acceptance package	30-day stability confirmed; State acceptance	PSAP-specific, Date XXX

Statewide Coordination and Governance. Lumen maintains full contractual responsibility for the NG911 project and assigns a dedicated PM to oversee all PSAP-by-PSAP activities. The PM coordinates subcontractors, OSPs, current solution providers, and State stakeholders, ensuring alignment with the master project schedule and change management controls. Lumen uses structured communications, risk management, and escalation processes to maintain transparency and rapid issue resolution.

Lumen coordinates closely with telecommunications providers through a designated OSP Coordinator to manage interconnection, testing, and cutover dependencies. Technical workshops, regular coordination meetings, and integrated scheduling ensure that OSP readiness aligns with PSAP deployment timing. Post-cutover, Lumen continues coordination through defined operational processes, SLAs, and performance monitoring.

Continuity of 911 Operations. Lumen prioritizes uninterrupted 911 service throughout deployment and transition. Lumen plans and executes parallel operations, phased migration, redundancy, and failover mechanisms to ensure continuous service availability. Lumen coordinates closely with incumbent solution providers to support seamless transition, conducts joint testing where required, and maintains rollback capability until the new system is fully validated and accepted.

Living PSAP-by-PSAP Work Plan Document. Lumen maintains the PSAP-by-PSAP work plan as a living deployment instrument that remains synchronized to the project schedule and controlled through change management. Lumen updates sequencing when readiness conditions, third-party dependencies, or State priorities change, and Lumen documents those updates for State visibility. This PSAP-centric deployment and transition model provides Nebraska a structured, low-risk path to statewide NG911 implementation while maintaining the controls, testing rigor, and operational handoff discipline required for public safety services.

Figure 4.1.3.6-1 depicts a high-level schedule view of our proposed transition to the modernized NG911 solution.

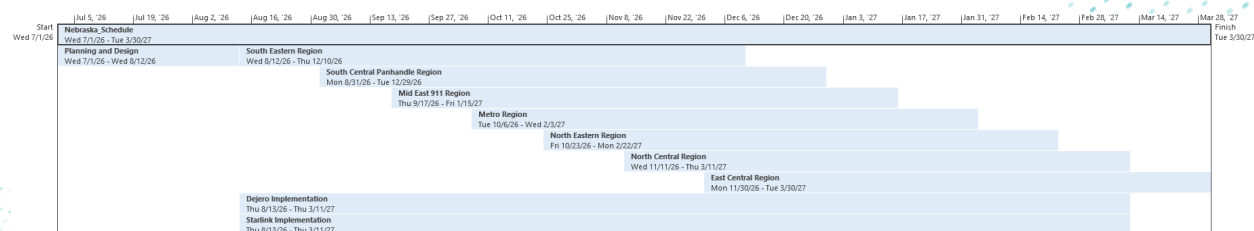


Figure 4.1.3.6-1. Modernized NG911 Schedule Timeline.

See **Section 4.4.1.1** for our proposed transition approach and schedule.

4.2. Staffing and Qualifications

4.2.1. Key Personnel

Identify Key Personnel (e.g., Project Manager, Technical Lead, Security Lead, Service Manager, Technical Engineer/Coordinator, Provisioning Coordinator). Provide resumes showing experience, qualifications, and relevant certifications. The State reserves approval rights for all Key Personnel and subsequent changes. Provide 30 days' written notice before a Key Person's departure.

LUMEN RESPONSE:

Key Personnel. Successful delivery of the State of Nebraska's statewide ESInet and NGCS depends on the continuity, authority, and technical depth of an experienced team organized within a clearly defined key personnel structure. NG911 deployment is inherently complex, involving concurrent network construction, NGCS integration, OSP coordination, PSAP-by-PSAP migration, cybersecurity controls, and

Experienced NG911 Leadership and Governance Alignment.

Lumen provides an experienced NG911 delivery and operations team (**current program management personnel**) with established familiarity with Nebraska's regulatory environment, operational workflows, and oversight expectations. Governance, reporting, risk management, and service management are aligned from day one through structured monthly reviews, SLA and KPI reporting, risk register updates, and defined escalation ownership.

Benefit to the State of Nebraska: Reduced learning curve, improved responsiveness, consistent performance, and transparent oversight throughout the contract term.

transition to 24x7x365 public safety operations. To manage this complexity without disrupting live 9-1-1 services, Lumen assigns experienced, role-specific key personnel with clearly delineated responsibilities and decision authority.

Lumen designates the following individuals as Key Personnel for the Nebraska ESInet and NGCS contract. These roles remain accountable throughout design, implementation, testing, acceptance, and transition to operations. Lumen recognizes the State's approval rights for all Key Personnel and commits to providing at least thirty (30) days' written notice prior to any proposed change, except in circumstances beyond Lumen's reasonable control. Lumen's Key Personnel, with the exception of our Security Lead, currently support the Nebraska NG911 program, ensuring no gaps in programmatic knowledge or skill sets.

Project Manager - Ms. Angela Schrawyer: The PM serves as the single point of accountability for execution of the Nebraska ESInet and NGCS program. This role controls scope, schedule, resources, risk, issue resolution, and stakeholder communications across all workstreams. The PM integrates network deployment, NGCS readiness, PSAP onboarding, OSP coordination, testing, and cutover into a single governed execution baseline.

For Nebraska, the PM's role is critical because ESInet and NGCS deployment must progress PSAP-by-PSAP while maintaining statewide operational continuity. The PM enforces readiness gates, manages dependencies between PSAPs and third-party providers, and ensures that no PSAP advances to cutover without meeting defined acceptance criteria. The PM also owns formal change management, status reporting, and executive escalation, ensuring the State retains continuous visibility and control.

Deputy Project Manager - Ms. Shelly Guenther: The Deputy Project Manager supports the Project Manager in the execution of the Nebraska ESInet and NGCS program by providing

day-to-day leadership for testing, operational readiness, and transition activities. This role focuses on coordinating lab-based, multi-Originating Service Provider (OSP), and end-to-end testing required to validate NG911 call flows, interoperability, and readiness for migration of live 9-1-1 traffic. The DPM works closely with delivery teams to sequence testing and cutover activities in alignment with PSAP readiness and statewide continuity requirements, and supports installation, testing, and turn-up of supporting components required for operational readiness.

For Nebraska, the DPM plays a key role in maintaining execution discipline during testing and transition phases by coordinating communications with PSAPs, OSPs, and State partners and ensuring readiness criteria are clearly understood and met. The DPM tracks risks, issues, and mitigation actions related to testing, transition, and acceptance activities and reports progress through the established program governance cadence. By reinforcing readiness gates and supporting acceptance activities, the DPM helps ensure that testing and cutover activities are conducted in a controlled manner that protects service continuity and supports successful system acceptance for the State.

Technical Lead (ESInet / NGCS - Engineer/NG911 Coordinator) - Mr. Charlie Knox: The Technical Lead provides architectural and technical authority over the ESInet and NGCS solution. This role ensures that network design, routing behavior, redundancy models, and NGCS functional elements align with NENA i3 requirements and Nebraska operational needs. The Technical Lead validates designs, resolves complex integration issues, and ensures technical consistency across regions and PSAP environments.

For a statewide NG911 deployment, the Technical Lead is essential to preventing implementation fragmentation and configuration drift. This role ensures that ESInet connectivity, NGCS behavior, and PSAP integrations operate as a coherent system rather than a collection of site-specific solutions.

Mr. Knox will also perform in the capacity of the Technical Engineer/NG911 Coordinator supporting detailed execution activities, including PSAP connectivity, integration testing, and cutover coordination. This role bridges high-level design intent and field-level implementation, ensuring that configurations, testing procedures, and cutover checklists are executed consistently.

This role is especially important in a PSAP-by-PSAP deployment model, where repeatability, documentation accuracy, and disciplined execution directly affect schedule predictability and operational safety.

Solution Architect - Mr. Doug Cunningham: The Solution Architect provides technical design leadership and architecture oversight for the Nebraska ESInet and NGCS solution, ensuring that customer requirements, operational needs, and NENA i3 standards are translated into a cohesive, implementable technical design. This role focuses on front-end technical discovery, solution definition, and architecture validation to ensure that the proposed design supports statewide NG911 objectives while enabling disciplined, repeatable implementation.

For Nebraska, the Solution Architect plays a critical role in aligning business, operational, and regulatory requirements with the underlying ESInet, NGCS, and Call Handling Equipment (CHE) architectures. Mr. Cunningham leads structured technical discovery with State stakeholders and internal delivery teams, defines ESInet and NGCS architectural frameworks, and ensures that redundancy models, routing behavior, interconnection designs, and PSAP

integration approaches are consistent across the statewide deployment. This architectural consistency is essential to supporting a PSAP-by-PSAP implementation model without introducing site-specific design drift or unnecessary operational risk.

The Solution Architect works closely with the PM and Technical Lead to ensure that architectural intent is preserved through detailed design, testing, and cutover execution. **Mr. Cunningham** also supports OSP and PSAP integration planning, architectural documentation, and technical reviews, and solution narratives, and architecture diagrams supporting the program. By providing continuity of architectural leadership across design, implementation, and transition, the Solution Architect helps ensure that Nebraska's NG911 solution operates as an integrated statewide system rather than a collection of independent deployments.

Security Lead - Mr. John Sintim

The Security Lead is responsible for ensuring that the ESInet and NGCS environment meets applicable cybersecurity, privacy, and public safety protection requirements. This role oversees network security controls, access management, monitoring, and incident response alignment, and ensures that security considerations are integrated into design, testing, and operations.

In Nebraska's NG911 environment, security is inseparable from availability. The Security Lead ensures that security controls protect systems without introducing latency, instability, or operational risk to 9-1-1 call handling. This role coordinates closely with the Technical Lead and Service Manager to ensure secure transition into operations.

Service Manager - Ms. Michelle Devlin: The Service Manager owns the transition from implementation into steady-state operations and ongoing service management. This role ensures that monitoring, escalation paths, incident response, and service level commitments are fully established prior to final acceptance. The Service Manager provides continuity of accountability once PSAPs transition to live NG911 operations.

For Nebraska, the Service Manager role is critical because PSAP cutovers occur incrementally over time. The Service Manager ensures that each PSAP enters operations with full support readiness and that operational responsibilities are clearly transferred from implementation teams to 24x7 service teams without gaps.

Provisioning/OSP Coordination Lead - Judy Ocondi: The Provisioning and OSP Coordination Lead manages all interactions with OSPs and supporting carriers. This role oversees LOA workflows, trunk provisioning, interconnection testing, and readiness validation to ensure that call ingress aligns with PSAP deployment sequencing. Ms. Blake is supported by Ms. Judy Ocondi who maintains a focus on OSP migrations.

In Nebraska's NG911 program, OSP readiness directly affects cutover timing and call routing integrity. This role ensures that OSP dependencies are actively managed, tested, and synchronized with PSAP readiness rather than becoming schedule-critical surprises.

Customer Engagement Manager - Ms. Mia Blake: Acts as the primary day to day customer engagement point for the State. Coordinates communications related to service performance, issue resolution, billing inquiries, and change notifications. Supports escalation management, cross functional coordination, and long term relationship management to maintain customer confidence and service continuity.

Account Director - Ms. Kim VanDenTop: The Account Director serves as the senior executive point of accountability for Lumen's relationship with the State of Nebraska for ESInet and NGCS services, providing customer governance, executive-level engagement, and strategic alignment throughout ongoing operations and modernization activities. This role maintains a regular communication cadence with State stakeholders to ensure transparency, alignment with State objectives, and timely awareness of service performance, risks, and emerging issues. The Account Director acts as the executive liaison between the State and Lumen's internal program management, operations, engineering, and delivery teams to ensure consistent understanding of priorities and expectations.

For Nebraska, the Account Director plays a critical role in safeguarding uninterrupted NG911 services by partnering closely with program and operations leadership to support service continuity during testing, transition, and steady-state operations. The Account Director aligns carriers, last-mile providers, and internal delivery teams to support statewide service delivery and coordinated issue resolution. When risks or issues arise, the Account Director ensures timely escalation and executive attention to protect mission-critical public safety services and confirms that service delivery, reporting, and operational performance remain aligned with contractual requirements and State expectations.

State Approval and Continuity Commitment. Lumen acknowledges the State of Nebraska's approval rights for all Key Personnel assigned to this contract. Lumen provides at least thirty (30) days' written notice prior to any proposed Key Personnel change and submits replacement qualifications for State review and approval. Lumen maintains role continuity throughout the contract term to preserve institutional knowledge, execution consistency, and operational stability.

Detailed resumes and biographies for each Key Personnel role are provided as **Attachment 2**. Lumen confirms that all Key Personnel possess relevant experience, qualifications, and certifications appropriate to their assigned responsibilities and the critical nature of statewide NG911 services.

4.2.2. Staff Qualifications

The contractor shall supply qualified, experienced personnel devoted to successful contract performance and, upon State request, remove or replace Key Personnel.

LUMEN RESPONSE:

Lumen deploys qualified, experienced personnel who are specifically assigned and devoted to the successful performance of the State of Nebraska ESInet and NGCS contract. Lumen assigns Key Personnel with demonstrated expertise in public safety communications, large-scale IP network deployment, NG911 standards, cybersecurity, service management, and PSAP-by-PSAP transition execution. These individuals maintain continuity of leadership and technical authority across design, implementation, testing, acceptance, and transition to operations.

Lumen recognizes that the effectiveness of the ESInet and NGCS solution depends not only on technical design, but also on the stability, decision-making authority, and experience of the personnel executing the work. Accordingly, Lumen ensures that Key Personnel remain actively engaged throughout the contract term and that staffing levels and skill sets remain aligned with project complexity and operational risk.

The State of Nebraska retains full authority to request the removal or replacement of any Key Personnel whose performance does not meet project requirements or State expectations. Upon receipt of such a request, Lumen acts promptly to address the concern and, when replacement is required, proposes a qualified substitute with equal or greater experience, credentials, and capability to perform the assigned role. Lumen submits replacement qualifications to the State for review and approval prior to assignment.

Lumen provides no less than thirty (30) days' written notice prior to the planned departure or reassignment of any Key Personnel, except in circumstances beyond Lumen's reasonable control. During any transition, Lumen ensures knowledge transfer, continuity of responsibilities, and uninterrupted project execution so that State oversight, schedule integrity, and operational readiness are not impacted.

Lumen's Key Personnel approach ensures that the Nebraska ESInet and NGCS program benefits from stable leadership, technical consistency, and accountability throughout the life of the contract.

4.2.3. Designations, Certifications, and Licenses

Provide evidence that assigned personnel – especially Key Personnel – hold the professional designations, certifications, and licenses necessary to perform their roles effectively.

LUMEN RESPONSE:

Training, Certification, and Professional Qualifications. Lumen ensures that all personnel assigned to the State of Nebraska ESInet and NGCS contract, particularly Key Personnel, possess the professional designations, licenses, certifications, and role-specific qualifications necessary to perform their responsibilities effectively in a public safety environment. NG911 deployment and operations require not only technical proficiency, but also demonstrated knowledge of applicable standards, regulatory obligations, and operational best practices. Lumen addresses this requirement through a combination of formal certifications, targeted training programs, and continuous professional development.

Lumen provides comprehensive training and certification programs to ensure assigned personnel remain current on applicable codes, standards, and regulations relevant to NG911 services. This training includes initial role-based qualification as well as recurring updates to address changes in standards, regulatory guidance, cybersecurity practices, and NG911 operational requirements. Lumen integrates training into both project execution and operational readiness activities to ensure personnel apply current knowledge directly to the Nebraska environment.

Key Personnel assigned to this contract hold, or will hold prior to assignment, professional credentials appropriate to their roles. These credentials include project management, network engineering, cybersecurity, service management, and NG911-specific technical qualifications. Lumen aligns certifications to functional responsibility rather than applying a one-size-fits-all model, ensuring that each Key Personnel role is supported by relevant and defensible credentials.

Project Manager - Ms. Angela Schrawyer. The PM holds a Project Management Professional (PMP) certification, Program Management Professional (PgMP) certification, and designations in Emergency Number Professional (ENP) and National Emergency Number Association (NENA), and maintains formal training in structured project delivery, risk

management, change control, and stakeholder communications. These certifications ensure disciplined control of scope, schedule, and risk across the statewide ESInet and NGCS deployment and supports consistent application of PMI best practices throughout the contract lifecycle.

Deputy Project Manager - Ms. Shelly Guenther. The Deputy PM holds designations in Emergency Number Professional (ENP), NENA, Scrum Product Owner Certified; Scrum Fundamentals Certified, Six Sigma Green Belt and Yellow Belt and maintains formal training in structured project delivery, risk management, change control, and stakeholder communications. These designations and participation in NENA Working Groups ensure disciplined control of scope, schedule, and risk across the statewide ESInet and NGCS deployment and supports consistent application of PMI best practices throughout the contract lifecycle.

Technical Lead - Technical Engineer (ESInet / NGCS) - Mr. Charlie Knox. The Technical Lead holds a Bachelor of Business Administration in Information Systems and brings demonstrated, hands-on NG911 technical leadership through direct experience designing, integrating, and supporting ESInet, NGCS, and Call Handling Equipment (CHE) environments. His qualifications are based on applied delivery experience rather than formal certifications.

Mr. Knox has supported the Nebraska NG911 program since 2023 and currently provides technical leadership for more than 50% of Nebraska PSAPs on CHE projects, including an 18-PSAP implementation completed in 2024. His experience includes NGCS integration, ESInet connectivity, PSAP onboarding support, and system testing in live public-safety environments.

Mr. Knox has also supported NGCS implementations in Sumter County, Lake County, and Osceola County, Florida, continues to support the State of Minnesota NGCS deployment, and contributed technical solution design to the New Jersey NG911 RFP. This combination of formal education and multi-state NG911 delivery experience provides clear evidence that Mr. Knox possesses the technical competence required to perform the Technical Lead role effectively and meet Nebraska's operational and resiliency requirements.

Solution Architect: Mr. Doug Cunningham. The Solution Architect holds professional certifications and role-specific qualifications aligned with NG911 architecture, ESInet design, and NGCS integration. Mr. Cunningham maintains multiple Cisco engineering and design certifications, including Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA), Cisco Certified Network Associate - Voice, and Cisco Certified Design Associate (CCDA). These certifications reflect formal training in network architecture, IP routing, redundancy design, voice and SIP-based services, and complex network integration—all of which are directly applicable to statewide ESInet and NGCS architectures.

In addition to formal certifications, Mr. Cunningham maintains ongoing training through active participation in National Emergency Number Association (NENA) working groups, including the i3 Architecture Working Group and ESInet/Public Broadband Safety Network (PSBN) Interconnection Working Group. He is also an inaugural participant in the NG9-1-1 Interoperability Commission, which provides oversight of NENA's interoperability mandates, PCA guidance, and Forest Guide requirements. This continued engagement ensures current knowledge of NG911 standards evolution, interoperability requirements, and best practices for multi-vendor and multi-provider environments.

Mr. Cunningham has been a member of Lumen's Public Safety organization since 2013 and has spent more than a decade supporting NG9-1-1 architecture, ESInet design, and call-handling integration efforts nationwide. His qualifications are reinforced by extensive applied experience translating regulatory, operational, and customer requirements into standards-aligned solution architectures and supporting those designs through implementation, testing, and operational transition. This combination of formal network certifications, standards participation, and hands-on NG911 architectural experience demonstrates that Mr. Cunningham possesses the professional qualifications necessary to perform the Solution Architect role effectively for Nebraska's statewide ESInet and NGCS program.

Security Lead - Mr. John Sintim. The Security Lead holds recognized cybersecurity certifications, Certified Information Security Manager (CISM), Certified Risk and Information Systems Control (CRISC), CompTIA Security+, Splunk Certified, ServiceNow Certified, and maintains ongoing training aligned with public safety, critical infrastructure protection, and secure network operations. This training ensures effective implementation of security controls, incident response coordination, and alignment with applicable cybersecurity frameworks while maintaining NG911 availability and performance.

Service Manager - Ms. Michelle Devlin. The Service Manager holds extensive service management and operational credentials aligned with ITIL-equivalent service management frameworks. Her qualifications demonstrate the capability to transition the Nebraska NG911 environment from implementation into steady-state operations while maintaining service quality, reliability, and accountability.

Ms. Devlin has completed formal training in service assurance, network performance monitoring, quality of service management, and incident escalation. These credentials support effective execution of incident, problem, and change management processes, including coordinated response to service events, root-cause analysis, corrective action tracking, and controlled change implementation.

Her service management training and hands-on operational experience ensure she can manage service levels, oversee restoration activities, and coordinate cross-functional operational teams to maintain uninterrupted NG911 services. Collectively, these credentials provide evidence that Ms. Devlin is fully qualified to perform the Service Manager role effectively in a mission-critical public safety environment.

Provisioning and OSP Coordination Lead - Ms. Judy Ocondi. The Provisioning and OSP Coordination Lead holds training relevant to carrier interconnection, provisioning workflows, and network service activation. These qualifications support effective coordination with Originating Service Providers, accurate execution of LOA processes, and alignment of interconnection readiness with PSAP deployment schedules.

Lumen maintains records of training completion, certifications, and professional qualifications for all Key Personnel and makes this information available to the State upon request. Detailed resumes and biographies documenting experience, certifications, and relevant qualifications will be provided as an appendix once personnel assignments are finalized.

Through this structured approach to training, certification, and professional qualification, Lumen ensures that the Nebraska ESInet and NGCS program is executed and operated by personnel with the demonstrated expertise required to support mission-critical 9-1-1

services, protect public safety operations, and meet the State's expectations for accountability and performance.

4.3. Implementation

4.3.1. Implementation Approach

The Respondent shall describe an end-to-end approach for implementing ESInet and NGCS to deliver NG911 to all PSAPs. The State will assist with coordination and scheduling; the Contractor is responsible for planning and executing all activities. No service, system, or function is Accepted until the State provides written approval after successful testing and cutover readiness.

LUMEN RESPONSE:

Migration to an IP-Based, SD-WAN-Enabled NG911 Enterprise. Lumen's implementation approach for Nebraska's NG911 environment is grounded in the fact that the State already operates a live, statewide ESInet and NGCS platform under Lumen's current responsibility. Implementation therefore focuses on upgrading and evolving that operational foundation into a fully IP-based, SD-WAN-enabled NG911 enterprise without interrupting emergency services, destabilizing call delivery, or transferring operational accountability.

Rather than recreating infrastructure or standing up parallel systems, Lumen modernizes and enhances the existing statewide architecture through a controlled, phased execution model. This model integrates ESInet deployment, NGCS expansion, PSAP onboarding, testing, cutover, and transition to operations into a single, end-to-end program framework. All activities align to a State-approved architecture baseline that defines transport design, NGCS functional elements, interconnection models, security posture, and operational boundaries consistent across all 68 PSAPs.

Proven OSP Migration Execution Across Nebraska

Lumen has already completed 854 of 879 OSP migrations, supporting 47 wireline, VoIP, and wireless service providers that deliver 9-1-1 traffic to Nebraska communities. This represents the vast majority of OSP migrations required for statewide NG911 enablement and demonstrates Lumen's proven ability to execute complex, multi-provider transitions at scale. The remaining 25 OSP migrations have received State approval for extension through October 2026, reflecting coordinated planning and controlled scheduling. Because Lumen already operates the ESInet and manages these interconnections, the State avoids the disruption, risk, and delay associated with re-establishing OSP relationships or recreating ingress connectivity.

Benefit to the State of Nebraska: This level of completion provides immediate operational stability and positions the State to focus on continued NG911 modernization enhancements rather than foundational migration activities.

Implementation activities focus on enabling SD-WAN orchestration across the existing ESInet, active-active NGCS capacity, and integrating real-time performance visibility across transport, routing, and application layers. These capabilities allow the network to dynamically steer traffic based on live conditions, enforce end-to-end quality of service for emergency communications, and automatically reroute around degradation. The resulting architecture eliminates single points of failure and supports continuous optimization of call delivery rather than static, reactive routing.

Lumen executes deployment using a PSAP-by-PSAP model within a single statewide program baseline. Each PSAP migration is managed as a discrete work package with defined readiness criteria, execution steps, testing requirements, and acceptance gates. This

approach allows Nebraska to advance statewide NG911 capability incrementally while avoiding simultaneous transition risk across all PSAPs. Sequencing is driven by objective readiness and dependency resolution rather than calendar-based assumptions.

Testing and cutover readiness are integrated directly into the implementation lifecycle. Lumen validates the ESInet and NGCS as a complete, end-to-end system, including call delivery from originating service provider ingress through NGCS routing to PSAP termination, failover and contingency scenarios, functional interoperability, performance and resilience behavior, and security enforcement. Cutovers occur only after documented readiness criteria are met, State-approved testing is completed, and formal acceptance evidence is provided.

All implementation activities operate under a unified project management and operational governance structure. Planning, execution, validation, cutover, and steady-state operations remain under a single accountable organization. Enhancements are introduced incrementally, validated under production conditions, and placed into service only after stability and performance are confirmed through a structured test and acceptance process. This approach enables Nebraska to realize modernization benefits early in the contract term while preserving continuous operational stability across the entire statewide NG911 environment.

Why This Matters to the State of Nebraska

For NG911, the greatest risk does not stem from technology selection but from how change is introduced into a live emergency services environment. The most failure-prone phase of NG911 programs occurs when live traffic is assumed by a new operator or when large-scale architectural change is introduced without operational continuity.

Lumen's approach removes that risk. The same organization that operates Nebraska's NG911 environment today designs, implements, validates, and governs all upgrades. There is no transfer of responsibility, no relearning of the network under live conditions, and no period where public safety services depend on an unproven operational model. Modernization occurs within a known, stable environment that already meets the State's performance, availability, and resiliency objectives.

This approach protects public safety operations while allowing Nebraska to advance its NG911 capabilities with confidence, predictability, and full operational transparency.

How This Approach Exceeds State Requirements

The State requires an implementation methodology that preserves service continuity, supports phased execution, enforces resiliency, and eliminates single points of failure. Lumen's approach exceeds these requirements by eliminating entire categories of implementation and transition risk rather than managing them procedurally.

By upgrading an operational NG911 environment instead of rebuilding it, Lumen removes the need for parallel systems, extended stabilization periods, and operational handoffs that other offerors cannot avoid. SD-WAN orchestration delivers continuous optimization and preemptive protection against degradation, exceeding static resiliency and failover models. End-to-end governance ensures uninterrupted accountability from implementation through steady-state operations.

The result is an implementation approach that delivers advanced, IP-based NG911 capabilities faster, with lower risk, and with greater operational certainty than any alternative model.

4.3.2. Elements of Implementation

Provide a comprehensive implementation plan that addresses the full project lifecycle - from design and engineering through testing, training, and final system cutover - aligned with NENA Standards and industry best practices.

LUMEN RESPONSE:

Comprehensive ESInet and NGCS Implementation Plan. This Implementation Plan (Attachment 4) defines Lumen's end-to-end methodology for designing, implementing, testing, training, cutting over, operating, and administering a statewide ESInet and NG911 solution for the State of Nebraska. The plan addresses the full project lifecycle and aligns with NENA i3 standards, FCC reliability requirements, and industry best practices. Lumen assumes responsibility for planning and executing all ESInet and NGCS activities statewide, while the State retains approval authority for milestones, testing outcomes, and acceptance decisions.

Program Governance and Lifecycle Management. Lumen executes the NG911 program using a single statewide governance model with PSAP-by-PSAP execution to maintain consistency, accountability, and risk control. Deployment progresses based on objective readiness rather than uniform timing and is governed through a State-approved Project Management Plan and Change Management process.

Design and Engineering Methodology. Lumen establishes a State-approved design baseline defining ESInet architecture, NGCS functional elements, security controls, redundancy, routing behavior, and operational boundaries. Design activities validate NENA i3 conformance, geographic diversity, OSP ingress models, PSAP egress models, logging, monitoring, interoperability with legacy environments, and accommodation of both TDM and IP ingress paths. The approved baseline becomes the authoritative reference for deployment, testing, and acceptance.

ESInet Implementation Methodology. Lumen builds the ESInet using geographically diverse transport, redundant core routing, Quality of Service (QoS) enforcement, and layered security controls. Implementation activities include circuit provisioning, IP addressing, routing configuration, failover validation, and enablement of continuous monitoring. Each ESInet segment must reach a documented connectivity-ready state before NGCS integration or PSAP cutover.

NGCS Implementation Methodology. Lumen deploys NGCS functional elements, including the Border Control Function, Emergency Services Routing Proxy, Emergency Call Routing Function and Location Validation Function, Location Information Server, logging services, policy routing, and security services across redundant data centers. Functional elements are integrated and tested as a cohesive system to ensure end-to-end call processing, routing, and data exchange operate under real-world conditions.

PSAP-by-PSAP Deployment Methodology. Each PSAP is treated as a discrete work package with defined entry criteria, implementation tasks, testing requirements, and acceptance gates. Lumen validates site readiness, provisions ESInet connectivity, integrates NGCS routing, coordinates OSP readiness, and executes structured testing prior to cutover. PSAP sequencing is actively managed to preserve statewide schedule integrity.

Originating Service Provider Integration Methodology. Lumen coordinates all OSP interconnections through a dedicated OSP Coordinator. Activities include LOA processing, trunk provisioning, interconnection configuration, and interoperability testing. Ingress paths are validated, including TDM-based and SIP-based delivery, with legacy gateways supporting SS7, PRI, or CAMA conversion to SIP. Redundant trunk groups and fallback paths are established for each OSP to prevent single-point failures during both steady-state and transition operations.

System Staging and Pre-Deployment Validation. Prior to field deployment, system components are staged in controlled environments to validate configurations, software and firmware versions, interoperability, and performance. Lumen executes the Staging Acceptance Test Plan (SATP, Attachment 7) and documents results for State review before authorizing production deployment.

Testing and Acceptance Methodology. Lumen conducts phased testing aligned to project milestones to validate the NG911 solution as an integrated system. Testing includes functional, integration, performance, failover, and security testing. Results are documented, deficiencies are resolved, and acceptance packages are submitted for State approval. No component advances without written authorization.

Cutover Methodology. PSAP cutovers are executed using a checklist-driven, phased approach coordinated with the State and PSAP staff. Cutover proceeds only after all prerequisites are met and readiness is demonstrated. Rollback procedures remain active until stability is confirmed and the State authorizes completion.

Training and Operational Readiness. Lumen delivers role-based training for PSAP personnel, State staff, and operational teams, covering system operation, incident management, reporting, and change processes. Documentation, runbooks, and escalation paths are provided prior to cutover.

Transition to Operations. Following cutover, Lumen supports a defined thirty-day operational burn-in period during which performance is monitored, issues are resolved, and operational readiness is confirmed. Upon successful completion, the system transitions to steady-state service management.

Ongoing Administration and Operations Methodology. Lumen administers the NG911 system throughout the contract term using ITIL-aligned service management practices, including twenty-four by seven monitoring, SLA management, incident response, change management, performance reporting, and standards compliance management.

Continuous Improvement and Standards Evolution. Lumen continuously evaluates system performance and evolving NENA standards. Required updates are implemented within contractual timelines and coordinated with the State for review and acceptance to ensure long-term compliance and sustainability.

End-to-End NG911 Capability. This implementation plan delivers a fully redundant, secure, and resilient statewide ESInet integrated with robust NGCS functionality. It supports all PSAPs and OSPs across Nebraska, accommodates legacy and IP-based ingress, and provides a future-ready, interoperable emergency communications environment suitable for long-term statewide operations.

At a minimum, the implementation plan should address:

4.3.2.1. METHODOLOGY FOR IMPLEMENTING THE ENTIRE NG911 SYSTEM

- *Methodology for implementing the entire NG911 system, establishing call delivery from all OSPs to all PSAPs across the State of Nebraska*

LUMEN RESPONSE:

Lumen implements the Nebraska NG911 system using a statewide, standards-based methodology that ensures reliable, secure, and validated call delivery from every OSP to every PSAP. The methodology establishes a single, cohesive NG911 environment while allowing controlled, readiness-based deployment across the State.

At the foundation of this approach is a State-approved ESInet and NGCS architecture aligned with NENA i3 standards. Lumen first establishes the statewide ESInet core, including geographically diverse transport, redundant routing, quality of service enforcement, and security controls. This core provides a consistent and resilient IP transport layer capable of supporting real-time emergency communications and associated data exchange across Nebraska.

In parallel, Lumen deploys and integrates the NGCS functional elements, policy routing, call routing, location validation, logging, security, and interconnection services, within redundant data center environments. These components are engineered and tested as an integrated system to ensure that calls, data, and control signaling traverse the ESInet and NGCS reliably under both normal and abnormal operating conditions.

Statewide call delivery is established through a structured OSP interconnection methodology. Lumen coordinates directly with each OSP to provision ingress connectivity into the ESInet, validate signaling and media handling, and confirm compliance with NG911 interconnection requirements. Each OSP connection is tested end-to-end through the NGCS to verify call setup, routing decisions, location handling, and delivery to the appropriate PSAPs. OSP readiness is tracked and governed to ensure that call delivery dependencies are satisfied before PSAP cutover.

PSAP implementation follows a PSAP-by-PSAP execution model within the single statewide system. For each PSAP, Lumen provisions ESInet connectivity, configures NGCS routing policies, and validates interoperability with call handling equipment. This approach allows each PSAP to be integrated into the statewide NG911 environment without disrupting existing 9-1-1 operations elsewhere in the State.

Before any PSAP is placed into service, Lumen executes comprehensive end-to-end testing that validates the complete call path—from OSP ingress, through the ESInet and NGCS, to PSAP termination. Testing confirms functional call delivery, routing accuracy, failover behavior, and system stability. Although deployment proceeds in phases, testing always validates the NG911 system as an integrated whole to ensure statewide interoperability.

Cutover to NG911 service occurs only after call delivery has been proven and accepted. Lumen performs controlled, coordinated cutovers that transition live traffic while maintaining rollback capability. Existing services remain available until the State confirms that NG911 call delivery is stable and operating as designed.

Through this methodology, Lumen establishes a single, statewide NG911 system that delivers calls consistently from all OSPs to all PSAPs, supports phased deployment without interruption, and provides Nebraska with a resilient, standards-compliant emergency communications environment capable of evolving over the life of the contract.

4.3.2.2. METHODOLOGY FOR ADMINISTERING & OPERATING THE NG911 SYSTEM

- *Methodology for administering and operating the NG911 system for the contract term.*

LUMEN RESPONSE:

Lumen administers and operates the State of Nebraska's NG911 system using a centralized, standards-aligned operational model designed to ensure continuous availability, consistent performance, and long-term sustainability of statewide NG911 services. This methodology governs the ESInet, NGCS, and all associated interconnections for the duration of the contract, while preserving State oversight and approval authority.

Operational responsibility transitions to Lumen following State acceptance and completion of the operational burn-in period. From that point forward, Lumen assumes full accountability for day-to-day system administration, monitoring, coordination, and service assurance, while maintaining transparent governance and reporting to the State.

Operational Governance and Service Management. Lumen administers the NG911 environment under a single statewide operational framework. This framework establishes defined roles, escalation paths, and decision authority to ensure issues are addressed rapidly and consistently. A designated Operations Service Manager serves as the primary operational interface with the State and coordinates across network, NGCS, security, and OSP teams to maintain system integrity.

Operational governance includes:

- Defined service management processes for incident, problem, and change management
- Formal escalation procedures aligned to service impact
- Regular operational reviews with the State to assess performance and trends

24x7 Monitoring, Incident Response, and Service Assurance. Lumen provides continuous monitoring of the ESInet and NGCS infrastructure to detect, isolate, and resolve issues before they affect emergency service delivery. Monitoring encompasses network performance, service availability, routing integrity, and security events. When incidents occur, Lumen follows a structured incident management process that prioritizes service restoration and communication with the State and affected stakeholders.

Incident response activities include:

- Immediate fault detection and classification
- Coordinated response across network, NGCS, and OSP interfaces
- Root cause analysis and corrective action documentation

Change, Configuration, and Release Management. Lumen administers all changes to the NG911 environment through a controlled change management process. This process ensures system stability while allowing necessary updates, enhancements, and standards-driven modifications. Configuration baselines are maintained for ESInet, NGCS, and interconnection components, and all changes are documented and tracked throughout their lifecycle.

No material change is implemented without appropriate review, impact assessment, and coordination with the State.

OSP and Stakeholder Coordination. Ongoing coordination with Originating Service Providers is a core operational function. Lumen maintains established communication channels and service expectations with all connected OSPs to ensure continued compliance, performance, and interoperability. This coordination supports incident resolution, planned maintenance, and onboarding of new or modified OSP connections without disruption to live 9-1-1 services.

Performance Monitoring and Reporting. Lumen tracks operational performance against defined service levels and operational metrics. Regular reports provide the State with visibility into system health, incidents, trends, and improvement initiatives. These reports support informed governance decisions and long-term planning for the NG911 environment.

Security and Compliance Management. Lumen administers NG911 operations in alignment with applicable regulatory, security, and industry requirements. Operational security controls protect the confidentiality, integrity, and availability of NG911 communications and data. Security events are monitored and addressed using established incident response procedures, with coordination as required to support State compliance obligations.

Continuous Improvement and Standards Alignment. Throughout the contract term, Lumen continuously evaluates system performance, operational processes, and evolving NG911 standards. Where updates or enhancements are required to maintain compliance or improve service quality, Lumen incorporates them through controlled operational processes, ensuring continuity of service and State visibility.

Through this operational methodology, Lumen provides Nebraska with a stable, resilient, and professionally administered NG911 environment. The approach emphasizes accountability, transparency, and disciplined service management, ensuring that statewide NG911 services remain reliable, secure, and aligned with evolving public safety requirements for the duration of the contract.

4.3.2.3. IP ROUTING PLAN

- *IP routing plan, how requirements are met, and governance of routing changes and documentation.*

LUMEN RESPONSE:

Lumen's ESInet IP routing plan upgrades the State of Nebraska's NG911 services into a resilient, fully IP-based, SD-WAN-enabled enterprise architecture designed to support continuous emergency communications under all operating conditions. The routing architecture integrates geographically diverse NGCS hub sites and Public Safety endpoints into a single, policy-driven network fabric that delivers deterministic performance, automated resiliency, and centralized operational control.

The routing design leverages a layered underlay and overlay model. Diverse transport networks provide physical and logical path diversity, while a Versa SD-WAN overlay delivers application-aware routing, encryption, segmentation, and real-time performance optimization. This approach ensures that NG911 signaling and media traffic always uses the most performant path while maintaining redundancy, security, and operational transparency across the entire ESInet.

Routing policies, performance thresholds, and change controls are centrally governed and documented, ensuring that all routing behavior remains consistent with State requirements, operational objectives, and approved design baselines.

High-Level ESInet IP Routing Architecture

Network Topology Overview. The ESInet routing architecture consists of geographically diverse NGCS hub sites and branch locations that include CHE host locations. All host sites deploy high-availability Versa SD-WAN appliances and connect through multiple diverse underlay transports to eliminate single points of failure.

Hub Sites (NGCS Hubs):

- Hub A: Diverse MPLS-A, MPLS-B, DIA Internet
- Hub B: Diverse MPLS-A, MPLS-B, DIA Internet
- Hub C: Diverse MPLS-A, MPLS-B, DIA Internet

Branch Sites (CHE Host Locations):

- High-availability Versa SD-WAN appliance pair
- MPLS-A and MPLS-B primary paths
- LEO satellite tertiary path (Optional)
- 5G wireless quaternary path (Optional)

This topology ensures geographic diversity, transport diversity, and device-level redundancy at all critical network locations.

Underlay Transport and Routing Protocols

Primary MPLS Transport Networks. Each hub and branch site connects to two digitally diverse MPLS transport networks, MPLS-A and MPLS-B, which serve as the primary underlay forwarding planes for latency-sensitive ESInet traffic. These transports provide deterministic performance characteristics and support real-time packet replication across both MPLS paths.

Routing across the MPLS underlay follows standard service provider WAN routing practices, including:

- BGP routing adjacency between Lumen provider edge routers and Versa SD-WAN appliances
- Interior gateway routing protocols such as OSPF or IS-IS within the Lumen backbone, outside the ESInet demarcation
- Quality of service and traffic engineering inherent to MPLS service delivery

Tertiary and Quaternary IP Transports. LEO satellite and 5G wireless transports provide tertiary and quaternary IP underlay paths. These transports operate as pure IP networks and carry only encrypted SD-WAN overlay traffic.

Routing on these paths uses default routing or lightweight dynamic routing as appropriate to site type and reachability. These transports do not carry native ESInet application traffic outside the encrypted overlay and serve as resilient continuity options during MPLS impairment.

SD-WAN Overlay Routing and Control Plane

Overlay Construction and Encryption. Versa establishes a secure SD-WAN overlay fabric across all available underlay transports, including:

- MPLS-A
- MPLS-B
- LEO satellite
- 5G wireless
- DIA Internet at hub locations

All overlay tunnels use IPsec encryption, ensuring that traffic remains confidential and isolated across all transport types. Only explicitly permitted traffic is allowed inside encrypted tunnels, and all other traffic is blocked by default.

Within these encrypted tunnels, VxLAN encapsulation provides logical segmentation of ESInet applications and functional domains.

Overlay Routing and Path Selection. Versa maintains secure overlay routing adjacencies between:

- NGCS hub locations
- Branch PSAP and CHE host sites

The overlay control plane distributes routing information, continuously evaluates path performance, and supports application-aware routing decisions based on real-time metrics.

Path scoring and SLA monitoring evaluate:

- Latency
- Jitter
- Packet loss
- Mean Opinion Score (MOS)

These metrics drive dynamic path selection and automated failover behavior, ensuring that NG911 signaling and media traffic consistently uses the best available path.

Overlay Data Plane Behavior. The overlay data plane uses:

- VxLAN for traffic segmentation
- IPsec with AES-based encryption across all underlay transports
- Real-time packet replication across dual MPLS paths for mission-critical ESInet traffic

This design preserves call integrity during partial failures, congestion events, or transport degradation without requiring manual intervention.

Security, Monitoring, and Operational Visibility. The routing architecture enforces segmentation of application traffic and encryption across all transport paths, including Internet, LEO, and 5G. Security policies restrict traffic strictly to approved ESInet flows within encrypted tunnels.

Continuous monitoring provides:

- Path scoring and SLA compliance visibility
- Automated failover events
- Centralized logging and event correlation

These capabilities provide the State and Lumen operations teams with real-time insight into network health and routing behavior.

Routing Governance, Change Control, and Documentation. Lumen governs ESInet IP routing through a State-approved architecture baseline and formal change management

process. The baseline defines routing policies, overlay behavior, transport utilization, and security controls across the ESInet.

Any routing changes, including policy adjustments, path preference updates, or topology modifications, follow documented change control procedures and require State review and approval prior to implementation. All routing configurations, policies, and updates are documented and maintained as part of the authoritative network design record.

As ESInet connections are expanded or modified, this routing plan may be augmented with detailed IP addressing tables, routing policies, and network diagrams that reflect physical path diversity and site-specific deployment details.

4.3.2.4. How NGCS will Operate with the ESInet and Functional Element will Deliver Required Functionality

- *How NGCS will operate with the ESInet, and how each Functional Element will deliver required functionality.*

LUMEN RESPONSE:

Lumen's NGCS operates as an integrated application layer delivered over the State of Nebraska's ESInet, leveraging the ESInet's diverse transports, encrypted SD-WAN overlay, dynamic routing, and application-aware traffic engineering to deliver all NG911 functional capabilities with high reliability, low latency, and full redundancy. The ESInet serves as the foundational transport and orchestration layer for NGCS application delivery, ensuring predictable performance, resiliency, and security across the entire statewide NG911 ecosystem.

The ESInet design incorporates dual MPLS transport paths, LEO satellite and 5G wireless tertiary paths, VxLAN encapsulation over IPsec, high-availability SD-WAN devices at all hubs and Public Safety endpoints, and SLA-driven path selection. Together, these elements provide the transport characteristics required for NGCS functional elements to operate consistently, securely, and without dependency on any single network component.

NGCS Functional Operation Over the ESInet. NGCS functional elements rely on the ESInet for all signaling, routing, and media transport between originating service providers, NGCS core services, and PSAP call handling environments. Because the ESInet is the transport mechanism for NG911 application delivery, most NGCS interactions occur within the lower four layers of the OSI model, where deterministic routing, latency control, resiliency, and packet integrity are critical.

Key interactions include:

- Session establishment and protection through BCF operating at ESInet boundaries
- Secure transport of SIP signaling and media flows across encrypted SD WAN overlay tunnels
- Deterministic routing of NG911 traffic based on real-time network performance rather than static path selection
- Continuous availability of routing, policy, and data services required by NGCS functional elements

While primary traffic flows occur at the transport and network layers, the ESInet also supports application-layer monitoring, logging, and telemetry. These capabilities provide visibility into

NGCS behavior, call flows, and system performance, supporting operational awareness, troubleshooting, and compliance reporting.

Functional Element Delivery and Reliability. Each NGCS functional element operates predictably because the ESInet provides:

- Multiple diverse transport paths to every NGCS hub and PSAP
- Active-active hub architectures supported by SD-WAN overlay connectivity
- Real-time path scoring and application-aware routing decisions
- Automated failover and packet replication across primary MPLS paths

This design ensures that NGCS functions such as call routing, location validation, policy enforcement, and inter-domain connectivity remain available during partial failures, congestion events, or transport impairments. The ESInet does not simply carry NGCS traffic; it actively optimizes and protects NGCS service delivery.

Security, Segmentation, and Performance Assurance. All NGCS traffic traverses the ESInet within encrypted IPsec tunnels, regardless of the underlying transport. VxLAN segmentation isolates NGCS traffic from other domains and enforces strict separation of functional services. Only explicitly authorized traffic is permitted within the overlay, and all other traffic is blocked by default.

Application-aware traffic engineering ensures that NGCS signaling and media flows receive priority handling and use the most performant available path based on real-time SLA metrics. This approach preserves call quality, minimizes latency, and ensures consistent delivery of NGCS services across the statewide environment.

Operational Integration and Governance. The operation of NGCS with the ESInet is governed through a State-approved architecture baseline that defines functional boundaries, routing behavior, security controls, and performance objectives. Any changes affecting NGCS operation, routing policy, or ESInet behavior follow formal change management procedures and require State review and approval prior to implementation.

This governance model ensures that NGCS and ESInet operate as a unified, controlled system rather than as independent components, preserving stability, accountability, and transparency throughout the contract term.

Result. By operating NGCS over a resilient, SD-WAN enabled ESInet, Lumen delivers NG911 functional capabilities that are secure, predictable, and continuously optimized. Each NGCS functional element benefits directly from the ESInet's transport diversity, encryption, application-aware routing, and real-time performance management, ensuring that NG911 services remain reliable and responsive under all operating conditions.

4.4. Transition

4.4.1. Transition Plan: Current and Future

This procurement may require transition from existing systems and/or services provided by the current service provider. The Respondent shall provide a Transition Plan ensuring services are not diminished, interrupted, or disabled and that SLA metrics remain enforced during transition.

LUMEN RESPONSE:

Controlled Evolution to an IP-Based, SD-WAN-Enabled NG911 Enterprise. Nebraska's transition to the proposed NG911 end state is not a migration between providers or a replacement of existing systems. It is a controlled evolution of an already operational NG911 environment under continuous Lumen responsibility. The transition approach is designed to enable advanced, IP-based and SD-WAN-enabled capabilities while preserving uninterrupted emergency services, stable PSAP operations, and established operational procedures statewide.

Because Lumen currently operates the State of Nebraska's NG911 ESInet and supports existing PSAP connectivity and originating service provider points of interconnection, transition activities focus on enhancement rather than replacement. Existing call paths, PSAP integrations, and carrier interconnections remain in service throughout the transition. There is no rip and replace of infrastructure, no forced adoption of unfamiliar systems, and no assumption of live traffic by a new operational entity.

Transition activities introduce modernization enhancements within the current operational framework using parallel operations, controlled activation, and State-approved cutovers. New routing, orchestration, or policy configurations operate alongside existing configurations until validated. All changes retain full rollback capability, ensuring that Nebraska maintains complete control over the timing, scope, and authorization of every transition event.

Where regional changes are required, including transitions associated with changes in call handling equipment or shifts from regional to site-specific delivery models, Lumen provides a detailed, region-specific migration plan within 60 days of contract signing. These plans define sequencing, technical procedures, validation steps, and fallback methods to ensure that each transition is

non-service-affective and aligned with regional operational realities. Migration sequencing accounts for regional complexity, PSAP readiness, position counts, and dependency resolution rather than calendar-based assumptions.

Lumen executes transition using a PSAP-by-PSAP model within a single statewide program baseline. Each PSAP transition is managed as a discrete work package with defined entry criteria, execution steps, testing requirements, and acceptance gates. Lumen's Program Management Office coordinates closely with State representatives, PSAP leadership, originating service providers, and NGCS platform partners to ensure readiness, alignment, and transparency throughout the transition lifecycle.

Integrated testing and cutover readiness are central to the transition approach. Lumen validates end-to-end call delivery, routing behavior, performance, resilience, and security prior to any live cutover. Each transition includes documented fallback procedures that allow a PSAP to be restored to its pre-transition operational state in the event of a catastrophic failure. No transition proceeds without confirmed rollback readiness.

Efficient Transition With Cost and Operational Discipline

Nebraska receives a transition approach informed by Lumen's extensive NG911 deployment experience, enabling parallel execution, staged cutovers, and coordinated training aligned to PSAP readiness. This approach avoids dual billing, limits overlap periods, minimizes repeated testing cycles, and reduces the operational burden placed on PSAP and State personnel.

Benefit to the State of Nebraska: Modernization proceeds on a predictable timeline without unnecessary expense or disruption to PSAP operations or other NG911 stakeholders.

Intrado, as the NGCS platform provider, supports this transition framework by delivering the core NGCS services, interoperability, diagnostics, and technical integration required for seamless validation, cutover, and fallback readiness. Their platform capabilities support end-to-end testing, issue isolation, and verification of system stability at each transition phase.

Why This Matters to the State of Nebraska

NG911 transitions fail most often when operational responsibility shifts or when live emergency services are exposed to untested architectures. Even brief service disruptions or performance degradation can have direct public safety consequences.

Lumen's transition approach avoids these risks entirely. Responsibility for live traffic never changes. Enhancements are introduced only after validation, existing operational states remain continuously available, and fallback procedures are maintained throughout the transition. PSAPs are not disrupted by unnecessary system replacement, retraining, or unfamiliar operational models, and the State is never placed in a position where emergency services depend on unproven infrastructure or processes.

This approach ensures that public safety operations remain stable, predictable, and protected throughout the transition while still allowing Nebraska to advance decisively toward its NG911 modernization objectives.

How This Approach Exceeds State Requirements

The State requires a transition methodology that preserves continuity, minimizes risk, supports rollback, and maintains service levels throughout change. Lumen's approach exceeds these requirements by structuring transition as an extension of ongoing NG911 operations rather than a discrete migration event.

By avoiding rip and replace activities, maintaining parallel operational states, and retaining continuous accountability, Lumen eliminates transition risks that other offerors must attempt to mitigate procedurally. State-controlled cutovers, documented fallback readiness, and PSAP-by-PSAP execution provide a level of control, assurance, and operational confidence that goes beyond baseline requirements.

The result is a transition that achieves the desired IP-based, SD-WAN-enabled NG911 end state with greater confidence, lower risk, and stronger protection of public safety services than any alternative approach.

Minimum topics:

4.4.1.1. TRANSITION SCHEDULE

- *Transition schedule with milestone dates for design, development, testing, implementation, and cutover to full operational readiness.*

LUMEN RESPONSE:

Lumen executes NGCS implementation and transition as a modernization program that advances an already operational statewide ESInet and NGCS environment. The Microsoft Project schedule provided as **Attachment 6** reflects a phased execution model that modernizes transport, expands NGCS resiliency, and upgrades regional connectivity while maintaining uninterrupted NG911 operations statewide.

Phased Regional Deployment Model. Lumen implements NGCS and ESInet modernization using a phased approach consisting of **seven regional deployments**, each staggered in

approximately **four-month cycles with planned overlap**. This sequencing allows Lumen to initiate provisioning and validation activities for subsequent regions while cutover preparation and stabilization activities are underway in the current region. The overlapping cycle structure accelerates statewide modernization while preserving operational continuity and minimizing risk.

Parallel Third NGCS Core Implementation. The schedule incorporates construction and activation of a third NGCS core as a parallel workstream coordinated with Intrado. Third-core activities are not sequenced as a prerequisite to regional SD-WAN deployments. Instead, core connectivity, transport updates, provisioning, and closed user group activities proceed concurrently with regional ESInet circuit upgrades. This parallel execution model allows NGCS resiliency enhancements to advance without delaying regional modernization milestones.

Key third-core activities reflected in **Attachment 6** include:

- Egress core network connectivity orders
- Transport updates to support the additional core
- Core provisioning and replication
- Closed user group provisioning

ESInet and IP Integration Status. The schedule reflects that **IP integration across the ESInet is already complete statewide**. All regions will transition to new ESInet circuits with the SD-WAN solution as part of the modernized end state.

SD-WAN Circuit Modernization. Regional deployment cycles focus on upgrading ESInet transport endpoints with SD-WAN-enabled circuits. These upgrades replace legacy routing endpoints while preserving existing call flows, routing logic, and operational interfaces. The schedule reflects staged, region-by-region SD-WAN introduction, followed by validation and stabilization prior to advancing to the next region.

OSP Interconnection Continuity and POI TDM/IP Strategy. The schedule maintains TDM Points of Interconnection as an ongoing option for OSPs, consistent with State requirements. Migration to IP POIs is performed only at an OSP's request. OSP interconnection activities are therefore not on the critical path for NGCS or ESInet modernization and do not introduce external dependencies that could delay statewide implementation milestones.

Isolated Regional Dependency. The only unresolved schedule dependency is tied to CHE readiness in the Mideast region, which requires completion before that region's i3 upgrade can proceed. This dependency is tracked independently and does not constrain SD-WAN upgrades, third-core implementation, or modernization activities in the remaining regions.

Schedule Governance and Alignment. **Attachment 6** serves as the authoritative Integrated Master Schedule (IMS) governing NGCS implementation and transition activities. Lumen manages sequencing, dependencies, and milestone alignment through formal program governance and change management processes, ensuring State visibility and control as modernization progresses.

All Transition Schedules throughout the life of the agreement will be a living document that accommodates for full alignment with all vendors providing the services to the PSAP.

4.4.1.2. SYSTEM TESTING APPROACH

- *System testing approach during transition.*

LUMEN RESPONSE:

The primary objective for system testing is to demonstrate system readiness leading to a migration of traffic from the current systems to the new one. Test execution will be sequenced starting with network connectivity followed by major system components and finishing with full call testing with each PSAP. The start of systems testing assumes that the component hardware and software has been installed, and the Lumen has completed our internal Network Readiness Testing (NRT). The Test Tools used to execute the testing 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

Lumen's NG911 solution includes a dedicated lab environment for testing CHE compatibility, ensuring that software releases are certified and function seamlessly with call-handling equipment. This lab is used to validate interoperability and performance prior to deployment.

4.4.1.3. PSAP/SITE CUTOVER APPROACH

- *PSAP/site cutover approach, including **phased migration** and **parallel operation** with current systems.*

LUMEN RESPONSE:

Structured Cutover and Acceptance Approach. Lumen's NG911 solution supports a structured and transparent final acceptance process. Each site that is undergoing a transition will have a (1) Readiness period where all connectivity and equipment is staged for each site as appropriate and validated live on the network, then (2) operational readiness testing will occur, followed by (3) migration and full post-migration testing. Each site will have the option to accept their calls on site in alignment with the migration testing, or may opt to have a neighboring PSAP take live calls during testing as appropriate for their site.

System final acceptance (4) will commence only after all designated PSAPs have successfully cut over to the live NG911 system. The acceptance period is defined as 14 consecutive calendar days, during which the solution's performance and reliability will be monitored and validated.

Throughout this period, all contract deliverables operate in full compliance with RFP and contractual requirements. If any failure to comply occurs, State of Nebraska will issue a written notification, and Lumen will respond by remedying the issue in accordance with the Service Levels and Service Management Performance Standards. Upon State of Nebraska's written acceptance of the remedy—or after three business days—the final acceptance period will restart. This cycle will continue until full compliance is achieved, at which point the deliverables will be deemed accepted and a formal Notice of System Final Acceptance will be executed mutually.

Intrado plays a critical role in this phase by ensuring the NGCS platform maintains operational integrity and meets all functional benchmarks during the acceptance period.

Their platform supports detailed logging, performance tracking, and fault isolation, which are essential for validating compliance and reliability.

4.4.1.4. CONTINGENCY AND ROLLBACK PLAN

- *Contingency and rollback plan for implementation or integration failures.*

LUMEN RESPONSE:

Prior to any migration or cutover, Lumen completes full operational readiness testing to validate system stability, integration, and all designed redundancy and failover scenarios. This pre-migration validation confirms that ESInet and NGCS components perform as designed under both steady-state and failure conditions.

Cutover proceeds only after all required vendors have confirmed readiness and each provides an explicit verbal "Go" during a formal Go/No-Go review conducted immediately prior to migration. This review confirms personnel availability, system readiness, and alignment across the State, PSAP, and vendor teams.

While contingencies are rarely required due to this level of preparation, Lumen maintains documented rollback procedures for every transition phase. If the PSAP, the State, or the Lumen PM determines that an issue cannot be mitigated within acceptable timeframes, Lumen executes a full rollback to the prior stable operating state. Rollback activities are completed with all parties present on the live coordination bridge and are followed by structured regression testing to confirm service integrity.

These contingency and rollback procedures are designed to protect 911 call delivery and ensure that no stage of deployment introduces service interruption or uncontrolled risk.

4.4.1.5. RISK, DEPENDENCIES AND INTERDEPENDENCIES AFFECTING CUTOVER

- *Risks, dependencies, and interdependencies affecting cutover.*

LUMEN RESPONSE:

Lumen recognizes that all changes to the NG911 network bring risks, dependencies, and interdependencies which can affect cutover. Lumen is dependent on schedule alignment with the State, the PSAP, Lumen's NGCS Core vendor PM and Engineering teams, Lumen's PM, Engineering, and Field Team resources, and could include other Carriers and vendors that provide services to the PSAP as well.

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 must manage and present these risks to the team to ensure they are considered and addressed as the project progresses.

Lumen will identify, analyze, and respond to all possible risks to ensure delivery of service is not interrupted. During the planning phase of the project, the PM will review each step of the project 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 lifecycle of the project, the PM will develop a mitigation or contingency plan to ensure a successful transition of all contracted services. The next section contains a few of the potential risks.

Potential Risks and Avoidance Measures. Table 4.4.1.5-1 identifies the known risks that may affect the execution and schedule of the project. Each risk identified is associated with a mitigation strategy and contingency plan.

Table 4.4.1.5-1. Risk Assessment and Avoidance Matrix

Area of Risk	Probability	Responsible Parties	Impact	Mitigation Strategy
Network/CPE Order Delayed	High	Lumen	MOE, Network, or Equipment not available within the timeline for install. Delay of installation.	Place all change order and Network orders ASAP and expedite where needed. Next Day ship equipment as needed.
Equipment Delivery Delay	Medium	Lumen	Any delays associated (shipping, order, errors, defective equipment) would impact delivery of final solution.	Staggered delivery schedule to be worked out with the procurement team to deliver as soon as equipment is available, regardless of fulfillment of entire order. Chip shortages are beyond Lumen's control, but we will be transparent with the State with any shortage delays as soon as we are made aware.
Third party (Intrado, & Sub-contractors)	Medium	All parties	Project delays	Urgent and effective communication between all parties will be required in order to maintain the project schedule and reduce delays
Pre-configuration of Equipment and Pre-testing is not successful.	High (when site is moving to a different vendor, equipment, new hardware, and software)	Lumen, Vendor and (possibly) Customer	Functionality of Power Ops must be signed off by customer prior to cut over. 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.	During Power Ops configuration fully vet what the customer would like and discuss any differences in the new system and any possible operational changes needed. Obtain technical support from Vendor as needed.
Purchase Order Errors	Avoidable	Lumen	Installation interval not met.	Conduct a PO review. Conduct a complete inventory when equipment gets on site.
Change of Scope	Medium	Lumen and Customer	Targeted completion date is not met.	Team will define and agree on scope early in the planning phase and follow Change Control process for any changes to the original scope.
Communication Breakdown	Avoidable	Lumen and Customer	Confusion is created in the installation and during implementation.	Set-up project communication mechanisms and guidelines. Full participation by all Team Members.

Lack of Resources	Low	Lumen and Customer	Implementation schedule is not met. Resources will be overworked.	All parties need to be involved in the planning stage and adequate resources secured for installation and cutover.
Customer Responsibilities	Low (with all necessary physical infrastructure in place) Upgrade. High (when all new infrastructure and all new systems) New Install	Customer.	If customer responsibilities are not completed on time, renegotiate project schedule.	Track progress. Request additional resources or work hours. Request installation group to run parallel tasks.
Out of Box Failure of Hardware or Software or recognition of additional equipment requirements to meet customer application	Low (when full scope of work has been fully agreed upon prior to installation) High (when full scope of work has not been fully agreed upon prior to installation)	Lumen, Vendor and (possibly) Customer	The impact will depend on when in the timeline the area of risk is uncovered. If there is time to place a PO and receive equipment leaving plenty of time to test prior to cut over it would not impact the dates. If it occurs to close to cutover, we will renegotiate cutover date.	Expedite PO/order by Sales team. Engage Technical team to assess critical nature to project and timeline. Renegotiate Project Schedule.

4.4.1.6. OSP INTERFACE

- **OSP interface** transition and service migration to the NG911 system.

LUMEN RESPONSE:

Lumen has completed agreements for interconnection with telecom carriers. The solution supports OSP connectivity for wireline, wireless, VoIP, and MLTS traffic, ensuring comprehensive coverage across all call origination types. Lumen coordinates with the State of Nebraska to obtain letters of authority/agency and manages interconnection agreements and trunking in alignment with ATIS-0700015 standards and industry best practices.

Lumen provides an Interface Control Document (ICD) for all OSPs, CHE vendors, and third-party providers requiring ESInet access. We oversee circuit ordering, testing, and integration, and conduct trunk engineering analysis and rebalancing to maintain public safety-grade service levels. The team manages all moves, adds, changes, and deletions for both TDM and IP-based OSP connections, with proactive monitoring and issue resolution workflows.

Connectivity to legacy selective routers is supported to ensure seamless call delivery and transfers to agencies not yet migrated to NG911. This includes bridging functionality and conveyance of Emergency Incident Data Objects (EIDOs). Lumen also facilitates inter-ESInet connectivity with neighboring states and agencies, and defines processes for split rate centers, local number portability, and national number portability.

Note: The EIDO creation and delivery is contingent on support of the interfaces at the PSAP. Current standards are still being developed to supporting these features.

4.4.1.7. INTEGRATION WITH OTHER SYSTEMS, SERVICES AND PROVIDERS

- *Integration with other systems, services, and providers.*

LUMEN RESPONSE:

As part of our deliverables, Lumen ensures each PSAP's Call Handling Equipment (CHE) is seamlessly integrated. CHE compatibility testing is completed with each change so that all call-taking software versions are certified to work with the new NGCS solution as outlined in this request. Policy routing configurations (for transfers, backups, etc.) will be implemented to mirror or improve existing call flows.

The solution includes full integration and provisioning for MLTS databases, enabling accurate location identification for multiline telephone systems and enterprise-originated emergency calls.

Lumen has worked with all OSP providers to integrate their services to the new NG911 POIs throughout Nebraska and will manage future alignment to the new SIP POI solution.

Responsibilities: *If a new provider is selected, the Contractor must engage the current provider and coordinate the transition. If a transition **away** from the Contractor's system is required later (including contract expiration), the Contractor shall cooperatively plan and execute the transition. Current 911 call delivery, features, functions, capabilities, and operations **must not be limited or impacted** by the proposed solution.*

LUMEN RESPONSE:

Lumen will assume responsibility for coordinating all integration and transition activities required to support Nebraska's NG911 environment without disruption to existing 9-1-1 services. If a new provider is selected, we will engage the current provider and work collaboratively to plan and execute a controlled transition that preserves existing call delivery, features, functions, and operational workflows. This coordination includes alignment on interfaces, routing configurations, testing schedules, and cutover sequencing to ensure continuity of service throughout the transition period.

Our approach ensures that all PSAP Call Handling Equipment remains fully functional and interoperable during and after transition. CHE compatibility testing is performed whenever changes are introduced so that existing call flows, transfers, backup routing, and operational capabilities are preserved or improved. Integration with originating service providers is maintained so that current NG911 points of interconnection remain aligned, and future alignment to updated SIP points of interconnection is managed without impacting live operations.

Should a transition away from Lumen's system be required in the future, including at contract expiration, Lumen will cooperatively plan and execute that transition with the State and any successor provider. This planning will be structured to ensure that current 9-1-1 call delivery,

features, functions, capabilities, and operations are not limited or degraded during the transition, preserving continuity of emergency services for Nebraska's PSAPs and the public they serve.

4.5. Testing and Acceptance

4.5.1. Comprehensive Test Plan

System testing is required before acceptance of any component or function and before cutover to full operational status and commencement of payment. With the proposal, provide an example NG911 System Test Plan covering each element of the proposed system. Post-award, the test plan must be submitted to the State for approval at least thirty (30) days prior to the start of testing of any system function or components.

LUMEN RESPONSE:

System testing is designed to confirm correct operation of NG911 functional elements and interfaces using a combination of existing production performance evidence, controlled validation activities, and targeted testing, as appropriate. Testing considerations include:

- Verification of NENA STA 010.3 functional alignment through configuration review, documented compliance artifacts, and observed operational behavior
- Validation of 911 call routing scenarios (primary, alternate, and last resort routing) using controlled test cases and existing production call flow examples
- End to end traffic flow validation across ESInet and NGCS interfaces
- Functional Element to Functional Element and protocol level interoperability confirmation
- Review of ESInet capacity, throughput design, and resiliency characteristics based on engineered capacity models and live operational benchmarks
- Validation of monitoring, fault detection, notification, and failover mechanisms already in service

Because the proposed platform is actively supporting live NG911 traffic, certain intrusive testing activities (e.g., fault injection, disruptive load testing, or prolonged stress testing at extreme levels) may not be appropriate for execution on production systems. Where such testing objectives are identified, Lumen and the State will collaboratively determine acceptable alternative validation methods, such as:

- Use of non-production or segmented test environments, where available
- Historical performance data and production traffic metrics
- Simulated or constrained test scenarios that do not impact live services

All NG911 testing activities will be conducted with State participation rights consistent with the RFP, including the ability to observe testing, require re testing where necessary, inspect test environments and equipment, and approve remediation actions prior to acceptance.

The comprehensive test plan will address, at minimum:

4.5.1.1. TEST ENVIRONMENT, FACILITIES, AND EQUIPMENT.

LUMEN RESPONSE:

Lumen conducts NG911 system testing within controlled lab, staging, and production-parallel environments designed to replicate operational ESInet and NGCS conditions prior to

cutover. Testing is performed in a manner that validates system performance while protecting live 9-1-1 traffic.

As documented in Lumen's NG911 System Test Plan (**Attachment 7**), testing environments include Lumen core network facilities, NGCS data centers, and PSAP sites. These environments support validation of centralized NGCS functions as well as PSAP-specific connectivity and call handling workflows.

Test equipment includes ESInet transport infrastructure, NGCS functional elements (including BCF, ESRP, ECRF/LVF, LIS, logging services), PSAP call handling equipment, and automated test tools such as EXFO Active Assurance probes and call generators. Network devices such as routers, SD-WAN appliances, and firewalls used in the production ESInet are included to ensure configuration fidelity between test and operational environments.

Post award, Lumen will work collaboratively with the State and the NGCS provider to develop a final, Nebraska specific test plan, which will be submitted for State review and approval in advance of execution. The final test plan will be mutually agreed upon to ensure testing objectives are met without introducing risk to live 911 operations or existing production traffic.

4.5.1.2. TEST CONFIGURATIONS AND THRESHOLDS.

LUMEN RESPONSE:

The NG911 System Test Plan defines repeatable test configurations and objective acceptance thresholds for all system components and interfaces. Test configurations include baseline, alternate, and failover routing scenarios supporting PSAP-to-PSAP, on-net, off-net, and Originating Service Provider (OSP) call delivery.

Test cases are executed across multiple call types, including wireline, wireless, VoIP, and business-originated calls. Configuration variables include routing policy, PSAP destination, transfer type, and network path selection.

Acceptance thresholds are defined for call setup and transfer timers, delivery of ANI/ALI and PIDF-LO location objects, media quality and continuity, and system stability during extended operation. Performance validation includes sustained operation and reliability testing, including extended-duration testing defined in the 30-day reliability plan.

4.5.1.3. SIMULATORS AND TEST-CALL PROCESSES.

LUMEN RESPONSE:

Lumen employs both automated simulators and live test-call processes to validate NG911 functionality under normal and fault conditions. Automated testing uses NG911-capable call generators and EXFO probes to generate i3-compliant test calls and measure end-to-end signaling, routing, and media performance.

Manual test calls are initiated through the ESInet and NGCS to PSAP call takers to validate operational workflows, call handling behavior, transfers, conferencing, and call termination.

The test plan includes simulation of fault conditions such as network outages, device failures, and alternate routing activation. These scenarios validate failover behavior, recovery, monitoring, and alarm notification mechanisms while confirming continuity of emergency service delivery.

4.5.1.4. FINAL DOCUMENTATION OF ALL TESTS AND RESULTS.

LUMEN RESPONSE:

All NG911 system testing activities are fully documented in accordance with the System Test Plan. Documentation includes test identifiers, configurations, execution dates and times, pass/fail results, observations, and issue notes.

Defects identified during testing are tracked through resolution, including documentation of corrective actions and retesting results. Acceptance test reports, cutover checklists, and reliability summaries are compiled and retained as part of the formal acceptance record.

Final test documentation is provided to the State for review prior to acceptance and supports auditability, traceability, and long-term operational reference.

4.5.1.5. SYSTEM TESTING MUST ADDRESS, AT MINIMUM:

- *NENA-STA-010.3 Functional Element testing.*

911 call flow: primary, alternate, last route.

- *End-to-end traffic flow.*
- *Functional Element ↔ Functional Element tests.*
- *Protocol ↔ Protocol tests.*
- *Port ↔ Port tests.*
- *Load testing: unexpected surge, short burst, sustained overflow.*

ESInet throughput and capacity.

ESInet end-to-end connectivity (fault tolerance, failover, alternate routing, monitoring systems, fault notification).

Security controls: firewalls, intrusion detection systems, intrusion prevention systems.

- *Throughput acceptance testing of ≥24 hours, simulating 200% peak traffic load.*

LUMEN RESPONSE:

State-Approved Acceptance Testing. Lumen conducts PSAP acceptance testing through the execution of approved pre-cutover Acceptance Test Procedures, as defined in **Attachment 7**, to confirm that the NG911 solution operates as expected and that each PSAP is ready for transition to live service. Testing validates PSAP-specific requirements, including policy enforcement, call transfer capabilities, location and incident data conveyance, and support for text conversation transfers.

Pre-Cutover Validation and Change Control. Lumen commits to completing PSAP acceptance testing no more than 30-days prior to cutover, providing documented confirmation of readiness. Upon successful completion of testing, Lumen enforces a change control freeze, except in extreme cases, to prevent system maintenance or configuration changes that could compromise PSAP readiness before go-live.

NGCS Functional and End-to-End Verification. Intrado supports PSAP testing by ensuring NGCS functional elements, including LoST routing, HELD queries, and ADR integration, are validated and operational, with detailed logging and traceability available to support compliance and audit readiness. Testing confirms end-to-end call flows for primary, alternate, and last-route scenarios from originating service provider ingress through the ESInet and NGCS to PSAP termination, along with interoperability, load, failover, throughput, and security controls. Throughput testing is conducted for a minimum of 24-hours at up to 200% of anticipated peak volumes, with results documented and submitted for State review.

4.5.1.6. STATE PARTICIPATION AND RIGHTS:

Share results with the project team prior to acceptance; the State may require re-tests and may assign observers. The State may inspect test equipment and/or applications and must approve remediation actions from failed tests.

LUMEN RESPONSE:

Lumen acknowledges that comprehensive system testing is a prerequisite to acceptance of any NG911 system component or function and to cutover to full operational status, consistent with the testing and acceptance framework established in the Nebraska NG911 RFP. Lumen will conduct system testing prior to acceptance to validate that the proposed ESInet and NGCS solution performs as designed and conforms to applicable NENA STA 010.3 requirements.

With this proposal, Lumen provides our NG911 System Test Plan (**Attachment 7**) representative of the testing approach to be used for the proposed solution. Post award, Lumen will submit a detailed, project specific comprehensive test plan to the State for review and approval no less than thirty (30) days prior to the start of testing for any system function or component.

The comprehensive test plan will address, at a minimum, the test environment, facilities, and equipment; test configurations and performance thresholds; simulators and test call processes; and final documentation of all tests performed and results obtained. System testing will include functional, interoperability, performance, and resiliency testing consistent with Nebraska NG911 requirements, including NENA STA 010.3 Functional Element testing; end to end 911 call flow validation; Functional Element to Functional Element, protocol to protocol, and port to port testing; load and stress testing; ESInet throughput and capacity validation; end to end connectivity and failover testing; and verification of applicable security controls.

Lumen will support extended throughput acceptance testing to validate system performance under sustained and peak traffic conditions prior to acceptance. Test results will be documented and shared with the State project team for review before acceptance decisions are made.

The State will be afforded participation rights consistent with the Nebraska RFP, including advance access to test results, the ability to assign observers, and the right to require re testing if acceptance criteria are not met. Lumen will cooperate with State inspection of test equipment or applications as requested and will propose and implement remediation actions for any failed tests, subject to State review and approval.

4.5.2. Test Plan Methodology

Describe the methodology for testing all NG911 system components, including those provided by Subcontractors or other suppliers, addressing the coverage area in §C-5.a. (Testing). Include regression testing procedures following defect remediation.

LUMEN RESPONSE:

Lumen applies a structured, end-to-end testing methodology to validate all NG911 system components prior to acceptance, including ESInet services provided by Lumen and NGCS components provided by its subcontractor, Intrado. The methodology ensures that all system

elements function as a fully integrated solution and perform in accordance with applicable NG911 requirements and NENA STA 010.3 across the defined coverage area.

Testing is planned and executed using a comprehensive test plan that defines test objectives, configurations, environments, and acceptance criteria for each system component and interface. The methodology includes functional, interoperability, performance, resiliency, and security testing and addresses both standalone component validation and integrated system behavior. Test scenarios validate NENA STA 010.3 Functional Elements, primary, alternate, and last-route 911 call flows, end-to-end traffic flow, Functional Element-to-Functional Element interactions, protocol-to-protocol interoperability, and port-to-port connectivity.

Lumen coordinates all testing activities with Intrado and any other applicable suppliers to ensure consistent test execution, shared visibility into results, and traceability of issues across system boundaries. Simulators and test-call processes are used as appropriate to validate normal operating conditions, fault scenarios, failover behavior, and recovery operations. Load and stress testing is performed to verify system performance under unexpected surge events, short-duration bursts, and sustained overflow conditions.

All test cases, execution results, defects, and resolutions are documented and provided to the State for review prior to acceptance decisions. When defects are identified, remediation actions are implemented and followed by structured regression testing to confirm that corrective changes resolve the issue without introducing unintended impacts to previously validated functionality. Regression testing includes re-execution of affected test cases and any dependent workflows necessary to confirm continued system stability and conformance.

This testing methodology ensures that all NG911 system components, whether provided directly by Lumen or by Intrado as a subcontractor, are fully validated, properly integrated, and operationally ready prior to acceptance.

4.5.3. System Acceptance Testing

Acceptance testing must be completed prior to the State's final acceptance of the system. Final certification and system acceptance occurs only after the Contractor has provided acceptance test results to the State and the State has certified that the testing satisfactorily meets all requirements.

The Respondent must describe their approach for documenting the test results and may use the following codes to discuss their methodology:

- TP - Test Passed
- TF - Test Failed
- RTP - Retest Passed
- RTF - Retest Failed
- NA - Feature not applicable to the final configuration

On any failure the Contractor shall correct the deficit and perform regression testing to re-validate and re-certify all affected tests. Results of failed tests shall be documented and presented in writing to the State. Successful regression testing results must be delivered to the State

LUMEN RESPONSE:

Lumen will complete system acceptance testing prior to the State's final acceptance of the NG911 solution. Final certification and system acceptance will occur only after Lumen has

provided documented acceptance test results to the State and the State has confirmed that all testing satisfactorily meets the requirements of the contract.

Acceptance testing will validate the integrated performance of all ESInet and NGCS components, including those provided by Lumen and those provided by its subcontractor, Intrado. Test execution will follow the approved comprehensive test plan and will confirm that the system functions as designed, performs within defined thresholds, and meets applicable NENA STA 010.3 requirements.

Test results will be documented in a structured acceptance test report that clearly identifies each test case, expected results, actual outcomes, and final status. Lumen will use the following standard status codes to document acceptance testing results:

- **TP (Test Passed):** Test executed successfully and met all acceptance criteria
- **TF (Test Failed):** Test executed but did not meet acceptance criteria
- **RTP (Retest Passed):** Corrective action completed and retest successfully met acceptance criteria
- **RTF (Retest Failed):** Retest executed but did not meet acceptance criteria
- **NA (Not Applicable):** Test not applicable to the final system configuration

If any test fails, Lumen will correct the identified deficiency and perform regression testing to re validate and re certify all affected functionality. Failed test results, root cause analysis, corrective actions, and retest outcomes will be documented and presented to the State in writing. Successful regression testing results will be provided to the State for review prior to acceptance.

Lumen will not request final system acceptance until all required acceptance tests have successfully passed or have been otherwise resolved to the State's satisfaction.

4.5.4. Independent Validation and Verification (IV&V)

Upon acceptance, the State will conduct IV&V testing using a third party. The Contractor shall collaborate to establish IV&V scope and priorities and support execution.

The Respondent MUST state acceptance of third-party IV&V testing of all elements required in this procurement document in its response to this RFP.

LUMEN RESPONSE:

Lumen acknowledges and accepts the State's right to conduct Independent Validation and Verification (IV&V) testing of the NG911 system using a third party provider. Lumen expressly accepts third party IV&V testing of all system elements required under this procurement, including ESInet components provided by Lumen and NGCS components provided by its subcontractor, Intrado.

Lumen will collaborate with the State and the State selected IV&V provider to establish the scope, priorities, and schedule for IV&V activities. This collaboration will include coordination of test objectives, access to relevant system documentation, test environments, configurations, and acceptance test results necessary to support effective IV&V execution.

Lumen and Intrado will support third-party IV&V testing activities by participating in planning sessions, responding to inquiries, assisting with test execution as appropriate, and addressing any findings identified during the IV&V process. Any issues identified through

IV&V will be reviewed collaboratively with the State, and corrective actions will be implemented and validated in accordance with the approved remediation and regression testing processes.

5. RESPONSE TO TECHNICAL REQUIREMENTS

5.1. ESInet Requirements

5.1.1. ESInet Compliance with NENA STA-010.3-2021

The Emergency Services IP Network (ESInet) must comply with NENA-STA-010.3-2021 (i3 Standard) and follow the recommendations in the NENA Emergency Services IP Network Design (ESIND) Information Document (NENA-INF-016.2-2018). The ESInet shall interconnect all NG911 components with Public Safety Answering Points (PSAPs) and Originating Service Providers (OSPs) using Internet Protocol (IP), and, where necessary, legacy methods.

The Respondent shall provide an ESInet design that conforms to the NENA i3 architecture for a managed IP-based emergency services network. The design shall support multi-tenant interconnects with the Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP), diverse physical routing paths, and network-level redundancy that eliminates any single point of failure. The ESInet must natively support IPv4 and IPv6, implement Quality of Service (QoS) to prioritize emergency traffic, and use virtual routing or equivalent technologies to segregate emergency services traffic from non-emergency traffic. The design shall include scalable bandwidth to handle peak loads, with automatic traffic shaping and congestion management.

LUMEN RESPONSE:

Lumen will provide an Emergency Services IP Network (ESInet) for the State of Nebraska that fully complies with NENA-STA-010.3-2021 (i3 Standard) and aligns with the design practices recommended in the NENA Emergency Services IP Network Design (ESIND) Information Document. Our ESInet architecture interconnects all NG911 system components, including PSAP call-handling equipment, NGCS functional elements, and Originating Service Providers (OSPs), using standards-based IP interfaces while supporting required legacy connectivity during the transition from legacy 911 to full i3 operations. The design is engineered to eliminate any single point of failure by incorporating geographically diverse core nodes, redundant network elements, and physically diverse routing paths that maintain end-to-end call and data delivery continuity.

The proposed ESInet design conforms to the NENA i3 architecture for a managed, mission-critical IP-based emergency services network. The ESInet supports multi-tenant interconnections with both the Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP)-based OSPs, enabling seamless ingress and egress of emergency traffic. Where legacy interconnection is required, we employ protocol and media gateway functions to bridge TDM and other non-IP signaling methods into the i3 environment without compromising routing integrity or standards alignment. We implement redundant transport paths, diverse carrier options where available, and high-availability routing so that failure of any single device, link, or facility does not interrupt call delivery to the NGCS platforms or PSAPs.

The solution provides native support for both IPv4 and IPv6 throughout the ESInet. We apply end-to-end Quality of Service (QoS) to prioritize emergency communications traffic—voice, media, signaling, and NG911 data flows—over all other permitted traffic. We use virtual routing and forwarding (VRF) or functionally equivalent network virtualization technologies to

ensure strict traffic segregation between emergency services and non-emergency or administrative traffic. This segmentation protects the performance, security, and integrity of 911 traffic while maintaining a clean separation of routing domains.

We deliver scalable bandwidth across the ESInet to accommodate normal and peak operational loads, including anticipated increases in multimedia traffic as NG911 capabilities expand. Our network elements support automatic traffic shaping, congestion management, and admission control mechanisms that maintain required service levels under abnormal or high-volume conditions.

This ESInet design provides a resilient, standards-compliant technical foundation for Nebraska's NG911 environment and supports the state's transition from legacy 911 infrastructure to a full i3 implementation.

5.1.2. The ESInet shall support SIP per RFC 3261 and applicable NG911 SIP extensions

*The ESInet shall support SIP per **RFC 3261** and applicable NG911 SIP extensions, including SIP over **Transport Layer Security (TLS)** for signaling and **Secure Real-time Transport Protocol (SRTP)** for media. Standard transports, including full IPv6 compatibility shall be supported, including TLS over TCP, and UDP where applicable. Interfaces must support both location-by-reference and location-by-value conveyance to ensure seamless integration with OSPs.*

LUMEN RESPONSE:

Lumen provides SIP support in accordance with RFC 3261 and applicable NG911 SIP extensions. Our ESInet enables SIP over Transport Layer Security (TLS) for signaling and Secure Real-time Transport Protocol (SRTP) for media to ensure secure, standards-compliant NG911 call processing across all network segments.

We support standard IP transports, including full IPv6 compatibility, with TLS over TCP and UDP where applicable. These transport options ensure interoperability with NG911 functional elements, PSAP equipment, and Originating Service Providers (OSPs) operating in mixed-protocol environments.

Our interfaces support both location-by-reference and location-by-value conveyance to maintain seamless integration with OSPs. This ensures accurate delivery of caller location information across the ESInet in alignment with NENA i3 expectations and Nebraska's NG911 operational requirements.

5.1.3. ESInet Support for Standard Cross-Connect & Peering Arrangements, Selective Routing and Boundary Elements

*The ESInet shall support standard cross-connect and peering arrangements, selective routing, and boundary elements such as **Border Control Functions (BCFs)**. **Border Gateway Protocol (BGP)** shall be used for multi-site reachability and load distribution. The Respondent shall provide documented procedures, application programming interfaces (APIs), and configuration templates for peering with adjacent ESInets, third-party providers, and legacy networks, including policy-based routing and traffic-exchange agreements.*

LUMEN RESPONSE:

Lumen provides an ESInet that supports standard cross-connect and peering arrangements, selective routing, and boundary elements such as Border Control Functions (BCFs). Border Gateway Protocol (BGP) is used to provide multi-site reachability and load distribution across Nebraska's ESInet core and edge locations.

Our design supports peering with adjacent ESInets, third-party providers, and legacy networks using standards-based interfaces and policy-driven routing. Boundary elements enforce traffic control, security, and interoperability so that NG911 traffic is exchanged predictably and in accordance with established routing policies.

We furnish documented procedures, application programming interfaces (APIs), and configuration templates to guide external entities in establishing and maintaining peering with the ESInet. These materials address policy-based routing behavior, traffic-exchange parameters, and peering conditions, supporting consistent implementation of traffic-exchange agreements across all interconnected networks.

5.1.4. Diversity, Redundancies and Transparent Failover

*The ESInet shall incorporate geographically diverse, redundant network cores; duplicate session border/edge elements; and automatic, transparent failover for signaling and media so that failure of any single component (e.g., link, router, or server) does not disrupt 911 service. The Respondent shall define and guarantee a **Recovery Point Objective (RPO)** of less than one (1) minute and a **Recovery Time Objective (RTO)** of less than five (5) seconds for critical paths, with active-active or active-passive configurations across data centers separated by at least 100 miles.*

LUMEN RESPONSE:

Lumen provides an ESInet solution designed with geographically diverse network cores and redundant session border and edge components to maintain uninterrupted 911 service. Our architecture distributes signaling and media processing across multiple core locations with independent power, transport, and facility paths so that failure of any single router, link, or server does not affect call delivery across Nebraska.

Our design maintains service continuity through automatic, transparent failover mechanisms for both signaling and media. These mechanisms monitor component health and shift traffic to alternate nodes without operator intervention, ensuring that active call sessions remain intact during device or path failures. We operate core sites in configurations that support active-active or active-passive roles, with data centers separated by more than 100 miles to mitigate regional hazards and meet the State's geographic-diversity expectations.

We engineer the ESInet to meet the required Recovery Point Objective of less than one minute and a Recovery Time Objective of less than five seconds for critical service paths. These objectives are met through synchronized state replication across redundant systems and rapid session re-establishment methods that enable NG911 functional elements to resume operations immediately following a fault. Our architecture ensures that Nebraska's 911 traffic remains protected from localized disruptions while preserving end-to-end service availability across all ESInet ingress, core, and egress points.

5.1.5. DiffServ or Equivalent QoS Policies

The ESInet shall enforce Differentiated Services (DiffServ) or equivalent QoS policies to prioritize 911 signaling (for example, SIP INVITE transactions) and media streams, with configurable DSCP markings. It must support bandwidth provisioning, traffic policing, and shaping to maintain PSAP-grade voice quality (Mean Opinion Score [MOS] greater than 4.0) and data integrity under load, including mechanisms to handle burst traffic and to prevent overload.

LUMEN RESPONSE:

Lumen provides Quality of Service (QoS) controls that enforce Differentiated Services (DiffServ) or equivalent mechanisms to ensure 911 signaling and media receive the highest priority across the ESInet. Our implementation applies configurable DSCP markings to SIP signaling, RTP media, and NG911 data flows so that critical traffic is consistently prioritized across all core and access segments of Nebraska's network.

We engineer bandwidth provisioning, traffic policing, and shaping into the ESInet to maintain PSAP-grade voice quality and data integrity under a wide range of operating conditions. These controls allocate sufficient capacity for real-time media, enforce rate limits to prevent congestion, and smooth burst traffic to preserve voice performance. Our QoS policies and media-handling architecture are designed to maintain a Mean Opinion Score (MOS) greater than 4.0 during normal and peak load conditions.

Our traffic-management approach includes mechanisms that detect and mitigate overload conditions before they affect service. By combining admission control, prioritization, and dynamic shaping, we protect signaling and media paths from degradation and ensure that emergency calls continue to be delivered with the required quality and reliability across Nebraska's ESInet.

5.1.6. Comprehensive Management Systems

*The Respondent shall supply a comprehensive **Network Management System (NMS)** or **Element Management System (EMS)** with real-time dashboards; syslog export; SNMPv3 polling and traps; and key performance indicators (KPIs) including latency, packet loss, jitter, and utilization, aligned with NENA operational guidance. The system must provide threshold-based alerting, historical trend analysis, and integration with external tools via APIs.*

LUMEN RESPONSE:

Lumen delivers an Executive Network Dashboard as part of the ESInet Network and Element Management System (NMS/EMS), providing State leadership and operational stakeholders with immediate, authoritative visibility into network performance and service health. The dashboard presents real-time operational statistics, supports historical analysis, and allows on-demand export of metrics to support oversight, reporting, and planning. The Executive Network Dashboard provides the State the following capabilities:

- **Real-Time Network Performance Statistics.** The dashboard displays live ESInet performance indicators, including latency, jitter, packet loss, and utilization, aligned with NENA operational guidance. Metrics update continuously to reflect current conditions across ingress, core, and egress segments.

- **Threshold-Based Alerting and Status Visualization.** Visual indicators and alerting logic identify when performance metrics approach or exceed defined thresholds, enabling executive and operational users to quickly understand network health and potential risks.
- **Downloadable and Exportable Metrics.** All dashboard statistics and performance data are downloadable in standard formats, allowing the State to retain records, support audits, conduct independent analysis, or incorporate data into executive reports and planning artifacts.
- **Historical Trending and Capacity Analysis.** The dashboard supports historical views and trend analysis to validate performance over time, support capacity planning, and confirm compliance with service objectives.
- **Standards-Aligned Data Collection and Integration.** Dashboard data is derived from SNMPv3 polling, traps, and syslog feeds from ESInet elements. Secure APIs are available to allow Nebraska to integrate NMS/EMS data with external monitoring or analytics tools while preserving access control and data integrity.

This NMS dashboard provides the State with clear, actionable insight into ESInet performance in both operational and executive contexts, combining real-time awareness with durable, exportable data for governance and long-term oversight.

Figure 5.1.6-1 provides an example report available through our NMS dashboard.



Figure 5.1.6-1. Executive Network Dashboard Statistics - Real-time and Downloadable

5.1.7. Documentation Supporting Requirements

The Respondent must provide a description and/or documentation that supports the requirements in this section, including a clear description of:

- Network operations management (operational policies, staffing, incident response, and system management procedures).
- Detailed physical and logical security measures (encryption protocols, access controls, secure access points, and physical security for data centers); strategies for achieving 99.999% uptime with contingency plans.

- *Continuous performance monitoring mechanisms with logging and alert systems; real-time alarm generation and notification strategies.*
- *Guidelines for routine, updates, and emergency maintenance; comprehensive disaster recovery plan with RTO and RPO details.*
- *Procedures for service restoration post-incident.*

LUMEN RESPONSE:

Lumen will provide documentation that describes how our network operations, security controls, monitoring systems, and recovery processes satisfy the ESInet requirements. Our operational framework includes policies for network management, staffing, incident response, and system administration that define how we maintain service continuity and govern day-to-day ESInet operations within Nebraska.

We detail the physical and logical security measures applied across the ESInet, including encryption protocols, access control enforcement, secured network entry points, and the physical protections used at geographically diverse data centers. These materials also explain the strategies we use to achieve **99.999%** availability, including redundancy models, contingency planning, and facility-level safeguards.

Our documentation outlines continuous performance-monitoring mechanisms with integrated logging, alerting, and real-time alarm generation. These tools provide immediate notification of conditions that could affect call delivery and support proactive issue resolution.

We also supply guidelines for routine maintenance, update procedures, and emergency maintenance workflows, along with a comprehensive disaster recovery plan that includes the ESInet's RTO and RPO. Procedures for restoring service following an incident are included to ensure that Nebraska has clear, actionable processes for post-event recovery and verification of full service restoration.

5.1.8. Proactive outage prevention and response strategies including redundancy testing

- *Technical specifications for core routing architecture with diverse paths and load balancing.*
- *Interfaces with hosted solutions or third-party providers.*
- *Fault zone design methodology identifying critical components and failure points.*
- *Bandwidth management protocols prioritizing emergency traffic.*
- *And any bandwidth sharing arrangements with implications for priority traffic.*
- *Any limitations in the "span of control" over connections to the OSPs or PSAPs that are linked to the ESInet to establish a risk register for future reference.*

Additionally, the Respondent must investigate and document potential single points of failure, explain detection and activation of standby systems if not active-active, and detail ESInet interconnection points with OSPs and PSAPs for full IP-based NG911 functionality.

LUMEN RESPONSE:

Lumen will provide technical documentation that addresses each of the requirements in this section and clearly describes how our ESInet architecture, operations, and risk management

approach are implemented for Nebraska. This material will be structured so evaluators can trace each requirement to specific design elements, interfaces, and controls.

We will include:

- **Core routing architecture:** Detailed physical and logical diagrams of the ESInet core, showing geographically diverse paths, redundant routers, and load-balancing mechanisms (such as Equal-Cost Multi-Path and policy-based routing) used to distribute traffic and avoid concentration on any single link or node.
- **Interfaces with hosted and third-party solutions:** Descriptions of how the ESInet interconnects with hosted NG911 platforms, third-party providers, and adjacent networks, including the use of SIP over TLS, secure VPN or private transport, and boundary functions that control and monitor traffic entering or leaving the ESInet.
- **Fault zone design methodology:** A documented fault-zone model that groups network elements into zones, identifies critical components and their dependencies, and analyzes how failures in each zone could affect call and data flows. This includes identification of protection mechanisms and failover behaviors for each fault scenario.
- **Bandwidth management and sharing arrangements:** Explanations of the QoS and bandwidth-management protocols used to prioritize emergency traffic, including class-based queuing, policing, and shaping policies applied to signaling, media, and NG911 data. Where any bandwidth is shared with non-911 services, we will document those arrangements and show how priority and preemption policies ensure that 911 traffic remains protected.
- **Span of control and risk register:** A clear description of our operational span of control versus portions of the end-to-end path managed by OSPs, PSAPs, or other entities. We will use this to establish a risk register that catalogs dependencies and potential exposure at these boundaries, along with associated risks and mitigation strategies for future reference.
- **Single points of failure, standby activation, and interconnection points:** An assessment of potential single points of failure within the ESInet design, including any residual risks that cannot be fully eliminated. We will explain how monitoring and health-check mechanisms detect failures and activate standby systems in configurations that are not active-active, and we will document ESInet interconnection points with OSPs and PSAPs, at both physical and logical levels, to demonstrate how full IP-based NG911 functionality is achieved end-to-end.

5.1.9. Architecture and Topology

5.1.9.1 ESINET DIAGRAMS

The contractor must submit comprehensive diagrams that visually represent the proposed ESInet architecture. These diagrams must be kept current and be included in a configuration management database that the 911 Advisory Committee and the State may access at any time during the contract to validate the deployment and system functionality.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive diagrams illustrating network maps (logical and physical topologies).
- Physical and logical path diversity for redundancy.
- One-time and transitional network elements.
- Network ingress and egress points with connections to OSPs, PSAPs, and external interfaces.
- Transport types (e.g., MPLS or Ethernet) with port speeds.
- Capacities and estimated bandwidth at ingress, core, and egress points.
- Interconnection locations (nodes, data centers, POIs, LRGs); and any additional technologies and interfaces.

LUMEN RESPONSE:

Lumen will provide comprehensive diagrams that visually represent the proposed ESInet architecture and maintain these artifacts within a configuration management database accessible to the State and the 911 Advisory Committee throughout the contract term. These diagrams will remain current as the deployment evolves and will serve as authoritative references for validating system functionality, interconnection points, and operational topology. **Figure 4.1.3.6-1** depicts the proposed Lumen ESInet - NG911 solution.

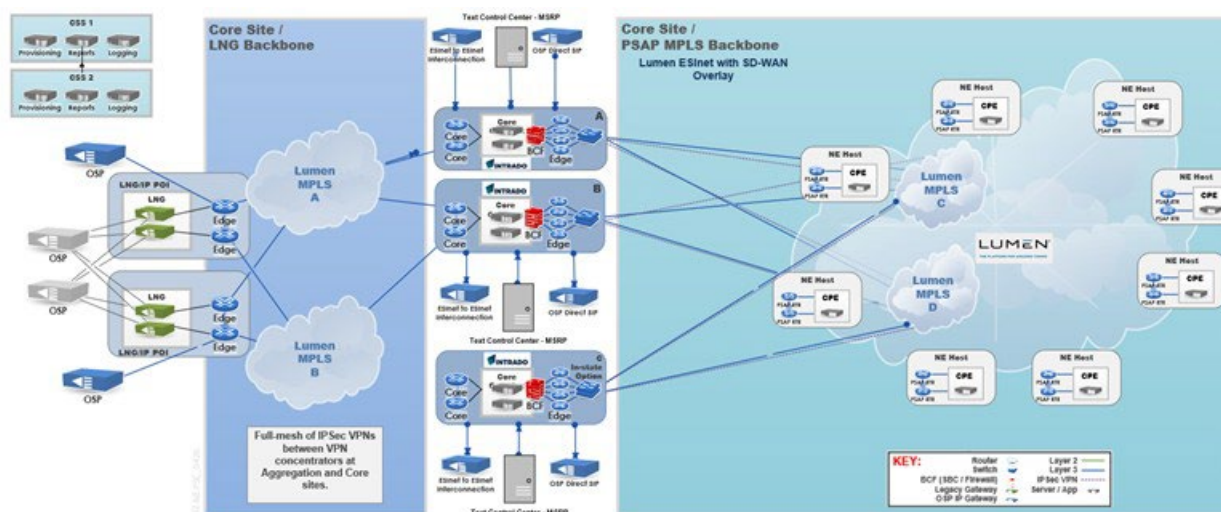


Figure 4.1.3.6-1. Lumen's Proposed ESInet Solution.

Physical and Logical Path Diversity. The ESInet diagrams explicitly document physical and logical path diversity engineered to eliminate single points of failure. This includes geographically diverse transport paths, redundant routing elements, and alternate ingress and egress routes. Diagrams identify diverse facilities, network segments, and routing paths to demonstrate how resiliency is achieved across ingress, core, and egress portions of the ESInet.

One-Time and Transitional Network Elements. Lumen identifies and documents all one-time, transitional, or interim network elements required to support phased deployment or cutover activities. These elements, including temporary interconnections, protocol-conversion components, or dual-stack interfaces, are clearly labeled in the diagrams and supporting documentation to distinguish them from steady-state architecture components.

Network Ingress and Egress Points. ESInet diagrams clearly depict all network ingress and egress points, including connections to originating service providers, PSAPs, NGCS components, and external interfaces. Each connection identifies its functional role, connectivity type, and relationship to the broader ESInet topology, providing transparency into how emergency traffic enters, traverses, and exits the network.

Transport Types and Port Speeds. Transport technologies used within the ESInet, such as MPLS, Ethernet, or equivalent IP transport services, are documented along with associated port speeds and interface characteristics. This information is provided in diagrammatic and descriptive form to support capacity planning, operational validation, and scalability assessments.

Capacity and Bandwidth Engineering. Capacity and estimated bandwidth are identified at ingress, core, and egress segments to show how engineered capacity supports peak and burst traffic conditions. This documentation provides the State with visibility into how bandwidth is provisioned and managed across the network.

Interconnection Locations and Technologies. Interconnection locations are documented, including core nodes, data centers, points of interconnection, legacy routing gateways, and other facilities supporting statewide ESInet operations. Diagrams and companion documentation identify the technologies and interfaces used to support interoperability and integration across the network.

Configuration Management and Ongoing Access. All ESInet diagrams and supporting documentation are maintained under Lumen's configuration management processes and kept current throughout the contract term. Updated diagrams are made available to the State and designated oversight entities to support validation of deployments, configuration changes, and ongoing system functionality.

Design Visibility and Accountability. Collectively, this design documentation provides comprehensive visibility into the ESInet topology, redundancy model, transport characteristics, and integration points, ensuring the State has a clear understanding of how the network is engineered to support end-to-end NG911 functionality with resiliency and accountability.

Section 3.1 provides detailed and complete information and diagrams in support of our proposed ESInet architecture solution for the State of Nebraska.

5.1.9.2 ESINET INTERCONNECTION

*The ESInet must facilitate seamless interconnections with neighboring states or regions upon deployment. The ESInet shall use the **Border Gateway Protocol (BGP)** as the sole **Exterior Gateway Protocol (EGP)**.*

Newly established ESInets in cooperating states must be able to connect to the State ESInet within a designated timeframe. To ensure robustness and resilience:

- Interconnection should occur at a minimum of two mutually agreed-upon points to guarantee redundancy.*
- Bandwidth provisioning must cater to **at least 200% of anticipated peak call volume**, ensuring ample capacity and robustness.*
- Interconnecting methods and locations should be balanced equitably to manage costs effectively among partners.*

- *If neighboring ESInets do not adhere to the State's Differentiated Services Code Point (DSCP) specifications, the state's routers will remap DSCPs as deemed appropriate.*
- *The establishment of BGP between the State ESInet and neighboring networks is recommended.*

All additional networks integrated with the ESInet must meet the specified minimum qualifications for interconnection to uphold security and performance standards. The State's security must be collaboratively protected by all involved network providers.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Seamless interconnections with neighboring states/regions upon deployment.*
- *Connection capability for new ESInets within designated timeframe.*
- *Minimum two interconnection points for redundancy.*
- *Bandwidth provisioning for 200% of peak call volume.*
- *Equitable interconnecting methods/locations for cost management.*
- *DSCP remapping if neighboring ESInets differ.*
- *Recommendation for BGP between networks.*
- *Minimum qualifications for additional integrated networks; and collaborative security protection by providers.*

LUMEN RESPONSE:

The proposed ESInet supports seamless interconnection with neighboring state or regional ESInets at deployment and throughout the contract term. We enable Network-to-Network Interfaces (NNIs) using NENA i3-compliant interfaces to support call routing, transfers, and policy-based handling between interconnected ESInets while maintaining standards-based interoperability. The ESInet is designed to support connection of newly established cooperating ESInets within a defined and mutually agreed timeframe, with interconnection timelines governed by standard provisioning activities such as circuit ordering and turn-up. We maintain established processes to support coordinated activation with peer ESInet operators.

Redundant Interconnection Points and Bandwidth Provisioning. Inter-ESInet connectivity is established at a minimum of two mutually agreed-upon, geographically diverse interconnection points to ensure redundancy, resiliency, and continued service availability in the event of a facility, path, or site failure. Bandwidth at these interconnection points is engineered and provisioned to support no less than 200% of anticipated peak call volume, providing capacity for surge conditions, failover scenarios, and future growth. Production NNIs are monitored and may be augmented as traffic patterns evolve to maintain PSAP-grade performance expectations.

Equitable Interconnection Methods and Locations. Interconnection methods and locations are selected collaboratively with neighboring ESInet operators to balance resiliency, operational efficiency, and cost considerations. We work with partner networks to identify interconnection points that meet technical, security, and redundancy requirements while managing cost impacts equitably among participating providers.

Quality of Service (QoS) and DSCP Alignment. The ESInet enforces Differentiated Services Code Point (DSCP)-based Quality of Service policies for emergency signaling and media.

Where neighboring ESInets apply DSCP markings that differ from Nebraska's QoS policies, ESInet edge routers will remap DSCP values as appropriate to preserve end-to-end prioritization and consistent handling of emergency traffic across interconnected networks.

Use of Border Gateway Protocol and Secure Interconnection. We use Border Gateway Protocol (BGP) as the sole Exterior Gateway Protocol for external ESInet peering to manage reachability, traffic engineering, controlled failover, and predictable routing exchange across jurisdictional boundaries. BGP session establishment between the Nebraska ESInet and external ESInets supports clear routing domains and policy enforcement. All integrated networks are required to meet minimum qualifications for secure interconnection to protect performance, interoperability, and the integrity of the State's NG911 environment, with security responsibilities at each boundary collaboratively supported by participating network providers.

Minimum Qualifications for Interconnected Networks. All additional networks interconnected with the Nebraska ESInet are required to meet defined minimum technical and security qualifications appropriate for NG911 traffic exchange. External networks interface with the ESInet through controlled boundary elements, including Border Control Functions (BCFs) and Session Border Controllers (SBCs), and support mutual authentication, encryption, and traffic validation consistent with NENA i3 security practices.

Collaborative Security and Boundary Protection. Security of the State's ESInet is collaboratively protected by all participating network providers through coordinated routing policies, boundary controls, and incident response practices. This shared responsibility model ensures a consistent and defensible security posture across inter-ESInet connections while preserving the integrity, availability, and interoperability of Nebraska's NG911 environment.

5.1.10 External and PSAP Connectivity

5.1.10.1 ORIGINATING SERVICE PROVIDER (OSP) CONNECTION

Contractors are responsible for facilitating all necessary connectivity to allow traffic to flow from OSPs into the ESInet.

- *Upon acceptance, sufficient bandwidth must be provisioned to support OSP traffic irrespective of connection method (CAMA, SS7, IP, etc.).*
- *Points of Interconnection (POI) must be deployed with the greatest extent of diversity possible. This means that the contractor **shall be required** to identify any situations where OSPs lack diverse connections to the POI(s).*
- *Where diversity is limited from an OSP to the POI, and/or from the egress gateway to the PSAP, or restricted for any reason, **the contractor must identify this as a risk to their NG911 service and discuss options with the PSC for limiting or eliminating the exposure of an OSP or PSAP if a lack of diversity may cause a disruption.***
- *Careful design should ensure **redundancy and diversity from the caller to the call-taker** to ensure that the system is as diverse and redundant as possible from end-to-end.*
- *Communications must enable smooth migration to the ESInet once operational, including aggregation of legacy 911 traffic into the core network.*

- *Contractors must continuously monitor the bandwidth at aggregation points to efficiently manage and increase bandwidth as required.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Facilitation of diverse and redundant connectivity for OSP traffic flow into the ESInet.*
- *Provisioning of sufficient bandwidth for OSP traffic (CAMA, SS7, IP, etc.) upon acceptance.*
- *Smooth migration to ESInet with aggregation of legacy traffic.*
- *Redundant and diverse design for disruptions, interfacing with network gateways based on OSP capabilities.*
- *Identification of any risks to their system due to lack of diversity or redundancy from caller to call-taker.*
- *Identification of risks from limited diversity and options to mitigate exposure for OSPs or PSAPs.*
- *Continuous monitoring/increase of bandwidth at aggregation points.*

LUMEN RESPONSE:

Lumen provides connectivity designs that ensure Originating Service Provider (OSP) traffic reaches the ESInet through diverse, redundant, and standards-aligned paths. The ESInet supports both legacy ingress (CAMA and SS7 via standards-based Legacy Network Gateways and Legacy Selective Router Gateways) and IP-based ingress through controlled Border Control Function (BCF) and Session Border Controller (SBC) boundaries. OSP interconnections are established at multiple Points of Interconnection (POIs), with geographic, technology, and path diversity engineered from ingress through the ESInet core to PSAP egress to eliminate single-point dependencies wherever diversity is feasible.

Bandwidth Provisioning and Capacity Management. Sufficient ingress and aggregation bandwidth is provisioned at acceptance to support all OSP traffic types, including CAMA, SS7, and IP. Legacy (TDM) aggregation capacity is engineered to be non-blocking based on DS0 requirements, while IP ingress is dimensioned based on concurrent session demand and signaling and media profiles. Capacity headroom is maintained to support surge conditions, transitional call flows, and expected growth during Nebraska's migration to a full i3 environment, with bandwidth expanded incrementally without service disruption as required.

End-to-End Redundancy and Legacy Traffic Migration. End-to-end redundancy is provided from caller to call-taker through diverse transport paths, redundant boundary elements, and multiple routing domains. Calls entering through legacy or IP gateways are routed across geographically diverse ESInet core sites with automatic reroute and reconvergence during impairments. Legacy 9-1-1 traffic is aggregated into the ESInet through controlled ingress points using LNG and LSRG functions to support parallel operations and a smooth, coordinated transition as OSPs migrate to direct IP or i3-based interconnections.

Identification of Limited Diversity and Risk Mitigation. Diversity and resiliency assessments are conducted as part of the design process to identify limitations in OSP-to-POI, gateway-to-core, or egress-to-PSAP connectivity. Where physical, geographic, or infrastructure constraints limit diversity, these conditions are documented and identified as potential risks to NG911 service availability. Mitigation options are evaluated collaboratively with the State and public safety stakeholders and may include additional POIs, alternate

access media, geographically diverse routing, tertiary connectivity options, or transitional elements. Routing policies and overflow strategies may also be applied to reduce the operational impact of a single impairment affecting an OSP or PSAP.

Continuous Monitoring and Operational Visibility. Ingress, aggregation, and core network bandwidth is continuously monitored through the Network Operations Center to ensure OSP traffic is processed without congestion. Utilization thresholds and performance indicators support proactive investigation and capacity planning, and bandwidth increases are implemented through established move/add/change processes coordinated with access media capabilities and operational requirements. This approach maintains consistent performance for signaling, media, and NG911 data flows while providing the State with clear visibility into bandwidth utilization and diversity-related risks affecting OSPs or PSAPs.

5.1.10.2 PSAP CONNECTION

At the point of system acceptance, the ESInet must guarantee sufficient bandwidth to support:

- **2 Mbps per PSAP + 2 Mbps per position** during standard operational conditions.
- **1 Mbps per PSAP + 1 Mbps per position** under conditions where network disruptions occur, which may include simultaneous failures of the largest link or comprehensive outages affecting all networks of a single ISP.

The contractor must commit to ongoing bandwidth monitoring throughout the contract duration and promptly increase capacity as necessary, including an annual growth factor of 10%.

The design must also facilitate interconnections with PSAP systems (like CAD and logging recorders), as well as with criminal justice networks and other secure public safety technologies, ensuring uninterrupted SIP traffic flow for 911 calls.

The ESInet shall allow for all egress connectivity, including gateways, and be configured to establish the capability for traffic to flow from the ESInet into the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

Guaranteed bandwidth of 2 Mbps per PSAP + 2 Mbps per position under standard conditions and 1 Mbps per PSAP/position under disruptions (e.g., largest link failure or ISP outage).

Commitment to ongoing bandwidth monitoring and increases with 10% annual growth factor.

Facilitation of interconnections with PSAP systems (CAD, logging recorders), criminal justice networks, and secure public safety technologies.

Ensuring uninterrupted SIP traffic for 911 calls.

LUMEN RESPONSE:

Lumen ensures sufficient ESInet bandwidth at system acceptance to support a minimum of 2Mbps per PSAP plus 2Mbps per call-taking position under standard operating conditions, and a minimum of 1Mbps per PSAP plus 1Mbps per call-taking position during defined disruption scenarios, such as failure of the largest access link or loss of all services from a single Internet Service Provider. Ingress, core, and egress paths are sized using engineered

transport capacity and QoS enforcement to preserve SIP signaling and media performance during peak and impaired conditions.

Redundancy Supporting Bandwidth Availability. These bandwidth levels are sustained through geographically diverse ESInet core processing, redundant PSAP access paths, and automatic reroute across diverse IP routes to maintain service continuity without manual intervention. Each PSAP is connected to the ESInet using a minimum of two diverse access circuits delivered over separate network paths, protecting against single-link or single-carrier failures and supporting continued availability during disruption scenarios.

Ongoing Bandwidth Monitoring and Growth Management. Bandwidth utilization is continuously monitored across PSAP access segments, aggregation points, and ESInet transport paths through Lumen's 24x7x365 NOC. Utilization and link health are tracked against defined thresholds to support proactive capacity planning, with bandwidth increases implemented as needed through established change processes. The ESInet design incorporates an annual bandwidth growth factor of 10% per PSAP to accommodate forecasted increases in call volume and NG911 data traffic over the life of the contract.

PSAP System Interconnections and SIP Traffic Protection. The ESInet supports secure interconnection with PSAP systems, including call handling equipment, CAD platforms, logging recorders, criminal justice networks, and other approved public safety technologies. Egress connectivity, including required gateways and boundary elements, is engineered to ensure uninterrupted SIP signaling and RTP media flow for 9-1-1 calls and NG911 data elements. End-to-end QoS using DSCP marking, traffic shaping, and prioritized handling of SIP and media traffic preserves consistent call delivery from the ESInet into the PSAP environment while supporting Nebraska's operational and integration requirements.

The ESInet supports all required egress connectivity, including gateways, and is configured to establish and maintain the capability for traffic to flow reliably from the ESInet into each PSAP. Gateway architectures are designed for redundancy and scalability to support both current and future PSAP connectivity requirements.

5.1.11 Legacy Interoperability

5.1.11.1 LEGACY NETWORK GATEWAY (LNG)

The Respondent must provide a Legacy Network Gateway (LNG) solution to serve as the ingress point for calls originating from legacy networks (e.g., wireline, wireless, VoIP) that have not yet transitioned to native i3 SIP origination. The LNG is responsible for converting legacy signaling to i3-compliant SIP and querying legacy ALI databases to obtain location information.

LNGs and/or LSRGs must conform to NENA-STA-010.3 and provide termination for all existing legacy OSPs until they migrate to i3 origination. The current solution utilizes an LSRG combining LNG and LSRG functions.

- *Interface Compatibility:*
 - *The LNG must maintain interface compatibility with existing Selective Routers, allowing for minimal disruption and cost implications.*
- *Geographical Redundancy:*
 - *Legacy OSPs must have access to connections at two geographically diverse LNGs to enhance resilience.*
- *Legacy Support:*

- *The LNG must be configured to manage legacy PSALI records, including migration processes outlined in the documentation provided.*

LNG Connectivity to ESInet

The LNG must securely connect to the ESInet, receive calls from legacy network trunks (e.g., CAMA, MF), and interface with the ESInet's Border Control Function (BCF) to forward calls into the NG911 core.

Protocol Conversion (Legacy to SIP)

The LNG must convert legacy in-band signaling (e.g., CAMA wink-start, MF tones) and associated trunk supervision into i3-compliant SIP (RFC 3261) for processing by the ESInet.

ALI Query and Location Formatting

The LNG must use the Automatic Number Identification (ANI) received from the legacy call to perform a query against the appropriate legacy ALI database. It **MUST** then format the retrieved ALI data into a NENA-compliant Presence Information Data Format - Location Object (PIDF-LO) for inclusion in the outbound SIP INVITE.

Security, Logging, Monitoring, and Redundancy

The LNG, as a critical ESInet functional element, must adhere to the same stringent requirements for security, logging, monitoring, and redundancy as other core components to ensure system integrity and high availability.

If separate LNGs are proposed, they must:

- Maintain interfaces similar to current systems
- Support TTY to RTT conversion
- Provide E2 connections to all MLCs, GMLCs, and VPCs
- Be positioned outside the ESInet, before the BCF

Support ElementState and ServiceState functionality

Each component has specific requirements for capacity, performance, integration, and conformance with NENA standards.

The solution must maintain appropriate spare parts at various locations to ensure immediate system restoration when needed, with specific requirements for inventory management, replacement schedules, and on-site spares at data centers.

The LNG must support the Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS.

The LNG shall support:

- Error checking
- GIS-based MSAG (for legacy OSP use)
- The Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS
- Service Order Address Validation

- Service Order Error checking
- Service Order history available/viewable for every telephone number
- Coordination with Telecommunications providers:
 - OSPs will be able to manage/make updates to their records directly in the database without having to submit SOI
 - OSPs will be able to run performance/statistical reports on their No Record Found (NRF)/Discrepancy and SOI processing
 - OSPs will be able to view discrepancies and NRFs directly from the web interface real time
- Data import / export
- Data integrity and availability
- ALI updates
 - OSP's have the ability to manually update their own records
 - OSP's have the ability to lock and unlock their own records
 - All manual updates be tracked in history
- Customer access to data
- Telco access to data
- Bulk modifications
- PSALI functionality
- Database reports
- NRF process
 - ALI discrepancies
- Tracking, reporting and timestamp for discrepancies and NRFs.
- Service Order exceptions
- ALI database audit
- MSAG database audit

The State expects the LNG to maintain connections to Text Control Centers (TCCs) so that NG PSAPs maintain a complete standard (NENA-STA-010.3) connection for Short Message Service (SMS) calls to 911 from legacy OSPs via the LNG.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LNG conformance to NENA-STA-010.3 for legacy OSPs until i3 migration.
- Interface compatibility with existing Selective Routers.
- Geographically diverse connections for legacy OSPs.
- Management of legacy PSALI records with migration processes.
- TTY to RTT conversion.
- E2 connections to MLCs/GMLCs/VPCs
- Positioning outside ESInet before BCF.
- ElementState/ServiceState support.

LUMEN RESPONSE:

Lumen will provide a Legacy Network Gateway (LNG) solution that conforms to the NENA i3 architecture and serves as the ingress point for calls from legacy wireline, wireless, and VoIP networks until those OSPs migrate to native i3 SIP origination. Our LNG/LSRG implementation converts legacy signaling (e.g., CAMA and MF) into i3-compliant SIP (RFC 3261), performs ALI queries using the received ANI, and formats location into PIDF-LO for

delivery to the NG911 core. The LNG is engineered with the same security, logging, monitoring, and redundancy characteristics as other ESInet core elements.

The proposed LNG solution provides the State the required performance standards and complies with all NENA standards:

- **NENA STA-010.3 Conformance and Standards Alignment.** LNG and LSRG functions are implemented in accordance with NENA STA-010.3 and related NENA standards. The solution provides termination for all existing legacy OSP trunks and maintains i3-compliant SIP call presentation, routing behavior, and location formatting until each OSP completes migration to native i3 origination, supporting standards evolution without service interruption.
- **Interface Compatibility with Existing Selective Routers.** The LNG maintains compatibility with existing selective routing infrastructure by supporting legacy signaling and trunking methods, including CAMA, MF, and SS7 where applicable. This approach minimizes operational disruption, avoids unnecessary reconfiguration, and enables continued operation of existing selective routers while calls are transitioned into the ESInet.
- **Protocol Conversion and Call Processing.** The LNG converts legacy in-band signaling, trunk supervision, and call control, such as CAMA wink start and MF tones, into i3-compliant SIP. Calls are processed using standardized SIP interfaces and presented to the NG911 core in a normalized format suitable for downstream NGCS handling.
- **ALI Query and Location Formatting.** Using ANI received from legacy call signaling, the LNG performs queries against the appropriate legacy ALI databases and formats retrieved location information into NENA-compliant PIDF-LO objects. These location objects are included in SIP INVITE messages delivered to the NG911 core, ensuring accurate and consistent location handling for legacy calls.
- **Legacy PSALI Record Management and Migration.** The LNG and associated location management components support legacy PSALI records, including GIS-based MSAG validation, service-order-driven updates, discrepancy handling, and auditing. PSALI data is stored in LVF-valid form within the Location Database and converted to and from legacy formats using the MCS, supporting staged migration from legacy ALI and PSALI workflows to NG911 location services.
- **Geographically Diverse Legacy OSP Connectivity.** Legacy OSPs are provided connectivity to at least two geographically diverse LNG locations. Dual connection options provide site and path redundancy so that failure of a single LNG, facility, or transport path does not interrupt legacy call ingress to the NG911 core.
- **E2 Connectivity for Wireless and VoIP Location.** The LNG supports E2-type interfaces to Mobile Location Centers, Gateway Mobile Location Centers, and VoIP Positioning Centers. These interfaces enable retrieval and delivery of network-based or device-based location information associated with legacy wireless and VoIP emergency calls.
- **Text and Accessibility Support.** Where required, the LNG supports conversion between legacy TTY call content and Real-Time Text to preserve accessibility as calls transition from legacy networks into the i3 environment. Connectivity with Text Control Centers is maintained to support SMS-to-911 from legacy OSPs during the transition period.
- **Network Placement and Boundary Protection.** LNGs are positioned at the network edge, outside the ESInet security boundary and in front of the Border Control Function. This placement allows termination of legacy trunks and protocol and location conversion

before standardized SIP traffic is presented to the BCF for controlled admission into the ESInet.

- **Security, Logging, Monitoring, and State Visibility.** As a critical ingress element, the LNG adheres to the same security, logging, monitoring, and redundancy requirements applied to other ESInet and NG911 core components. The LNG exposes ElementState and ServiceState information consistent with NENA operational guidance, integrating with network management, logging, and alerting to support rapid fault detection and failover activation.
- **Service Order Activation and Data Management.** The LNG supports Service Order Activation interfaces toward legacy OSPs, controlled OSP access to records, history tracking, auditing, reporting, and error management. Data integrity is maintained through validation, discrepancy management, and coordinated update workflows aligned with NG911 operational practices.
- **End-State Transition Assurance.** This architecture ensures Nebraska can continue accepting 911 calls from all legacy OSPs while preserving full location accuracy, accessibility support, and resiliency. The LNG enables a controlled transition to a fully native i3 environment without disrupting NG911 services or public safety operations.

The proposed architecture ensures that Nebraska can continue to accept 911 calls from all legacy OSPs, maintain full location and accessibility capabilities, and transition to an end-state i3 environment without disrupting public safety services.

5.1.11.2 LEGACY SELECTIVE ROUTER GATEWAY (LSRG)

A Legacy Selective Router Gateway (LSRG) must serve as the interface for legacy selective routers to terminate ISUP SS7 trunks utilizing an inter-tandem trunk group method of termination.

The LSRG must convert the call signaling to SIP/RTP, query the existing ALI data management system to retrieve location information for the call and then route the call to the next nominal "hop" based on a LoST query to an ECRF.

Additionally, the LSRG must be able to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

If Respondents utilize an LSRG for their proposed solution, they must include a timeline and plan for removing the LSRG during the contract period. The LSRG is to be only a temporary solution that can be used to initially gateway OSP traffic.

Any LSRG implemented as part of the Contractor's solution must conform to the NENA Legacy Selective Router Gateway (LSRG) Standard (NENA-STA-034.1-2022), and should be deployed to align with the relevant sections of the NENA NG9-1-1 Transition Plan Considerations Information Document (NENA-INF-008.2-2013).

LSRG Connectivity to ESInet and Legacy SR

The LSRG must provide a secure interface to the ESInet to receive routing queries from the ECRF and a separate, secure interface compatible with the legacy Selective Router's query/response protocol.

Routing Protocol Conversion (LoST to Legacy)

The core function of the LSRG is to receive a standards-based Location-to-Service Translation (LoST) protocol query (RFC 5222) from the ECRF, translate it into a format the

legacy SR can process (often a proprietary format or a simplified query containing an ESN), and translate the SR's response back into a LoST response for the ECRF.

Security, Logging, Monitoring, and Redundancy

The LSRG must meet the same core requirements for security, logging, monitoring, and geo-diverse redundancy as other critical ESInet functional elements to ensure the integrity and availability of call routing.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Interface for legacy Selective Routers via ISUP SS7 trunks.*
- *Conversion to SIP/RTP.*
- *ALL query and LoST-based routing.*
- *Bi-directional communications for voice/data (star codes).*
- *Timeline/plan for LSRG removal as temporary solution for OSP traffic.*
- *Deployed LSRG (where applicable) in conformance with NENA LSRG Standard (STA-034.1)*

LUMEN RESPONSE:

Lumen provides a Legacy Selective Router Gateway (LSRG) that interfaces directly with legacy Selective Routers using ISUP SS7 trunks terminated through inter-tandem trunk group methods. The LSRG converts legacy call signaling to SIP signaling and RTP media, performs ALL queries using the received ANI, and submits Location-to-Service Translation (LoST) queries to the ECRF to determine the appropriate next hop in the NG911 call flow. This approach delivers legacy calls into Nebraska's ESInet in an i3-compliant format while preserving compatibility with existing selective routing infrastructure.

Standards Conformance and Interface Compatibility. The LSRG is implemented in conformance with the NENA Legacy Selective Router Gateway Standard (NENA-STA-034.1-2022) and aligns with applicable NENA NG9-1-1 transition guidance. Secure interfaces are provided to both the ESInet for LoST-based routing queries and to legacy Selective Routers using their native signaling and query formats, maintaining separation between legacy signaling environments and the IP-based ESInet.

Signaling, Media, and Routing Interworking. Legacy ISUP call signaling is transparently converted to SIP signaling and RTP media for delivery into the ESInet and NGCS environment, preserving call integrity and continuity without requiring changes to legacy OSP configurations. The LSRG performs LoST-to-legacy routing protocol interworking by translating standardized LoST queries into the formats required by the legacy selective routing environment and converting responses back into LoST format for use by the ECRF, maintaining routing accuracy during the transition period.

Bi-Directional Communications/Legacy Feature Support. Bi-directional communications with legacy Selective Routers are supported for both voice and data transactions, including star-code features. This capability preserves legacy feature parity, such as established routing behaviors and inter-PSAP transfer workflows, while operating within a mixed legacy and NG911 environment until selective routing dependencies are retired.

Resiliency, Security, and Operational Controls. Redundant and geographically diverse LSRG instances are deployed to support continuity of service during maintenance or failure

scenarios. The same security, logging, monitoring, and geo-diverse redundancy controls applied to other critical ESInet and NGCS functional elements are applied to the LSRG to maintain the integrity, availability, and observability of legacy-sourced call routing throughout the contract period.

Transitional Use and Planned Removal. The LSRG is treated as a temporary transitional component used to support legacy OSP traffic during migration to full NG911 connectivity. Where deployed, a coordinated timeline and removal plan is developed with the State and participating OSPs as legacy SS7 trunks are decommissioned and traffic is migrated to native SIP-based ingress, aligning with NG911 transition milestones and minimizing long-term dependency on legacy infrastructure.

5.1.11.3. LEGACY PSAP GATEWAY (LPG)

The State requires Legacy PSAP Gateways (LPGs) that conform to NENA-STA-010.3. LPGs shall provide origination for all legacy PSAPs until those PSAPs migrate to i3 termination. LPGs must allow PSAPs to continue to use existing equipment and processes except where NENA-STA-010.3 requires change (for example, use of Pseudo-Automatic Number Identification [pANI]). Each LPG shall connect legacy PSAPs to the ESInet using SIP and legacy interfaces such as CAMA and ALI and shall convert NG911 SIP signaling and media to legacy protocols such as TDM and ISDN to maintain compatibility.

Protocol Conversion (SIP to Legacy)

The LPG must convert the SIP-based signaling and media from the ESInet into legacy circuit-switched formats (e.g., CAMA, ISDN PRI) that are compatible with the legacy PSAP's CHE.

Location and ALI Integration

The LPG must extract location information (PIDF-LO) from the incoming SIP signaling and convert it into a legacy Automatic Location Identification (ALI) format for delivery to the PSAP's ALI database/controller.

Text Support (TTY to RTT Conversion)

The LPG must support interworking between Real-time Text (RTT) on the ESInet, and legacy Baudot-based Teletypewriter (TTY) devices used in the PSAP, ensuring seamless communication for hearing-impaired users.

Call Transfer Support

The LPG must support call transfer scenarios, including the ability to relay transfer requests from the legacy PSAP back into the ESInet to enable transfers to other NG911-capable agencies or PSAPs.

Logging and Reporting

The LPG must generate detailed logs for all call processing events, alarms, and system activities and forward them to a central logging service in a standard format (e.g., Syslog) as defined by NENA standards.

Security Mechanisms

The LPG must implement robust security measures, including access control, authentication, and encryption, to protect the interface between the ESInet and the legacy PSAP network, adhering to NG911 security standards.

Monitoring and Maintenance

The LPG must be capable of being monitored for operational status, performance, and alarms. It must support standard monitoring protocols (e.g., SNMP) and provide mechanisms for remote administration and maintenance.

Geo-Diversity and Redundancy

The LPG must be deployed in a geographically diverse and redundant configuration to ensure high availability and failover capabilities, preventing a single point of failure from isolating a legacy PSAP.

Discrepancy Reporting

The LPG must support a mechanism for reporting discrepancies, such as call routing errors or ALI data problems, from the legacy PSAP environment back to the NG911 systems Discrepancy Report service.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *The LPG must be able to maintain the PSAP's existing ALI format.*
- *The LPG must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3.*
- *The State must be able to subscribe to ServiceState and receive the standard state change*
- *LPG connections shall allow for PSAPs to directly connect systems (cable IP) to the ESInet*
- *LPG queries ALI databases and maps NG911 location data to legacy formats.*
- *Converts TTY to RTT for text-to-911 in legacy PSAPs.*
- *Supports call transfers to/from legacy PSAPs, mapping i3 transfers to legacy systems.*
- *Logs call events, protocol conversions, and errors; supports discrepancy reporting.*
- *Implements TLS and authentication for secure connectivity.*
- *Monitors LPG performance; supports maintenance with minimal disruption.*
- *LPG deployed with geo-redundancy to ensure high availability.*
- *Reports errors in call delivery, location, or protocol conversion.*

LUMEN RESPONSE:

Lumen provides Legacy PSAP Gateways (LPGs) that conform to NENA-STA-010.3 and enable legacy PSAPs to continue operating with existing call-handling equipment and workflows until they transition to native i3 termination. The LPG converts SIP signaling and RTP media from the ESInet into legacy circuit-switched protocols used by PSAP equipment, including CAMA and ISDN PRI, allowing seamless interoperability during Nebraska's transition period.

Legacy ALI Format Preservation and Location Interworking. PIDF-LO location information is extracted from incoming SIP signaling and converted into the legacy ALI formats required by PSAP systems. ALI databases are queried as needed, and NG911 location data is mapped

into legacy structures so PSAPs continue to receive accurate location information without requiring changes to existing ALI controllers or CAD integrations. This approach preserves established call-taking workflows while supporting staged migration to NG911 location services.

Text Accessibility and Call Transfer Support. Interworking between NG911 Real-Time Text (RTT) and legacy Baudot-based TTY devices is supported to ensure uninterrupted text-to-911 accessibility for PSAPs that have not yet migrated to NG-native call-handling systems. Call transfer scenarios are supported in both directions, with i3 transfer signaling mapped into legacy equivalents and transfers from legacy PSAPs converted for delivery back into the ESInet, preserving established operational workflows during the transition.

Security, Logging, and Discrepancy Reporting. The LPG generates detailed logs related to call processing, protocol conversions, alarms, and error conditions and forwards these events to centralized logging services using standard formats. Interfaces implement TLS-based encryption, authentication, and access controls consistent with ESInet security expectations to protect signaling and data exchanges between the ESInet and legacy PSAP networks. Errors related to call delivery, location mapping, or protocol conversion are detected and reported through NENA-aligned discrepancy reporting mechanisms to support timely identification and resolution.

Operational State Visibility and Monitoring. ElementState and ServiceState SUBSCRIBE / NOTIFY functionality is supported in accordance with NENA-STA-010.3, enabling the State and authorized systems to subscribe to LPG availability and operational status. State change notifications are generated using standard NENA-defined formats and integrate with centralized monitoring and operational dashboards. LPG performance and health are monitored using standard protocols, such as SNMP, and remote administration is supported to enable maintenance activities with minimal disruption to PSAP operations.

PSAP Interconnections and High Availability. Direct IP connectivity between PSAP systems and the ESInet is supported through LPG interfaces where compatible with local infrastructure, enabling incremental modernization without requiring immediate replacement of legacy PSAP equipment. LPGs are deployed in geographically diverse, redundant configurations to avoid single points of failure and maintain service continuity for legacy PSAPs throughout the transition to full NG911 operation.

5.1.12. Network Behavior and Performance

5.1.12.1. ESINET IP ROUTING

*The ESInet must follow the NENA standards to ensure that IP routing across the ESInet can handle all traffic effectively under varying conditions. **Ongoing bandwidth assessments, risk assessments, diversity, and redundancy testing must be documented and updated in a configuration management database as the ESInet evolves.** Proactive measures to trace IP routing within the diverse and redundant paths is required. Any change to the system must include testing of IP routing failover mechanisms prior to acceptance of a change.*

*No specific link shall be provisioned with **more than 50% of the physical limit** of that link to allow for expansion without physical changes to the link, router, or switch to which it connects. As changes in the network are completed, the IP address plan shall be updated and remain accessible to the State or designee.*

Every element proposed supports both IPv4 and IPv6 (dual stack).

- All elements in the network have globally routable IP IPv4 and IPv6 addresses.*
- The network shall use one Interior Gateway Protocol (IGP) throughout, and no routers use Routing Information Protocol (RIP).*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance with NENA standards for handling traffic under varying conditions.*
- Documentation of ongoing bandwidth assessments, risk assessments, diversity and redundancy testing in a configuration management database.*
- Proactive measures to trace IP routing in diverse and redundant paths.*
- Testing of IP routing failover mechanisms prior to any system change acceptance.*

LUMEN RESPONSE:

Lumen ensures that IP routing across the ESInet conforms to applicable NENA ESInet design and NENA i3 standards and is engineered to support reliable traffic handling under normal, degraded, and failure conditions. The ESInet uses a single Interior Gateway Protocol consistently across the network, supports full dual-stack IPv4 and IPv6 operation, uses globally routable addressing for all elements, and does not employ Routing Information Protocol. This approach delivers predictable routing behavior, consistent path selection, and rapid convergence statewide.

Dual-Stack and Addressing Strategy. Every ESInet element supports IPv4 and IPv6 concurrently to ensure compatibility with current systems and long-term future readiness. Globally routable addressing is applied throughout the ESInet to support end-to-end reachability, standards compliance, and consistent routing behavior across the NG911 environment. An authoritative IP address plan is maintained and updated as changes occur and is made available to the State or its designee.

Bandwidth Engineering and Capacity Management. ESInet links are engineered to operate below 50% of physical capacity to preserve headroom for burst traffic, growth, and failover conditions without requiring immediate upgrades to circuits or network devices. Capacity planning accounts for both steady-state and failure scenarios to ensure continuity of service during abnormal conditions.

Diversity and Redundancy Evaluation. Lumen designs the ESInet with physically and logically diverse routing paths and redundant network elements to eliminate single points of failure. Diversity and redundancy are validated through documented testing and analysis to confirm that alternate paths do not share common failure domains and remain available during maintenance or outages.

Proactive Routing Visibility and Path Validation. Proactive route tracing and path validation are used to confirm traffic flows across diverse and redundant ESInet paths and to verify routing behavior under both normal and impaired conditions. These practices support rapid identification of anomalies, confirmation of proper path selection, and assurance of rapid reconvergence during link or node failures.

Failover Testing and Change Acceptance. All ESInet routing, capacity, or topology changes follow formal change management procedures. Pre-acceptance testing validates IP routing behavior and failover performance under simulated failure conditions to confirm that traffic

shifts to alternate paths without service interruption. Test results and acceptance evidence are documented prior to production deployment.

Configuration Management and Ongoing Assurance. Bandwidth assessments, routing diversity evaluations, redundancy validation results, network diagrams, and capacity records are maintained within Lumen's configuration management database and kept current throughout the contract term. This documentation provides transparency and supports ongoing operational assurance as the ESInet evolves.

Collectively, Lumen's ESInet architecture satisfies the State's network behavior and performance requirements by implementing a NENA-aligned, resilient, and scalable IP routing design. Disciplined capacity thresholds, consistent routing controls, proactive monitoring, and mandatory failover validation ensure sustained operational integrity across all conditions.

5.1.12.2. ESINET BANDWIDTH

The ESInet is expected to deliver sufficient end-to-end bandwidth to accommodate traffic to and from PSAPs effectively.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Adequate sizing must consider 911 voice and video calls, text communications, data transmissions, and a calculated surge factor based upon the State of Nebraska PSAPs.*
- *An **annual growth factor of 10%** must be incorporated into capacity planning.*
- *Bandwidth sharing with other networks within the State of Nebraska is encouraged, **especially for secondary routes, provided the contractor implements provisions to ensure that using these networks does not impact the primary ESInet performance.***
- *The ESInet should be structured for future expansion, allowing scalable growth throughout the duration of the contract without impeding current services. A detailed plan should outline how the ESInet will readily accommodate increases in bandwidth, as necessary.*
- *A detailed plan for scalable expansion throughout the contract without impeding services.*

LUMEN RESPONSE:

Lumen sizes ESInet bandwidth to support end-to-end NG911 traffic demands for Nebraska PSAPs, including 9-1-1 voice, video, text, and NG911 data exchanges, with additional capacity to accommodate a calculated surge factor based on PSAP operational profiles. Capacity planning incorporates baseline traffic analysis and peak-event modeling to ensure the ESInet can sustain elevated call and data volumes during major incidents without service degradation.

Annual Growth Planning. An annual growth factor of at least 10% is incorporated into ESInet capacity planning to accommodate increases in call volume, data usage, and NG911-enabled functionality over time. Growth planning is applied across PSAP access circuits, aggregation points, and core transport, and capacity is periodically reviewed to confirm that growth assumptions remain aligned with operational conditions throughout the contract term.

Bandwidth Sharing on Secondary Routes. Where appropriate, bandwidth sharing is supported on secondary or diverse routes, including facilities available through State networks, provided that primary ESInet performance is not impacted. Traffic isolation, prioritization, and QoS controls are applied to ensure NG911 signaling and media traffic remains protected, and shared usage is prevented from degrading call delivery or data integrity on primary ESInet paths.

Scalable Expansion Without Service Disruption. The ESInet is structured to support scalable expansion throughout the contract term, enabling incremental increases in bandwidth without disrupting active services. Expansion may be achieved through logical upgrades, circuit augmentation, and transport scaling at CHE host edges, aggregation layers, and core sites, rather than physical redesign. A scalable expansion approach is coordinated through formal change management processes to maintain continuous service availability while allowing the State to adopt new NG911 capabilities and accommodate future traffic growth.

5.1.12.3. QUALITY OF SERVICE (QoS)

The ESInet must provide Quality of Service (QoS) features at all ingress, core, and egress points.

The ESInet must employ DiffServ throughout, adhering to packet marking specifications per NENA-STA-010.3. A commitment to maintaining packet loss below 0.5%, jitter under 15 milliseconds, and (one-way) latency below 25 milliseconds is required during standard operational periods.

- Performance metrics for these characteristics should be established on a standby measurement basis, with the State stakeholders allowed to initiate specific measurements as required.*
- Regular reporting must provide comprehensive insights into network performance metrics, including averages and worst-case scenarios.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Employment of DiffServ throughout with packet marking per NENA-STA-010.3.*
- Commitment to packet loss below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during operations.*
- Standby measurement basis for performance metrics with State-initiated measurements.*
- Regular reporting on network performance including averages and worst-case scenarios.*

LUMEN RESPONSE:

Lumen employs Differentiated Services (DiffServ) end to end across all ESInet ingress, core, and egress points, with DSCP packet marking applied in accordance with NENA-STA-010.3. SIP signaling, RTP media, and NG911 data traffic are classified and marked at ingress and preserved or remapped as necessary to ensure consistent prioritization across all ESInet segments, paths, and interconnection points. QoS policies are engineered to support PSAP-grade service performance and predictable handling of emergency communications under both normal and degraded conditions.

Performance Objectives for Packet Loss, Jitter, and Latency. The ESInet is designed and operated to meet the State's performance objectives during normal operations, including packet loss below 0.5%, jitter under 15-milliseconds, and one-way latency below 25-milliseconds. These thresholds are supported through appropriate capacity sizing, non-oversubscribed links, traffic prioritization, and a resilient ESInet architecture that maintains consistent call quality and NG911 data delivery during steady-state operations and traffic shifts.

Standby Measurement Basis and State-Initiated Testing. Performance metrics for packet loss, jitter, and latency are maintained on a standby measurement basis and continuously collected using ESInet monitoring and assurance capabilities. In addition to ongoing measurement, the State and authorized stakeholders may initiate targeted performance testing, including path-specific, site-specific, or event-driven measurements, to validate QoS behavior under real-world conditions. Results from State-initiated testing are captured using the same monitoring framework to ensure consistency, transparency, and repeatability.

Performance Reporting and Operational Visibility. Regular reporting provides the State with comprehensive visibility into ESInet performance, including average and worst-case values for latency, jitter, and packet loss. Reports and dashboards support operational oversight, trend analysis, and verification of QoS compliance at ESInet edges, regional, and statewide levels, enabling informed performance management throughout the contract term.

QoS Compliance and Ongoing Assurance. These controls ensure full compliance with the State's Quality of Service requirements. Disciplined QoS enforcement, defined performance thresholds, continuous measurement, State-initiated testing, and transparent reporting provide sustained operational assurance and support continuous performance improvement across the ESInet.

5.1.12.4. TRAFFIC FLOW REQUIREMENTS

Respondents must describe how traffic will flow from end to end across the network in a fashion that is compliant with applicable standards. ESInet and NG Core Services functions be described to allow the evaluator to clearly identify where specific operations on the traffic occur. If necessary, diagrams may be used to assist the visualization of traffic flow through the proposed solution.

*The ESInet and NGCS must operate in concert with one another to establish the flow of traffic from the caller to the call-taker. This flow of traffic utilizes physical and logical connections to the resources required for call delivery. Traffic flow shall include a description of traffic flow under **NORMAL** operating conditions and traffic flow under **ABNORMAL** operating conditions.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *End-to-end traffic flow description compliant with standards.*
- *Identification of operations on traffic in ESInet and NGCS.*
- *Diagrams for visualization if necessary; traffic flow under normal and abnormal conditions.*
- *Handling of use cases such as legacy OSP to NG PSAP, NG OSP to NG PSAP, Internet to NG PSAP, text/ALI/GIS traffic, virtual PSAPs, BCF to ECRF, ECRF to SI/ESRP/PSAP/LPG, LSRG to OSP, OSP to LNG, logging/recording, and*

monitoring/management. Additional or modified use cases specific to the solution should be expanded upon.

LUMEN RESPONSE:

Lumen provides an end-to-end traffic flow design that is compliant with applicable NENA i3 standards and clearly distinguishes ESInet transport functions from NG Core Services (NGCS) processing. The design (**detailed in Section 3.1**) depicts how voice, video, text, and associated data traverse from the caller, through originating networks and ESInet boundary elements, into NGCS components such as the BCF, ESRP, ECRF/LVF/LIS, and then to PSAP call handling equipment or LPGs. We identify key operations such as protocol normalization, LoST/ECRF queries, policy-based routing, location validation and formatting, logging, and security enforcement, so evaluators can see which functions reside in the ESInet and which are performed within NGCS.

We include end-to-end traffic flow diagrams, **Figure 5.1.12.4-1**, which depict normal and abnormal routing paths, ESInet versus NGCS functional boundaries, and the specific use cases listed above. **Figure 5.1.12.4-1** depicts the proposed ESInet architecture.

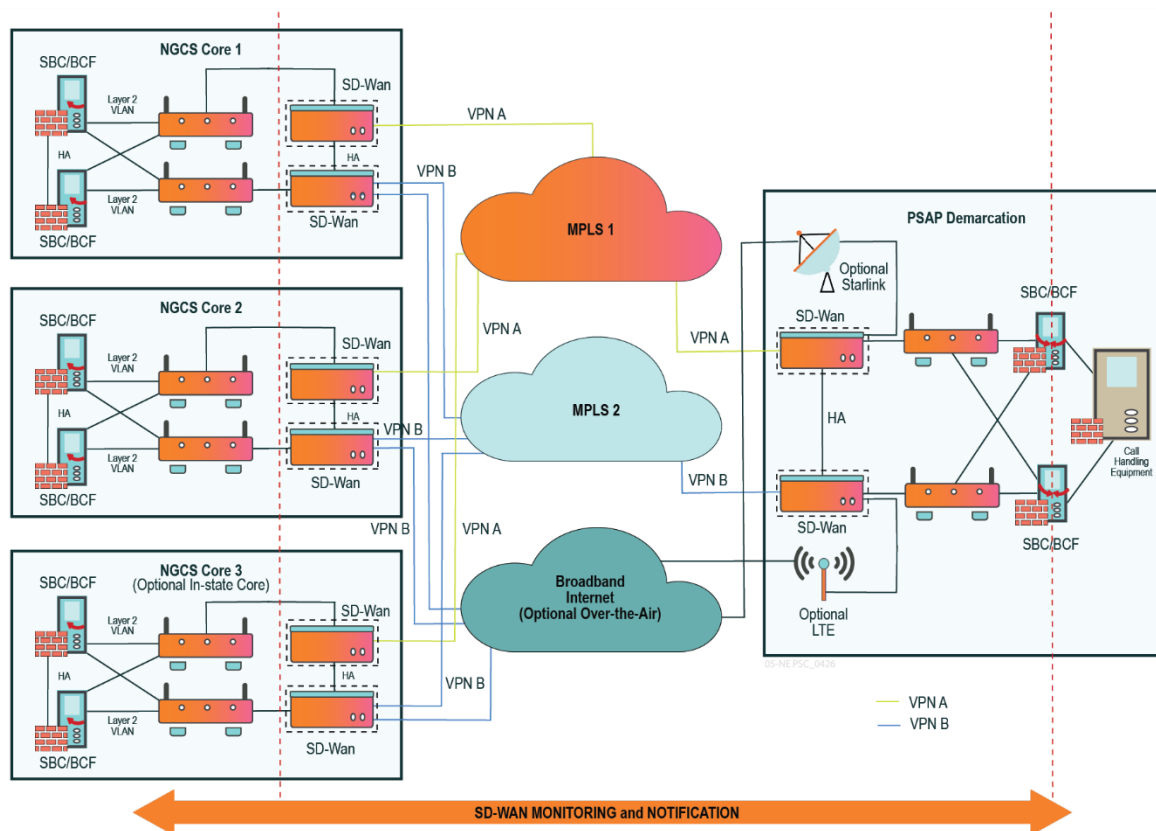


Figure 5.1.12.4-1. Lumen ESInet Architecture Design

We describe traffic behavior under normal conditions as following primary, engineered ESInet paths with NGCS functions operating at primary data centers, using standard policy routing and ECRF-driven call routing to reach the serving PSAP or virtual PSAP. Under abnormal conditions, such as link, node, or site failures, traffic is automatically rerouted across redundant ESInet paths and to redundant NGCS instances, while policy rules support overflow, alternate routing, and transfers to backup or virtual PSAPs. This ensures continuity

of voice, text, and data delivery even when specific components, routes, or PSAPs are impaired.

To address the specific use cases (**Section 5.10**) required by the State, our end-to-end traffic flow description and supporting diagrams cover:

- **Legacy OSP to NG PSAP:** Calls originate on legacy trunks (e.g., CAMA, SS7) and enter through LNG/LSRG functions, where signaling is converted to SIP/RTP, ALI is queried and formatted into PIDF-LO, and traffic is passed through the BCF to NGCS (ESRP/ECRF) for routing to the NG PSAP.
- **NG OSP to NG PSAP:** Native i3 SIP calls with location (by-value or by-reference) enter via secure SIP interconnects at the ESInet edge, traverse the BCF into NGCS, and are routed by the ESRP using ECRF/LoST responses to the target PSAP or virtual PSAP.
- **Internet to NG PSAP:** 911 calls originating from IP-based applications or partners enter through secured IP/SIP interfaces at ESInet boundaries, undergo policy and security controls at the BCF, and then follow the same ESRP/ECRF-based routing as other NG OSP calls.
- **Text / ALI / GIS Traffic:** Text sessions (including RTT and text control center traffic), ALI/location queries, and GIS-based routing updates traverse the ESInet using dedicated SIP and web service interfaces, with NGCS elements (ECRF, LVF, LIS, ALI interfaces) performing location validation, routing determination, and synchronization with GIS data.
- **Virtual PSAPs:** Traffic destined for virtual or distributed PSAP configurations is routed by NGCS using policy and ECRF results to multiple PSAP sites or positions, maintaining consistent treatment of media and text while allowing dynamic distribution of calls.
- **BCF to ECRF:** SIP sessions entering through the BCF are forwarded to NGCS components, where the ESRP invokes ECRF/LoST queries to obtain routing data based on the caller's location, with the ESInet providing underlying IP transport for these control transactions.
- **ECRF to SI/ESRP/PSAP/LPG:** ECRF results (e.g., URLs or route targets) are returned to the ESRP or policy routing function, which then selects the appropriate next hop—PSAP call handling, LPG for legacy PSAPs, or additional ESRP/SI elements—for final call delivery.
- **LSRG to OSP / OSP to LNG:** When LSRGs are used, they interface with legacy selective routers via SS7 trunk groups; calls are passed from the OSP into the LSRG/LNG complex, converted to SIP, and routed via NGCS. Corresponding responses and star-code transactions flow back toward the legacy selective routers over the same path.
- **Logging/Recording:** Media and signaling streams are duplicated or forwarded to logging recorders via SIP/RTP or dedicated interfaces, with NGCS and PSAP systems generating CDRs and detailed logs that traverse secure ESInet paths to recording and audit systems.
- **Monitoring/Management:** Management and telemetry traffic (SNMP, syslog, KPI collection) flows from ESInet and NGCS elements to centralized NMS/EMS platforms over secured management VLANs or VRFs, separated from 911 service traffic while still using the common ESInet infrastructure.

5.1.12.5. TRAFFIC SHAPING

*Respondents must include a description of where traffic shaping will be employed, detailing the techniques used and their intended benefits. A formal **traffic shaping policy document** must be created, ensuring transparency and regular updates are made available to State personnel.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Description of where traffic shaping is employed, the techniques used, and their intended benefits.
- Creation of a formal traffic shaping policy document with transparency, regular updates, and availability to State personnel.

LUMEN RESPONSE:

Lumen employs traffic shaping at defined control points within the ESInet to protect SIP signaling, RTP media, and NG911 data traffic during congestion, abnormal conditions, or failure scenarios. Shaping is applied at ESInet ingress points to prevent oversubscription from originating service providers, legacy interworking gateways, and interconnecting networks; within core and aggregation layers to preserve priority handling for emergency services traffic; and at egress points toward PSAPs and NGCS to maintain consistent service quality regardless of upstream behavior.

Traffic Shaping Techniques and Operational Benefits. Traffic shaping controls include class-based prioritization aligned to DiffServ markings, selective rate limiting and policing, traffic segmentation, priority scheduling, and adaptive controls that respond to congestion or anomalous traffic patterns. These techniques prevent lower-priority, malformed, or excessive traffic from degrading 9-1-1 call delivery, preserve low latency and minimal packet loss for emergency communications, protect NGCS and PSAP resources, and maintain service continuity during surge events or network impairments while ensuring standards-aligned performance across the ESInet.

Protection of NGCS and ESInet Interconnection Boundaries. At defined interconnection points between the ESInet and NG Core Services, traffic shaping mechanisms protect call processing, routing, and supporting services from unintended or disruptive traffic conditions. These controls ensure that NGCS functional elements remain insulated from abnormal volumes or malformed traffic that could otherwise impact statewide NG911 operations.

Traffic Shaping Policy Documentation and Transparency. Lumen develops and maintains a formal Traffic Shaping Policy applicable to the ESInet and its interconnections with NGCS. The policy documents where traffic shaping is employed, the techniques used, the classes of traffic affected, and the operational intent of each control. The policy is maintained as a living document and updated as network conditions, standards, or operational requirements evolve.

State Visibility and Ongoing Governance. Current versions of the Traffic Shaping Policy are made available to designated State personnel to support ongoing oversight, operational coordination, and confidence in how traffic management controls are applied across the NG911 environment throughout the contract term.

5.1.12.6. ESINET NETWORK TIME

Network Time Protocol servers must be provided. The NTP servers must provide service to all elements in the ESInet including all PSAPs and other agencies on the ESInet. Time service must permit every system and every agency to maintain time within 1 millisecond of absolute time with 4 nines (99.99%) availability. The network shall have a hardware clock. However, in no circumstances, including failure of the hardware clock, must time as maintained by the time server(s) vary by more than 20 milliseconds from absolute time.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Provision of NTP servers serving all ESInet elements (NGCS FEs, PSAPs, agencies) within 1 millisecond of absolute time with 4 nines (99.99%) availability.*
- *Preference for hardware clock but ensuring no more than 20 millisecond variances even on failure.*
- *Descriptions of NTP service provision, confirmation of 1 millisecond accuracy with 4 nines availability, and meeting 20 millisecond variance threshold.*

LUMEN RESPONSE:

We provide a dedicated Network Time Protocol (NTP) service for the Nebraska ESInet designed to support consistent, high-accuracy time synchronization across NGCS functional elements, PSAPs, and participating public safety agencies. The NTP service is engineered to meet the State's requirements for accuracy, availability, and resilience, including hardware-anchored time sources, controlled variance under failure conditions, and documented monitoring and compliance assurance. The proposed solution includes:

- **Provision of NTP servers serving all ESInet elements within 1-millisecond and 99.99% availability.** We provide authoritative NTP servers that serve all ESInet elements, including NGCS functional elements, PSAPs, and connected public safety agencies. The service is engineered to deliver synchronized time within 1-millisecond of absolute time and to achieve 99.99% availability, supporting consistent timestamps for call processing, routing, logging, security events, and operational reporting.
- **Preference for hardware clock with controlled variance on failure.** Time synchronization is anchored by a hardware-based reference clock to provide a stable and authoritative time source under normal operating conditions. Redundant design and isolation safeguards ensure that, in the event of hardware clock failure or loss of an upstream reference, time variance does not exceed 20-milliseconds from absolute time, preserving timestamp integrity for all time-dependent NG911 functions.
- **Description and confirmation of NTP service provision and compliance.** We document the NTP service architecture, including time sources, redundancy, and distribution mechanisms, to describe how synchronized time is delivered across the ESInet and NGCS. Continuous monitoring is used to confirm compliance with the 1-millisecond accuracy objective and 99.99% availability requirement, and operational controls support detection and response to any out-of-tolerance conditions. Time synchronization performance, including adherence to the 20-millisecond variance threshold, is reflected consistently across logs, call records, system traces, and reports.

Together, these capabilities ensure that Nebraska's ESInet maintains accurate, resilient, and observable time synchronization in support of NG911 operations, security, and statewide operational integrity.

5.1.13. Resilience and Service Levels

5.1.13.1. ESINET AVAILABILITY

The ESInet must maintain the integrity of emergency call processes, ensuring availability of 99.999% at all network points (Ingress, Core, Egress). Key provisions include:

- *The entire call path must be resilient and monitored for compliance with the availability standard.*
- *Support services not related to call handling should achieve an availability of 99.9%.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Resilience and monitoring of the entire call path for 99.999% availability at ingress, core, and egress with clear identification of any boundaries that are outside of the span of control of the contractor which may be a risk to achieving five nines (e.g., OSP ingress, PSAP egress). 99.9% availability is acceptable for non-call-handling support services.*
- *Uptime calculations assessing physical device MTBF for critical equipment in serial/parallel configurations.*
- *A comprehensive sparing plan for all sites with replacement strategies.*
- *Established technician response times for outages.*
- *Calculated MTTR based on spares and response times.*
- *A consolidated overview of overall availability combining MTBF and MTTR data.*

LUMEN RESPONSE:

Lumen designs and operates the Nebraska ESInet and NG911 core to meet the State's availability objectives through engineered redundancy, quantitative modeling, and disciplined operational practices. Our approach addresses end-to-end call-handling availability, supporting infrastructure resilience, defined demarcation points with external domains, and transparent documentation of how availability targets are achieved and sustained. The proposed solution provides the State:

- **Resilience and Monitoring of the Entire Call Path for 99.999% Availability.** We engineer the ESInet to achieve **99.999%** availability across call-handling paths, including ingress, core, and egress elements under our operational control, using geographically redundant nodes, diverse transport paths, and continuous monitoring of each hop in the call path. Clear demarcation points are identified where responsibility transitions to Originating Service Providers or PSAP environments, and these boundaries are documented as potential risk areas to achieving end-to-end five-nines availability. Non-call-handling support services are engineered and monitored to a 99.9% availability objective consistent with their role.
- **Uptime Calculations Using MTBF-Based Availability Modeling.** Availability is assessed using Mean Time Between Failure (MTBF) data provided by equipment manufacturers for critical ESInet and NGCS components, including routers, session border elements, servers, and access infrastructure. Modeling accounts for serial and parallel configurations, including redundant pairs and clustered designs, to validate that composite availability meets call-path objectives.
- **Comprehensive Sparing Strategy Supporting Availability Targets.** A sparing strategy is maintained for critical ESInet and NGCS components, with replacement equipment staged at core facilities and designated regional locations. The strategy defines which components are stocked, how replacements are deployed, and how replenishment is managed to ensure that MTTR assumptions used in availability modeling remain valid throughout the contract term.

- **Defined Technician Response Expectations and MTTR Calculations.** Technician response expectations for service-affecting outages are established and incorporated into Mean Time to Repair (MTTR) calculations. MTTR values reflect both diagnostic and restoration activities, including use of pre-positioned spares or failover mechanisms, and are combined with MTBF data to produce availability estimates for individual functions and the end-to-end call path.
- **Consolidated Availability Documentation and Transparency.** Availability assumptions, MTBF and MTTR inputs, calculated uptime for serial and parallel configurations, sparing plans, and response assumptions are documented and maintained within configuration and service management records. This documentation provides the State with visibility into how availability objectives are engineered, monitored, and maintained, and where external dependencies may introduce residual risk.

Together, these design, modeling, and operational practices provide a transparent and defensible basis for achieving **99.999%** availability for call-handling services and 99.9% availability for non-call-handling support services within Nebraska's NG911 environment.

5.1.13.2. ESINET RELIABILITY

*The design of the ESInet must emphasize reliability through strategic diversity across geographic regions, technology, and vendors. Each node within the network must utilize **at least two routers from different manufacturers** to deliver redundancy. If this is unfeasible, a rationale for maintaining reliability under specific failure conditions must be provided. **No segment of the network should hinge on a single point of potential failure, such as a "backhoe incident."***

The reliability design must conform to guidelines specified in the FCC Report and Order 13-158 aimed at enhancing 911 reliability across all communication networks.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Strategic diversity across geographic regions, technology, and vendors.
- Use of at least two routers from different manufacturers per node for redundancy (or rationale if unfeasible).
- Elimination of single points of failure (e.g., "backhoe incident").
- Conformance to FCC Report and Order FCC 13-158 for enhancing 911 reliability.

LUMEN RESPONSE:

Lumen designs the Nebraska ESInet with reliability engineered through layered geographic, technological, and vendor diversity to eliminate single points of failure and to meet the reliability objectives outlined in FCC Report and Order 13-158. The ESInet architecture incorporates diversity across transport providers, facilities, routing domains, and core processing locations so that no single physical incident—such as a fiber cut, equipment failure, or localized facility outage—can disrupt end-to-end 9-1-1 call delivery.

- **Geographic, Technology, and Vendor Diversity.** The ESInet is designed with geographically separated core facilities, diverse aggregation locations, and physically diverse access paths to reduce correlated risk from localized or regional events. Technology diversity is applied across transport, routing, security, and application layers so that failures in one domain do not propagate across the ESInet. Vendor diversity is

leveraged where practical within the infrastructure ecosystem, consistent with established NG911 design practices.

- **Redundant Routing Equipment and Documented Exceptions.** Where feasible, ESInet nodes are designed with redundant router pairs, including the use of routers from different manufacturers to provide vendor-level diversity and continuous forwarding during device or link failures. In locations where multi-vendor routing pairs are not technically practical or do not materially improve reliability, the rationale is documented, and equivalent resilience is achieved through compensating measures such as redundant chassis, diverse uplinks, dual power sources, and geographically separated failover nodes.
- **Elimination of Single Points of Failure.** The ESInet is engineered to eliminate single points of failure across ingress, core, and egress through diverse physical entrances, independent fiber routes, redundant network elements, and automatic rerouting with fast reconvergence. Transport paths are selected to avoid shared conduits and common failure zones where available, specifically addressing risks associated with localized physical incidents such as “backhoe” events.
- **Conformance with FCC Report and Order 13-158.** The ESInet reliability design aligns with the principles of FCC Report and Order 13-158, including circuit diversity, backup power considerations at critical facilities, continuous network monitoring, and improved outage detection and reporting. Operational practices support rapid fault detection, escalation, and remediation to maintain continuity of 9-1-1 services consistent with FCC reliability objectives.

This reliability approach provides Nebraska with an ESInet design that reduces correlated risk through layered diversity, supports continued 9-1-1 call delivery during common failure scenarios, and includes clear documentation of any design exceptions and compensating protections used to maintain service continuity and FCC 13-158 alignment.

5.1.14. Operations and Management

5.1.14.1. ESINET MONITORING AND MANAGEMENT

A dedicated 24/7/365 Network Operations Center (NOC) must oversee continual ESInet monitoring to ensure immediate detection of any functional disruption within the system. §E-9.3.1 contains minimum NOC requirements that must be met as part of this proposal.

- **All network links require constant congestion monitoring,** with timely mitigation strategies implemented by contractors.
- **Failure alerts should be generated within a minute for any link or component malfunction** of the ESInet.

Thresholds for triggering mitigation must be explicitly delineated, especially in response to network congestion, with proactive communication to the State regarding the mitigation plan, implementation timelines, and ongoing progress reports.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A dedicated 24/7/365 NOC for continual monitoring and immediate detection of disruptions.*
- *Constant congestion monitoring of links with timely mitigation.*
- *Failure alerts within 1 minute for malfunctions.*

- *Explicit thresholds for mitigation (e.g., congestion).*
- *Proactive communication to the State on mitigation plans, timelines, and progress.*

LUMEN RESPONSE:

Lumen provides continuous 24x7x365 operational support for Nebraska's ESInet and associated NG911 services through a dedicated, CONUS-based NG911 Network Operations Center, supported by geographically diverse backup NOCs. The NG911 NOC operates within Lumen's Public Safety Services and Compliance organization and serves as the single point of contact for all service issues through a dedicated, toll-free help desk. The NOC is staffed 24x7x365, providing Tier 1, Tier 2, and Tier 3 support.

Staffing, Expertise, and Continuity. NG911 NOC personnel bring deep experience in the design, implementation, and operation of mission-critical networks and systems. The team includes front-line technical support and senior support engineers with relevant industry certifications and public safety experience. NOC operations are supported by redundant facilities and secure remote access capabilities, ensuring continuity of operations during localized disruptions. The specialized NG911 NOC draws upon the support and resources of the full Public Safety Services and Compliance group, **Figure 5.1.14.1-1**.

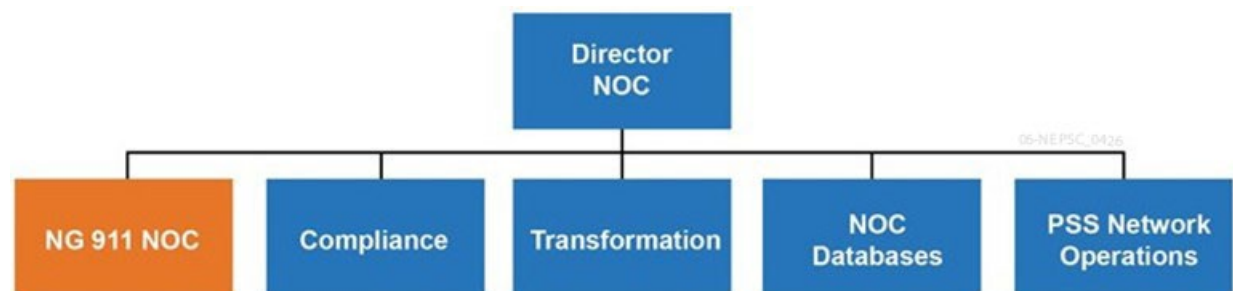


Figure 5.1.14.1-1. Organizational placement of Lumen's NG9-1-1 NOC

End-to-End Monitoring and Visibility. The NG911 NOC provides real-time visibility across ESInet ingress, core, and egress segments, including transport links, routing elements, interconnections, and critical NG911 services. Automated monitoring and alerting are applied to detect abnormal conditions affecting throughput, latency, jitter, packet loss, routing stability, device health, and service availability. Monitoring systems are configured to detect failures or instability and generate actionable alerts within approximately one minute of occurrence.

Figure 5.1.14.1-2 provides a notional overview of our NG911 tools and their integration, and the role and relationship of an Intrado (Sentry) NOC, which in this solution to State of Nebraska, monitors and supports the hosted CPE at the data centers.

Lumen's operational tools provide NG911 NOC personnel with a deep and clear understanding of network and service operations.

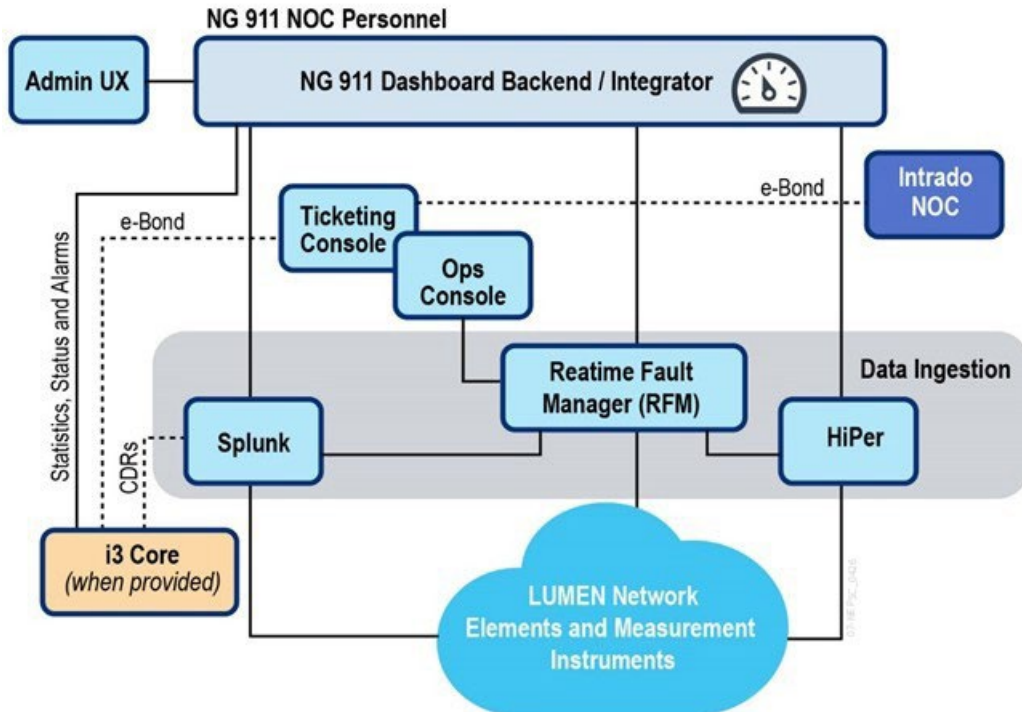


Figure 5.1.14.1-2. Summary of NOC Tools and Systems

Performance Management and Congestion Mitigation. All ESInet links are continuously monitored for utilization and performance trends. Defined operational thresholds trigger mitigation actions when congestion or degradation is approaching service-impacting levels. This repeatable, threshold-driven response model allows the NOC to intervene early and preserve NG911 signaling and media performance.

Operational Toolsets and Analytics. Lumen employs a comprehensive suite of automated monitoring, alarming, ticketing, and analytics platforms to support NG911 operations. These tools collect and correlate data from network devices, applications, and service components, providing single-pane operational views specific to NG911 services. Analytics support proactive fault detection, SLA compliance monitoring, and rapid diagnosis of service-affecting conditions.

Incident Management and Escalation. NOC operations follow ITIL-aligned and ISO-compliant service management practices. When a potential or actual service-affecting condition is identified, the NOC initiates incident management procedures that include automated ticket creation, triage, escalation, notification, resolution, and reporting. Escalation occurs at defined intervals if progress is not achieved, and senior technical and management resources are engaged as required. Lumen sustains continuous resolution efforts until full service restoration is achieved.

Proactive Notification and State Communication. The NOC provides proactive notification to designated State stakeholders for service-impacting or congestion-related events. Notifications describe the nature of the issue, mitigation actions, anticipated timelines, and status updates through resolution. Communication practices align with applicable public safety reliability and continuity requirements and support transparency and coordinated response.

Security Operations Integration. Cybersecurity monitoring and response activities are coordinated with Lumen's Security Operations Center (SOC). While specific security operations details are restricted for security reasons, security-related alerts and incidents are monitored, correlated, and escalated through automated processes consistent with network incident handling.

Ticketing, Reporting, and Review. All incidents and service requests are tracked through Lumen's centralized ticketing platform, which maintains detailed records for operational review, trend analysis, and audit purposes. Ticket status, resolution details, and post-incident information are available to the State. Root cause analysis and reason-for-outage reporting are performed when appropriate, and ticket activity is reviewed with the State through regular operational review meetings.

State Visibility and Dashboards. Network performance and service status information is made available to the State through a secure customer portal and dashboard, **Figure 5.1.14.1-3**.

The portal provides customizable views, charts, reporting, and data export capabilities, allowing the State to monitor ESInet health, performance, and trends independently.

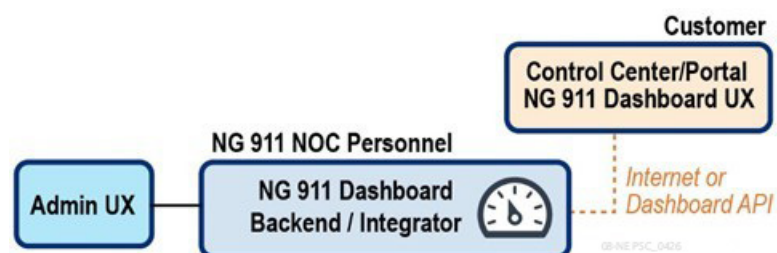


Figure 5.1.14.1-3. State of Nebraska Monitoring Portal

Data on network performance and status collected at the NOC, and overall service status is always available to the State of Nebraska in a dashboard presentation via our NG911 customer portal. As depicted in **Figure 5.1.14.1-3**, the portal is reached via a secure Internet connection, although there is an option to connect using an API. The portal features a tool to produce 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.

Coordinated Specialized Support. The NG911 NOC coordinates with specialized operational teams, including SD-WAN support, NGCS platform support, and security operations, to ensure rapid access to subject-matter expertise when required. This coordinated model ensures that issues are addressed holistically across transport, routing, application, and security domains.

Lumen uses a proactive monitoring and notification process to rapidly detect and respond to service issues. The process engages platform-specific alarm thresholds to identify potential service impairments. Network alarms generate trouble tickets that automatically notify the State of Nebraska via e-mail, telephone and/or other means as defined. Proactive Customer Notification (PCN) gives the State the flexibility to specify certain notification parameters on a service-by-service basis. Although the specific toolsets can differ, security issues are monitored and alarmed in a similarly automated fashion. Where practical, Lumen automation may perform initial triage or repair concurrently with customer notification that a service issue has occurred.

Note that tickets can be generated from internal alarms, and that alarms also can come from external e-bonded networks or suppliers. The figure also highlights the operational relationships between the NG9-1-1 NOC and other specialized operational centers. As

shown in the figure these include the Security Operations Center (SOC), which manages Lumen's response to cybersecurity threats or attacks, deep support for the NGCS elements within our NG9-1-1 solution (when included, but in this proposal addressing CHE and CPE), and the SD-WAN support center. As discussed elsewhere in this proposal, Lumen's NG9-1-1 solution applies SD-WAN in its ESInet for routing, traffic management, and security.

Lumen adheres to strict escalation procedures and measurable timeframes to ensure the rapid resolution of network issues. We use our Clarify database-derived Ticketing Console to track all NG911 proactive and reactive trouble reports. In the event of an outage Lumen applies immediate and sustained effort, 24x7, until a final resolution is in place. Escalation for all trouble reports occurs every 30-minutes or as appropriate if an ETA/ETR is provided. As part of an escalation chain, Tier 2 support is engaged within 30-minutes if no significant progress in the repair of the trouble is occurring. Internal Lumen notification processes engage Director/VP leadership if significant service impairment occurs. Separately, Lumen's communications with the State of Nebraska regarding the outage condition is consistent with FCC Report and Order 13-158, Improving 9-1-1 Reliability and Continuity of Communications Networks, Including Broadband Technologies.

Figure 5.1.14.1-4 depicts the Lumen operations model for ticket resolution by the NOC.

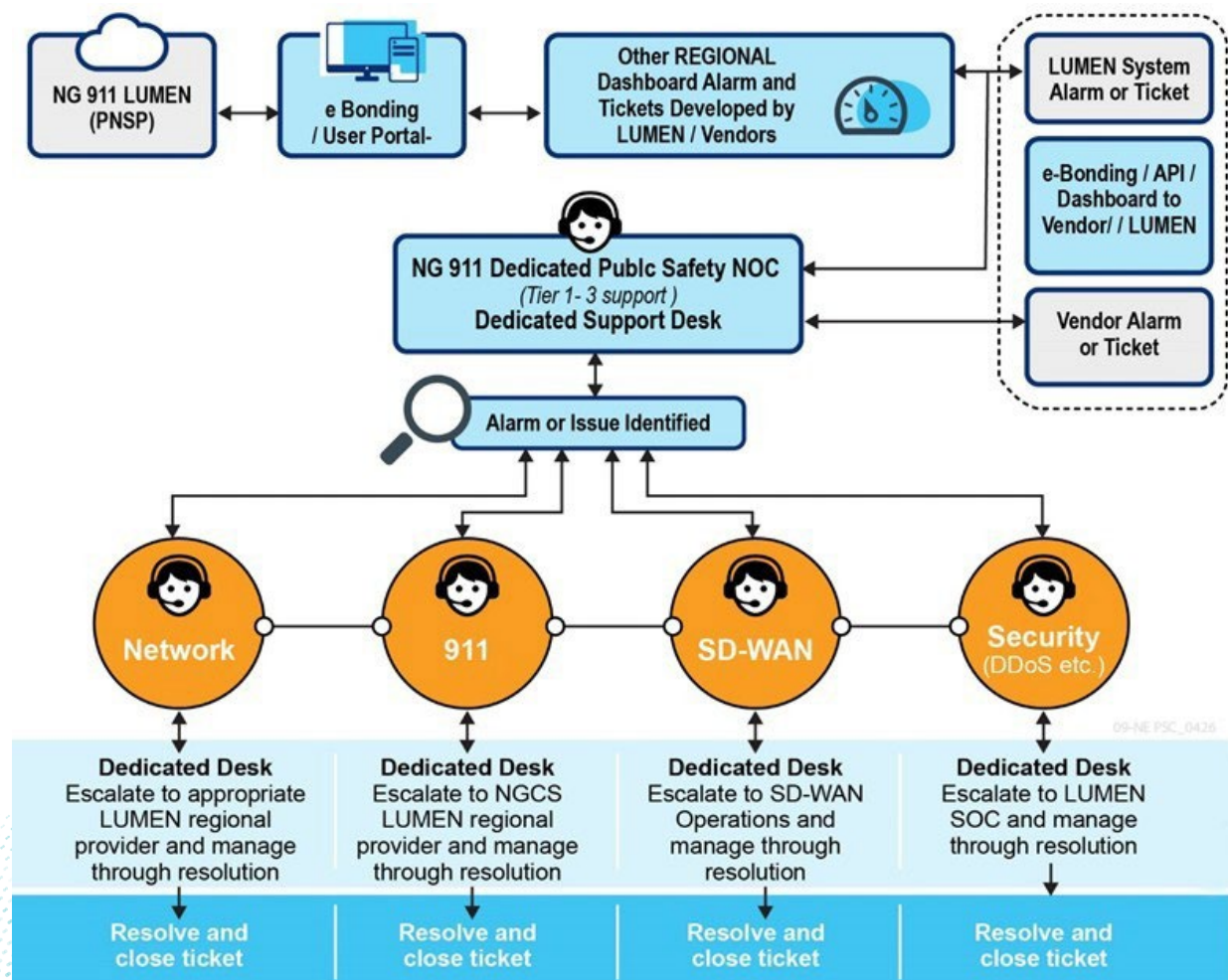


Figure 5.1.14.1-4. Ticket/Issue Problem Resolution Flow

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. Lumen will continue resolution activity until full service is restored. If active progress and meaningful status updates are not being made, Lumen technicians are empowered to escalate issues internally and externally as required. The state of Nebraska can also request escalations. Lumen customer service is chartered to provide world-class customer support that attempts to resolve issues on a first contact basis.

Lumen maintains records (logs) 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 Lumen customer our response is not complete until Lumen representatives contact the customer with an explanation of the problem and a discussion of the actions that Lumen took to resolve issues and of how the problem will be avoided in the future. As they do today, the project team dedicated to the State of Nebraska reports on and reviews all tickets in weekly and/or quarterly program review meetings.

5.1.14.2. ESINET MAINTENANCE WINDOW

*The proposed ESInet **must have no scheduled down time.** If maintenance is required, which would temporarily cause the network to have lower than 99.999% availability while the maintenance activity is underway, the contractor must provide a **pre-maintenance risk register** prior to commencing the maintenance and complete the maintenance under the terms of §E-9.5.1 (Change Management Requirements) and §E-9.5.2 (Scheduled Maintenance Process) below. **No maintenance activity which, if improperly completed, which could cause an outage of any part of the network, shall be permitted outside the terms of §E-9.5.1 and §E-9.5.2.***

*All maintenance activity must be preceded by a Maintenance Operation Plan (MOP) required **at least 14 days** prior to the maintenance. The MOP shall include the provisional operating configuration to ensure that performance continually meets the 99.999% service level as the maintenance is being performed.*

Scheduled downtime is unacceptable under routine operations.** If maintenance is essential, it must follow as stringent Scheduled Maintenance Process to maintain or exceed 99.999% availability. Any maintenance that could jeopardize network functionality **must be strictly controlled.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *No scheduled downtime; completion of any maintenance impacting availability under specified terms (§E-9.5.1 and §E-9.5.2).*
- *Prohibition of maintenance causing outages outside those terms.*
- *Requirement for a Maintenance Operation Plan (MOP) at least 14 days prior, including provisional configurations to maintain 99.999% service level.*
- *Descriptions of handling no-downtime requirements, planning/conducting maintenance without impacting availability, and the MOP process for guiding activities.*

LUMEN RESPONSE:

Lumen performs all ESInet maintenance for Nebraska in a manner that preserves uninterrupted 9-1-1 call handling and complies with the State's no scheduled downtime requirement. The ESInet is engineered and operated to sustain 99.999% availability through active-active architectures, geographic diversity, and redundant network elements. Any activity that could temporarily affect availability is executed only under the State-defined Change Management and Scheduled Maintenance processes, with full governance and oversight.

Prohibition of Uncontrolled Maintenance Activities. No maintenance activity that could jeopardize ESInet functionality or introduce outage risk is permitted outside formally governed change and scheduled maintenance processes. All potentially impactful work requires documented risk assessment, State approval, rollback planning, and continuous monitoring during execution to protect emergency services and call delivery.

Maintenance Operation Plan (MOP) Requirements. All maintenance activities are preceded by a Maintenance Operation Plan (MOP) submitted at least fourteen days prior to the proposed maintenance window. The MOP documents the scope of work, pre-maintenance risk register, provisional operating configuration, redundant paths and failover mechanisms, rollback procedures, communications plan, validation activities, and escalation contacts necessary to maintain the 99.999% availability objective throughout the maintenance activity.

Controlled Execution and Verification. Maintenance is planned and conducted by isolating individual components and leveraging redundant infrastructure, alternate routing, and active-active processing to avoid service disruption. Continuous NOC oversight is maintained to monitor performance and detect anomalies. Pre-maintenance and post-maintenance validation, including functional and failover checks, is performed to confirm service integrity before, during, and after the activity.

Transparency, Documentation, and State Assurance. Upon completion of maintenance activities, documentation is updated and outcomes are communicated to the State, including confirmation that service levels and availability objectives continue to be met. This disciplined approach ensures all ESInet maintenance is predictable, transparent, and tightly controlled, providing the State confidence that required work can be completed without compromising 9-1-1 call delivery or violating mandated availability thresholds.

5.1.15. Implementation Details**5.1.15.1. PORT MAPPING**

Comprehensive documentation of port block/mapping/forwarding policies must be maintained, providing access to both the State and PSAPs. This documentation should include provisions that allow stakeholders to request traffic on specific ports to be allowed from external sources into predetermined network points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Comprehensive documentation of port block/mapping/forwarding policies accessible to the State and PSAPs.*

- *Provisions allowing stakeholders to request traffic on specific ports from external sources to predetermined network points.*

LUMEN RESPONSE:

Lumen maintains controlled and transparent port-level security across the Nebraska ESInet to ensure that external traffic enters the network only through authorized interfaces and in accordance with NG911 security and interoperability requirements. Port blocking, mapping, and forwarding policies are documented and governed so that the State and PSAP stakeholders have clear visibility into how traffic is permitted, restricted, and protected at ESInet boundaries.

Comprehensive Documentation Of Port Policies. We maintain comprehensive documentation of ESInet port blocking, mapping, and forwarding policies across ingress, core, and egress interconnection points. Documentation identifies permitted, restricted, and blocked ports and protocols, their intended purpose, applicable traffic types, and associated ESInet or NGCS functions. This documentation is maintained as controlled operational material and made accessible to authorized State personnel and PSAP stakeholders.

Controlled Updates Through Change Management. Port mapping and forwarding policies are updated only through governed change management processes to ensure accuracy, version control, and continued alignment with security and operational requirements. Approved changes are reflected in the documentation to maintain an accurate operational baseline.

Stakeholder Requests For Port Enablement. Authorized State stakeholders may request that traffic on specific ports be permitted from external sources into predefined ESInet interfaces. Requests are evaluated for technical feasibility, security impact, and operational risk prior to approval and implementation.

Secure Implementation And Ongoing Visibility. Approved port access requests are implemented using established security controls to protect the integrity and performance of ESInet and NGCS operations. All changes are documented within the port policy records to ensure continued visibility for the State and PSAPs and to support coordination and troubleshooting.

This approach provides Nebraska with clear governance, security, and transparency for port-level controls while enabling required interoperability in a controlled and auditable manner consistent with NG911 operational expectations.

Deliverables - ESInet Architecture and Design

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires a complete, standards-aligned definition of the ESInet architecture that demonstrates resilience, deterministic traffic handling, and measurable recovery performance across the end-to-end NG911 call path. Lumen complies by delivering detailed ESInet architecture documentation that fully defines IP addressing,

VLAN segmentation, Quality of Service (QoS) policies, physical and logical diversity, and the redundancy model used to eliminate single points of failure. These materials clearly depict ingress, core, and egress paths, including interfaces to OSPs and PSAPs, and are maintained as controlled artifacts to support acceptance, operations, and ongoing governance.

Lumen further complies by demonstrating secure call signaling and media handling using SIP over TLS and SRTP across the ESInet, including documented failover scenarios that validate continuity of signaling and media traversal without packet loss during component, link, or site failures. Demonstrations and supporting evidence confirm that failover is automatic, transparent to call processing, and does not degrade NG911 call delivery or quality.

In addition, Lumen provides documented recovery objectives and operational performance commitments, including defined RTO and RPO targets, MTTR service levels of less than two hours for critical issues, and formal failure mode and effects analyses. These deliverables identify potential fault conditions, detection and alerting mechanisms, recovery actions, and mitigation strategies, ensuring the State has clear visibility into how the ESInet is engineered to meet 99.999% availability requirements. Collectively, these deliverables provide the State with verifiable evidence that the proposed ESInet architecture is resilient, secure, and operationally mature, and that it meets the technical and performance expectations defined in the RFP.

5.2. Next Generation Core Services (NGCS) Requirements

The proposal must include a Next Generation Core Services (NGCS) implementation deployed across multiple redundant data centers. The system shall use at least three (3) data centers, with a preference for at least one in-state and at least one geographically distant (more than 100 miles away - preferably several states away) to avoid common-cause failures such as severe weather or localized incidents. The state will permit a shared facility but prefers a separate NGCS instance (distinct virtual machines and management) from other tenants. Each NGCS component - physical and virtual - must be redundantly deployed in every data center with no single point of failure.

The NGCS must also be isolated and resilient against external threats and against faults arising elsewhere in the provider's NG911 ecosystem. Respondents must describe and demonstrate how their design prevents impact from incidents in another ESInet or statewide NGCS service offered by the provider, ensuring Nebraska's NG911 operations continue without degradation.

All NGCS elements which use policies must retrieve policies from a NENA-STA-010.3-compliant policy server and must be

provisioned with the host name of the policy server it uses. See §E-2.2.1.1 for the NGCS Policy Store requirements.

- The State desires redundant functional elements, including all databases to be deployed active-active such that all redundant elements are actually serving traffic at all times.*
- The Respondent must state which functional elements and databases are not actually serving traffic at all times and for each such element; the mechanism for failover that will reliably guarantee the 99.999% availability requirement of the entire system.*

- *For active-active elements, the Respondent must describe how the client determines an element has failed, and how it recovers (typically via retry), noting what the worst-case timing for the detection and retry is, and how the appropriate Service Level Objective within that Service Level Agreement is maintained.*
- *For each database, and each call-state data object, the Respondent must describe how state is reliably maintained, and failover within the 99.999% availability is assured, including any retry operations required at the client.*
- *For databases that are updated at call time, the Respondent must describe the replication strategy, specify a maximum data sync time, and describe how it is achieved. Note that the State requires the ability to update a service boundary polygon in the ECRF dynamically, and replication/data sync of that operation must be described in the proposal.*
- *The State expects that the LPG, LNG, and MCS be the only element that supports legacy functions.*

The contractor shall **supply or ensure interoperability with all NGCS functional elements as defined by NENA**, including but not limited to the Location Validation Function (LVF), Location Information Server (LIS), Emergency Call Routing Function (ECRF), Emergency Services Routing Proxy (ESRP), Policy Routing Function (PRF), and Legacy Network Gateway (LNG). All elements must expose the NGCS interfaces specified in the standard, with the contractor documenting implementation details for each (e.g., integrated software modules, hosted cloud services, or third-party integrations). The system must support bridging to legacy systems via appropriate gateways.

All NGCS interfaces shall adhere to defined specifications, including SIP messaging extensions, RESTful APIs (using JSON/XML payloads), and NENA-defined ESInet ↔ Core interfaces. Payloads and schemas must comply with NENA requirements, such as Presence Information Data Format - Location Object (PIDF-LO) for location data, with support for HTTP-Enabled Location Delivery (HELD) protocols.

NGCS components (e.g., ECRF queries, LVF validations) **must achieve performance targets**, including lookup latency SLAs of 200 millisecond median and 500 milliseconds at the 95th percentile under peak load (jurisdiction may adjust based on scale). The system must handle at least 10 queries per second per component with no degradation.

The NGCS must scale horizontally to support jurisdiction-specific peak call rates (e.g., 1,000 calls per hour per PSAP) and data volumes, with tenant isolation for multiple PSAPs via virtual instances or containers. It shall enable dynamic provisioning of PSAP service boundaries through administrative interfaces.

All NGCS transactions shall be logged comprehensively, including timestamps, full request/response payloads (redacted for privacy where necessary), originator identities, correlation IDs, and error codes, enabling end-to-end tracing across components. Logs must be stored in a searchable database with retention support.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NGCS deployment in multiple redundant data centers (preference for at least 3, with one in-state and one >100 miles away).
- Preference for separate instances (different VMs) if sharing data centers.

- *Redundant deployment of all components without single points of failure; resistance to external threats and internal disruptions from other ESInets/NGCS.*
- *Description/demonstration of unimpeded operation during disruptions.*
- *Policy retrieval from NENA-STA-010.3-compliant policy server with host name provisioning.*
- *Preference for active-active redundant elements/databases serving traffic at all times.*
- *Statements on non-active elements with failover mechanisms guaranteeing 99.999% availability.*
- *Descriptions of failure detection/recovery for active-active elements (worst-case timing, SLO maintenance).*
- *State maintenance/failover for databases/call-state data.*
- *Replication strategy for call-time updated databases with max sync time.*
- *Dynamic ECRF service boundary updates with replication/sync description.*

LUMEN RESPONSE:

Lumen deploys Nebraska's NGCS across geographically redundant data centers engineered to eliminate single points of failure and sustain uninterrupted NG911 operations. The architecture supports deployment across a minimum of three data centers, including at least one in-state location and one more than 100 miles away. All NGCS components, physical and virtual, are deployed redundantly so the loss of any single server, storage system, network device, or facility does not interrupt call handling or routing functions. Where shared data center facilities are used, Nebraska's NGCS operates as a logically isolated environment with dedicated virtual resources, management domains, routing instances, logging pipelines, and security boundaries.

Current Proven Operational Footprint and Third NGCS Core Data Center. Nebraska's NGCS is currently operated across two fully redundant, geographically diverse data centers in Longmont, Colorado and Miami, Florida. These sites have supported Nebraska's NG911 operations for more than four years with sustained 100% availability, providing true geographic separation from regional hazards and eliminating dependency on any single facility or network corridor. To address the State's preference for a third data center, Lumen will deploy an additional NGCS site within Nebraska to participate fully in active-active load sharing and synchronized replication. Based on demonstrated operational performance, Lumen recommends continuing the existing two-site architecture, with the in-state site offered as an optional enhancement as depicted in **Section 3.1, Figure 3.1-1**.

Tenant Isolation and Cross-State Protection. Nebraska's NGCS is isolated from other states' ESInets and NGCS instances through separate routing domains, dedicated ingress and egress controls, independent security policies at the BCF and application layers, and segmented management and logging environments. Incidents, traffic surges, or misconfigurations affecting other jurisdictions cannot consume Nebraska's NGCS capacity, alter routing or policy behavior, or degrade PSAP operations.

NGCS Functional Coverage and Standards-Based Interfaces. The solution includes all NENA-defined NGCS functional elements required by Nebraska, including ESRP, ECRF, LVF, LIS, PRF, BCF, LNG, LPG, MCS, logging, monitoring, and the Spatial Interface. All non-legacy functional elements operate natively within an i3-compliant environment. Interfaces follow NENA-defined profiles, including SIP with i3 extensions for call signaling, REST-based APIs

for policy and location services, and standardized ESInet-to-Core interfaces. Location is conveyed using PIDF-LO, with HELD supported where applicable.

Policy Management and Retrieval. All routing and treatment policies are retrieved from a NENA-STA-010.3-compliant policy server using host name-based provisioning. NGCS components retrieve policies over authenticated, encrypted channels using fully qualified domain names, ensuring policy lookup is decoupled from physical infrastructure. Policies defined by PSAPs and authorized State administrators undergo validation and are synchronized across all NGCS nodes to ensure consistent behavior statewide under all operating conditions.

Active-Active Operation and Controlled Standby Elements. NGCS components and supporting databases operate in active-active mode wherever feasible, including ESRP, PRF, BCF, logging services, API endpoints, and ECRF/LVF query interfaces. Where any element operates in active-standby mode, it is explicitly identified and implemented with continuous synchronization and automated failover to maintain the 99.999% availability objective.

Failure Detection and Automated Recovery. NGCS components continuously exchange health telemetry using application-level monitoring, heartbeat signaling, SNMP, and path integrity checks. When an impairment is detected, traffic is automatically rerouted to healthy peer instances without manual intervention. Network-layer fast convergence mechanisms provide sub-50 millisecond recovery, while application-layer logic ensures uninterrupted call signaling, policy retrieval, and location validation within defined service level objectives.

Database Replication and Call-State Continuity. All NGCS databases, including call-state records, routing tables, ECRF/LVF datasets, policy repositories, GIS data, logging stores, and configuration data, are replicated across geographically diverse data centers in near real time. Call-time-updated data is synchronized within 200 milliseconds under normal load, ensuring any node can immediately assume full processing responsibility during a failure without call loss, routing ambiguity, or retransmission.

Dynamic ECRF Boundary Management. PSAP and agency service boundaries are updated dynamically through the Spatial Interface using a controlled staging process. Boundary updates are validated, staged in inactive datasets, and promoted only after successful verification. Updates are replicated in real time across all NGCS nodes so routing decisions remain consistent and authoritative statewide. Automatic rollback protection ensures active routing datasets are never compromised.

Performance Scaling and PSAP Isolation. NGCS components are engineered to meet lookup latency and throughput expectations under peak load and scale horizontally through additional active instances. PSAPs and agencies are isolated through virtualized or containerized deployments so one entity's activity cannot degrade another's performance, while administrative interfaces support dynamic adjustments without disruption.

Security and Threat Isolation. Security is enforced across all layers using strict zone segmentation, mutual TLS, certificate-based authentication, firewalls, IDS/IPS inspection, rate limiting, and protocol validation. Cross-ESInet exchanges are authenticated and filtered at dedicated boundary points to prevent propagation of faults or threats from external networks. Continuous monitoring, vulnerability scanning, RBAC, hardened system images, and full audit logging support operational integrity and forensic analysis.

Unimpeded Operation During Disruptions. During network, system, or facility disruptions, NGCS automatically reroutes traffic across remaining healthy network paths without PSAP intervention. Predefined routing policies support hierarchical overflow, load balancing, GIS-based alternates, and abandonment routing to ensure uninterrupted call delivery. Active-active routing databases and synchronized service boundaries ensure routing accuracy during all failure scenarios.

Comprehensive Logging and Traceability. All NGCS transactions are logged with timestamps, correlation identifiers, and request and response metadata. Logs are centrally collected and indexed to enable end-to-end traceability, auditability, troubleshooting, and performance verification consistent with State policy.

5.2.1. Edge Security and Ingress

5.2.1.1. BORDER CONTROL FUNCTION (BCF)

The BCF must conform to NENA-STA-010.3 standards, preferably constructed from a commercial Session Border Controller (SBC), Firewall, and NG911-specific capabilities.

- **Call Processing:** *The BCF must handle all inbound calls from OSPs and should be configured between the ESInet and any interconnected ESInets to facilitate external connections.*
- **Call Egress:** *While optional, a BCF to manage outgoing communications between the ESInet and a PSAP may be necessary.*
- **Security Features:** *The BCF must incorporate the Bad Actor and Call Suspicion mechanisms as specified in NENA-STA-010.3. Calls directed to the ESInet should be accepted unless the source is blocklisted as a Bad Actor.*
- **Media Handling:** *The BCF must not anchor media unless it is necessary to do so. If the BCF does anchor media, it must implement ICE, STUN, and TURN mechanisms to navigate Network Address Translation (NAT) as applicable.*
- **Logging and Monitoring:** *The BCF must facilitate media logging per NENA-STA-010.3 specifications, with the ability to disable logging while retaining swift reactivation capabilities for diagnostic purposes.*

The BCF must:

- *Addresses on BCFs receiving traffic shall be globally routable IP addresses*
- *Process all calls from OSPs on the ingress side*
- *Support Bad Actor and Call Suspicion mechanisms*
- *Mitigate DDoS/TDoS attacks up to terabit capacity levels*
- *Accept calls directed to the ESInet regardless of source (unless marked as Bad Actor)*
- *Implement B2BUA if calls do not support REFER*
- *Avoid media anchoring where possible and implement ICE, STUN, and TURN when necessary*
- *Support ElementState and ServiceState SUBSCRIBE/NOTIFY*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Conformance to NENA-STA-010.3 preferably from commercial SBC, Firewall, and NG911 capabilities.*
- *Handling inbound calls from OSPs and between ESInets; optional egress BCF for outgoing to PSAP.*
- *Bad Actor/Call Suspicion mechanisms; acceptance of calls unless blocklisted.*
- *No media anchoring unless necessary with ICE/STUN/TURN for NAT.*
- *Media logging per standard with disable/reactivate capabilities.*
- *DDoS/TDoS mitigation up to terabit levels.*
- *B2BUA for non-REFER calls.*
- *ElementState/ServiceState support.*
- *Descriptions of BCF locations, Bad Actor/Call Suspicion implementation, DDoS/TDoS capacity, B2BUA details, tromboning avoidance, ICE/STUN/TURN, media recording, and ElementState/ServiceState support.*

LUMEN RESPONSE:

Lumen provides Border Control Function capabilities for the Nebraska ESInet that conform to NENA-STA-010.3 and are implemented using carrier-grade Session Border Controllers integrated with firewall services and NG911-specific application logic. BCFs are deployed at ESInet ingress points for Originating Service Providers, at ESInet-to-ESInet interconnections, and where required at PSAP-facing egress points. This deployment model enforces security, normalizes signaling, and ensures standards-compliant call delivery into the NG911 core.

Standards-Compliant Boundary Control and SIP Processing. Inbound SIP over TLS sessions from OSPs and interconnected ESInets terminate at the BCF using globally routable IPv4 and IPv6 addressing. The BCF performs SIP normalization, admission control, and security enforcement before forwarding validated traffic to NGCS functional elements such as the ESRP. Where originating endpoints do not support SIP REFER or where topology hiding is required, the BCF operates as a back-to-back user agent while maintaining standards-compliant SIP behavior. Routing controls are applied to avoid unnecessary tromboning by keeping intra-ESInet traffic on local paths unless interconnection traversal is required by policy.

Bad Actor, Call Suspicion, and DDoS/TDoS Protection. The BCF implements Bad Actor and Call Suspicion mechanisms consistent with NENA-STA-010.3 to identify and manage malicious, malformed, or abusive signaling sources. Calls are accepted by default unless a source is explicitly blocklisted or exceeds defined suspicion thresholds, protecting access for legitimate emergency communications. The BCF is deployed within Lumen's carrier-grade security environment and supports mitigation of volumetric DDoS and telephony denial-of-service attacks through rate limiting, anomaly detection, SIP-aware overload controls, traffic scrubbing, and coordinated filtering with upstream network protections, including large-scale attack scenarios.

Media Handling and NAT Traversal. Media anchoring is avoided unless required for interoperability, security, or NAT traversal. When anchoring is necessary, the BCF supports ICE, STUN, and TURN mechanisms to ensure reliable media establishment across firewalls and NAT boundaries while preserving call quality. Where safe and appropriate, direct media paths are permitted to minimize latency and processing overhead.

Operational Visibility, Logging, and State Reporting. The BCF supports ElementState and ServiceState SUBSCRIBE and NOTIFY interfaces as defined in NENA-STA-010.3, enabling

real-time visibility into functional health and service availability. Signaling and media logging capabilities consistent with NENA guidance are supported and can be selectively enabled for diagnostics or troubleshooting and disabled during normal operations. Logs are exported in standard formats to centralized monitoring and logging platforms to support observability, incident response, and forensic analysis.

Architecture Governance and Documentation. Lumen's documentation identifies the placement of BCF clusters at ESInet ingress locations for all OSP and ESInet-to-ESInet connections and, where applicable, at PSAP egress points. Documentation describes how BCFs are implemented using commercial SBC and firewall platforms with NG911-specific capabilities, how inbound calls are processed and secured, how Bad Actor and Call Suspicion mechanisms are applied, how media handling decisions are made, and how logging and state reporting integrate with Nebraska's monitoring and management processes.

Implementation and Documentation. Lumen's documentation will describe the placement of BCF clusters at ESInet ingress points for all OSP and ESInet-to-ESInet connections, and where applicable at PSAP egress, and detail how we implement:

- Conformance with NENA-STA-010.3 using commercial SBC/firewall platforms with NG911-specific functions.
- Handling of all inbound calls from OSPs and interconnected ESInets, and optional egress BCF functions for PSAP-facing traffic.
- Bad Actor and Call Suspicion mechanisms, default acceptance of calls unless blocklisted, and DDoS/TDoS protection up to Terabit-scale attacks.
- B2BUA operation for calls that do not support REFER, with routing policies that avoid tromboning.
- Minimal media anchoring with ICE/STUN/TURN support when anchoring is necessary.
- Media and signaling logging that can be enabled/disabled quickly for diagnostics.
- ElementState and ServiceState SUBSCRIBE/NOTIFY support for integration with Nebraska's monitoring and management processes.

Secure, High-Availability Boundary Protection. Operated as part of Lumen's geographically diverse, highly available ESInet architecture, the BCF provides a secure and standards-based boundary layer that protects the ESInet from external threats, preserves interoperability with OSPs and peer ESInets, and supports reliable NG911 call handling without introducing unnecessary routing or processing complexity.

This BCF design provides Nebraska with a secure, standards based boundary layer that protects the ESInet from external threats, preserves interoperability with OSPs and peer ESInets, and supports highly available NG911 call handling without introducing unnecessary processing or routing complexity.

5.2.1.2. STIR/SHAKEN SUPPORT

The State requires that incoming calls be validated, and the attestation results be supplied to PSAPs as specified in NENA-STA-010.3. Additionally, calls placed through the OCIF must be signed and receive A-level attestation when validated by the terminating service provider.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Validation of incoming calls with attestation to PSAPs per NENA-STA-010.3.*
- *Signing OCIF calls for A-level attestation.*
- *Explanation of STIR/SHAKEN implementation/conformance.*

LUMEN RESPONSE:

Lumen implements call identity validation and attestation handling for the Nebraska ESInet in accordance with NENA-STA-010.3, ensuring that trusted caller identity information is conveyed to PSAPs as part of NG911 call delivery. The solution integrates STIR/SHAKEN processing at ESInet ingress and for outbound calls placed through the Outgoing Call Interface Function (OCIF), supporting authenticated identity while preserving uninterrupted emergency call handling.

- **Validation Of Incoming Calls And Attestation Delivery To PSAPs.** Incoming calls are evaluated using STIR/SHAKEN mechanisms consistent with NENA-STA-010.3. When calls arrive with identity headers and attestation information provided by Originating Service Providers, the attestation level (A, B, or C) is preserved and conveyed through SIP signaling toward the PSAP, enabling call takers and downstream systems to receive authoritative attestation results without altering call flow or availability.
- **Signing Of OCIF-Originated Calls.** Calls placed through the Outgoing Call Interface Function, including callbacks, transfers, and conference scenarios, are signed to enable full attestation when validated by terminating service providers and supported by interconnecting networks. Signing is performed using certificate-based credentials and secure key handling consistent with STIR/SHAKEN requirements, allowing trusted caller identity to be asserted for OCIF-originated traffic.
- **Standards-Aligned STIR/SHAKEN Implementation.** The STIR/SHAKEN implementation aligns with the NENA i3 architecture and supports the handling of PASSporT information, attestation indicators, and secure identity headers across the ESInet. Attestation data is interoperable with OSP-provided STIR/SHAKEN services and is preserved end-to-end to the PSAP, operating in conjunction with other NG911 security controls such as TLS, certificate-based authentication, and policy enforcement.
- **Documentation And Transparency Of Identity Handling.** Documentation describes how call verification results are determined at ESInet ingress, how attestation information is included in SIP signaling toward the PSAP, and how failed or unverifiable signatures are handled in accordance with standards. This documentation provides the State with visibility into identity validation behavior while maintaining consistent and predictable call delivery. Today, the NGCS solution passes on attestation, but does not sign them.

Our approach enables Nebraska PSAPs to receive validated caller identity information for both inbound and outbound NG911 calls, enhancing trust and situational awareness while maintaining standards-based interoperability and uninterrupted emergency service delivery.

5.2.1.3. SECURITY MECHANISMS

Until the PCA exists, the Contractor shall provide a Certificate Authority with a certificate traceable to a Certificate Authority trusted in mainstream browsers. All NGCS components must conform to NENA-STA-010.3 and NENA-STA-040.2 security requirements:

- *All transactions across the ESInet (including local area network connections at NGCS sites) shall be encrypted as required in NENA-STA-010.3.*

- Every entity must have credentials traceable to the PSAP Certificate Authority (PCA) as trusted root
- All TCP transactions must use TLS with mutual authentication
- Minimum cipher suite as specified in NENA-STA-010.3, with TLS 1.3 support required
- Server Name Indication support required in all systems
- All SIP "hops" within the ESInet must use TLS with mutual authentication
- Data access must conform to owner's Data Rights Management policy
- Single Sign On (SSO) mechanism with SAML authorization required
- No sharing of credentials permitted
- Public-facing connections require additional protection against security attacks
- JWS signatures required for policies and log events
- SIP transactions from OSPs at the BCF shall have appropriately strong minimum cipher suite.
- The Contractor shall notify the State if an OSP cannot support a cipher suite minimally acceptable to the Contractor.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 security with PCA-traceable credentials as trusted root.
- Mutual TLS for TCP transactions with minimum cipher suite and TLS 1.3 support.
- Server Name Indication support; TLS with mutual authentication for SIP hops in ESInet.
- Data access per owner's DRM policy.
- SSO with SAML authorization; no credential sharing.
- Additional protection for public-facing connections.
- JWS signatures for policies/log events.
- Descriptions of PCA implementation/traceability, TLS mutual authentication, cipher suite compliance, TLS
- 1.3 support, Server Name Indication, and SIP hop security.

LUMEN RESPONSE:

Lumen provides a Nebraska-specific certificate and encryption approach aligned with the NENA ESInet trust and security model to support authenticated identities, protected communications, and policy-based access control for ESInet and NGCS functions. Until a State-designated PSAP Certificate Authority is established, Lumen operates an interim Certificate Authority hierarchy using certificates traceable to a publicly trusted root. This approach supports secure NG911 operations from day one while enabling a controlled transition to PCA-anchored trust without service disruption when available.

All ESInet core elements remain in a Lumen/Intrado managed trusted secure zone. Since the elements, transactions and data all reside within this trusted zone, and due to the time-sensitive nature of possible production troubleshooting efforts, we have designed a secure solution which allows immediately available, real time viewable actionable data.

Certificate Authority Hierarchy and Credential Management. All ESInet and NGCS entities are provisioned with credentials using standard certificate chaining practices and widely trusted root anchors. When a Nebraska PCA is introduced, credentials and validation

workflows are migrated to align with the PCA trust chain while maintaining continuity of operations. Certificate issuance, validation, and lifecycle management follow disciplined governance to preserve trust at all NG911 boundaries.

Encryption, Mutual Authentication, and TLS Profiles. ESInet and NGCS communications are protected using encryption and mutual authentication consistent with NENA-STA-010.3 and NENA-STA-040.2. All applicable TCP-based transactions support TLS 1.3 with enforced cipher suites aligned to NENA security expectations. Where peer interoperability constraints prevent use of minimum profiles, Lumen notifies the State and coordinates a remediation approach that preserves Nebraska's security posture while ensuring uninterrupted service delivery. All SIP hops are secured using TLS with mutual authentication.

Server Name Indication and Multi-Service Hosting. Server Name Indication (SNI) is supported where applicable to enable secure hosting of multiple services on shared interfaces. SNI ensures correct certificate selection and policy application for each service while maintaining consistent enforcement of security controls.

Identity, SSO, and Role-Based Data Access. Access to NGCS and ESInet data is enforced using least-privilege principles aligned to the data owner's Data Rights Management policy. The solution supports per-user identities and Single Sign-On using SAML-based authorization. Credentials are uniquely assigned to individual users and system entities and are not shared, ensuring accountability and controlled access across operational and administrative interfaces.

Protection of Public-Facing Interfaces. Public-facing connections, including Originating Service Provider interconnects and administrative access points, are protected through layered security controls. These include network segmentation, inspection and filtering, rate limiting where appropriate, strong authentication, and boundary enforcement. These measures reduce exposure to external threats while preserving required interoperability for NG911 operations.

Integrity Controls for Policies and Security-Relevant Records. Security-relevant policies and records are protected using integrity mechanisms, including digital signatures applied through JSON Web Signature processes. Certificate validation behavior at trust boundaries is documented, including handling of failed or unverifiable validations in accordance with standards and operational requirements. These controls ensure authenticity, integrity, and non-repudiation of policy artifacts and security-related events.

Standards Compliance and Operational Assurance. Lumen's NG911 solution fully complies with the State's Security Mechanisms requirements and conforms to NENA-STA-010.3 and NENA-STA-040.2. All NGCS components operate within a secure, standards-based architecture that enforces encryption for ESInet transactions, mutual authentication for SIP and TCP communications, strong cipher enforcement with TLS 1.3 support, disciplined certificate management, role-based access control, SAML-based SSO, and comprehensive protections for public-facing interfaces. This approach ensures confidentiality, integrity, and trust across Nebraska's NG911 ecosystem.

5.2.2. Core Routing and Location

5.2.2.1. EMERGENCY SERVICES ROUTING PROXY (ESRP)

The ESRP must conform to NENA-STA-010.3 standards and function as both originating and terminating ESRP. It shall be possible for a region or group of PSAPs to provide a terminating ESRP to which the State's ESRP must route calls to as appropriate.

The proposed solution must utilize the PRF functionality to support the ability to dynamically change the primary, alternate, and contingent routes available by the ESRP. The ESRP shall retrieve rule sets from a Policy Store using the NENA-STA-010.3 proscribed Policy Store web service. The ESRP must be capable of being provisioned to use any Policy Store conforming to NENA-STA-010.3. The ESRP shall implement the test call condition modifications described in NENA-STA-010.3 to enable automated testing of policy routing rules.

All calls must be location-routed with no ALI/MSAG-based routing. Requirements include:

- *The ESRP shall be able to query any Location Information Servers using either HELD or SIP Presence.*
- *The ESRP shall support the QueueState and DequeueRegistration mechanisms for all queues it operates. It must support QueueState clients for queues for all PSAPs in the State.*
- *Policy Routing Rule function (PRF) supporting all NENA-STA-010.3 conditions and actions*
- *Policy retrieval from a Policy Store with dynamic updates (within 10 seconds)*
- *Handling at least 100 calls per second*
- *Support for admin calls*
- *Ability to query any compliant ECRF and Location Information Servers*
- *Support for call routing and EIDOs for any responder agency*
- *Implementation of overload and diversion mechanisms*
- *Additional Data mechanisms for routing based on call data*
- *ElementState and ServiceState support*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Conformance to NENA-STA-010.3 as originating/terminating ESRP.*
- *Location-based routing only (no ALI/MSAG).*
- *PRF supporting all conditions/actions.*
- *Policy retrieval from Policy Store with <10s updates.*
- *Handling 100 calls/second.*
- *Admin call support.*
- *Querying compliant ECRF/LIS.*
- *Routing/EIDOs for responder agencies.*
- *Overload/diversion mechanisms.*
- *Additional Data routing; and ElementState/ServiceState support.*

LUMEN RESPONSE:

Lumen provides an Emergency Services Routing Proxy (ESRP) solution for Nebraska that conforms to NENA-STA-010.3 and operates as both an originating and terminating ESRP within the NG911 architecture. The design supports a State-level ESRP and enables regions or groups of PSAPs to deploy their own terminating ESRP instances. Routing policies determine when calls are delivered directly to PSAPs or routed to regional ESRPs based on operational, geographic, or policy conditions, supporting a scalable and federated NG911 deployment model.

Location-Based Routing Without ALI or MSAG Dependency. All call routing decisions are made using real-time, GIS-based location information obtained from compliant Location Information Servers and Emergency Call Routing Functions. The ESRP does not rely on legacy ALI or MSAG-based routing for i3-capable originating service providers. PIDF-LO location objects are used for routing determinations, supporting accurate and future-ready NG911 operations. Where transitional support is required, an interim location database managed by Lumen supports routing and PIDF-LO generation until full i3 location delivery is available.

Policy Routing Function Integration. The ESRP implements the full Policy Routing Function as defined in NENA-STA-010.3. Routing policies are retrieved from a standards-compliant Policy Store using the defined web service interface and are applied dynamically without requiring changes to underlying call-handling systems. Policy updates are consumed within seconds of being applied, enabling near real-time changes to routing behavior. Test call conditions specified by the standard are supported, allowing routing logic to be exercised and validated without impacting live emergency traffic.

Routing Conditions and Decision Inputs. The PRF supports dynamic routing decisions based on multiple inputs, including location and jurisdictional boundaries, call and service type, PSAP and queue operational status, ElementState and ServiceState, test call indicators, and call-associated attributes. This capability enables primary, alternate, overflow, and contingent routing strategies that can be modified without service disruption.

Call Capacity, Performance, and Scalability. The ESRP is designed to support high call throughput per instance, including both emergency and administrative calls, with identical policy and routing logic applied to each. The architecture supports a minimum of 100 calls per second per instance and scales horizontally to accommodate higher sustained or burst volumes. High availability and resiliency are maintained during peak demand, major incidents, or disaster scenarios.

Queue Management and PSAP Visibility. QueueState and DequeueRegistration mechanisms are supported for all queues operated by the ESRP. QueueState visibility is available for queues associated with PSAPs statewide, enabling routing decisions to account for real-time PSAP capacity and readiness. This supports informed overflow, diversion, and load-balancing strategies.

Overload Handling and Continuity of Operations. Overload and diversion mechanisms are implemented consistent with NENA i3 standards. When a PSAP or regional ESRP experiences congestion, degradation, or outage conditions, calls are automatically rerouted to alternate destinations in accordance with PRF rules. Contingent routing paths ensure continuity of operations during partial or full service impairments.

Additional Data and Incident-Aware Routing. The ESRP supports routing decisions that incorporate Additional Data associated with a call, including Emergency Incident Data Objects. This enables routing behavior to consider incident-specific information in addition to location and policy criteria, supporting specialized handling scenarios and coordinated response.

ECRF, LIS, and Responder Interoperability. The ESRP can query any compliant ECRF and LIS using standards-based interfaces, including HELD and SIP presence. Routing decisions support delivery of calls and associated data to responder agencies and PSAPs across disciplines, ensuring interoperability within Nebraska's NG911 ecosystem.

Service State Visibility and Monitoring. The ESRP exposes ElementState and ServiceState interfaces so management systems and State stakeholders can monitor component health and service availability. Routing clients can respond dynamically to state changes to preserve the 99.999% availability objective for Nebraska's NGCS.

Compliance and Operational Assurance. Collectively, these capabilities confirm full compliance with the State's ESRP functional, performance, and standards conformance requirements. The ESRP operates as a resilient, location-driven, policy-controlled routing engine that supports statewide and regional routing models, automated testing, overload handling, and uninterrupted NG911 operations aligned with NENA-STA-010.3.

5.2.2.1.1. Policy Store

The State requires a Policy Store conforming to NENA-STA-010.3. The Policy Store must be capable of being the sole source of policies for the NGCS.

- The State **desires a flexible policy editor** that can create and modify policies conforming to NENA-STA-010.3 with an easy-to-use Graphical User Interface.
- The Policy Store **must have the capacity to support policies for all PSAPs and all elements in the NGCS** at the peak call rates specified in this RFS.
- Storage and retrieval of policies must be limited by the NENA-STA-010.3 Data Rights Management mechanism.
- The Policy Store must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy Store per NENA-STA-010.3 as sole policy source.
- Flexible GUI policy editor.
- Capacity for all PSAPs/elements at peak rates.
- DRM-limited storage/retrieval.
- ElementState/ServiceState support with State subscription.
- Detailed Policy Store description.

LUMEN RESPONSE:

Lumen provides a Policy Store for Nebraska that conforms to NENA-STA-010.3 and serves as the single authoritative source of routing and treatment policies for all NGCS functional elements. The Policy Store exposes the standard i3 web service interface and supports the full NENA policy schema, enabling ESRP, PRF, ECRF, LVF, LIS, and other policy-driven

components to retrieve policies from a centralized, consistent repository. Our Policy Store solution provides the State:

- **Centralized Policy Management and Distribution.** Policy storage, retrieval, and distribution are centralized to ensure consistent evaluation and enforcement across the ESInet and NGCS. Policies are delivered in real time using standards-based interfaces so routing and treatment decisions remain synchronized statewide, without divergence between PSAPs, regions, or functional elements.
- **Graphical Policy Editing and Governance Controls.** The solution includes a browser-based graphical policy editor that enables authorized State personnel to create, view, and modify policies in NENA-STA-010.3 format. The editor supports standard policy constructs, conditional logic, and actions defined by the specification. Controlled workflows, versioning, and validation are applied to reduce configuration errors and preserve policy integrity across statewide deployments.
- **Capacity, Performance, and Scalability.** The Policy Store is architected to support policies for all PSAPs and NGCS elements at the peak call and query rates defined by the RFP. Scalable and redundant deployment models ensure policy retrieval latency and throughput remain within required bounds during steady-state operations, major incidents, and high-demand scenarios, without introducing delays into call routing or processing.
- **Data Rights Management and Access Control.** Policy access is governed using the Data Rights Management mechanisms defined in NENA-STA-010.3. Viewing, modification, and distribution of policies are restricted based on ownership, role, and authorization, enforcing least-privilege access and protecting against unauthorized policy use or modification.
- **Operational State Visibility and Monitoring.** The Policy Store supports ElementState and ServiceState SUBSCRIBE and NOTIFY interfaces in accordance with NENA-STA-010.3. The State may subscribe to receive standardized state change notifications, enabling real-time visibility into policy service availability and early detection of conditions that could affect routing behavior.
- **Highly Available NGCS Integration.** The Policy Store is deployed as part of Lumen's highly available NGCS architecture and is monitored continuously for availability, performance, and integrity. Policy updates are applied dynamically and consumed by NGCS elements without service disruption, and the architecture supports future evolution as NENA standards and State requirements mature.
- **Compliance and Operational Outcome.** Collectively, these capabilities ensure full compliance with the State's Policy Store requirements. Nebraska benefits from centralized, standards-aligned policy governance; rapid and consistent policy enforcement; controlled access; real-time visibility into policy service health; and a scalable foundation that supports uninterrupted NG911 operations across the ESInet.

5.2.2.2. LOCATION INFORMATION SERVER (LIS)

The State utilizes a Location Information Server (LIS) provided by the existing service provider. Respondents must provide a description of their LIS solution in conformance with NENA-STA-010.3.

- *The LIS must supply location in the form of a PIDF-LO (location by value) or a location URI (location by reference).*

- The LIS must also provide a dereference service for a location URI it supplies given the URI, the LIS provides the location value as a PIDF-LO.
- A LIS may be a database, or may be a protocol interworking function to an access network-specific protocol.
- If the LIS supply's location by reference, it must also provide dereferencing service for that location URI.
- Elements in the ESInet, including the ESRP, and the PSAP may dereference a location URI as part of processing a call.
- The LIS must support HELD, HELD Dereferencing and/or SIP Presence Event Package.
- The SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing, especially when tracking of the caller is needed. However, HELD is acceptable on any location URI.
- The LIS must support location filters and event rate control.

The LIS may support SIP Presence to provide location-by-reference as defined by RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package at the location URI provided containing a PIDF (Presence Information Data Format) document that will include the location in the Location Object (LO) part, forming the PIDF-LO.

- The LIS may validate locations prior to entering them into the LIS using the LVF.
- The LIS may support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes¹.
- The LIS must accept credentials traceable to the PCA for authenticating queries for a location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely on any other credential source to authorize location dereferencing.
- Storage and Retrieval of location data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism

When location is provided by reference there is a need for the reference to be valid, at least for the length of the call. Since the call may be transferred to a transfer-to PSAP for handling, the transfer-to PSAP must have the ability to dereference the location reference provided with the call. It is therefore critical that the location URI does not expire before the transfer-to PSAP has the opportunity to dereference it.

Any LIS that provides a dereferencing service for a location must provide an expiration time associated with that URI set at a minimum of 30 minutes, with a maximum of 24 hours.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LIS per NENA-STA-010.3 providing PIDF-LO or location URI with dereference service.
- As database or protocol interworking.
- HELD/dereferencing/SIP Presence support.
- Location filters/event rate control.
- SIP Presence for location-by-reference per RFC.
- Validation via LVF; support for planned changes draft.
- PCA-traceable credentials for dereferencing.

- *DRM-controlled storage/retrieval; and minimum 30-min/max 24-hour URI expiration.*

LUMEN RESPONSE:

Lumen provides a Location Information Server (LIS) solution for Nebraska that conforms to NENA-STA-010.3 and supports both location-by-value and location-by-reference delivery models. The LIS returns location as PIDF-LO when location by value is requested and issues a location URI when location by reference is requested, with a standards-based dereferencing service that returns the associated PIDF-LO to authorized entities. The LIS is implemented as a logical service backed by a location database and, where required, protocol interworking functions to access network-specific location sources.

Standards-Based Location Acquisition And Dereferencing. We support HELD for location acquisition, HELD dereferencing for retrieving location values from valid location URIs, and SIP Presence event packages where subscription-based location updates are required. ESInet elements, including the ESRP and PSAP systems, can obtain current location and, when appropriate, receive refreshed PIDF-LO documents through standards-compliant mechanisms.

Location By Reference Management And Update Controls. When location by reference is used, SIP Presence subscriptions may be employed to receive updated location information, including changes in caller position. Location filters and event-rate controls are supported to manage update frequency and scope, allowing continuous tracking where required while limiting unnecessary signaling or processing load.

Location URI Lifetime And Transfer Support. Location URIs issued by the LIS are configured with expiration times that are never shorter than 30 minutes and never longer than 24 hours. This ensures that location by reference remains usable for the full life of a call and any subsequent transfers, and that PSAPs receiving transferred calls retain the ability to dereference any still-valid URI.

Validation And Planned Change Support. Location information may be validated against the Location Validation Function (LVF) prior to storage or update. Support is provided for validation workflows associated with planned changes to service boundaries, consistent with the intent of emerging NENA guidance referenced by the State, to help preserve location accuracy during scheduled updates or transitions.

Security, DRM, And PCA-Based Authorization. Storage and retrieval of location data are governed by the Data Rights Management mechanisms defined in NENA-STA-010.3, ensuring access is limited to authorized roles and use cases. Dereference requests are authenticated using credentials that chain to the PSAP Certificate Authority trust root, enabling any PSAP that legitimately receives a call to dereference the associated location URI without reliance on alternative credential authorities.

5.2.3. Location Database (LDB)

The State requires a Location Database (LDB) solution as a core component of the Emergency Services IP Network (ESInet). Respondents must provide a detailed description of their LDB solution that is conformant with NENA standards, primarily the NENA Next Generation 911 GIS Data Model (NENA-STA-005.2). The LDB serves as the authoritative geospatial database for the Location Validation Function (LVF) and the Emergency Call Routing Function (ECRF).

- The LDB must store and manage all mandatory and conditional geospatial data layers as specified in NENA-STA-005.2, including but not limited to:
 - Public Safety Answering Point (PSAP) Boundaries
 - Emergency Service Boundaries (Law, Fire, EMS)
 - Road Centerlines
 - Site / Structure Address Points
- The LDB must interface directly with the LVF to enable validation of civic location information against the authoritative GIS data contained within it.
- The LDB must interface with the ECRF to provide the necessary geospatial data for determining the appropriate PSAP and emergency service agencies for a given dispatchable location. This location-to-service mapping **MUST** utilize a standard protocol, such as the Location-to-Service Translation (LoST) protocol.
- The solution must provide a secure and robust mechanism for the provisioning, aggregation, and ongoing maintenance of GIS data from various authoritative local sources (e.g., county, and municipal GIS departments). This includes tools for data normalization, quality control, and discrepancy resolution.
- The LDB must be architected for high availability and geographic redundancy to ensure uninterrupted location validation and call routing services. The system must meet stringent performance requirements for real-time query processing during emergency call handling.
- The LDB must control access for data provisioning and system queries through secure authentication and authorization mechanisms, protecting data from unauthorized access, modification, or deletion.
- Storage, management, and retrieval of location data **MUST** be controlled by policies consistent with NENA data security and privacy standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LDB conformance with the NENA-STA-005.2 GIS Data Model.
- Standard-based interfaces with the LVF and ECRF (e.g., LoST).
- Support for all required NENA GIS data layers and their lifecycle management.
- A detailed process for GIS data provisioning, aggregation, updates, and quality control.
- Description of the high-availability and redundant architecture.
- Mechanisms for secure access control for both data management and system queries.
- Tools and processes for managing data quality and resolving discrepancies from multiple sources.

LUMEN RESPONSE:

Lumen provides a Location Database (LDB) solution for Nebraska that conforms to NENA-STA-005.2 and the NENA Next Generation 911 GIS Data Model. The LDB serves as the authoritative geospatial repository supporting both the Location Validation Function and the Emergency Call Routing Function, ensuring that validation and routing decisions use current, authoritative GIS data statewide.

Comprehensive GIS Data Layer Support. The LDB stores and manages all mandatory and conditional GIS data layers required by the NENA model, including PSAP boundaries; law,

fire, and EMS service boundaries; road centerlines; and site or structure address points. Lifecycle management of these layers ensures accuracy, currency, and consistency as data evolves.

Standards-Based Interfaces for LVF and ECRF. The LDB exposes standards-based interfaces to both the LVF and ECRF using LoST or equivalent NENA-compliant protocols. Civic locations are validated by the LVF against the authoritative GIS dataset, and the same data is used by the ECRF to resolve dispatchable locations to the correct PSAP and responder agencies, ensuring consistent outcomes across NGCS components.

GIS Data Provisioning, Quality Control, and Stewardship. Lumen supports a structured process for GIS data provisioning, aggregation, update, and quality control. Authoritative local sources, including county and municipal GIS organizations, submit data into controlled staging environments where normalization, schema validation, topology checks, and attribute consistency reviews are performed. Tools and workflows identify overlaps, gaps, boundary conflicts, and attribute discrepancies before data is promoted to production, allowing corrections without impacting live routing or validation.

Statewide Aggregation with Local Data Ownership. Aggregation logic reconciles multiple authoritative sources into a unified statewide Location Database while preserving local ownership and stewardship responsibilities. This approach supports consistent statewide NG911 operations while respecting jurisdictional control over source data maintenance.

High Availability and Geographic Redundancy. The LDB is deployed in a geographically redundant, highly available architecture aligned with ESInet and NGCS data center locations. Replicated data stores and redundant application instances ensure that LVF and ECRF queries meet real-time performance requirements during normal operations, maintenance activities, or degraded conditions, without introducing single points of failure.

Secure Access Control, Privacy, and Auditability. Access to the LDB is protected using secure authentication and authorization mechanisms consistent with NENA security and privacy expectations. Role-based access control separates data provisioning, quality assurance, and operational query functions, ensuring only authorized users can modify GIS features while NGCS components are granted read access as required for call handling. All data access and changes are auditable.

Discrepancy Management and Ongoing Data Quality. The solution includes defined processes and tooling to identify, track, and resolve data quality issues across multiple authoritative sources. Discrepancy management workflows support review and correction prior to affecting LVF or ECRF operations, maintaining accurate and reliable location-based routing across Nebraska's NG911 environment.

Compliance and Operational Outcome. Collectively, these capabilities ensure full compliance with the State's Location Database requirements and applicable NENA standards. Nebraska benefits from a secure, highly available, and authoritative geospatial foundation that supports accurate location validation, dependable emergency call routing, and long-term NG911 sustainability across the statewide ESInet.

5.2.4. Emergency Call Routing Function / Location Validation Function (ECRF/LVF)

The implementation requires two independent, redundant ECRFs and LVFs (one inside, one outside the ESInet) with identical data. The ECRF/LVF must support the extensions to

LoST defined in NENA-STA-010.3 and the similar-location and planned-changes extensions defined in draft-ietf-ecrit-similar-location² and draft-ietf-ecrit-lost-planned-changes³ (or RFCs issued based on those drafts).

Query Capability:

The external ECRF/LVF must be queryable from the public internet and by any i3 OSP, supporting both iterative and recursive queries.

Responder Types:

The system must handle up to 20 responder types and various service URNs as specified.

Data Synchronization:

Both the internal ECRF and LVF must achieve 99.999% availability, while the external ECRF must meet the same 99.999% availability SLA, and the external LVF must maintain 99.9% availability.

Performance Metrics:

The internal ECRF/LVF must handle 500 queries per second effectively, ensuring that combined services meet the specified thresholds for external queries.

Key requirements:

- External ECRF/LVF accessible from the public Internet and i3 OSPs
- Support for iterative and recursive queries
- Support for up to 20 responder and all service URNs
- LoST sync interface to National Forest Guide and interconnected ESInets
- The ECRFs and LVFs must be capable of being provisioned from an SI conforming to NENA-STA 010.3.
- Routing/validation must change within eight (8) seconds of an update via the SI.
- The internal ECRF/LVF shall be capable of handling 100 queries per second for any valid Location Information shape as specified in OGC 06-142r1.
- The external ECRF/LVF shall be capable of handling an aggregate of 5000 queries per second with any mix of civic or geo points.
- The external ECRF/LVF shall be capable of handling an aggregate 500 queries per second.
- The external ECRF/LVF shall limit transactions from the same querier to, at most, 10 per second and fewer, if it is under a sustained excessive load. If the ECRF and LVFs are combined, the combination must meet the 5000/500 rate (not twice the rate of a single service).
- 99.999% availability for internal ECRF/LVF and external ECRF
- 99.9% availability for external LVF
- Support for Spatial Interface (SI) with routing/validation updates within seconds
- Capacity to handle specified query volumes
- ElementState and ServiceState support

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Two independents are redundant ECRFs/LVFs (internal/external) with identical data.
- External queryable from public Internet/i3 OSPs with iterative/recursive support.

- *Handling up to 20 responder /service URNs; LoST sync to National Forest Guide/interconnected ESInets.*
- *99.999% availability for internal/external ECRF and internal LVF, 99.9% for external LVF.*
- *SI support with seconds-level updates.*
- *Capacity for 500 queries/second internal; and ElementState/ServiceState support.*

LUMEN RESPONSE:

Lumen provides independent, redundant Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) capabilities for Nebraska that conform to NENA-STA-010.3 and operate on identical authoritative datasets sourced from the Location Database. Internal ECRF/LVF services support ESInet and NGCS traffic, while external ECRF/LVF services are accessible to i3 Originating Service Providers and other authorized external systems. Both environments are synchronized to ensure consistent routing and validation outcomes regardless of query origin.

Identical Data Sets and High Availability Design. Internal and external ECRF/LVF environments are maintained on the same authoritative data and updated through synchronized provisioning workflows. Each environment is deployed with geographic redundancy and fault isolation to preserve continuity of service during maintenance events or unplanned disruptions, eliminating single points of failure.

Standards-Based Query Support and Interjurisdictional Coordination. The ECRF/LVF supports both iterative and recursive Location-to-Service Translation queries in accordance with NENA-STA-010.3. Support includes responder types and service URNs as defined by NENA standards. LoST synchronization interfaces are implemented to support coordination with the National Forest Guide and with interconnected ESInets as required for interjurisdictional routing.

Spatial Interface Provisioning and Rapid Update Propagation. Authoritative GIS and routing updates are provisioned through a Spatial Interface conformant with NENA-STA-010.3. Updates propagate to both internal and external ECRF/LVF services within seconds, and in all cases within the required eight-second threshold, ensuring routing and validation behavior aligns rapidly with authoritative data changes.

Performance, Capacity, and Rate Control. The internal ECRF/LVF is engineered to support high-volume NG911 routing and validation workloads, including at least 100 queries per second for any valid location shape and an aggregate of 500 queries per second across combined internal services. External ECRF/LVF services support aggregate query volumes of up to 5,000 queries per second across civic and geodetic inputs. Per-querier rate limits and adaptive load protections are enforced to maintain system stability and prevent external query activity from affecting NG911 call handling.

Availability Objectives and Operational State Visibility. Internal ECRF and LVF services are designed to meet 99.999% availability, while external LVF services meet 99.9% availability targets. The architecture includes geographic redundancy, continuous monitoring, and automated failover. ElementState and ServiceState SUBSCRIBE and NOTIFY interfaces are exposed in accordance with NENA-STA-010.3, enabling the State to monitor service health, availability, and operational status in real time.

Compliance and Operational Outcome. Collectively, these capabilities fully satisfy the State's ECRF and LVF requirements. Nebraska benefits from standards-based, highly available, and scalable location validation and routing services that deliver consistent results to internal NGCS functions, i3 Originating Service Providers, and authorized external systems while protecting NG911 operations under all load and failure conditions.

5.2.5. Forest Guide

The NGCS must handle calls transferred between interconnected ESInets, maintaining Forest Guide entries for the State's ECRF and LVF, and support recursive queries for locations outside the state's service area.

If a National Forest Guide is available, the contractor must ensure the State's ECRF and LVF entries are entered promptly.

Fallback Procedures:

In scenarios where queries fall outside the State's service area, the ECRF/LVF must initiate recursive queries to the Forest Guide.

Commercial Relationships:

Frequent and excessive queries from the same entity may not be accommodated unless a reasonable commercial relationship exists.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Handling transfers between ESInets with Forest Guide entries for State's ECRF/LVF.*
- *Recursive queries for out-of-area locations.*
- *Prompt entry into National Forest Guide if available.*
- *Fallback recursive queries to Forest Guide for non-State areas.*
- *Limitations on excessive queries without commercial relationships.*

LUMEN RESPONSE:

Lumen ensures that NGCS supports call transfers between interconnected ESInets and that Nebraska's routing and validation services are discoverable by external systems through appropriate Forest Guide entries. The ECRF and LVF maintain entries that allow out-of-state systems and interconnected ESInets to locate Nebraska's authoritative services, and where a national Forest Guide is available, those entries are registered and kept current so cross-jurisdictional queries resolve accurately. To address these requirements, the following capabilities are implemented and documented:

- **Handling Transfers Between ESInets Using Forest Guide Entries.** We support standards-based call transfers between interconnected ESInets, with Nebraska's ECRF and LVF represented through Forest Guide entries so external networks can discover the correct authoritative routing and validation services. This ensures continuity of routing and validation when calls traverse ESInet boundaries.
- **Recursive Queries For Locations Outside Nebraska.** When a query references a location outside Nebraska's service area, recursive queries are initiated to the Forest Guide to identify the appropriate authoritative routing or validation source. This approach supports calls involving out-of-state callers or transfers spanning multiple jurisdictions without requiring prior knowledge of external service boundaries.

- **Publication And Maintenance Of National Forest Guide Entries.** If a national Forest Guide is available, we support timely publication and ongoing maintenance of Nebraska's ECRF and LVF entries. Updates are coordinated as part of ESInet operations so external ESInets and i3-compliant OSPs can reliably locate Nebraska's services.
- **Fallback Routing And Validation Via The Forest Guide.** When a location cannot be resolved within Nebraska's ESInet, fallback recursive queries to the Forest Guide are supported to obtain authoritative routing or validation results. This ensures continued call handling and validation during inter-ESInet transfers or cross-jurisdictional incidents.
- **Controls On Excessive External Queries.** Query handling policies include rate controls to manage excessive or sustained query activity from external entities. Higher volumes are supported where a commercial or operational relationship exists, while limits are applied to protect system performance and availability and prevent misuse of Nebraska's external ECRF and LVF.

These capabilities ensure that Nebraska's NGCS remains interoperable with peer ESInets and external systems, while preserving routing accuracy, service continuity, and operational protections consistent with NENA i3 expectations.

5.2.5.1 SERVICE/AGENCY LOCATOR (SAL)

The State requires a Service/Agency Locator function as described in NENA-STA-010.3.

- *The S/AL must support at least 1000 entries.*
- *The S/AL must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.*
- *The proposal must describe how agency entries are provisioned in the S/AL.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Service/Agency Locator per NENA-STA-010.3 supporting 1000+ entries.*
- *ElementState/ServiceState support with State subscription.*
- *Descriptions of agency entry provisioning and detailed S/AL.*

LUMEN RESPONSE:

Lumen provides a Service and Agency Locator (S/AL) solution for Nebraska that conforms to NENA-STA-010.3 and supports statewide scale for agency and service lookup during NG911 call processing. The S/AL functions as the authoritative directory for NGCS routing and operational logic, maintaining accurate agency metadata and enabling consistent service selection across PSAPs and emergency service organizations. Our solution offers the State of Nebraska:

- **Standards-Based Service and Agency Locator at Statewide Scale.** The S/AL is engineered to manage more than one thousand agency and service entries, providing statewide coverage across PSAPs, law enforcement, fire, EMS, and supporting organizations. NGCS functional elements query the S/AL during call handling to obtain reliable and authoritative agency information without divergence across the NG911 environment.
- **Authoritative Agency Metadata Repository.** The S/AL maintains structured agency data including agency identifiers, supported service types, contact URLs, and operational state

attributes. This information is used by NGCS routing, treatment, and operational logic to ensure accurate and policy-aligned call delivery.

- **ElementState and ServiceState Visibility.** The S/AL supports ElementState and ServiceState SUBSCRIBE and NOTIFY interfaces in accordance with NENA-STA-010.3. The State and authorized NGCS components may subscribe to receive near real-time notifications when an agency's availability or operational status changes, allowing routing decisions to reflect current service conditions.
- **Controlled Provisioning and Governance.** Agency and service records are provisioned through controlled administrative workflows that enforce schema validation, role-based authorization, version control, and change tracking. Authorized personnel create, update, and retire entries using GUI- or API-based interfaces designed to preserve data integrity and alignment with State governance requirements.
- **Integration with NGCS Functions.** The S/AL integrates directly with NGCS routing and lookup components so ESRP and policy-driven elements can reference authoritative agency data during call handling, transfers, and contingency routing scenarios.
- **Architecture, Availability, and Operations.** The S/AL is deployed as part of Lumen's highly available NGCS architecture and is continuously monitored to ensure reliability and performance. Updates to agency data follow coordinated change management practices to maintain operational continuity and standards compliance.
- **Documentation and State Visibility.** Lumen provides documentation describing S/AL architecture, data schemas, provisioning workflows, and state notification mechanisms, including how agency data is governed and consumed across the NG911 environment.

These capabilities ensure Nebraska's NGCS has continuous access to accurate, authoritative agency information while providing the State with the visibility, control, scalability, and standards-aligned service and agency lookup required for statewide NG911 operations.

5.2.6. Data and Enrichment

5.2.6.1. ADDITIONAL DATA REPOSITORY (ADR)

The State requires an Additional Data Repository (ADR) database function.

URLs pointing to the ADR may be passed in a call, in an EIDO, or by other mechanisms. The ADR shall return an XML data structure in response to an HTTPS GET of the URI.

The ADR provided by the contractor must:

- *Supply Provider Info and Service Info for all calls handled by the LNG, and any OSP that does not provide its own ADR or AdditionalData by value when it sends a call to the ESInet*
- *Supply any of the valid AdditionalData blocks for any location, where the URI for the AdditionalData blocks would be returned from the ECRF when searched with an urn of "urn:emergency:service:AdditionalData"*

The proposal must detail how ADR records are provisioned into the repository. Storage and retrieval of S/AL records must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.

A call-stateful ADR may limit the length of time that it will serve data after the end of the associated emergency call. Such a time limit shall be at least five minutes. ADRs may not have the data themselves but may know where the data can be found. The response to a

dereference request can be redirected to another ADR with an HTTPS 303 response (Iterative Refer).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- ADR returning XML via HTTPS GET.
- Supplying Provider/Service Info for LNG/OSPs without own ADR.
- Valid Additional Data blocks via ECRF URI.
- Provisioning details.
- DRM-controlled storage/retrieval.
- Minimum 5-minute time limit for call-stateful ADR.
- Redirect capability via HTTPS 303.

LUMEN RESPONSE:

Lumen provides an Additional Data Repository (ADR) that conforms to NENA-STA-010.3 and returns XML data structures in response to HTTPS GET requests for any valid ADR URI conveyed with a call, within an Emergency Incident Data Object (EIDO), or through other NENA-defined mechanisms. The ADR supplies Provider Information and Service Information for calls handled by the LNG and for originating service providers that do not supply their own ADR or AdditionalData by value. The ADR also returns valid AdditionalData blocks associated with a location when the Emergency Call Routing Function (ECRF) provides a URI using the *urn:emergency:service:AdditionalData* service identifier.

Standards-Based Dereferencing And Data Delivery. The ADR supports standards-based dereferencing by returning XML content over HTTPS in response to valid ADR URIs. URIs may be conveyed through call signaling, EIDOs, or other NENA-defined mechanisms, enabling consistent retrieval of supplemental call data by authorized NGCS elements and PSAP systems.

Provider And Service Information Support. Provider Information and Service Information are supplied for LNG-originated calls and for calls from originating service providers that do not provide their own ADR or AdditionalData by value. This ensures consistent availability of supplemental call data for all calls entering the ESInet, regardless of originating network capabilities.

Controlled Provisioning And Lifecycle Management. ADR records are provisioned through controlled workflows that validate content, enforce role-based authorization, and support lifecycle management. These workflows ensure authoritative data is available at call time while preserving data integrity and governance across the NG911 environment.

Data Rights Management And Access Control. Storage and retrieval of ADR data are governed by the Data Rights Management mechanisms defined in NENA-STA-010.3. Access to view, modify, or query ADR records is limited to authorized entities based on ownership and role, protecting sensitive information while enabling necessary data sharing during emergency call handling.

Call-Stateful Data Availability And Redirect Handling. When operating in a call-stateful mode, the ADR serves associated data for a minimum of five (5)-minutes following the end of the related call, with longer availability supported based on configuration. Where requested data is hosted by another ADR, dereference requests may be redirected using an HTTPS 303

response, enabling iterative resolution without exposing internal topology and supporting distributed ADR architectures.

5.2.7. Call Flow and Media Handling

5.2.7.1. CALL FLOW AND SESSION HANDLING REQUIREMENTS

The Contractor shall implement call-flow behaviors consistent with the NENA i3 call model, including processing SIP INVITE requests from access networks into the ESInet, interactions with the ESRP, location queries to LIS, LVF, and ECRF, and routing to the appropriate PSAP through gateways or Call Handling Equipment (CHE). The system must support call queuing, overflow routing, and abandonment handling.

SIP signaling and location:

Headers such as P-Asserted-Identity, Diversion, History-Info, and Geolocation shall be correctly handled, and PIDF-LO location information shall be preserved during retargeting, bridging, and transfers.

Media and additional data:

The system shall handle voice, Real-Time Text (RTT), real-time video, and additional data (for example, messaging and sensor or biometric data from caller applications) per NENA definitions, with SDP negotiation, fallback to voice-only, and transcoding as needed.

Transfers:

Support is required for warm (attended) transfers, blind transfers, and inter-PSAP transfers, preserving all call metadata, location, timestamps, and media sessions without interruption.

Identity and trust:

The system shall enforce SIP identity assertions, correctly process P-Asserted-Identity and related headers, differentiate and display validated versus unvalidated identities at the PSAP, and integrate with STIR/SHAKEN for caller authenticity.

End-to-end conformance:

The ESInet and NGCS shall manage end-to-end call flows in conformance with applicable NENA and IETF standards, including origination, routing, delivery to the appropriate PSAP, transfers, and termination, while ensuring reliable session handling for all supported media.

LUMEN RESPONSE:

Lumen provides NGCS call handling for Nebraska that follows the NENA i3 call model and manages end-to-end SIP call flows from originating access networks, through the ESInet and NGCS, and to the appropriate PSAP via gateways or Call Handling Equipment (CHE). SIP INVITE requests are terminated at the Border Control Function (BCF), normalized, and forwarded to the Emergency Services Routing Proxy (ESRP), which performs policy-based routing using location information obtained from the LIS, LVF, and ECRF.

Standards-Based Call Routing, Queuing, And Overflow Handling. Call routing is performed using location-based policies consistent with NENA i3 behavior, with support for queuing and overflow at the NGCS layer. Calls may be placed into PSAP or regional queues, redirected to alternate destinations when primary targets are impaired or saturated, and

handled appropriately when abandoned. These mechanisms ensure consistent call treatment during congestion, failover conditions, or planned maintenance events.

SIP Signaling And Location Preservation. Required SIP headers and public-safety signaling elements—including P-Asserted-Identity, Diversion, History-Info, and Geolocation—are processed and preserved in accordance with NENA and applicable IETF standards. PIDF-LO location information, or location references where applicable, remains bound to the call across retargeting, bridging, and transfer operations so downstream PSAPs receive accurate and traceable location data.

Media And Additional Data Negotiation. Media and additional data are negotiated using SDP to support voice, Real-Time Text (RTT), real-time video, and defined additional data types when supported by both endpoints. Where required for interoperability, codec and media transcoding are supported, with fallback to voice-only operation when richer media cannot be accepted by the far end, while preserving the call session and associated data.

Transfer Handling And Call Context Continuity. Warm (attended) transfers, blind transfers, and inter-PSAP transfers within and between ESInet regions are supported without interruption of service. Call metadata, including location information, timestamps, caller identity, and active media sessions, is preserved so receiving PSAPs obtain the full call context necessary for effective call handling.

Identity, Trust, And Authentication. SIP identity assertions are enforced throughout origination, routing, delivery, transfer, and termination. Correct handling of P-Asserted-Identity and related headers enables differentiation between validated and unvalidated caller identity. Integration with STIR/SHAKEN supports caller authentication and verification where available, enhancing trust and situational awareness while maintaining compatibility with legacy and transitional environments.

End-To-End Standards Conformance. End-to-end call flows are managed in conformance with applicable NENA i3 and IETF standards, including call origination, routing, delivery to the appropriate PSAP, transfers, and termination. These behaviors are applied consistently across all supported media types and operational scenarios, providing a reliable and standards-based NG911 call handling environment for Nebraska.

5.2.7.2. MEDIA QUALITY OF SERVICE (QoS)

5.2.7.2.1. Audio

The proposed solution shall support high-quality, reliable audio for all emergency calls. The solution must be conformant with NENA and IETF standards for audio codecs and media transport to ensure interoperability between originating networks, the ESInet, and PSAPs.

- *MOS-equivalent POLQA score of 4 minimum, 4.5 average from OSP edge to PSAP edge*
- *Continuous sampling of >1% of calls randomly distributed*
- *Capability to monitor 100% of calls between any two points for up to 5 days upon request*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *High call quality with audio MOS-equivalent POLQA score of 4 minimum/4.5 average from OSP to PSAP edge.*
- *Continuous sampling >1% of calls; capability to monitor 100% of calls between points for up to 5 days.*
- *Descriptions of end-to-end media path measurement, POLQA monitoring/measurement, and logging/reporting procedures.*

LUMEN RESPONSE:

Lumen provides an audio transport solution for Nebraska that is engineered to meet the State's requirements for high-quality, reliable media delivery across the ESInet and NGCS. The design supports NENA- and IETF-compliant codecs and RTP transport to preserve end-to-end interoperability from originating service provider ingress, through the ESInet core, and to PSAP egress. Media paths are engineered so calls meet or exceed a MOS-equivalent POLQA score of at least 4.0, with an average score of 4.5, measured from OSP ingress to PSAP delivery.

End-To-End Audio Quality Objectives. Audio performance is engineered to deliver PSAP-grade voice quality across all call paths. Quality of Service controls are applied consistently across ingress, core, and egress segments to protect RTP media and maintain predictable performance during normal operations, rerouting events, and failover scenarios.

Continuous Sampling And Targeted Monitoring. Audio quality metrics are continuously validated through randomized sampling of more than 1% of calls across time, media types, and network segments to provide statistically meaningful insight into overall performance. When requested by the State, targeted monitoring of 100% of calls between defined measurement points is supported for periods of up to five days to enable focused analysis without impacting live service.

Media Path Measurement And Analysis. End-to-end media path measurement is performed using RTP-level statistics, including jitter, latency, and packet loss, combined with external POLQA analysis to assess user-perceived audio quality. Measurement data captures timing, participating nodes, and correlation identifiers so results can be tied to specific call sessions.

Logging, Reporting, And Operational Visibility. Media quality measurements and impairment events are logged and retained within ESInet monitoring systems. Reporting provides detailed visibility into MOS-equivalent scores, worst-case observations, and detected impairments to support operational oversight, troubleshooting, and trend analysis consistent with State requirements.

5.2.7.2.2. Video

For video services, the proposed service must utilize MOS-equivalent PEVQ score of 4 minimum, 4.5 average from OSP edge to PSAP edge, and have continuous sampling of >1% of calls randomly distributed. They should also have the capability to monitor 100% of video calls between any two points for up to 5 days upon request.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Video MOS-equivalent PEVQ score of 4 minimum/4.5 average from OSP to PSAP edge.*

- *Continuous sampling >1% of calls.*
- *Capability to monitor 100% of video calls between points for up to 5 days; and descriptions of end-to-end video path measurement, PEVQ monitoring/measurement, and logging/reporting procedures.*

LUMEN RESPONSE:

Lumen provides NG911 video services engineered to meet the State's required quality objectives across the full media path from originating service provider ingress through the ESInet and NGCS to PSAP delivery. The design supports standards-based codecs, RTP transport, and Quality of Service mechanisms so video sessions achieve a MOS-equivalent PEVQ score of at least 4.0 with an average score of 4.5 under expected operating conditions. To address the State's requirements for quality, monitoring, and visibility, the following capabilities are implemented and documented:

- **End-To-End Video Quality Objectives.** Video services are engineered to deliver PSAP-grade performance from OSP edge to PSAP edge. PEVQ-based MOS-equivalent metrics are used to evaluate video quality, with operational objectives aligned to a minimum score of 4.0 and an average score of 4.5 across monitored call paths. QoS controls applied across ingress, core, and egress segments preserve frame quality, motion integrity, and synchronization during normal operations and network transitions.
- **Continuous Sampling Of Video Calls.** Video quality metrics are continuously validated through randomized sampling of more than 1% of video calls across time, media paths, and network segments. Sampling provides statistically representative insight into overall performance without impacting live call handling and supports identification of localized or systemic quality trends.
- **Targeted Monitoring Of 100% Of Video Calls.** On-demand monitoring of 100% of video calls between defined ESInet measurement points is supported for periods of up to five days when requested by the State. This capability enables focused end-to-end analysis for specific PSAPs, OSPs, or network segments during investigations or validation activities.
- **Video Path Measurement And PEVQ Analysis.** End-to-end video performance is measured using RTP-level indicators, including packet loss, jitter, and latency, correlated with external PEVQ analysis to assess user-perceived video quality. Measurements are correlated with signaling and network conditions to identify sources of impairment.
- **Logging, Reporting, And Operational Visibility.** Video performance data is logged within ESInet monitoring systems, including measurement timing, correlation identifiers, and media path elements involved. Reporting provides visibility into MOS-equivalent scores, impairment events, and worst-case observations to support troubleshooting, validation, and trend analysis consistent with State oversight requirements.

These capabilities ensure that Nebraska's NG911 video services maintain standards-aligned quality, provide continuous and targeted performance visibility, and support reliable delivery of real-time video across the ESInet and NGCS.

5.2.7.3 TEXT

The State requires that text to 911 and text from 911 be supported for both legacy and NG PSAPs and OSPs.

- *For NG911, text to 911 shall be provided via Message Session Relay Protocol (MSRP) using standard NENA-STA-010.3 interfaces.*

- For text from 911, Contractor shall maintain an interface to a commercial text gateway.
- For Legacy PSAPs, MSRP or web interfaces to the outgoing text service are required.

Text from NG PSAPs shall be able to send MSRP to an element in the NGCS which will send SMS text using the text gateway.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 100% correct text delivery 99.99% of the time.
- Foreign language translation for all texts; and descriptions of end-to-end text path measurement, translation delivery/display, monitoring for 99.99% availability, and logging/reporting procedures.

LUMEN RESPONSE:

Lumen provides statewide support for text-to-911 and text-from-911 services for both legacy and NG911 PSAPs and originating service providers, ensuring consistent delivery, monitoring, and availability across the ESInet and NGCS. The solution supports standards-based interfaces for NG911 traffic and accommodates transitional PSAP environments while maintaining required performance, accuracy, and operational visibility. To meet the State's requirements, the following capabilities are implemented and documented:

- **Standards-Based Text-To-911 And Text-From-911 Handling.** NG911 text sessions are supported using MSRP interfaces conformant with NENA-STA-010.3 so text flows through the ESInet and NGCS with the same routing, policy, and security controls applied to other i3 communications. Text-from-911 is supported through integration with a commercial text gateway that converts outbound MSRP messages to SMS for delivery to callers when required. Legacy PSAPs are supported through MSRP-based connections or secure web-based interfaces, ensuring continuity regardless of PSAP readiness.
- **Text Delivery Accuracy And Availability.** End-to-end text delivery is engineered and monitored to achieve 100% correct delivery 99.99% of the time across ESInet ingress, NGCS processing, and PSAP interfaces. Text sessions are monitored throughout their lifecycle to confirm delivery success, latency, and integrity.
- **Continuous Sampling And Targeted Monitoring.** Continuous, randomized sampling of more than 1% of text sessions is performed to provide statistically meaningful insight into delivery performance across time, PSAPs, OSPs, and network segments. When requested by the State, targeted monitoring of 100% of text sessions between defined points is supported for periods of up to five days to enable focused performance analysis without impacting live service.
- **Foreign Language Translation Support.** Foreign language translation is supported for all inbound and outbound text messages. Translation occurs within Call Handling Equipment offers not the text gateway path or an integrated translation component, depending on routing and message context. MSRP is presented to PSAP displays in the format sent preserving the original message content for audit and review or translation purposes.
- **Logging, Reporting, And Operational Visibility.** Text signaling events, delivery outcomes, translation activity, timestamps, and correlation identifiers are logged across

the ESInet and NGCS. Reporting provides visibility into availability, delivery performance, worst-case observations, and translation success rates, supporting troubleshooting, auditing, and confirmation that text services meet State performance and accuracy requirements.

These capabilities ensure that Nebraska's text-to-911 and text-from-911 services operate reliably across legacy and NG911 environments while maintaining standards conformance, required availability, and full operational transparency.

5.2.7.4 INTERACTIVE MULTIMEDIA RESPONSE SERVICE (IMRS)

The Respondent must provide a description and/or documentation that supports the requirements in this section, including IMR conforming to NENA-STA-010.3.

LUMEN RESPONSE:

Lumen provides an Interactive Multimedia Response (IMR) Service implementation for Nebraska that conforms to NENA-STA-010.3 and supports NG911 call processing, routing, and operational requirements. The IMR Service captures, stores, and makes available a complete, standards-compliant record of SIP signaling, media interactions, routing decisions, policy evaluations, and associated NGCS transactions for each emergency session, enabling analysis, troubleshooting, audit, and compliance validation.

Standards-Aligned IMR Service Integration. The IMR Service is implemented as a native NGCS function that interoperates with SIP signaling, media handling, routing, and policy components within the ESInet. Interactions leverage the same secure transport, session control, and media handling mechanisms used for other NG911 communications, ensuring consistent behavior across voice, text, and multimedia workflows.

Comprehensive Session Recording And Traceability. The IMR Service records message sequences, timestamps, identities, routing outcomes, and state transitions associated with each emergency session. Captured records provide a coherent, end-to-end view of session behavior suitable for technical analysis, operational troubleshooting, audit review, and standards conformance verification.

Discrepancy Reporting And Issue Management. Support is provided for the IMR Discrepancy Report (DR) mechanism defined in NENA-STA-010.3, enabling authorized NG911 entities to report issues related to IMR behavior, including failed interactions, unexpected termination, or media handling errors. Reported discrepancies are captured and managed within the broader NGCS discrepancy management framework to support traceability, root cause analysis, and corrective action.

5.2.7.5 BRIDGE

The State requires a multimedia bridge conforming to NENA-STA-010.3. The State expressly requires the bridge to handle audio, video, MSRP and RTT.

- *The State has no preference on which model (ad hoc or answer all calls at a conference aware UA), but the bridge must be able to transfer calls to and from ESInets using either model as specified in NENA-STA-010.3.*
- *The bridge must have capacity to maintain 20 simultaneous 3-way video calls or 100 simultaneous 3-way audio calls or a mix thereof.*
- *The bridge must be capable of supporting up to 6 parties (caller, call taker and up to four other parties) in any conference, with any mix of media.*

- *The bridge must have a mechanism to support RTT mixing when the end points do not support multiple RTT streams conforming to RFC 9071, as specified in NENA-STA-010.3.*
- *The bridge must support logging of media using the NENA-STA-010.3 specified mechanisms.*
- *The bridge must support the RFC 4575 Conference Event Package.*
- *The bridge must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3. The State must be able to subscribe to ServiceState and receive the standard state changes. The proposal must describe the bridge in detail.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Multimedia bridge conforming to NENA-STA-010.3 handling audio/video/MSRP/RTT.*
- *Support for ad hoc or answer-all models with transfers using either.*
- *Capacity for 20 simultaneous 3-way video or 100 audio calls (mix).*
- *Up to 6 parties per conference with media mix.*
- *RTT mixing per RFC 9071.*
- *Media logging per standard; RFC 4575 Conference Event Package.*
- *ElementState/ServiceState support.*
- *Detailed bridge description.*

LUMEN RESPONSE:

Lumen provides a multimedia bridge for Nebraska that conforms to NENA-STA-010.3 and supports audio, video, MSRP, and Real-Time Text (RTT) within the NG911 environment. The bridge integrates with ESInet and NGCS signaling paths and supports both ad-hoc conferencing and the answer-all (conference-aware user agent) model defined by the standard, including transfers to and from other ESInets using either approach as appropriate for PSAP workflows.

Standards-Based Multimedia Conferencing Integration. The multimedia bridge operates as a native NGCS functional element and interoperates with SIP signaling, media handling, routing, and policy functions. Supported media types include audio, video, MSRP, and RTT, enabling standards-based conferencing and call-transfer scenarios within Nebraska's ESInet and across interconnected ESInets.

Conference Models And Transfer Support. Both ad hoc conferencing and answer-all conferencing models are supported in accordance with NENA-STA-010.3. Calls may be transferred into or out of conferences using either model, allowing flexibility based on PSAP capabilities, responder participation needs, and inter-ESInet interoperability requirements.

Conference Capacity And Participant Support. The bridge is engineered to support at least twenty simultaneous three-way video conferences or one hundred simultaneous three-way audio conferences, or a proportional combination of audio and video sessions. Each conference supports up to six participants, including the caller, call taker, and up to four additional parties, with any supported mix of media types.

RTT Mixing And Accessibility. RTT mixing is supported when participating endpoints do not support multiple concurrent RTT streams. RTT handling follows the behavior defined in

RFC 9071 and applicable NENA-STA-010.3 requirements to ensure continuity of text communications within mixed-media conferences and to preserve accessibility across heterogeneous endpoint capabilities.

Logging, Conference State, And Operational Visibility. Media and conference logging are supported in accordance with NENA-STA-010.3 so signaling, media, and conference state events can be captured for diagnostics, audit, and compliance review. Support for the RFC 4575 Conference Event Package allows NGCS and PSAP equipment to subscribe to conference state and participant changes. ElementState and ServiceState interfaces are exposed so the State may subscribe to operational state notifications and monitor availability and service status.

Documentation And Architectural Transparency. Documentation describes the multimedia bridge architecture, supported media types, conferencing models, capacity characteristics, state notification behavior, and logging capabilities. This information supports State review, governance, and ongoing operational planning for NG911 multimedia conferencing services.

These capabilities ensure that Nebraska's NG911 environment supports standards-compliant, scalable, and observable multimedia conferencing while maintaining interoperability, accessibility, and operational resilience across the ESInet and NGCS.

5.2.8. Egress and External Interfaces

5.2.8.1. OUTGOING CALL INTERFACE FUNCTION (OCIF)

The State requires an OCIF conforming to NENA-STA-010.3. The OCIF must be capable of directing a call back of an emergency call to the OSP that originated the emergency call, offering at least the same media streams negotiated in the emergency call. The contractor must obtain appropriate identities (for example, telephone numbers) for calls sent to other service providers. Use of those identities must be controlled by the Data Rights Management system specified in NENA-STA-010.3.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *OCIF per NENA-STA-010.3 for call backs to OSP with same media streams.*
- *Obtaining identities for other providers controlled by DRM.*
- *Description of OCIF utilization for call backs with implementation/integration details.*

LUMEN RESPONSE:

Lumen provides an Outgoing Call Interface Function (OCIF) for Nebraska that conforms to NENA-STA-010.3 and supports PSAP-initiated callbacks to originating service providers with preservation of the media characteristics negotiated during the original emergency call. The OCIF uses identity information associated with the original session to determine the correct callback destination and reestablishes the session through the ESInet and NGCS so PSAPs can resume communications with full context.

Standards-Based Callback Routing And Media Continuity. Callbacks are directed to the originating OSP using the same or equivalent media streams negotiated during the initial emergency call, including audio and other supported media types. Media parameters established during the original session are reused so callbacks preserve multimedia fidelity and session continuity in accordance with the NENA i3 call model.

Identity Determination And STIR/SHAKEN Integration. Identity information used for callbacks is derived from SIP signaling and identifiers supplied by originating networks. Where STIR/SHAKEN verification results are available from upstream validation elements, those results are incorporated into callback handling to inform identity confidence while preserving interoperability with originating networks.

Data Rights Management And Identity Protection. Use of callback identity information is governed by the Data Rights Management mechanisms defined in NENA-STA-010.3. Authorized NGCS elements and PSAP systems may retrieve and use identity data for callback initiation, while access, storage, and retrieval remain subject to authentication and authorization controls consistent with NG911 data protection requirements.

Integration With NGCS Routing And Security Controls. The OCIF integrates with NGCS routing, policy, and security functions so callbacks follow the same ESInet pathing, certificate-based trust model, and secure SIP signaling applied during the initial emergency call. SIP signaling, location information (PIDF-LO or valid location references), negotiated media capabilities, and required Additional Data are preserved and propagated during callback setup.

Documentation And Architectural Transparency. Documentation describes OCIF placement within the NGCS architecture, callback decision logic, DRM protections applied to identity information, and interaction with ESRP, BCF, and OSP interfaces. This information demonstrates how Nebraska's PSAPs can initiate high-fidelity multimedia callbacks without loss of identity, location, or media continuity while maintaining standards conformance and operational integrity.

Deliverables - NG911 Core Services (NGCS)

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires clear traceability, standards conformance visibility, and operational proof for all NGCS functional elements supporting NG911 call processing, routing, and data services. Lumen complies by providing a comprehensive mapping and traceability document that explicitly aligns proposed system components and service modules to defined NGCS functions and required interfaces. This documentation identifies how each functional element maps to NENA i3 requirements and includes interface conformance statements to demonstrate adherence to applicable SIP and REST specifications.

Lumen further complies by supplying interoperability test results that validate NGCS operation with SIP-based call flows, including packet-level evidence. Test artifacts include SIP call scenarios exercised across NGCS interfaces, supported by packet traces and test outcomes that demonstrate correct signaling behavior, header preservation, and standards-aligned interoperability with connected elements and peers.

In addition, Lumen provides documented performance test results and scalability benchmarks for NGCS components. These deliverables demonstrate system behavior under

load, verify routing and lookup performance metrics, and confirm the ability of NGCS services to scale to peak and stress conditions without degradation of call handling, routing accuracy, or availability. Collectively, these deliverables provide the State with verifiable evidence that the proposed NGCS implementation is standards-aligned, interoperable, and capable of meeting required performance and scalability expectations for statewide NG911 operations.

5.3. GIS and Database Services Requirements

The Contractor shall implement location-based routing and ECRF/LVF functions using GIS data that conforms to the NENA GIS Data Model (NENA-STA-006.2), including civic address points, road centerlines, PSAP boundaries, emergency service polygons, and other required layers. The GIS repository must support spatial indexing for efficient queries.

Operations and Administration:

Location information is handled by the PSAPs while the State handles the PSAP boundaries and provisioning boundaries. The proposal shall include measures to maintain the PSAP interaction and where the PSAP utilizes a vendor must not interfere or materially change the contract a PSAP currently has for GIS support.

Location conveyance:

Location data shall be transported using PIDF-LO per RFC 4119 and RFC 5139 with applicable NENA extensions. The system shall deliver location information to PSAP CHE and mapping clients via standardized NG911 interfaces, supporting both push and pull mechanisms.

Validation and determination:

Integrate LVF/LIS to validate caller-provided locations, supporting geodetic coordinates (for example, WGS84) and civic addresses, including complex scenarios such as multi-line enterprises and multi-tenant buildings with address reformatting. The ECRF shall use authoritative GIS to determine the correct ESN/PSAP, with defined fallback to default routing.

Data governance and provisioning:

The GIS system shall provide change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning formats (for example, GML and GeoJSON). Provide a GIS data-provisioning API and a comprehensive audit log of changes, including user, timestamp, and deltas.

Rules-based routing (RBR):

Support RBR features, including time-of-day routing, temporary boundary adjustments, alternate routing logic, and attribute-driven decisions derived from GIS layers or an integrated rules engine.

LUMEN RESPONSE:

Lumen provides a location-based routing and validation solution for Nebraska that uses the Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) backed by an authoritative GIS repository conformant with the NENA GIS Data Model defined in

NENA-STA-006.2. The GIS repository maintains all required layers, including PSAP boundaries, emergency service boundaries for law, fire, and EMS, road centerlines, and site or structure address points, with spatial indexing applied to ensure efficient real-time query performance under call load.

Authoritative GIS Repository And Operational Responsibility Alignment. The GIS repository serves as the authoritative source for routing and validation while preserving established operational roles. PSAPs retain responsibility for location data associated with their operations, and the State maintains PSAP boundary and provisioning boundary layers within the same repository. Existing PSAP GIS vendor relationships are preserved by accepting GIS feeds and update practices from current providers, without requiring changes to or replacement of existing GIS contracts.

Location Conveyance Using PIDF-LO And Standard NG911 Interfaces. Location information is conveyed using PIDF-LO in accordance with RFC 4119, RFC 5139, and applicable NENA extensions. Location delivery to PSAP Call Handling Equipment and mapping clients supports both push and pull models, allowing location to be delivered with the call or retrieved or refreshed by PSAP or NGCS systems using standard NG911 interfaces.

Location Validation And Determination Across Geodetic And Civic Formats. The LVF and LIS operate together to validate caller-provided location information prior to routing. Validation supports geodetic coordinates, such as WGS-84, and civic address formats, including complex scenarios such as multiline enterprises and multi-tenant structures where unit-level addressing and reformatting rules apply. When a validated location cannot be mapped to a service boundary, the ECRF applies State-defined fallback routing logic using authoritative GIS layers so calls are still delivered to an appropriate PSAP.

GIS Data Governance, Provisioning, And Auditability. GIS data governance and provisioning mechanisms support change tracking, version control, and time-stamped snapshots of authoritative data. Automated batch and incremental updates are supported using NENA-recommended provisioning formats, including GML and GeoJSON. A provisioning API allows authorized State and local entities to submit updates, and each change is recorded in an audit log capturing user identity, timestamp, and a description of data deltas to support review and rollback when necessary.

Rules-Based Routing Using GIS Attributes And Policy Logic. Rules-Based Routing is supported by combining ECRF results with GIS layer attributes and a rules engine within the Policy Routing Function. This enables time-of-day routing, temporary boundary adjustments for events or outages, alternate routing based on operational policy, and attribute-driven decisions such as routing by jurisdiction, facility type, or designated overflow destination. These capabilities allow routing behavior to be adjusted dynamically without requiring structural changes to the underlying GIS data.

This approach ensures that Nebraska's NG911 environment uses authoritative, standards-aligned GIS data to support accurate routing and validation, while preserving existing governance models, enabling controlled updates, and providing the flexibility required for operational and incident-driven routing decisions.

5.3.1. Data Management and Interfaces

5.3.1.1. GIS AND DATABASE MANAGEMENT FUNCTIONALITY

The contractor will utilize the PSAP and State provided data for geospatial routing from the caller to the PSAP. Management of the data will be the responsibility of the State.

The contractor will have a web interface and/or automated method to provision data and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system. The contractor will ensure that an update to the system will be reflected in a change in routes (where the change does affect routes) within 5 minutes of such a change, assuming no errors are detected (online, real time update capability).

All data associated with call routing and plotting will be provided in conformance with NENA Data Model standards - NENA-STA-015.10 for remaining Legacy/Enhanced 911 systems and NENA-STA-006.2 for NG911 systems.

Originating call network operators will verify civic address location information against the NG911 GIS data using the LVF provisioned as required.

The preferred data exchange will be in Environmental System Research Institute's (ESRI) Structured Query Language (SQL) Spatial Database Engine (SDE).

The managed GIS map data will replace the traditional MSAG database as the primary database for location-based call routing and location validation (ECRF/LVF) functions within the NG911 system.

The maintenance of this GIS dataset will be completed by PSAP staff or designee. It is a requirement that the discrepancy reports of the data are delivered for remediation.

The contractor will be utilizing all existing and available source data and the management and coordination necessary.

- *The PSAP will be responsible for providing all GIS data used in the location routing, validation, mapping services, and maintenance of such data that are part of the contractor's system.*
- *The data from the PSAP will include the road centerline and address range data, address structure points, PSAP boundaries, municipal boundaries, police, fire, EMS, and medical transport boundaries and many additional GIS layers useful for display in the PSAPs. GIS data used for call routing and call locations will be provided in a NENA NG911 standard format.*
- *The contractor will be required to establish a working relationship with the State and to work out mutually acceptable procedures for the maintenance of these databases.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Use of PSAP GIS data for geospatial routing.*
- *Web interface or automated method for provisioning and retrieving post-QA data for maps.*
- *Reflection of PSAP updates in routes within 5 mins (online, real-time).*
- *Data structures organized in conformance to NENA Data Model Standards - NENA-STA-015.10 and NENA-STA-006.2.*

- *LVF for OSP civic address verification.*
- *Preferred ESRI SQL SDE exchange.*
- *Replacement of MSAG with GIS for routing/validation.*
- *PSAP maintenance with contractor discrepancy reports.*
- *Use of existing source data.*
- *Responsibility for all GIS data maintenance.*
- *Inclusion of road centerline, address points, PSAP emergency boundaries, and additional layers.*
- *Mutually acceptable maintenance procedures with State.*

LUMEN RESPONSE:

Lumen provides a location-based routing and validation solution for Nebraska that uses the Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) backed by an authoritative GIS repository conformant with the NENA GIS Data Model defined in NENA-STA-006.2. The GIS repository maintains all required layers, including PSAP boundaries, emergency service boundaries for law, fire, and EMS, road centerlines, and site or structure address points, with spatial indexing applied to ensure efficient real-time query performance under call load.

Authoritative GIS Repository And Operational Responsibility Alignment. The GIS repository serves as the authoritative source for routing and validation while preserving established operational roles. PSAPs retain responsibility for location data associated with their operations, and the State maintains PSAP boundary and provisioning boundary layers within the same repository. Existing PSAP GIS vendor relationships are preserved by accepting GIS feeds and update practices from current providers, without requiring changes to or replacement of existing GIS contracts.

Location Conveyance Using PIDF-LO And Standard NG911 Interfaces. Location information is conveyed using PIDF-LO in accordance with RFC 4119, RFC 5139, and applicable NENA extensions. Location delivery to PSAP Call Handling Equipment and mapping clients supports both push and pull models, allowing location to be delivered with the call or retrieved or refreshed by PSAP or NGCS systems using standard NG911 interfaces.

Location Validation And Determination Across Geodetic And Civic Formats. The LVF and LIS operate together to validate caller-provided location information prior to routing. Validation supports geodetic coordinates, such as WGS-84, and civic address formats, including complex scenarios such as multiline enterprises and multi-tenant structures where unit-level addressing and reformatting rules apply. When a validated location cannot be mapped to a service boundary, the ECRF applies State-defined fallback routing logic using authoritative GIS layers so calls are still delivered to an appropriate PSAP.

GIS Data Governance, Provisioning, And Auditability. GIS data governance and provisioning mechanisms support change tracking, version control, and time-stamped snapshots of authoritative data. Automated batch and incremental updates are supported using NENA-recommended provisioning formats, including GML and GeoJSON. A provisioning API allows authorized State and local entities to submit updates, and each change is recorded in an audit log capturing user identity, timestamp, and a description of data deltas to support review and rollback when necessary.

Rules-Based Routing Using GIS Attributes And Policy Logic. Rules-Based Routing is supported by combining ECRF results with GIS layer attributes and a rules engine within the

Policy Routing Function. This enables time-of-day routing, temporary boundary adjustments for events or outages, alternate routing based on operational policy, and attribute-driven decisions such as routing by jurisdiction, facility type, or designated overflow destination. These capabilities allow routing behavior to be adjusted dynamically without requiring structural changes to the underlying GIS data.

5.3.1.2. SPATIAL INTERFACE (SI) FUNCTIONALITY

The contractor will implement a Spatial Interface and ensure following capabilities are implemented:

- *GIS data provisioned by the spatial interface (SI) will undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA-STA-006.2-2022, NENA-02-014 and NENA-STA-010.3-2021 while maintaining the online, real time update capability.*
- *The SI will convert the GIS data meeting these requirements 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 will be able to provision and perform incremental updates, in near-real-time, to the ECRF, LVF, the map viewer service, the PSAP map display and similar applications that consume GIS data.*
- *Validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of online real-time provisioning of updates to the GIS data provisioned to the ECRF and LVF.*
- *The SI operation will align with the data maintenance processes with minimal impact to existing operations.*
- *The SI will receive and incorporate the SI datasets that have been prepared by the PSAP as previously described.*
- *Web interface tool for viewing and submitting incidents and change tickets.*
- *Web interface tool for viewing policy-routing plans.*

The contractor will be able to test and then apply updates to the operating ECRF by a secure and reliable method that does not create operational problems.

The contractor's GIS functions will be able to perform database audits for common problems and errors, such as gaps, overlaps or number range conflicts, which if encountered, will be referred back to the PSAP for resolution.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *SI implementation with data-quality and integrity checks per NENA standards while maintaining real-time updates.*
- *Conversion to ECRF/LVF format via Web feature service.*
- *Incremental near real-time updates to ECRF/LVF, map viewer, and PSAP displays.*
- *Validation prior to provisioning with online real-time updates.*
- *Alignment with PSAP processes.*
- *Incorporation of PSAP prepared datasets.*
- *Web tools for incidents, change tickets and policy-routing views.*
- *Secure reliable update and testing application without problems.*

- Database audits for gaps/overlaps/conflicts referred to PSAP.

LUMEN RESPONSE:

Lumen provides a Spatial Interface (SI) for Nebraska that supports authoritative GIS data provisioning for NG911 while enforcing data quality, integrity, and standards conformance. The SI is designed to validate, transform, and distribute GIS data to NGCS components in near real time, ensuring routing and validation functions reflect current authoritative data without disrupting operations.

Standards-Based Data Quality And Integrity Validation. The Spatial Interface performs comprehensive data quality and integrity checks on all GIS datasets provisioned by PSAPs and the State. Validation includes schema conformance, geometry correctness, topology integrity, and required attribution in alignment with NENA-STA-015.10, NENA-STA-006.2, NENA-02-014, and NENA-STA-010.3. Only datasets that pass validation are eligible for activation, preventing erroneous data from impacting operational routing or validation.

Real-Time Conversion And Distribution To NGCS Components. Validated GIS data is converted into the formats and spatial projections required by the ECRF and LVF using a Web Feature Service-based approach. The SI provisions both full and incremental updates to ECRF, LVF, map viewer services, PSAP mapping displays, and other GIS-consuming applications with near real-time delivery so routing and validation outcomes reflect recent changes with minimal delay.

Online Provisioning Without Service Interruption. All GIS data and incremental updates are validated prior to provisioning and then applied online so operational ECRF and LVF instances update without service interruption. Failed validations are blocked and flagged, ensuring that only error-free data is promoted into the live environment.

Alignment With Existing PSAP Processes And Data Ownership. SI operations are designed to align with existing PSAP data maintenance practices and workflows. Datasets prepared by PSAPs or their designated GIS providers are ingested exactly as described in established PSAP data management processes, preserving local data ownership while enabling controlled statewide NG911 routing and validation.

Web-Based Tools For Incidents, Changes, And Routing Visibility. Web-based tools support submission and tracking of GIS-related incidents and change tickets and provide visibility into routing plans derived from GIS data and routing rules. These tools enable authorized users to review update status, discrepancies, and routing behavior, supporting coordination, transparency, and operational awareness.

Secure Testing, Promotion, And Audit Controls. GIS updates are tested prior to activation using secure, controlled workflows. Updates are applied to non-active instances first and promoted only after successful validation and testing, ensuring operational stability. Database audit capabilities detect gaps, overlaps, number-range conflicts, topology issues, and attribution discrepancies, and identified issues are documented and referred to the PSAP or designated authority for remediation.

5.3.2. Core Data Services

5.3.2.1. MAPPING DATA SERVICE

A Mapping Data Service conforming to NENA-STA-010.3 will be provided. This must be available within 18 months. The MDS will be capable of providing maps for all calls for all entities inside the ESInet and for calls handled out of area in other ESInets.

- The MDS must support both images and features as described in NENA-STA-010.3*
- The MDS must support all layers defined in NENA-STA-006.2. Additional layers may be supported, and the proposal will describe what additional layers the MDS will support.*
- Retrieval of map data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.*
- The MDS must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- MDS per NENA-STA-010.3 available within 18 months for all calls/entities.*
- Support for images/features.*
- All layers per NENA-STA-006.2.*
- Additional layers described; DRM-controlled retrieval; ElementState/ServiceState support with State subscription.*

LUMEN RESPONSE:

Lumen provides a Mapping Data Service (MDS) for Nebraska that conforms to NENA-STA-010.3 and is planned to be available within eighteen months to support map delivery for all calls handled within the ESInet and for calls routed through interconnected ESInets. The MDS delivers both map images and feature-based data as defined by the standard and provides mapping content to PSAPs, NGCS elements, and authorized out-of-area entities to support call handling and situational awareness.

Standards-Based Mapping Data Service Availability. The MDS is implemented as a native NGCS service and integrates with core NG911 call flows so mapping information is available for all supported call scenarios, including inter-ESInet routing. The service supports statewide and cross-jurisdictional interoperability by ensuring mapping data can be retrieved by authorized entities regardless of call origin.

Support For Images And Feature-Based Mapping Data. Both rendered map images and feature-level GIS data are supported in accordance with NENA-STA-010.3. This dual-mode delivery enables PSAP mapping clients and authorized NG911 applications to consume map content in the format best suited to their operational environment and display capabilities.

Alignment With The NENA GIS Data Model. All mandatory GIS layers defined in the NENA NG911 GIS Data Model (NENA-STA-006.2) are supported, including PSAP boundaries, emergency service boundaries, road centerlines, and site or structure address points. Support for additional GIS layers available within the enterprise GIS environment may be provided where authorized to enhance operational awareness, with any such layers identified and documented for Nebraska's NG911 deployment.

Controlled Access Using Data Rights Management. Retrieval of map images, features, and associated metadata is governed by the Data Rights Management mechanisms defined in NENA-STA-010.3. DRM enforcement ensures that only authorized users and systems can access mapping content, applying role-based and policy-driven controls consistent with NG911 security and privacy requirements.

Operational State Visibility And State Subscription. ElementState and ServiceState SUBSCRIBE/NOTIFY interfaces are supported so the State may subscribe to service-state notifications and monitor the availability and operational status of the Mapping Data Service. This capability provides visibility into service health and supports operational oversight of mapping functions used during emergency call handling.

Documentation And Architectural Transparency. Documentation describes the MDS architecture, supported image and feature layers, DRM enforcement approach, State subscription capabilities, and any additional GIS layers included in Nebraska's NG911 mapping environment. This information supports State review, governance, and long-term planning for standards-based mapping services within the ESInet and NGCS.

5.3.2.2. MSAG CONVERSION SERVICE (MCS)

The MSAG Conversion Service (MCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The State expects the LNG to support the SOA interface towards the legacy OSP, store the data in the Location Database in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The State expects the LPG to support the MF/ALI interface towards the legacy PSAP, retrieve the location from a Location Information Server in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *An MSAG Conversion Service (MCS) conforming to NENA-STA-010.3 will be implemented.*
- *The MCS must support Element State and Service State SUBSCRIBE/NOTIFY per NENA-STA 010.3.*
- *The State must be able to subscribe to Service State and receive the standard state changes.*

LUMEN RESPONSE:

Lumen provides a Master Street Address Guide Conversion Service (MCS) for Nebraska that conforms to NENA-STA-010.3 and supports the State's transition from MSAG-based routing to GIS-based NG911 routing and validation. The MCS implements the standard Spatial Interface (SI) for provisioning so legacy address data can be ingested, validated, converted, and stored in LVF-valid form for use by NGCS elements, enabling continued support for legacy environments without disrupting existing PSAP GIS workflows.

Standards-Based MSAG Ingestion And Conversion. The MCS accepts legacy-formatted MSAG and related addressing data supplied by PSAPs or originating service providers and converts that data into NG911-compliant civic location structures. Conversion processes

validate address elements, normalize formats, and store results in LVF-valid form so NGCS components can perform standards-based validation and routing.

Support For LNG Legacy Origination Interfaces. The MCS supports LNG operations by converting legacy Service Order Administration (SOA) data received from originating service providers into LVF-valid civic locations stored in the Location Database. Where required for originating provider processes, NG-formatted data can also be converted back into legacy formats, supporting bidirectional interoperability during the transition period.

Support For LPG Legacy PSAP Interfaces. The MCS supports Legacy PSAP Gateway (LPG) operations by converting legacy MF or ALL interface data used by PSAPs into NG-formatted civic or geodetic location information obtained from the Location Information Server. This allows legacy PSAPs to continue operating with existing interfaces while receiving accurate NG911 location information.

Bidirectional Conversion For Hybrid Environments. Bidirectional conversion is provided for all required legacy-to-NG and NG-to-legacy data paths, supporting Nebraska's hybrid operating environment during the transition to full i3 operation. This approach ensures continuity across LNG, LPG, and NGCS components without requiring immediate replacement of legacy systems.

ElementState And ServiceState Visibility. The MCS exposes ElementState and ServiceState SUBSCRIBE/NOTIFY interfaces as defined in NENA-STA-010.3 so the State may subscribe to service-state notifications and monitor operational availability. This capability provides visibility into MCS status and enables timely awareness of conditions that could affect LNG or LPG functionality.

Documentation And Operational Transparency. Documentation describes MCS architecture, SI-based provisioning workflows, legacy-to-NG and NG-to-legacy conversion behavior, Data Rights Management controls applied to addressing data, and ElementState and ServiceState support. This documentation demonstrates how the MCS supports Nebraska's NG911 transition while preserving data integrity, governance, and continuous operations.

5.3.2.3. GEOCODE CONVERSION SERVICE (GCS)

The Geocode Conversion Service (GCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- GCS per NENA-STA-010.3 with SI provisioning (additional options for PSAP GIS upgrades).
- Return of ECRF routing location for civic addresses.
- ElementState/ServiceState support.
- ServiceState and receive the standard state changes.
- The GCS must return the same location that the ECRF uses for routing when given a civic address.

LUMEN RESPONSE:

Lumen provides a Geocode Conversion Service (GCS) for Nebraska that conforms to NENA-STA-010.3 and supports normalization and conversion of civic address inputs into routing-equivalent locations used by the Emergency Call Routing Function (ECRF). The GCS is provisioned through the standard Spatial Interface (SI) and consumes PSAP-prepared datasets so address resolution aligns with the authoritative GIS data used for NG911 routing and validation.

Standards-Based Geocode Conversion And SI Provisioning. The GCS performs geocode conversion using the same authoritative GIS datasets and processing logic applied by NGCS routing and validation functions. Civic address inputs are normalized and validated through SI-based provisioning workflows, ensuring consistency between geocoding results and operational NG911 data without requiring changes to established PSAP GIS practices.

Return Of Routing-Equivalent Locations. When provided with a civic address, the GCS returns the same routing location used by the ECRF for call routing decisions. This ensures that geocode outputs match the dispatchable location applied during call processing, eliminating discrepancies between geocoding, validation, mapping, and routing functions.

Consistency Across NGCS Components. The GCS and ECRF share a common authoritative GIS source and consistent conversion logic so that address resolution results remain predictable and auditable across NGCS components. This alignment supports accurate downstream mapping, validation, and operational review.

ElementState And ServiceState Visibility. The GCS supports ElementState and ServiceState SUBSCRIBE/NOTIFY interfaces in accordance with NENA-STA-010.3. These interfaces allow the State to subscribe to standard service-state notifications and monitor operational health and availability of the GCS as part of the NGCS ecosystem.

Documentation And Architectural Transparency. Documentation describes the GCS architecture, SI-based provisioning workflow, geocode conversion process, use of authoritative GIS data, and the ElementState and ServiceState interfaces provided for monitoring. This information demonstrates how geocode conversion integrates with Nebraska's NG911 routing and validation environment while maintaining standards conformance and operational integrity.

5.3.3. PSAP-Facing Services**5.3.3.1. PSAP MAPPING SERVICE**

The State requires a Mapping Data Service (MDS) conforming to NENA-STA-010.3.

The services required must enable the PSAP mapping system and ECRF/LVF system to support multiple methods for reporting location errors. They include:

- ECRF civic location geocoding errors are automatically captured by the data management application utilized by the PSAP.*
- LVF failures are automatically captured by the LVF and forwarded to the data management application utilized by the PSAP.*
- 911 call mapping failures (calls that could not be mapped automatically) are captured by the system and forwarded to the data management application utilized by the PSAP.*

- 911 telecommunicators and dispatchers may manually generate a discrepancy report, and the system can automatically forward the reports to the data management application utilized by the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PSAP mapping using PSAP geospatial info.
- Support for error reporting methods (ECRF geocoding errors captured).
- LVF failures forwarded; unmapped calls captured; manual discrepancy reports forwarded.

LUMEN RESPONSE:

Lumen provides a MDS for Nebraska that conforms to NENA-STA-010.3 and supports PSAP mapping using PSAP-supplied geospatial information. The MDS integrates with PSAP mapping systems and with the Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) so that mapping and routing functions consume the same authoritative GIS layers provided by the State and PSAPs.

Integration With Authoritative GIS For Mapping And Routing. The MDS makes authoritative GIS layers available to PSAP mapping clients and NGCS components so that visual mapping, routing, and validation functions remain aligned. This ensures that the location displayed to call takers corresponds directly to the location used for routing and validation decisions within NGCS.

Automated Capture Of Location-Related Errors. Location-related errors are captured through standards-aligned mechanisms across NGCS components. Civic geocoding errors generated by the ECRF are automatically recorded by the PSAP's data management application, and LVF validation failures are forwarded to the same application for review and correction. Calls that cannot be mapped are also identified and captured for follow-up analysis.

Manual Discrepancy Reporting By PSAP Personnel. PSAP telecommunicators and dispatchers may generate manual discrepancy reports when mapping or location issues are observed during call handling. These reports are automatically forwarded to the PSAP's data management application so issues can be reviewed, tracked, and corrected within established PSAP and State data governance workflows.

This approach ensures that Nebraska's NG911 environment maintains consistent mapping and routing behavior, provides multiple paths for identifying and correcting location data issues, and preserves alignment between PSAP mapping displays and NGCS routing functions.

5.3.3.2. MAP DISCREPANCY REPORTING

The Respondent must provide a description and/or documentation that supports the requirements in this section for referral of all geospatial discrepancies to the State for remediation.

Note:

GIS-related discrepancy reporting technical requirements are detailed in §E-6.7.2, et seq. of this document.

LUMEN RESPONSE:

Lumen will provide mechanisms within the MDS and associated NGCS components to ensure that all geospatial discrepancies identified during routing, validation, or call mapping are referred to the State for remediation. Our implementation forwards discrepancy information generated by ECRF geocoding errors, LVF validation failures, unmapped 911 calls, and manually reported PSAP mapping issues to the State's designated data management application so the State can perform authoritative review and correction.

We support the referral of these discrepancies in alignment with the GIS related discrepancy reporting requirements specified by the State, including forwarding structured discrepancy details to the State for evaluation and resolution. This ensures the State receives complete visibility into geospatial issues that affect routing accuracy and can coordinate necessary remediations with PSAPs and GIS data stewards.

5.3.4. External Integrations

The Respondent must provide a description and/or documentation that supports the integration with additional vendors as required to provide functionality to all PSAPs as currently utilized.

LUMEN RESPONSE:

Lumen provides integration capabilities that support interoperability with additional vendors required by Nebraska so PSAPs may continue operating their existing systems without disruption. The NG911 architecture accepts PSAP-supplied interfaces, data formats, and workflows consistent with systems currently in use, ensuring continuity of operations and preservation of existing functional components.

Standards-Based Interoperability With PSAP Vendor Systems. Compatibility with PSAP vendor systems is maintained through the use of NENA-defined interfaces for call handling, mapping, CAD data exchange, GIS provisioning, and related integrations. This approach allows additional vendors to connect to the ESInet, NGCS elements, and associated services without requiring modification of PSAP contracts or replacement of existing operational tools.

Open Architecture Supporting Additional And Legacy Vendors. The NGCS and ESInet are designed using an open, standards-based architecture that supports integration with additional vendors and third-party systems required to maintain and enhance PSAP functionality, including environments utilizing external or legacy solutions. This architecture aligns with established NG911 interoperability frameworks and complies with applicable NENA i3 standards.

Use Of Published NENA Interfaces And Protocols. Integration with external vendors is supported through published, NENA-defined interfaces and protocols, including SIP for call signaling, RTP for media, LoST and ECRF/LVF interfaces for routing and validation, HELD for location conveyance, and Additional Data interfaces. These standards enable interoperability with originating service providers, neighboring ESInets, CAD systems, logging recorders, GIS providers, analytics platforms, and other PSAP-utilized systems without reliance on proprietary integrations.

Coordination And Joint Testing For Multi-Vendor Environments. For environments requiring coordination with other service providers, collaboration with the State and affected vendors is supported to define, document, and validate interface specifications, meet points,

and data exchange requirements. This includes support for ESInet-to-ESInet interconnection and structured joint testing to confirm routing, transfers, failover behavior, location delivery, and data interoperability prior to acceptance.

Integration Documentation And Change Governance. Integration documentation is provided as part of project deliverables and includes interface descriptions, network diagrams, data flows, and testing artifacts. Integration activities are governed by formal change management and testing processes to maintain continuity of operations and minimize disruption to PSAP workflows while enabling future interoperability and technology evolution.

Deliverables - GIS and Location-Based Routing

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires authoritative, standards-aligned GIS data and transparent routing behavior to ensure every NG911 call is accurately validated and delivered to the correct PSAP under all conditions. Lumen complies by providing comprehensive GIS data model documentation that conforms to the NENA NG911 GIS Data Model, along with representative sample datasets and entity-relationship diagrams that clearly depict data structures, relationships, and dependencies across routing, validation, and display services.

Lumen further complies by demonstrating location-based routing using authoritative GIS data for both civic and geodetic location inputs. Demonstrations validate that calls are routed to the correct PSAP based on validated location information and include edge cases such as boundary conditions, overlaps, gaps, and degraded or partial location scenarios. These demonstrations provide the State with clear evidence that routing decisions are deterministic, standards-aligned, and resilient to real-world data variability.

In addition, Lumen provides documented GIS update procedures and API specifications that define how authoritative data is provisioned, validated, versioned, and synchronized across NGCS components. These deliverables describe update workflows, timing expectations, and interfaces used to ensure routing changes are reflected accurately and without operational disruption. Collectively, these artifacts give the State full visibility into how GIS data is managed and used for NG911 routing, confirming accuracy, traceability, and ongoing operational integrity.

5.4. Security Requirements

The contractor shall implement the NENA NG-SEC security and trust model, featuring strong authentication and authorization for all interfaces, mutual TLS for inter-service communications, edge security via SBCs and Back-to-Back User Agents (B2BUAs), network segmentation, and secure management planes. Threat mitigations must address Denial of Service (DoS), Distributed DoS (DDoS), Telephony Denial of Service (TDoS), SIP flooding, spoofing, and injection attacks through rate limiting, anomaly detection, and firewalls.

Implement Role-Based Access Control (RBAC) with granular permissions, multifactor authentication (MFA) for all administrative access, least privilege enforcement, and auditing of service accounts. Integration with external identity providers (e.g., SAML/OAuth) must be supported.

All location data, call content, and PII must be encrypted in transit (TLS 1.3) and at rest (AES-256 or stronger), with data minimization, pseudonymization, and compliance with laws like HIPAA and CJIS where applicable. Access to sensitive data shall require explicit consent logging.

Provide Public Key Infrastructure (PKI) processes for certificate issuance/rotation, Certificate Revocation List (CRL)/Online Certificate Status Protocol (OCSP) validation, and secure key storage using Hardware Security Modules (HSMs) or compliant vaults. Automated alerts for expiring certificates must be included.

The contractor shall supply an incident response plan aligned with NENA, including vulnerability disclosure protocols, regular patch schedules (e.g., critical patches within 30 days), and forwarding of security event logs to the jurisdiction's Security Information and Event Management (SIEM) system via secure channels (e.g., Syslog over TLS).

Provide results from independent penetration testing (conducted within the last 12 months), SSAE 18/SOC 2 audit reports, and support for jurisdiction-led security acceptance testing, including network scans, application fuzzing, and red-team exercises.

LUMEN RESPONSE:

Lumen delivers a comprehensive, defense-in-depth security architecture for Nebraska's ESInet and NGCS that aligns with the NENA NG-SEC trust model and applies consistent protections across all network, service, and management interfaces. The architecture is designed to protect signaling, media, data, and administrative planes while preserving interoperability, resiliency, and uninterrupted emergency operations. Our solution provides the State the following security capabilities:

- **NENA NG-SEC Trust Model Alignment and Interface Protection.** Strong authentication and authorization are enforced on all interfaces, including inter-service communications, external integrations, and management access. Service-to-service communications use mutual TLS to authenticate both endpoints prior to session establishment, ensuring trusted interactions across ESInet and NGCS components.
- **Edge Security and Network Segmentation.** Session Border Controllers and Back-to-Back User Agents are deployed at all ingress and egress points to secure SIP signaling and media flows. Logical and physical segmentation is enforced using network zoning, firewalls, and access control policies to isolate signaling, media, data, and management domains, with dedicated secure management networks for administrative access.
- **Threat Detection and Mitigation Controls.** Layered threat mitigation mechanisms protect against DoS, DDoS, TDoS, SIP flooding, spoofing, replay, and injection attacks. Controls include rate limiting, protocol validation, anomaly detection, firewall enforcement, and continuous monitoring to identify abnormal patterns and initiate response actions without degrading call handling.
- **Role-Based Access Control and Identity Integration.** Granular role-based access control is applied using least-privilege principles. Multifactor authentication is required for all administrative and privileged access, service accounts are restricted and audited,

and access events are fully logged. Integration with external identity providers is supported using standards such as SAML or OAuth for centralized identity management when required by the State.

- **Data Protection and Privacy Safeguards.** Location data, call content, and personally identifiable information are encrypted in transit using TLS 1.3 and at rest using AES-256 or stronger encryption. Data handling follows minimization and pseudonymization practices where applicable, and access to sensitive data is logged and auditable to support accountability and regulatory compliance.
- **Public Key Infrastructure and Certificate Management.** PKI processes support certificate issuance, validation, rotation, and lifecycle management for ESInet and NGCS components. Certificate validation includes CRL and OCSP checks, cryptographic keys are protected using HSMs or compliant secure vaults, and automated monitoring alerts identify impending certificate expiration to prevent service disruption.
- **Incident Response, Patch Management, and Security Logging.** A formal incident response framework aligned with NENA guidance is maintained, including coordinated vulnerability disclosure and response procedures. Patch management is performed based on severity and risk, and security event logs are forwarded to the State's monitoring systems using secure transport to support centralized visibility and incident correlation.
- **Independent Security Validation and State-Led Testing.** Independent penetration testing conducted within the past twelve months and applicable SSAE 18 or SOC 2 reports are provided. Lumen also supports State-led security acceptance testing, including network scanning, application testing, and red-team exercises, with verified findings addressed through agreed remediation processes.

Together, these controls implement a secure, standards-based NG911 security architecture that prevents, detects, and responds to cyber threats without impairing call handling. The approach delivers consistent protection, operational transparency, and validated resilience across Nebraska's ESInet and NGCS environments.

5.4.1. Management and Process Control

5.4.1.1. PERSONNEL ROLES AND RESPONSIBILITIES

*Safeguarding NG911 assets – across **NGCS platforms** and the **ESInet** – is a shared duty. The contractor must **define, assign, and document** minimum security roles and responsibilities, whether performed internally or by external providers. At a minimum, the following roles must be covered by **named, accountable** individuals. Where third parties perform duties (carriers, cloud, managed services, subcontractors), the contractor remains responsible for assignment and verification.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An organizational roles matrix (e.g., org chart and/or RACI) identifying named individuals (or positions) for: Security Manager, Security Administrator, Data Owner(s), Data Custodian(s), Data User populations, and Security Audit Manager. Note any shared/combined roles and the accountable individual for each responsibility. Map these to NGCS components and ESInet segments.
- Documented role definitions aligned to the duties above, including authorities (e.g., the Security Manager's authority to set security policy for all NGCS/ESInet).

components; Security Administrator authority to implement and enforce controls across applications, network, cloud).

- Evidence that personnel are informed of their roles and responsibilities (e.g., acknowledgement forms, training records, onboarding materials, policy attestations).
- A data ownership register mapping every NG911 data set (local and remote) to a Data Owner; include classification and handling responsibilities.
- A data custodianship register mapping every NG911 data set (at rest and in transit, local and remote) to a Data Custodian; include the operational security measures they manage (encryption, key management touchpoints, access administration, backup/restore).
- Security administration procedures showing how the Security Administrator implements and maintains security controls in accordance with NG911 policies – for NGCS applications, the ESInet, edge devices, and management portals).
- An audit governance plan for the Security Audit Manager covering periodic audit cadence (internal/external), scope, reporting, and risk rating of findings, and tracking to closure.
- Role coverage procedures (e.g., delegation during absence) ensuring continuity while preserving single-point accountability for each required responsibility.
- If external parties are involved, contractual or policy evidence assigning role responsibilities to vendors/contractors/subcontractors and showing how the prime provider verifies fulfillment (e.g., attestations, SLAs, right-to-audit).

LUMEN RESPONSE:

Lumen provides a security governance structure that defines, assigns, and documents all required NG911 security roles and responsibilities for the ESInet and NGCS. Our structure identifies accountable individuals or positions for each mandated role and maintains responsibility even when duties are performed by external entities such as carriers, cloud providers, managed services, or subcontractors.

We maintain a roles matrix (**Table 5.4.1.1-1**) that identifies each required role, the position accountable for that role, and how each responsibility maps to NGCS components and ESInet segments.

Table 5.4.1.1-1. Responsibilities Matrix.

Required Role	Accountability	Responsibility Scope
Security Manager	John Sintim	Overall authority for NG911 security policy, governance, and risk acceptance across NGCS platforms and the ESInet. Accountable for compliance with NENA NG-SEC, contractual security requirements, and jurisdictional policies.
Security Administrator	Project Manager	Implementation and enforcement of technical security controls for network, applications and management portals. Executes access controls, encryption configurations, logging, monitoring, and security tooling.
Data Owner(s)	Lumen and Intrado Project Personnel	Classification and handling responsibilities for each NG911 dataset, permitted uses, retention requirements, and access authorization.
Data Custodian(s)	Lumen and Intrado Project Personnel	Execution of operational security measures including data at rest and in transit. encryption, key management

		touchpoints, access administration and backup or restore actions.
Data Users	All NGCS users	Authorized operational use of NG911 data. Defined groups (e.g., operations staff, support engineers) with approved, role-based access to NG911 data.
Security Audit Manager	Lumen and Intrado Project Personnel	Independent oversight role responsible for audit planning, execution coordination, reporting, and tracking remediation to closure.

We maintain documented definitions for each role, including the Security Manager's authority to set mandatory security policy and the Security Administrator's authority to apply and maintain controls across ESInet and NGCS components. Personnel receive role notification through onboarding materials, training records or policy acknowledgements so each individual is aware of assigned responsibilities.

Each security role is supported by formal role definitions that describe:

- Scope of responsibility
- Decision-making authority
- Escalation rights
- Interfaces with State or jurisdiction representatives

For example:

The Security Manager has authority to establish and approve security policies and standards for all NG911 systems operated under the contract.

The Security Administrator has authority to configure and enforce controls across NGCS applications, ESInet routing and transport, boundary devices (SBCs/BCF/B2BUAs), and management platforms, consistent with approved policy.

Personnel Awareness and Acknowledgement. Lumen ensures personnel are informed of their security responsibilities through formal processes, including:

- Security onboarding materials specific to NG911 services
- Role-based security training
- Policy acknowledgement and attestation records
- Ongoing refresher training tied to updated standards or threat conditions

Records of training completion, acknowledgements, and attestations are retained and made available for audit upon request.

Data Ownership Register. Lumen maintains a Data Ownership Register that maps every NG911 data set – local and remote – to an assigned Data Owner. For each data set, the register documents:

- Data description and system location
- Classification level (e.g., sensitive, restricted, mission-critical)
- Regulatory considerations (e.g., HIPAA, CJIS where applicable)
- Handling, retention, and authorized use requirements

The Data Ownership Register is reviewed periodically and updated as systems or data flows change.

Data Custodianship Register. A complementary Data Custodianship Register maps each NG911 data set, both at rest and in transit, to one or more Data Custodians. For each data set, the register identifies:

- Operational security measures applied
- Encryption mechanisms and key management touchpoints
- Access administration responsibilities
- Backup, recovery, and secure deletion controls

This register ensures clear operational accountability for protecting NG911 data throughout its lifecycle.

Security Administration Procedures. Lumen maintains documented security administration procedures that describe how the Security Administrator implements and sustains controls across:

- NGCS applications and databases
- ESInet transport, routing, and segmentation
- Edge devices (SBCs, BCFs, gateways)
- Management, monitoring, and reporting portals

Procedures cover access provisioning, configuration management, logging enablement, vulnerability remediation coordination, and verification of control effectiveness.

Audit Governance Plan. The Security Audit Manager operates under a documented audit governance plan that defines:

- Audit cadence: periodic internal reviews and independent third-party assessments
- Scope: NGCS applications, ESInet infrastructure, security controls, and operational processes
- Reporting: formal findings with severity/risk ratings
- Remediation tracking: documented corrective actions tracked to closure

Audit outcomes are reviewed with executive security leadership and, where contractually required, shared with the jurisdiction.

Continuity and Role Coverage Procedures. To ensure uninterrupted security oversight, Lumen defines role coverage and delegation procedures that:

- Identify approved alternates for each required security role
- Ensure temporary delegation during absence or transition
- Preserve single-point accountability for every responsibility

Delegation is documented, time-bound, and subject to the same access and authentication controls as primary role assignments.

External Parties and Prime Contractor Accountability. Where third parties (e.g., network carriers, cloud service providers, managed security services, subcontractors) perform security-relevant duties:

- Responsibilities are explicitly assigned through contracts, policies, and service level agreements (SLAs).
- Lumen retains accountability as the prime provider.
- Verification mechanisms include:
 - Formal attestations

- SLA performance reporting
- Compliance evidence (e.g., audit reports)
- Right-to-audit provisions where applicable

Lumen actively oversees and validates third-party role fulfillment to ensure continuous alignment with NG911 security requirements.

We maintain a data ownership register that maps every NG911 dataset, local or remote, to a Data Owner responsible for classification and handling. A data custodianship register maps each dataset at rest and in transit to a Data Custodian and identifies encryption, key management, access control and backup processes they manage. Security administration procedures describe how controls are implemented and maintained in accordance with NG911 security policies.

Our audit governance plan identifies audit cadence, internal and external scope, finding severity rating and closure tracking, and the Security Audit Manager administers this plan. Role coverage procedures ensure continuity during absences while preserving single point accountability. Where external parties perform functions, we maintain contractual or policy evidence assigning responsibilities to those entities and use mechanisms such as attestations, SLAs or right to audit provisions to verify fulfillment.

5.4.1.2. IDENTITY MANAGEMENT

The contractor must operate a standards-based Public Key Infrastructure (PKI) to uniquely identify and authenticate every participating agency and agent across all NGCS and ESInet interfaces. An agency's identity must be a globally unique FQDN (e.g., `erie.psap.ny.us`) encoded in the X.509 `SubjectAltName` (SAN). An agent's identity must use the `user@agencyfqdn` format (e.g., `nancy@erie.psap.ny.us`) and be encoded in the SAN of the agent certificate.

*For PSAPs and 911 Authorities, the **PSAP Credentialing Agency (PCA)** is the **root of trust** for agency and agent certificates. The trust chain may include **national** → **state** → **agency/PSAP CAs**. Issuance may be performed directly by the PCA or by approved subordinate CAs under that chain. Any issuing authority must operate under a formal **Certificate Policy/Certification Practice Statement (CP/CPS)** with documented identity proofing and issuance controls. If an agency cannot meet those controls, it must use a **managed CA** that enforces the CP/CPS.*

*Private keys must be safeguarded in **FIPS 140-2** validated cryptographic modules at these minimum levels: **Level 2** for agency private keys (**Level 3 preferred**), **Level 3** for agency CA keys, and **Level 4** for state/national CA keys. **Certificate-based authentication (e.g., mTLS)** must be enforced so that valid identities and credentials are required for access to **all** NGCS/ESInet services and data (e.g., SIP signaling, APIs, management portals, interconnects).*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An identity and certificate schema showing agency FQDN conventions and agent identifier format (`user@agencyfqdn`), with confirmation these identifiers appear in X.509 SAN fields for agency and agent certificates.

- A PCA/PKI trust architecture (diagram & narrative) showing the PCA root, any national → state → agency CA tiers, and permitted subordinate issuing models (e.g., PSAP/Authority issuing agent certs).
- A current CP/CPS (or binding reference) for each issuing authority, defining identity proofing, issuance, renewal, revocation, auditing, and key management; state who operates each CA (Respondent, State, third party) and how compliance is enforced.
- Key protection evidence demonstrating FIPS 140-2 validation and deployment at required levels:
 - Agency private keys: Level 2 minimum (note if Level 3 is implemented).
 - Agency CA keys: Level 3
 - State/National CA keys: Level 4
- Key protection evidence should include device inventories, validation certificates, hosting locations, and any escrow arrangements.
- Access control enforcement description confirming certificate-based authentication (e.g., mTLS) is required for all NGCS/ESInet services and data, where enforcement occurs (interfaces, APIs, signaling paths), and how failed, expired, or revoked certificates are detected and blocked.
- Certificate profiles and samples (agency and agent): SAN contents, Key Usage/EKU, validity periods, revocation mechanisms (CRL/OCSP), and sample chains validating to the PCA.
- Operational lifecycle procedures for issuance, renewal, suspension/revocation, replacement, and compromise response; include joiner/mover/leaver workflows for agents and rollover plans for CA keys.
- Contingency approach if an entity cannot securely operate a CA (e.g., use of a managed CA aligned to the CP/CPS), including contractual controls, SLAs/SLOs, and audit rights.

LUMEN RESPONSE:

Lumen will provide a PKI architecture that uniquely identifies and authenticates every participating agency and agent across ESInet and NGCS interfaces using the required FQDN and user@agencyfqdn conventions in the SAN field of agent certificates. Our PKI is rooted in the PCA trust chain, supports national to state to agency CA tiers where required, and uses issuing authorities that operate under documented CP or CPS controls. We protect private keys with FIPS 140-2 validated cryptographic modules at the levels specified by the State and enforce certificate based authentication using mTLS across all NGCS and ESInet services.

We summarize the requirements and our corresponding approach in **Table 5.4.1.2-1**.

Table 5.4.1.2-1 Lumen's Identity Management Approach.

Requirement	Lumen Approach
Identity and certificate schema using agency FQDN and user\@agencyfqdn in X.509 SAN fields	We define agency identities as globally unique FQDNs and encode them in the SAN of agency certificates, and we define agent identities in the user@agencyfqdn format and encode them in the SAN of agent certificates.

PCA and PKI trust architecture including national, state and agency CAs	We implement a PCA rooted trust architecture that can include national, state and agency CA tiers, with issuance performed by the PCA or approved subordinate CAs operating under the same trust chain.
CP or CPS for each issuing authority with defined identity proofing and lifecycle controls	We maintain or reference a CP or CPS for each issuing authority, describing identity proofing, issuance, renewal, revocation, auditing and key management, and identify who operates each CA and how compliance is enforced.
FIPS 140-2 key protection levels for agency, agency CA and state or national CA keys	We deploy agency private keys in FIPS 140-2 Level 2 modules, note where Level 3 is used, deploy agency CA keys in Level 3 modules and deploy state or national CA keys in Level 4 modules, supported by device inventories, validation evidence and hosting details.
Certificate based authentication using mTLS for all NGCS and ESInet services and data	We require certificate based mTLS for access to NGCS and ESInet services and data, describe where enforcement occurs on interfaces, APIs and signaling paths, and document how failed, expired or revoked certificates are detected and blocked.
Certificate profiles and sample chains validating to the PCA	We define certificate profiles for agency and agent certificates, including SAN contents, key usage and EKU, validity periods and CRL or OCSP based revocation, and provide sample certificate chains that validate to the PCA.
Operational lifecycle procedures for certificate and key management	We document issuance, renewal, suspension, revocation, replacement and compromise response procedures, including joiner, mover and leaver workflows for agents and CA key rollover plans.
Contingency approach using a managed CA when an entity cannot securely operate a CA	We support use of a managed CA aligned to the applicable CP or CPS and governed by contracts, SLAs or SLOs and audit rights when an agency cannot securely operate its own CA.

Identity Model and Certificate Schema. Lumen's NG911 identity model is based on globally unique, DNS-resolvable identifiers encoded in X.509 certificates and enforced through certificate-based authentication mechanisms.

■ **Agency Identity**

Each PSAP or 911 Authority is identified by a globally unique Fully Qualified Domain Name (FQDN) (e.g., erie.psap.ny.us).

- The agency FQDN is encoded in the Subject Alternative Name (SAN) field of the agency certificate.
- The FQDN is used consistently across SIP signaling, APIs, interconnects, and management interfaces.

■ **Agent (User) Identity**

Individual agents are identified using the format user@agencyfqdn (e.g., nancy@erie.psap.ny.us).

- The agent identifier is encoded in the SAN field of the agent certificate.

- Agent certificates are bound to individual users and are never shared.

This identity schema ensures global uniqueness, interoperability across ESInets, and consistent authorization decisions throughout the NG911 environment.

Identity Lifecycle Management. Identity lifecycle management is enforced through formal Identity Management (IDM) processes that govern user and agency onboarding, modification, and de-provisioning. User identities are provisioned through controlled workflows with appropriate approvals, role assignment, and periodic review. Authentication mechanisms integrate Single Sign-On (SSO) and multi-factor authentication, where applicable, and are used to unlock private keys associated with agent certificates for secure session establishment.

For PSAPs and 911 Authorities, the PCA serves as the root of trust for agency and agent credentials. The Contractor supports a hierarchical PKI trust model consistent with NENA guidance, including national, state, and agency tiers. PCA-compliant certificates are issued and managed using an approved Certificate Authority operating under the PCA Certificate Policy and Certification Practice Statement (CP/CPS). The Contractor supports the use of DigiCert as a PCA-approved Certificate Authority for issuing and managing agency and agent certificates, providing a managed CA capability for entities that do not operate their own CA infrastructure.

The PCA trust hierarchy and certificate issuance model is illustrated in **Figure 5.4.1.2-1**.

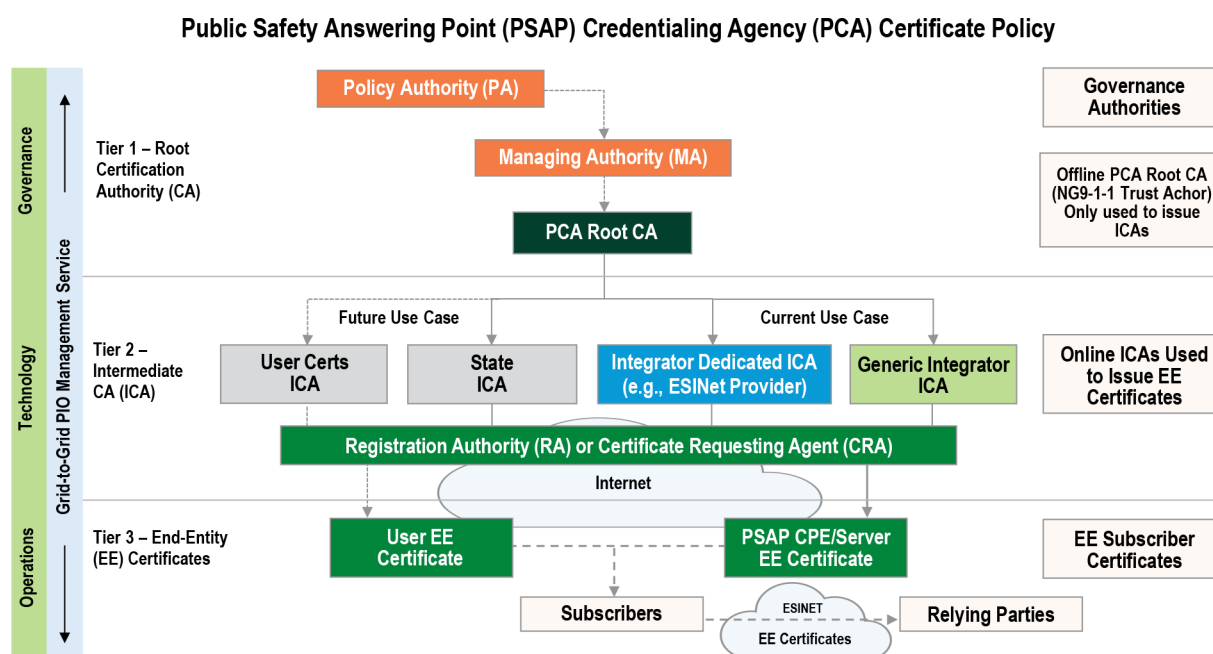


Figure 5.4.1.2-1. PCA Trust Hierarchy and Certificate Issuance Model

Certificate-based authentication is enforced for access to NGCS and ESInet services and data. Mutual TLS (mTLS) is required for service-to-service, agency-to-service, and agent-to-service communications, including SIP signaling, data interfaces, APIs, and administrative access points. Certificates are validated against the PCA trust chain, and expired, revoked, or non-compliant credentials are automatically denied access.

Authorization decisions are enforced independently of authentication and are based on identity attributes, assigned roles, and applicable access policies. This ensures that authenticated entities are permitted to access only those services and data required to perform their authorized functions, supporting the principle of least privilege across the system.

All cryptographic keys are protected in accordance with FIPS 140-2 requirements. Data is encrypted in transit using industry-standard cryptographic protocols and strong cipher suites, and encryption controls are enforced at network, application, and interconnection boundaries to protect sensitive operational and emergency services data.

PCA / PKI Trust Architecture. Lumen's trust architecture follows the NENA i3 model and the approach, where the PSAP Credentialing Agency (PCA) serves as the root of trust for NG911 identities.

■ Root of Trust

- The PCA is the authoritative root for PSAP and 911 Authority identities.

■ Trust Chain Structure

- The trust chain may include national → state → agency/PSAP Certificate Authorities
- Subordinate issuing authorities may be operated by:
 - The PCA directly
 - A state-designated CA
 - An approved managed CA operating under the PCA trust chain

■ Issuance Models

- PSAPs or Authorities may issue agent certificates if they meet CP/CPS and key-protection requirements.
- Agencies unable to meet those requirements must use a managed CA that enforces the approved CP/CPS.

Lumen interoperates with PCA-issued and PCA-approved certificates and enforces trust validation at all NGCS and ESInet boundaries.

Certificate Policy / Certification Practice Statement (CP/CPS). All issuing authorities within the trust chain operate under a formal Certificate Policy / Certification Practice Statement (CP/CPS) that defines:

- Identity proofing and validation requirements
- Certificate issuance and renewal procedures
- Revocation and suspension processes
- Audit and compliance controls
- Key generation, storage, and lifecycle management

For each CA in the trust chain, Lumen will identify:

- The operating entity (Respondent, State, or approved third party)
- The applicable CP/CPS or binding reference
- The enforcement and audit mechanisms used to ensure compliance

Where a managed CA is used, contractual controls require adherence to the CP/CPS, defined service levels, and audit rights.

Key Protection and Cryptographic Controls. Lumen enforces strong private-key protection consistent with NG911 security requirements.

- Agency Private Keys
 - Protected in FIPS 140-2 Level 2 validated cryptographic modules (Level 3 implemented where available).
- Agency CA Private Keys
 - Protected in FIPS 140-2 Level 3 validated hardware security modules (HSMs).
- State / National CA Private Keys
 - Protected in FIPS 140-2 Level 4 validated HSMs.

Key protection evidence includes:

- Device inventories and hosting location
- FIPS validation certificates
- Key custody and access controls
- Any escrow or recovery arrangements (where permitted by policy)

Certificate-Based Access Control Enforcement. Certificate-based authentication is mandatory for access to all NGCS and ESInet services and data.

- Enforcement Mechanisms
 - Mutual TLS (mTLS) is enforced for:
 - SIP signaling between trusted NG911 elements
 - REST and API interfaces
 - Inter-ESInet connections
 - Management and administrative portals
- Validation Controls
 - Certificates are validated against the PCA trust chain
 - SAN values are verified against expected agency and agent identifiers
 - Certificate status is checked using CRLs and/or OCSP
- Failure Handling
 - Expired, revoked, untrusted, or malformed certificates are automatically rejected
 - Access attempts are logged and surfaced through security monitoring systems

Certificate Profiles and Samples. Lumen supports standardized certificate profiles for both agency and agent certificates, including:

- SAN contents (agency FQDN, user@agencyfqdn)
- Key Usage and Extended Key Usage (EKU) appropriate for SIP, TLS, and API authentication
- Validity periods aligned with operational risk and renewal practices
- Revocation mechanisms using CRL and OCSP
- Sample certificate chains validating to the PCA root

Operational Lifecycle Management. Lumen supports full certificate lifecycle operations, including:

- Issuance and enrollment
- Renewal and rotation
- Suspension and revocation
- Replacement following compromise
- Joiner / mover / leaver workflows for agents
- Planned rollover procedures for CA keys

Incident response procedures address certificate compromise, unauthorized access attempts, and rapid revocation to maintain trust integrity.

Contingency for Agencies Unable to Operate a CA. If an agency cannot securely operate its own CA:

- The agency must use a PCA-approved managed CA
- Managed CA services operate under the approved CP/CPS
- Contracts define:
 - Service level objectives (SLOs)
 - Incident response timelines
 - Audit and compliance rights
 - Revocation and recovery procedures

This approach ensures consistent security posture while reducing operational burden on PSAPs and Authorities.

We maintain lifecycle procedures for issuance, renewal, suspension, revocation, replacement, compromise response, and agent joiner or leaver workflows, and we support CA key rollover within the defined trust hierarchy. When an entity cannot securely operate a CA, we support the use of a managed CA that aligns with the applicable CP or CPS and is governed by contractual controls, service levels, and audit rights.

5.4.1.2.1. Roles

Every **agency** and **agent** must authenticate with an X.509 certificate that asserts one or more roles used for authorization.

- **Agency roles** define organizational authority, optionally constrained by **scope**.
- **Agent roles** define individual privileges and may include **modifiers** as identified in NENA-STA-010.3
- §5.3.

Role assignment for any agency or agent must be **approved and limited by the immediately superior agency's policy**. Solutions may support local roles, but **full functionality must work with baseline roles and scopes** for mutual aid and roaming. Roles must be **encoded in certificates** (role OIDs/attributes per profile) and **enforced at NGCS/ESInet interfaces**.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A role model and governance describing agency role, agent roles, and allowed scopes, including how the immediately superior agency approves/limits assignments and how those policies are enforced.
- Role encoding specification for X.509 showing exactly how roles/modifiers/scopes are carried (e.g., OIDs or SAN/subject attributes) with minimal sample certs limited to the role fields and a description of validation during authentication.
- An authorization design that consumes certificate-asserted roles to make access decisions across NGCS/ESInet services, with least-privilege mappings from each role (and modifier) to permissions.

- Evidence of baseline role coverage showing agencies exist that assume all baseline agency roles and that no custom roles are required for full system functionality.
- A role registry integration plan (reference NENA-STA-010.3 §10.27 & §10.28) describing how the solution references the Agency and Agent Role registries, maps them to authorization objects, and process registry updates.
- Role lifecycle controls: request to and approval by the superior agency, assignment changes, revocation, and timely de-provisioning; include joiner/mover/leaver workflows for agents' roles.
- Operational procedures for modifiers showing how modifiers adjust privileges without creating new base roles.
- Monitoring and audit showing how role use is logged, reviewed, and tied back to the approving superior agency; include alerts for unauthorized role elevation.
- Exception handling for temporary/emergency role increases: approval, time bounds, logging, and revocation; include how conflicts between local custom roles and baseline roles are resolved while keeping services available.

LUMEN RESPONSE:

Lumen provides a standards-based role authentication and authorization model for Nebraska's ESInet and NGCS that uses X.509 certificate-asserted roles to enforce consistent, interoperable access control across all interfaces. The model aligns with NENA-STA-010.3 and applies least-privilege authorization based on agency authority, individual agent privileges, defined scopes, and approved modifiers.

Role Model and Governance. Lumen's role model differentiates between agency roles, which define organizational authority, and agent roles, which define individual privileges. All role assignments, scopes, and modifiers are constrained by, and require approval from, the immediately superior agency, ensuring alignment with State and PSAP governance policies and preventing unauthorized privilege escalation.

To ensure role assertions are consistently validated and enforced across the NG911 environment, Lumen implements certificate-based role encoding and authorization using the following mechanisms:

- **Role Encoding in X.509 Certificates.** Agency roles, agent roles, scopes, and modifiers are encoded directly within X.509 certificates using approved NENA-STA-010.3 certificate profiles and role object identifiers. Roles are asserted at authentication time and consumed uniformly by NGCS and ESInet interfaces.
- **Authorization Using Certificate-Asserted Roles.** Authorization decisions are enforced using roles extracted during mutual TLS authentication. Each asserted role and modifier is mapped to defined permissions and enforced at every service request across NGCS services, ESInet interfaces, APIs, management portals, and inter-ESInet connections in accordance with least-privilege principles.

Baseline Role Coverage and Interoperability. Lumen supports the complete set of baseline agency and agent roles defined by NENA-STA-010.3. All NG911 functionality operates using baseline roles without requiring custom roles for core operations, interoperability, roaming, or mutual-aid scenarios. Where local or custom roles are supported for jurisdiction-specific use cases, baseline roles remain authoritative to preserve interoperability.

To ensure alignment with national standards and future extensibility, Lumen integrates role governance with NENA-defined registries and lifecycle controls as follows:

- **Role Registry Integration.** The Agency Role Registry and Agent Role Registry defined in NENA-STA-010.3 are treated as authoritative sources for baseline roles and modifiers. Registry identifiers are mapped to internal authorization objects without semantic modification, and updates are incorporated through controlled configuration management while preserving backward compatibility.
- **Role Lifecycle Controls.** Lumen supports full lifecycle management for role request, approval, assignment, modification, revocation, and de-provisioning. Joiner, mover, and leaver workflows are enforced through certificate issuance, update, and revocation processes to ensure access reflects current authorization status at all times.

Modifier Handling. Role modifiers are used to adjust privileges within an approved base role without creating new role definitions. Modifiers are encoded in certificates, validated at runtime, and constrained by superior-agency policy so defined privilege boundaries are never exceeded.

Operational accountability is maintained through continuous visibility and formal audit controls implemented across the NGCS and ESInet:

- **Monitoring and Audit.** All role-based access decisions are logged with certificate identity, asserted role and modifier, requesting interface, timestamp, and approving agency. Logs support audit review, traceability to the authorizing entity, and automated alerting for unauthorized role assertions or attempted privilege escalation.
- **Exception Handling for Temporary or Emergency Privileges.** Temporary or emergency role elevations require explicit superior-agency approval, defined validity periods, comprehensive logging, and automatic revocation upon expiration or early termination. Baseline roles take precedence over any local custom roles to preserve interoperability and service availability.

These controls ensure that role assignments and authorization decisions across Nebraska's NGCS and ESInet remain controlled, auditable, interoperable, and fully aligned with State NG911 governance requirements, while supporting both current operational needs and future standards-driven role enforcement.

5.4.1.3. POLICIES AND PROCEDURES

*The contractor must maintain a comprehensive cybersecurity policy framework for **NGCS platforms** and the **ESInet**. Policies may be separate or consolidated, but each required area must have clear **purpose, scope, roles, approval, version control, distribution, and compliance expectations**. Policies must be **approved, communicated to personnel**, and **reviewed and/or updated on a defined cadence** (at least annually or upon material change) to reflect new and emerging technologies, threats, and processes.*

*Policies must **flow down** to vendors/contractors/subcontractors and be backed by **Standard Operating Procedures (SOPs)** that turn policy into repeatable tasks. (e.g., user onboarding, vendor remote access, incident handling, recovery). SOPs must be created, kept current, and used in daily operations.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Policy governance covering ownership, approval authority, versioning, distribution/acknowledgement, training, and review/update cadence.*
- *A policy inventory (or consolidated policy) including, at minimum, the policies identified in NENA-STA-040.2 §4.1.2.*
- *Contractual flow-down language proving applicable policies bind all vendors, contractors, and subcontractors supporting NGCS/ESInet.*
- *A complete SOP catalog mapped to the above policies.*
- *SOP governance describing authorship, approval, version control, authoritative storage, and periodic update cycle; include triggers for out-of-band updates (e.g., new technology implementation or threat vectors)*
- *Training and attestation evidence showing personnel have been informed of relevant policies and procedures.*
- *Compliance and exception processes describing how adherence is monitored; how exceptions/waivers are requested, risk-assessed, time-bounded, approved; and how they are revisited/closed.*
- *Cross-references showing how policies and SOPs align with the Risk Management program and Incident Response, ensuring non-compliance items route to corrective action and/or formal risk acceptance.*

LUMEN RESPONSE:

Lumen maintains a comprehensive, standards-based cybersecurity policy framework governing all NGCS platforms and the ESInet. This framework defines required policy elements, establishes ownership and approval authority, enforces version control and distribution, and requires review at least annually or upon material change. Policies are operationalized through Standard Operating Procedures and flow down contractually to all vendors and subcontractors supporting Nebraska's NG911 environment. Lumen's cybersecurity policy framework provides the State the following capabilities:

- **Policy Governance and Oversight.** Each NG911 security policy is assigned a designated owner and approval authority. Lumen enforces version control, controlled distribution, personnel acknowledgement, training integration, and scheduled annual or change-driven reviews to ensure policies remain current as technologies, threats, regulations, and standards evolve.
- **Comprehensive Policy Inventory.** Lumen maintains a complete inventory of cybersecurity policies aligned with NENA-STA-040.2 §4.1.2. Required control domains are addressed through either individual policies or a consolidated policy set, ensuring complete coverage of NG911 cybersecurity requirements.
- **Contractual Flow-Down To Vendors And Subcontractors.** Applicable security policies and requirements are incorporated contractually into all vendor, contractor, and subcontractor agreements supporting NGCS and ESInet operations. Compliance obligations, audit rights, remediation requirements, and corrective actions are clearly defined and enforceable.
- **Standard Operating Procedure (SOP) Catalog.** Lumen maintains a comprehensive SOP catalog directly mapped to the cybersecurity policy framework so that each policy is supported by corresponding, repeatable operational procedures. SOPs translate policy intent into consistent daily execution across operational, administrative, and security functions.

- **SOP Governance and Maintenance.** SOPs are governed with defined authorship, approval authority, version control, and authoritative storage. Procedures are reviewed on a defined cadence and updated when triggered by new technologies, operational changes, emerging threats, standards updates, or lessons learned from incidents and exercises.
- **Training and Attestation.** Personnel supporting NGCS and ESInet operations receive role-based training aligned to applicable policies and SOPs. Formal attestation records are maintained to confirm acknowledgement and understanding, supporting accountability and audit readiness.
- **Compliance Monitoring and Exception Management.** Lumen monitors adherence to policies and SOPs through audits, reviews, and operational metrics. A documented exception and waiver process governs requests, risk assessments, approvals, time-bounded exceptions, periodic review, and formal closure.
- **Alignment With Risk Management and Incident Response.** Cybersecurity policies and SOPs are explicitly cross-referenced to Lumen's Risk Management and Incident Response programs. Non-compliance findings are routed to corrective action plans or formal risk acceptance, and incident response procedures reference governing policies to ensure coordinated and repeatable actions.

This framework ensures Nebraska receives a governable, auditable, and enforceable cybersecurity policy structure that supports secure NGCS and ESInet operations while remaining aligned with NENA standards and State NG911 governance requirements.

5.4.1.3.1. Incident Response Plans

*Early detection and disciplined response are essential to protect NG911 operations. Detection should use tooling (e.g., SIEM, IDS/IPS) and informed personnel, with trained staff triaging scope and impact. The contractor must maintain a formal, written **Cybersecurity Incident Response Plan (CIRP)** that is adaptable, periodically evaluated and tested, and staffed by trained responders. The CIRP should follow **Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity** and define when and how to engage external resources.*

*Because NG911 must continue answering calls and dispatching responders even under attack, recovery planning must be rigorous. The contractor must maintain **Business Continuity (BC)** and **Disaster Recovery (DR)** plans (separate or combined; separate recommended), store all plans offline yet accessible to recovery teams, and review/test at least annually, updating plans as needed.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A CIRP aligned to Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity, with incident declaration/classification criteria and communications/notification procedures.
- Detection capabilities and processes showing how SIEM, IDS/IPS, and staff reports enable early detection; include triage workflows, severity classification, and criteria to escalate to incident status.
- Training and exercise evidence for personnel with plan duties and proof the CIRP is tested (tabletop/live); include after-action reviews and documented improvements.

- *A Business Continuity (BC) Plan for maintaining critical services during and after disruption.*
- *A Disaster Recovery (DR) Plan detailing IT restoration and coordination with ongoing mission-critical operations.*
- *Plan maintenance & accessibility controls proving CIRP/BC/DR are maintained offline yet readily accessible to recovery teams, with clear ownership, version control, and distribution.*
- *Review and test cadence showing at least annual reviews/tests of CIRP/BC/DR, with triggers for interim updates and documented results.*
- *Containment and recovery playbooks/SOPs translating plans into actionable steps for common scenarios (malware/ransomware, denial of service, critical service outage), including initial containment, eradication, service restoration, and lessons learned.*
- *External assistance procedures specifying when/how outside help is engaged, required approvals, and current contact lists/resources.*

LUMEN RESPONSE:

Emergency Call Routing Function (ECRF) and Location Validation Function (LVF). Lumen deploys independent, redundant ECRF and LVF capabilities for Nebraska that conform to NENA-STA-010.3 and operate on identical authoritative datasets sourced from the Location Database. Internal ECRF/LVF services support ESInet and NGCS traffic, while external ECRF/LVF services are accessible to i3 Originating Service Providers and other authorized external systems. This architecture ensures consistent routing and validation outcomes regardless of query origin. Our solution provides the State the following capabilities:

- **Internal and External Implementations with Identical Data.** Internal and external ECRF/LVF environments are continuously synchronized so both operate on the same authoritative data and produce consistent validation and routing results. Each environment is deployed with redundancy and fault isolation to avoid single points of failure and preserve service continuity during maintenance or unplanned events.
- **Standards-Based LoST Query Support and Interjurisdictional Synchronization.** External ECRF/LVF services support both iterative and recursive LoST query modes in accordance with NENA-STA-010.3. Support includes responder type handling, service URNs, and LoST-based synchronization with the National Forest Guide and interconnected ESInets when required for interjurisdictional routing.
- **Spatial Interface Provisioning and Rapid Update Propagation.** Authoritative GIS and routing updates are provisioned through a Spatial Interface conforming to NENA-STA-010.3. Updates propagate to internal and external ECRF/LVF services within seconds of application, ensuring timely alignment between authoritative data maintenance and live routing behavior.
- **Capacity, Rate Controls, and Load Protection.** Internal ECRF/LVF services are engineered for high-volume NG911 routing and validation workloads, including support for valid location shapes defined by applicable geospatial standards. External query services support large aggregate query volumes across civic and geodetic inputs while enforcing per-querier rate limits and adaptive protections to prevent sustained excessive load from impacting NG911 operations.
- **Availability Targets and Operational State Visibility.** Availability objectives are met through geographically redundant deployments, active-active clustering where appropriate, and monitored failover paths. ElementState and ServiceState interfaces are

exposed so the State may subscribe to status changes, monitor service health, and ensure validation and routing functions remain within required service levels for Nebraska NG911 call handling.

Incident Response, Business Continuity, and Disaster Recovery. Lumen maintains formal, written, and operationally mature Cybersecurity Incident Response, Business Continuity, and Disaster Recovery plans designed to protect NG911 operations and ensure the continuous ability to answer emergency calls and dispatch responders, even during cyber incidents or disruptive events. These plans are integrated with NGCS and ESInet architectures and are exercised, governed, and updated on a defined cadence. Our approach provides the State the following capabilities:

- **Cybersecurity Incident Response Plan (CIRP).** Lumen's CIRP follows an industry-recognized lifecycle and is tailored specifically to NGCS platforms and the ESInet. The plan defines preparation, detection and analysis, containment and eradication, recovery, and post-incident activities, including roles, escalation criteria, communication paths, and coordination with legal, forensic, vendor, and government resources when required.
- **Layered Detection and Escalation Capabilities.** Incident detection is supported through centralized monitoring, SIEM correlation, IDS/IPS controls, and network and application telemetry, combined with defined triage and escalation workflows to rapidly assess severity, scope, and potential NG911 service impact.
- **Training, Exercises, and Continuous Improvement.** Personnel with incident response responsibilities receive role-based training and participate in regular tabletop or live exercises. After-action reviews document lessons learned, corrective actions, and improvement tracking to closure.
- **Business Continuity Planning.** Lumen's Business Continuity Plan identifies critical NG911 functions and dependencies and defines strategies to sustain call intake, routing, and dispatch during and after disruptive events. The plan aligns operational coordination across technical teams and State stakeholders with ESInet and NGCS redundancy designs.
- **Disaster Recovery Planning.** The Disaster Recovery Plan defines recovery time objectives and recovery point objectives, prioritizes restoration sequencing for NGCS and ESInet components, and coordinates recovery activities with live NG911 operations to avoid service disruption during restoration.
- **Plan Governance, Accessibility, and Maintenance.** CIRP, BC, and DR plans are governed with clear ownership, version control, and controlled distribution. Plans are stored offline yet remain readily accessible to authorized recovery teams. Plans are reviewed and tested at least annually and upon triggers such as significant technology changes, emerging threats, or material incidents, with outcomes documented and tracked.
- **Containment and Recovery Playbooks.** SOPs and playbooks translate plans into actionable steps for common scenarios, including malware or ransomware events, denial-of-service attacks, and critical infrastructure outages. Each playbook defines containment actions, remediation steps, service restoration procedures, and post-incident review activities.
- **External Assistance Coordination.** Clear procedures govern when and how external assistance is engaged, including required approvals, escalation paths, and maintained

contact lists for security specialists, technology vendors, and legal or regulatory coordination resources.

5.4.1.4. AUTHORIZATION AND DATA RIGHTS MANAGEMENT

The contractor must enforce **XACML 2.0-based authorization** for all NG911 interfaces and protected data. Policies must evaluate **subject, resource, action, and context attributes**; be stored in a **Policy Store** (§E-2.2.1.1); decided by a **Policy Decision Point (PDP)**; and enforced at a **Policy Enforcement Point (PEP)**. Interfaces and data must use consistent names (NENA-STA-010.3 §10, et seq.). Actions must be explicit – **Read, Create, Update, Delete, Execute** – with **permit/deny rules** and an **explicit default rule** for every policy set.

Provisioning data is owned by the agency that operates the element and must be governed by **data rights management**. Each XACML policy must be **packaged as a JWS** and **signed by the policy owner**, including the **signing certificate and full chain** for validation.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Authorization architecture showing XACML 2.0 components, PDP placement, and how authorization is invoked on all NGCS/ESInet interfaces and protected data paths.
- Policy naming conventions & registries usage, including:
 - Interface policy names derived from **ServiceID**, and an interface keyword (NENA-STA-010.3
 - §10.30) formatted **ServiceID~keyword** (e.g., **LoST~ecrf.state.pa.us**)
 - Data item names derived from OpenAPI JSON object names and optional element tags, using dot notation (e.g., **civicAddr.A3**, or **<ido.AgencyDataComponent.AgencyName>**)
 - Mapping to the Policy Type Registry (NENA-STA-010.3 §10.33)
- Action model defining Read, Create, Update, Delete, Execute, with examples showing how each applies to representative Interfaces and data structures.
- Example XACML policy sets for:
 - One or more interfaces
 - One or more data structures
 - Each example policy set provided must include permit/deny rules, an explicit default rule, and attribute conditions (subject/resource/action/date/time as applicable).
- JWS packaging & validation: how the policy owner signs policies; how the certificate and chain are included (by value or reference); how PEP/PDP validate signatures (CRL/OCSP) and how key rotation and revocation are handled.
- Data rights management procedures establishing ownership of provisioning data and how ownership is enforced in policy.
- Policy lifecycle controls: authoring, peer review, change management, pre-production testing/evaluation, promotion, versioning, rollback, archival; include who is authorized to sign and publish policies.
- Logging & auditability: decision logs at PEP/PDP, retention, and procedures for reviewing denied/exception events.

- *Performance & availability targets: PDP availability/latency, decision/policy caching (TTL/invalidations), and fail-secure behavior if policies or validators are unavailable.*

LUMEN RESPONSE:

Lumen will enforce XACML 2.0 based authorization across all NGCS and ESInet interfaces and protected data paths. Our authorization design evaluates subject, resource, action and context attributes, stores policy sets in the Policy Store, renders decisions at the PDP and enforces decisions at the PEP. We use explicit Read, Create, Update, Delete and Execute actions with permit or deny rules and an explicit default rule for every policy set. Provisioning data is governed by the owning agency under data rights management requirements, and each XACML policy is packaged as a JWS signed by the policy owner with the certificate and full chain included for validation. Our approach to each requirement is as follows:

- **Authorization Architecture:** Lumen uses XACML 2.0 with policy sets stored in the Policy Store, decisions evaluated by the PDP and enforced at PEPs across all NGCS and ESInet interfaces and data paths.
- **Policy Naming Conventions and Registry Usage:** Lumen derives interface policy names from the ServiceID and interface keyword in the ServiceID~keyword format and derives data item names from OpenAPI JSON object names using dot notation, mapping all policy sets to the Policy Type Registry as required.
- **Action Model:** Lumen defines Read, Create, Update, Delete and Execute actions and applies them to interface operations and data structures according to XACML semantics.
- **Example Policy Sets:** Lumen provides example XACML policy sets for selected interfaces and data elements, each containing permit or deny rules, an explicit default rule and attribute conditions based on subject, resource, action or context.
- **JWS Packaging and Validation:** Lumen signs each XACML policy as a JWS, includes the certificate and chain by value or reference and validates signatures using CRL or OCSP, supporting key rotation and revocation.
- **Data Rights Management:** Lumen enforces data ownership for all provisioning data through XACML policies that restrict or permit access based on the owning agency's rights.
- **Policy Lifecycle Controls:** Lumen maintains authoring, peer review, change management, pre-production evaluation, promotion, versioning, rollback and archival procedures and identifies authorized policy signers and publishers.
- **Logging and Auditability:** Lumen records authorization decisions at PEP and PDP components, maintains retention for review and examines denied or exception events.
- **Performance and Availability Targets:** Lumen maintains PDP availability and latency targets and supports decision and policy caching with defined TTL and invalidation and implements fail secure behavior when policies or validators are unavailable.

This approach ensures that Nebraska receives a consistent, standards based authorization system capable of protecting NG911 interfaces and data.

5.4.2. Information System Infrastructure and Management

5.4.2.1. DEVICE INVENTORY

*The contractor must maintain a **continuously updated inventory** of all **devices, software/applications, software libraries, data sets, and cloud/third-party services** that support the NGCS platform and the ESInet. Use automated discovery and reconciliation where possible to keep records accurate, quickly identify unauthorized*

items, verify patch/firmware levels, and support zoning/segmentation. If full visibility is limited by span of control or contracts, clearly define what is in scope, assumptions, and responsibilities. Inventory outputs must inform critical impact analysis (BC/DR inputs) and drive trusted vs. untrusted zone design and controls at all ingress/egress points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Inventory management approach describing data sources, automated discovery tools/processes (where used), manual reconciliation, update frequency, and how unauthorized/unknown items are identified and removed or quarantined.
- Scope and span-of-control statement clarifying which assets/services fall under the Provider vs. the Customer or other vendors; include contractual boundaries, dependencies, and any blind spots.
- Comprehensive inventory documentation should identify sufficient detail - at minimum, documenting inventory elements identified in NENA-STA-040.2 §5.4 - for all aspects of NGCS and ESInet infrastructure.
- Classification linkage showing how inventories map to the provider's data classification policy and define required protections.
- Impact analysis methodology showing how the inventory feeds critical impact analysis and integrates with Business Continuity and Disaster Recovery planning
- Zoning/segmentation mapping that uses the inventory to define trusted vs. untrusted zones and sets control placement and rule scope at all ingress/egress points.
- Governance & lifecycle controls for the inventory: ownership, update cadence, audit/attestation of accuracy, change triggers, reconciliation with change management processes, and evidence of periodic cleanup of stale records.

LUMEN RESPONSE:

Lumen maintains a continuously updated, authoritative inventory of all NGCS and ESInet assets supporting Nebraska's NG911 environment. This includes devices, software, applications, software libraries, datasets, and cloud or third-party services. Inventory processes combine automated discovery with manual reconciliation to ensure accuracy, support zoning and segmentation decisions, detect unauthorized or unknown assets, and inform impact analysis and Business Continuity and Disaster Recovery planning.

Inventory Management Approach. Lumen employs a defense-in-depth inventory methodology that uses automated discovery where available and controlled reconciliation to maintain accuracy. Inventory updates occur on a defined cadence and in response to change events, with unauthorized or unknown items flagged for investigation, quarantine, removal, or formal exception handling in accordance with policy.

To ensure clarity and accountability across all NG911 components, Lumen's inventory management addresses the following asset governance requirements:

- **Scope and Span of Control.** Lumen documents which assets and services fall under Lumen management versus those managed by the State or third-party vendors. This includes contractual boundaries, dependencies, assumptions, and any limitations in visibility, with residual risks explicitly identified and managed.
- **Comprehensive Inventory Documentation.** Inventory records are maintained with the level of detail required by NENA-STA-040.2 §5.4 for all NGCS and ESInet infrastructure

elements, including asset type, function, location, ownership, software or firmware versions, interfaces, dependencies, and data sensitivity.

- **Classification Linkage.** Inventory elements are mapped to Lumen's data and system classification policy so required security controls are derived based on classification. Classification informs access controls, monitoring requirements, zoning decisions, and incident response prioritization.

Impact Analysis Integration. Lumen uses the inventory to support critical impact analysis by mapping assets to NG911 services and functions. Dependency relationships and criticality ratings inform Business Continuity strategies and Disaster Recovery sequencing, and inventory updates automatically propagate to BC and DR planning inputs.

To support secure network design, inventory data is actively used to drive zoning and segmentation decisions:

- **Zoning and Segmentation Mapping.** Assets are grouped by trust level, function, and exposure to define trusted and untrusted zones. Inventory attributes determine the placement of security controls, access rules at ingress and egress points, and interface-specific protections between zones. Changes to inventory trigger reassessment of zone placement and control scope.

Inventory Governance and Lifecycle Controls. Lumen enforces defined ownership, update cadence, audit and attestation processes, and reconciliation with formal change management procedures. Periodic reviews identify and remove stale or retired assets, with evidence of cleanup retained to support audit requirements.

This approach provides Nebraska with **accurate, actionable visibility into NG911 assets**, supporting secure, resilient NGCS and ESInet operations and enabling informed governance, impact analysis, and continuity planning.

5.4.2.2. PATCHING AND UPDATE MANAGEMENT

*The contractor must implement a disciplined, **change-managed patching program** covering **firmware, hardware drivers, operating systems, applications, and middleware**. The program must take in vendor, CERT, or other security advisories, use a common severity scale (e.g., Common Vulnerability Scoring System [CVSS]) to set priority, and check the environment for indicators of compromise (IoC) when a vulnerability is disclosed. Patching must be timely and paired with post-patch verification. The program should align with timelines and processes defined in NENA-STA-040.2 §5.5.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A process to validate - at least monthly - that all required patches are installed across in-scope hardware and software (plus event-driven checks upon major vulnerability disclosures).*
- *A change-managed deployment workflow ensuring approved and appropriately tested mitigations/patches are applied as soon as possible, with defined rollback steps.*
- *Post-patch verification to confirm remediation and to check for exploitation and/or other IoCs across the ESInet and NGCS.*

- *A CVSS-based timeline policy that sets SLAs by severity/criticality (e.g., critical expedited; target ≤ 48 hours from disclosure or patch availability), and an emergency change path.*
- *Evidence of advisory intake and triage, including how severity, affected scope, available mitigations, and permanent vs. temporary fixes are evaluated and tracked.*
- *Exception handling with compensating controls when patches cannot be applied immediately, with documented risk acceptance under the Entity's risk management process.*
- *Reporting and metrics showing patch compliance, age of open findings by CVSS band, time-to-patch, and reconciliation with the inventory/CMDB to ensure complete coverage.*

LUMEN RESPONSE:

Lumen maintains a disciplined, change-managed patching program for Nebraska's ESInet and NGCS that aligns with NENA-STA-040.2 §5.5 and covers firmware, hardware drivers, operating systems, applications, and middleware. The program incorporates continuous advisory intake, CVSS-based prioritization, formal change control, post-deployment validation, and integrated reporting to ensure vulnerabilities are remediated promptly without compromising NG911 availability or operational integrity.

Advisory Intake, Triage, and Risk Prioritization. Lumen continuously ingests vendor advisories, CERT notifications, and trusted threat intelligence feeds. Each advisory is evaluated for severity, affected scope, exploitability, and availability of mitigations. CVSS scoring is used to prioritize remediation, and items are tracked through remediation to closure with visibility maintained for operational awareness and auditability.

To ensure patches are applied safely and consistently across the NG911 environment, Lumen executes patch deployment using the following controlled workflow elements:

- **Change-Managed Patch Deployment Workflow.** All patches and mitigations are deployed through a formal, ITIL-aligned change management process that includes approval, testing in non-production environments where applicable, controlled rollout, defined rollback procedures, and documented reconciliation with the asset inventory in the CMDB.
- **Emergency Change Handling.** An emergency change path is available for urgent conditions requiring rapid action to reduce risk to NG911 operations. Emergency changes are documented, reviewed post-implementation, and incorporated into standard change records to maintain traceability.

Post-Patch Verification and Compromise Checks. Following deployment, Lumen verifies successful remediation through service health checks, version validation, and configuration confirmation. The environment is also assessed for indicators of compromise using SIEM correlation, IDS/IPS telemetry, and anomaly detection to confirm the vulnerability has not been exploited.

Patch effectiveness and coverage are continuously validated to maintain confidence in the security posture of the ESInet and NGCS:

- **Monthly and Event-Driven Validation.** Lumen performs at least monthly validation to confirm required patches are applied across all in-scope components. Event-driven

validation is performed when significant vulnerabilities are disclosed, leveraging automated checks, monitoring data, and change records to confirm coverage.

- **Coverage Assurance Across Asset Classes.** Validation includes firmware, drivers, operating systems, applications, and middleware, with reconciliation against the CMDB to identify gaps or drift.

CVSS-Based Timelines and Remediation Expectations. CVSS severity ratings establish internal remediation priorities and timelines:

- Critical vulnerabilities are handled on an expedited basis where operationally feasible.
- High, medium, and low vulnerabilities follow defined remediation targets consistent with risk and exposure.
- Remediation progress is tracked until closure or formal risk acceptance.

Exception Management and Compensating Controls. When a patch cannot be applied immediately due to operational constraints or vendor dependencies, Lumen documents a risk-based exception and applies compensating controls such as segmentation, access restrictions, or increased monitoring. Exceptions are time-bounded, formally approved under the State's risk management process, and reviewed until permanent remediation is completed.

Reporting, Metrics, and Auditability. CMDB-based reporting provides visibility into patch compliance, age of open vulnerabilities by CVSS category, mean time to patch, and reconciliation of patch status against the asset inventory. These metrics support operational oversight, governance reviews, audit readiness, and continuous improvement across Nebraska's NG911 environment.

This patch management approach delivers timely remediation, controlled deployment, and verifiable security improvements while preserving the availability, stability, and integrity required for statewide NG911 operations.

5.4.2.3. SEGMENTATION AND TRAFFIC SEPARATION

*The contractor must implement **domain-level network segmentation** to contain incidents, reduce lateral movement, and improve resiliency. Segmentation may be physical or logical (e.g., firewall-enforced choke points) and should extend to **zero-trust/micro-segmentation** at the endpoint or workload wherever feasible. Production and non-production (test/training) must be strictly separated so non-production activity cannot affect production services. **Development tools are prohibited in the production environment.** Within each environment, distinct traffic classes (e.g., call/signaling, management/monitoring, administrative) must be segregated and filtered (VLANs and/or dedicated equipment) with explicit allow-lists and firewall policy. Management/monitoring traffic must be out-of-band, normal traffic must not use the default VLAN, and configuration access to traffic-handling devices must use administrator-level accounts under appropriate controls.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A segmentation architecture showing production vs. non-production separation, inter-segment demarcation points, and isolation/containment controls.

- *A traffic separation design identifying major traffic classes and how they are segregated and filtered.*
- *Evidence that production is protected from non-production, including controls preventing any non-production impact on production systems, and an explicit statement that no development tools exist in the production environment.*
- *Out-of-band management/monitoring implementation details and confirmation that normal traffic is not on the default VLAN.*
- *Administrative access controls for traffic-handling devices: administrator-level account use, authorization model, MFA, logging, and audit.*
- *Operational procedures/SOPs for change, testing, and validation of segmentation and filtering rules, including onboarding of new services without weakening isolation.*
- *Monitoring & alerting for policy violation and lateral movement detection within/across segments, with procedures for rapid containment.*

LUMEN RESPONSE:

Lumen implements domain-level network segmentation for Nebraska's NG911 environment to contain incidents, reduce lateral movement, and maintain resiliency across the ESInet and NGCS. The segmentation strategy separates production and non-production environments, enforces traffic-class isolation, and applies explicit filtering at defined control points to protect signaling, media, data, and management planes.

Segmentation Architecture. Lumen maintains a segmentation architecture that establishes clear boundaries between environments and functional domains, with controlled interconnections and enforced isolation. Activity within one segment is prevented from affecting services in another segment, limiting blast radius during faults or security events.

Within each environment, traffic separation is enforced using clearly defined controls that address NG911 operational needs:

- **Traffic Separation Design.** Call processing and signaling traffic, management and monitoring traffic, and administrative or support traffic are segregated using VLANs, filtering rules, and dedicated paths or equipment. Each traffic class is handled independently and permitted only where explicitly authorized.
- **Filtering and Policy Enforcement.** Inter-segment communication occurs only at defined, firewall-protected demarcation points. A deny-by-default posture is enforced, with explicit allow rules for approved protocols, ports, sources, destinations, and directions.

Production Environment Protection. Lumen applies strict controls to prevent non-production activity from impacting production NG911 services. Test, training, and development environments are isolated, and development tools are excluded from production systems so testing activity cannot disrupt live call handling.

To preserve separation between operational traffic and administrative access, management and monitoring functions are implemented using dedicated control paths:

- **Out-of-Band Management and VLAN Controls.** Management and monitoring traffic is carried on dedicated out-of-band networks, restricted to authorized systems and personnel. Operational traffic does not traverse default VLANs, and each traffic class uses explicitly defined VLANs or equivalent segmentation constructs.

Administrative Access Controls. Configuration access to routers, firewalls, switches, and other traffic-handling devices is restricted to authorized administrator accounts. Role-based authorization, multi-factor authentication, logging, and audit capabilities are enforced to protect control planes and support accountability.

Segmentation integrity is preserved through formal operational discipline:

- **Segmentation Change and Validation Procedures.** Standard operating procedures govern changes to segmentation and filtering rules. Changes follow formal change control and include testing and validation to ensure new services or modifications do not weaken isolation or containment boundaries.
- **Monitoring, Detection, and Containment.** Lumen continuously monitors traffic flows within and across segments to detect policy violations or attempted lateral movement. Defined procedures enable rapid containment and isolation of affected segments to protect NG911 operations.

This network segmentation approach provides containment, isolation, and operational protection across Nebraska's ESInet and NGCS while supporting resilient, standards-aligned NG911 operations.

5.4.2.4. NETWORK BOUNDARY PROTECTION

Firewalls and Next Generation Firewalls (NGFWs) are key perimeter and inter-segment controls, but they are not the only defense. Internal systems must also be secure. The contractor must deploy a NENA-standard Border Control Function (BCF) or other boundary protections at all ESInet ingress/egress points and each segment entry/exit using explicit allow-lists that document required traffic and block all else. Specific BCF behaviors and requirements are identified in §E-2.1.1 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A boundary architecture showing boundary controls (BCF or NGFW) at all ESInet ingress and segment entry/exit. The BCF must conform to requirements in §E-2.1.1 of this document.*
- *A traffic matrix for each firewall listing required services, ports, and protocols, with explicit allow rules; unnecessary traffic must be blocked by default.*
- *Performance & availability: high availability (HA) and/or failover capability, and traffic inspection features must be configured so boundary protections do not degrade service delivery capabilities.*

LUMEN RESPONSE:

Lumen implements layered boundary protections for Nebraska's NG911 environment using Border Control Function (BCF) and next-generation firewall (NGFW) controls at all ESInet ingress points and at each defined segmentation boundary. These protections restrict traffic to explicitly authorized services, enforce a default-deny posture for all other traffic, and preserve the performance and availability required for NG911 call handling.

Boundary Architecture. Lumen deploys BCF and NGFW controls at every ESInet ingress and egress point and at each inter-segment entry and exit. These boundary devices establish controlled trust boundaries and ensure that no signaling, media, or data flow traverses between environments or segments without passing through an explicitly defined and

monitored enforcement point. Where BCFs are used, they conform to the applicable NGCS and ESInet boundary protection requirements, including protocol normalization, security enforcement, and controlled session handling.

To ensure deterministic control over all permitted communications, boundary enforcement is implemented using documented allow-listing and traffic control mechanisms:

- **Traffic Matrix and Allow-Listing Controls.** Lumen maintains a traffic matrix for each boundary enforcement point that documents authorized services, ports, protocols, and source and destination zones. Boundary devices enforce explicit allow rules derived from these matrices and block all unnecessary or undocumented traffic by default.
- **Change Control for Boundary Rules.** Traffic matrices and allow lists are reviewed, approved, and updated through formal change management processes to ensure continued alignment with operational needs and to prevent unauthorized expansion of permitted traffic.

Performance and High-Availability Design. Boundary protection components are deployed in high-availability or failover configurations so the failure of a single device does not interrupt NG911 call signaling, media flow, or data exchange. Inspection and enforcement features are tuned to balance security with performance and are designed not to introduce latency or degradation that would affect emergency call delivery.

Boundary protections operate as part of a broader, integrated security architecture:

- **Integration with Segmentation and Internal Controls.** Boundary controls complement internal network segmentation, zoning, and policy enforcement mechanisms to limit attack surfaces and prevent lateral movement within the ESInet and NGCS environments.
- **Monitoring and Operational Visibility.** Boundary devices are continuously monitored to detect unauthorized traffic, policy violations, or anomalous behavior, with defined procedures to support rapid investigation and containment.

This boundary protection approach ensures consistent, standards-aligned enforcement across all ESInet and NGCS trust boundaries while preserving the resiliency, performance, and availability required for statewide NG911 operations.

5.4.2.4.1. External Connections

NG911 relies on external connections; with these links often traversing the public internet, they must follow a zero-trust approach (NENA-STA-040.2 Appendix A & NIST Special Publication 800-207) and use layered protections. At minimum, each external connection must be protected by a boundary protection device conforming to requirements identified in §E-5.2.4 above, and any connection transporting sensitive information must use an encryption that conforms with the requirements identified in NENA-STA-040.2 §4.2.2.6 (Safeguarding Sensitive Electronic Information).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *An external connectivity architecture listing counterparties, paths, and media, and how zero-trust principles are applied.*
- *Evidence that all external links are protected by a firewall with placement, explicit allow-lists, and default-deny posture per §E-5.2.4.*

- *An encryption approach for links carrying sensitive information, conforming to requirements of NENA-STA-040.2 §4.2.2.6, indicating where encryption is enforced.*
- *Operational controls for onboarding/approval, continuous monitoring, periodic review, and change/termination of external connections – consistent with zero-trust and boundary protection requirements.*

LUMEN RESPONSE:

Lumen enforces a Zero Trust security model for all external NG911 connections, including those traversing the public internet, so that no external entity, network path, or transport medium is implicitly trusted. All external interfaces are protected using boundary devices consistent with ESInet and NGCS boundary requirements, and sensitive NG911 information carried over these links is protected using standards-aligned encryption.

External Connectivity Architecture and Zero Trust Application. Lumen maintains a documented external connectivity architecture that identifies all approved NG911 counterparties, connection paths, and supported transport media. Zero Trust principles are applied uniformly so trust is never derived from network location, source address, or transport path alone. Every external connection requires authenticated identity, least-privilege authorization, and continuous verification to remain enabled.

To ensure all external connections are tightly controlled and monitored, Lumen applies the following boundary protection measures at every ingress and egress point:

- **Boundary Protections for External Links.** Border Control Function and next-generation firewall controls are deployed at every ESInet ingress point supporting external connectivity. These controls enforce explicit allow lists with a default-deny posture, ensuring only documented and authorized signaling, media, and data flows are permitted to traverse ESInet and NGCS boundaries.
- **Traffic Control and Enforcement Governance.** Boundary configurations, including allow lists and traffic matrices, are documented, reviewed, and maintained under formal change management to prevent unauthorized expansion of permitted access.

Encryption for Sensitive NG911 Information. All external connections carrying sensitive NG911 information, including call signaling, location data, and personally identifiable information, are protected using encryption mechanisms aligned with NG911 security safeguards and NENA-STA-040.2 requirements. Encryption enforcement points are defined at ESInet ingress and egress locations, NGCS inter-service interfaces, OSP and peer-ESInet interconnections, authorized third-party services, and management or monitoring interfaces that transport sensitive operational data.

Media and Control Plane Protection. SIP signaling, real-time media, and supporting control-plane communications are protected using secure, standards-based mechanisms appropriate to each protocol and use case. Traffic is terminated, inspected, and re-established only at trusted boundary components, such as SBCs and other Border Control Functions, to preserve confidentiality and integrity without degrading call quality.

External connectivity is governed through formal operational discipline across its full lifecycle:

- **Operational Controls for External Connections.** Lumen applies documented onboarding, approval, monitoring, periodic review, change management, and

termination procedures for all external connections. Connectivity is enabled only after business need, authorized endpoints, approved paths, protocols, and services are validated.

- **Governance, Auditability, and Lifecycle Management.** Periodic reviews confirm continued necessity, accuracy of allow lists, encryption enforcement, and adherence to least-privilege principles. Changes follow formal change management, termination processes retire access and credentials when no longer required, and all onboarding, changes, reviews, and terminations are logged and auditable.

This Zero Trust external connectivity approach ensures all NG911 connections are authenticated, encrypted, continuously governed, and protected in alignment with Nebraska's security requirements and applicable NENA standards.

5.4.2.4.2. Demilitarized Zones (DMZ)

Some NG911 services must be reachable from untrusted networks. Any externally accessible resource not otherwise protected by equivalent controls must reside in a Demilitarized Zone (DMZ) that is segments from internal NGCS/ESInet segments and mediated by a boundary protection device per §E-5.2.4 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A DMZ architecture showing externally accessible resources, segmentation from internal networks, and firewall/SBC/BCF demarcation points.*
- *A traffic controls strategy for the DMZ: default-deny posture, explicit allow lists, tightly limited ingress/egress, and no lateral access to internal segments.*
- *Hardening & monitoring for DMZ assets: patch cadence, configuration baselines, centralized logging, telemetry, and alerting.*
- *Operational procedures for onboarding and retiring DMZ-hosted services, plus periodic reviews to confirm resources that require external access remain correctly isolated in the DMZ.*

LUMEN RESPONSE:

Lumen implements a demilitarized zone (DMZ) architecture for Nebraska's NG911 environment to protect externally accessible services by isolating them from internal ESInet and NGCS segments. Externally reachable resources are placed in dedicated DMZ segments that are logically and physically separated from trusted internal environments and mediated by boundary protection devices that meet State requirements.

DMZ Architecture and Boundary Demarcation. Externally accessible NG911 services are hosted within segmented DMZ environments that are isolated from all internal ESInet and NGCS networks. Firewall, Session Border Controller (SBC), and Border Control Function (BCF) demarcation points mediate all traffic entering or leaving the DMZ and enforce strict separation between untrusted external networks and internal NGCS functional elements. Only services requiring external reachability are placed within the DMZ, and no internal-only NGCS components reside in externally accessible zones.

To limit exposure and prevent unauthorized access, Lumen enforces strict traffic controls for all DMZ-hosted services:

- **DMZ Traffic Controls and Default-Deny Enforcement.** A default-deny security posture is applied to all DMZ services. Explicit allow lists define permitted ingress and egress traffic, including approved source and destination addresses, ports, protocols, and services. Ingress and egress paths are tightly scoped to required flows only, and lateral movement from the DMZ into internal ESInet or NGCS segments is prohibited unless explicitly authorized and mediated through controlled boundary functions.

Hardening, Patching, and Monitoring of DMZ Assets. DMZ-resident assets are built and maintained using documented configuration baselines aligned with NG911 security standards. Routine patching is performed on a defined cadence, with expedited remediation for critical vulnerabilities affecting externally exposed components. Centralized logging, telemetry collection, and automated alerting provide real-time visibility and support rapid detection of anomalous behavior or security events.

The lifecycle of externally hosted services is governed through formal operational discipline.

- **Operational Procedures for DMZ-Hosted Services.** Defined procedures govern the onboarding, modification, and retirement of DMZ resources. New services are introduced only after validating business need, security controls, segmentation requirements, and boundary rule definitions. Controlled retirement procedures decommission resources, update firewall and SBC rules, and remove access when services are no longer required.
- **Periodic Review and Compliance Validation.** Regular reviews confirm continued necessity of DMZ-hosted services, correct isolation, and compliance with security policies and boundary enforcement requirements.

Defense-in-Depth and Layered Control Validation. The DMZ operates as part of a broader defense-in-depth security model that applies overlapping controls across endpoint hardening, identity and access management, boundary protection, segmentation, and monitoring. Independent and redundant control layers ensure no single point of failure and preserve protective enforcement even during component degradation or attack conditions.

This DMZ architecture ensures that externally accessible NG911 services remain isolated, controlled, and protected, while preserving the resiliency, availability, and operational integrity required for Nebraska's ESInet and NGCS platforms.

5.4.2.4.3. Defense in Depth

The contractor must apply Defense in Depth (DiD) - layered, overlapping controls that protect confidentiality, integrity, and availability across physical access, endpoints, data protection, boundary defenses, network and traffic separation, system monitoring, and (where applicable) vendor diversity. DiD ensures that if one control fails, others maintain security. Critical systems and sensitive information shall utilize Defense in Depth with deliberate redundancy and no single points of failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A DiD architecture showing layered controls across the stack: physical access, endpoints, identity/authorization/authentication, boundary protections, and segmentation/traffic separation.*

- *A control-to-risk mapping for critical systems and sensitive data identifying how multiple independent controls address key threats, with no single-control dependencies.*
- *Failure mode and fallback analysis demonstrating how security is maintained if a layer is bypassed or fails.*
- *Operational integration with related sections (e.g., IAM/roles, segmentation, boundary protections, incident response, logging/monitoring), including runbooks for escalation between layers.*
- *Validation and review evidence and metrics showing layered control effectiveness over time.*

LUMEN RESPONSE:

Lumen applies a Defense-in-Depth (DiD) security model for Nebraska's NG911 environment that layers independent and complementary security controls across the ESInet and NGCS. The model is designed to maintain confidentiality, integrity, and availability even if an individual control is degraded or bypassed, and incorporates protections at the physical, network, system, identity, and monitoring layers with deliberate redundancy for critical systems and sensitive data.

Defense-in-Depth Architecture. Layered security controls are implemented across physical access, hardened endpoints, identity and access management, authorization and authentication functions, boundary protections, and network segmentation. Each layer operates independently so that multiple mechanisms restrict unauthorized access or movement and no single control is relied upon to protect NGCS or ESInet resources.

Control-to-Risk Mapping. Critical systems and sensitive data flows are mapped to multiple distinct security controls at different layers. This mapping demonstrates how relevant threats—such as unauthorized access, signaling abuse, data exfiltration, and denial-of-service conditions—are mitigated through overlapping safeguards rather than a single defensive measure.

Failure Mode And Fallback Analysis. Potential failure or bypass scenarios for individual security layers are analyzed, and fallback behavior is defined to ensure continued protection when a control becomes unavailable. Examples include redundant boundary devices, alternate enforcement points, segmented network paths, and failover monitoring that preserve security posture during component degradation or attack conditions.

Operational Integration Across Security Domains. Defense-in-Depth controls are integrated with identity and access management, role definitions, network segmentation, boundary protections, logging, monitoring, and incident response processes. Operational runbooks define how events detected at one layer are escalated and correlated across other layers to support coordinated response and enforcement.

Validation, Review, And Effectiveness Metrics. Effectiveness of layered controls is validated through continuous monitoring, vulnerability assessments, and periodic security reviews. Metrics such as alert trends, control coverage, incident outcomes, and remediation timelines are used to assess performance over time and inform adjustments to controls, configurations, and procedures as NG911 security risks and standards evolve.

5.4.2.4.4. Remote Access

Remote access connects users to systems outside a physical location. External remote access carries the highest risk and must be allowed only for documented business need, routed through authorized, secured, encrypted connections (e.g., VPN aligned to NIST SP 800-77), and enforced with strong authentication and centralized logging.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Access control & eligibility: Processes ensuring external remote access is granted only for valid business need, with at least annual account reviews and timely removal when no longer required.*
- *Secure connectivity: Use of an authorized, encrypted connection for all external remote access. MFA must be implemented for all remote connectivity.*
- *Operational governance: SOPs for requesting, approving, establishing, and terminating remote access, plus periodic tests/reviews to confirm controls remain effective.*
- *Logging & monitoring: centralized logging for remote connectivity in conformance with minimum requirements identified in NENA-STA-040.2 §6.17.*

LUMEN RESPONSE:

Lumen enforces strict controls for external remote access to Nebraska's NG911 environment to ensure that only authorized users connect using secured, encrypted methods consistent with zero-trust expectations. External remote connectivity is limited to documented business need, routed through approved secure channels, and governed by strong authentication and centralized logging to maintain accountability and auditability.

Access Control And Eligibility. External remote access is granted only when a documented business need exists to support ESInet or NGCS operations, maintenance, or incident response. Eligibility is approved through formal authorization processes aligned with role-based access control and least-privilege principles. Remote access accounts are reviewed at least annually to confirm continued necessity and are promptly removed when access is no longer required, roles change, or personnel separate from the project.

Secure Connectivity And Authentication. All external remote access uses authorized, encrypted connectivity consistent with NG911 security safeguards and industry-recognized secure remote access practices. Multifactor authentication is enforced for every remote session, including administrative, operational, and support access. Remote connectivity terminates at defined, monitored access gateways and does not provide direct connectivity to internal ESInet or NGCS segments.

Operational Governance And Lifecycle Management. Standard operating procedures govern the request, approval, provisioning, modification, and termination of external remote access. Remote access configurations are subject to formal change management processes, including validation of security controls prior to activation. Periodic testing and review activities confirm that remote access mechanisms remain effective and aligned with NG911 security policies.

Logging, Monitoring, And Auditability. All remote access activity, including authentication attempts, session establishment, privilege use, and session termination, is captured through

centralized logging. Remote connectivity is continuously monitored to detect unauthorized access attempts, anomalous behavior, or policy violations. Logging and monitoring practices align with the minimum requirements identified in NENA-STA-040.2 §6.17 to support auditability, incident investigation, and compliance oversight.

5.4.3 Infrastructure Resilience

Mission-critical NG911 functions must remain available despite single-component failures and localized outages. The contractor must employ redundancy and diversity across the ESInet and NGCS, through the deployment of high-availability mechanisms with supported infrastructure where appropriate. Because infrastructure failures can drop in-progress sessions, applications and signaling must gracefully recover during a path or site failure. NGCS/ESInet components must be both redundant and diverse, and ingress traffic must enter the NG911 system through diverse paths. (Additional redundancy guidance in NENA-STA-010.3 §2.9)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *An end-to-end High Availability (HA) architecture showing redundant components and physically diverse ingress/egress, transport, facilities, and power; include call/signaling paths proving diverse 911 call entry.*
- *Component-level HA designs with health checks, failover criteria, and state synchronization.*
- *A diversity plan detailing route/provider diversity, facility/region separation, and power diversity.*
- *Application/session continuity methods that demonstrate graceful recovery during device/site failover.*
- *Testing & exercise evidence for failover/fallback, with measured recovery objectives and tracked corrective actions.*
- *Operations & monitoring for infrastructure health; maintenance procedures that avoid creating single points of failure during changes, and SOPs for failure scenarios.*

LUMEN RESPONSE:

Lumen designs Nebraska's NG911 environment so mission-critical functions remain available during single-component failures, localized outages, or loss of a path or facility. The ESInet and NGCS architecture employs redundant and diverse components, transport paths, facilities, and power sources, and applies application- and signaling-level resilience consistent with NENA guidance to ensure continued 9-1-1 call handling.

End-To-End High-Availability Architecture. A high-availability architecture is maintained with redundant NGCS functional elements and physically and logically diverse ingress and egress paths, transport segments, facilities, and power sources. Call and signaling entry points are engineered to provide multiple independent routes into the NG911 environment so that loss of any single entry path does not interrupt call intake.

Component-Level High-Availability Design. Each NGCS and ESInet component incorporates continuous health monitoring, defined failure and degradation thresholds, and automated failover behavior. State information required for routing, policy enforcement, and

data services is synchronized using active-active or active-standby designs, as appropriate, to preserve service continuity when individual components fail.

Diversity Plan For Routes, Providers, Facilities, And Power. Route and provider diversity is implemented to reduce exposure to single-provider or single-route failures. NGCS and ESInet components are deployed across physically separate facilities and regions to mitigate localized disruptions, and critical infrastructure is supported by redundant power feeds, uninterruptible power supplies, and backup generation.

Application And Session Continuity. NGCS applications and signaling functions are designed to recover gracefully during device, path, or site failures. Dynamic routing and load-balancing mechanisms redirect traffic in real time to available resources, and in-progress sessions are preserved or re-established where feasible to minimize call disruption.

Testing And Exercise Validation. Structured failover and fallback testing is conducted to validate high-availability and diversity mechanisms under simulated failure conditions. Recovery objectives and service restoration behavior are measured during exercises, and corrective actions identified through testing are documented and tracked to closure.

Operations And Continuous Monitoring. ESInet and NGCS infrastructure health is monitored continuously through centralized operational monitoring. Maintenance activities follow formal change management procedures designed to avoid introducing single points of failure, and standard operating procedures define detection, escalation, response, and restoration actions for infrastructure failure scenarios.

This high-availability and diversity strategy ensures Nebraska's NG911 services remain resilient and available during component, path, or facility failures while maintaining standards-aligned operation across the ESInet and NGCS.

5.4.4. Authentication and Federated SSO

Agent authentication across NG911 must use federated Single Sign-On (SSO) based on OASIS SAML v2.0. Identity Providers (IdPs) authenticate agents and issues assertions to Relying Parties (RPs) for authorization. For HTTP-bound apps, IdPs and RPs must support Web Browser SSO, Identity Provider Discovery, and Single Logout; ECP and Artifact Resolution may be supported. SAML metadata should be aggregated under one `<EntitiesDescriptor>` and digitally signed by an identified administrative body using a well-known certificate to bootstrap trust.

For session establishment between agents and elements, SSO authenticates the agent and unlocks the agent's private key; the agent's X.509 certificate is then used to form the TLS session. For SIP and HTTPS, mutual TLS (mTLS) must be used with certificates traceable to the PCA for agents, agencies, and elements. RSA-2048 must be supported and accepted and accepted ESInet-wide (alternatives may be accepted only if cryptographically equivalent to, or stronger than RSA-2048). Each IdP must enforce multifactor authentication (MFA) for agents using a combination of at least two (additional factors preferred) of the following: password, token, smart card, or biometrics. Offline or other locally available backup authentication methods should be implemented for use if network access to primary authentication methods is unavailable.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An SSO architecture showing IdP(s), RPs, and assertion flows; conform all agent operations requiring authorization rely on SAML v2.0
- mTLS designs for SIP and HTTPS using PCA-traceable certificates for agents, agencies, and elements; include trust anchors, path validation, and revocation checks.
- A cryptographic baseline confirming RSA-2048 support and acceptance ESInet-wide and policy for accepting alternatives only if equivalent to, or stronger than RSA-2048.
- IdP MFA enforcement: supported factors, enrollment of multiple factors, and backup local authentication.
- The TLS establishment flow where SSO authentication unlocks the agent's private key used with the agent's certificate to negotiate the TLS session.
- Operational controls: onboarding/offboarding, key & certificate lifecycle, assertion & metadata signing key rotation, and monitoring/logging of authentication events.

LUMEN RESPONSE:

Lumen enforces federated single sign-on (SSO) and mutual authentication for Nebraska's NG911 environment to ensure secure, standards-compliant agent authentication and session establishment across ESInet and NGCS components. The solution applies SAML v2.0-based federated SSO for agent authentication and requires mutual TLS (mTLS) for SIP and HTTPS sessions using PCA-traceable certificates for agents, agencies, and NGCS or ESInet elements, with multi-factor authentication enforced for every agent authentication event.

SSO Architecture And Federated Authentication. A federated SSO architecture based on SAML v2.0 is implemented using Identity Providers (IdPs) and Relying Parties (RPs) to authenticate NG911 agents and issue assertions used for authorization decisions. The architecture supports Web Browser SSO, Identity Provider discovery, and Single Logout for HTTP-bound applications. Trust is established through SAML metadata aggregated under a digitally signed <EntitiesDescriptor>, providing a controlled mechanism for trust bootstrap consistent with the State's administrative model.

Mutual TLS For SIP And HTTPS Sessions. Mutual TLS is enforced for SIP and HTTPS traffic using X.509 certificates traceable to the PSAP Credentialing Agency (PCA) for agents, agencies, and NGCS or ESInet elements. Trust anchors, certificate path validation, and revocation checks are applied at TLS termination points to ensure that only authenticated and authorized entities participate in NG911 signaling, media control, and data exchange.

Cryptographic Baseline And Accepted Algorithms. The cryptographic baseline supports RSA 2048 across ESInet and NGCS interfaces. Alternative algorithms are accepted only when cryptographically equivalent to or stronger than the baseline, in accordance with documented security policy and applicable NG911 requirements.

Multi-Factor Authentication Enforcement. Multi-factor authentication is enforced at the Identity Provider for all agent authentication events using at least two factors, such as password, hardware or software token, smart card, or biometrics. Enrollment procedures support registration of multiple factors per agent to reduce lockout risk and support operational continuity. Backup authentication methods are documented for use when primary authentication mechanisms are unavailable, consistent with agency operational models.

TLS Establishment Flow And Key Protection. The authentication flow requires successful SSO authentication to unlock the agent's private key, which is then used in conjunction with the agent's X.509 certificate to negotiate the TLS session. This flow ensures that identity authentication and cryptographic session establishment are tightly bound and verifiable.

Operational Controls And Lifecycle Management. Operational controls govern agent onboarding and offboarding, prohibition of credential sharing, certificate and key lifecycle management, and rotation of assertion-signing and metadata-signing keys. Authentication and authorization events, including IdP authentication, assertion issuance and consumption, and mTLS outcomes, are centrally logged and monitored to support auditability and incident response.

This federated SSO and mTLS approach ensures secure, auditable, and standards-compliant authentication and session establishment for all NG911 agent operations within Nebraska's ESInet and NGCS.

5.4.5. Cryptography and Public Key Infrastructure

Cryptography in NG911 primarily secures connections and proves identity: asymmetric keys/X.509 certificates authenticate endpoints and establish sessions; symmetric ciphers then protect data in transit. The NG911 PKI is PCA-rooted: the PSAP Credentialing Agency (PCA) issues subordinate CA certificates to ESInet-operated Intermediate CAs (ICAs). Approved ICAs may, in turn, issue end-entity certificates to NGCS/ESInet service elements, and personnel. Full controlling specifications for the NG911 PKI are: NG911 Interoperability Oversight Commission (NIOC) PSAP Credentialing Agency Certificate Policy, and NIOC PSAP Credentialing Agency Certificate Validation Policy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *PKI trust architecture showing the PCA root, Contractor-operated ICA(s), end-entity certificate issuance, and provision for subordinate ICA implementation and certificate issuance.*
- *Operational practices for certificate lifecycle and key management, including how asymmetric authentication bootstraps TLS/mTLS and how symmetric session keys are negotiated.*
- *Certificate profiles & example chains demonstrating path validation to the PCA, with revocation checking and trust-anchor management*
- *Conformance statements confirming acceptance of PCA-rooted RSA-compatible credentials, consistent with the controlling specifications from the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy.*
- *TLS alignment: where and how TLS/mTLS is enforced across NGCS/ESInet interfaces showing asymmetric establishment and symmetric protection in session.*

LUMEN RESPONSE:

Lumen implements a PSAP Credentialing Agency (PCA)-rooted Public Key Infrastructure (PKI) for Nebraska's NG911 environment to support asymmetric authentication for session establishment and symmetric cryptography for data protection across NGCS and the ESInet. The trust model follows the controlling specifications defined by the NIOC PCA Certificate Policy and the NIOC PCA Certificate Validation Policy and supports certificate issuance to

NGCS and ESInet elements, agencies, and authorized personnel through Lumen-operated Intermediate Certificate Authorities (ICAs).

PKI Trust Architecture (PCA Root - ICA(s) - End-Entity Certificates). A PKI trust architecture is maintained with the PCA as the root of trust and one or more authorized ICAs issuing end-entity certificates. The architecture supports issuance to NGCS functional elements, ESInet components, agencies, and personnel and accommodates subordinate ICA deployment where permitted by PCA governance so certificate issuance remains consistent with controlling policy requirements.

Certificate Lifecycle And Key Management. Operational practices support certificate issuance, renewal, rotation, suspension, and revocation in alignment with PCA policy. Asymmetric key pairs are used to authenticate endpoints and bootstrap TLS or mutual TLS sessions, and symmetric session keys are negotiated during session establishment to protect data in transit. Key protection practices are applied to safeguard private and symmetric keys against loss, compromise, or unauthorized access.

Certificate Profiles, Path Validation, And Revocation. Certificate profiles define required key sizes, algorithms, extensions, and usage consistent with PCA-rooted NG911 requirements. Path validation to the PCA root is enforced at TLS termination points, including validation through intermediate ICAs and revocation checking using mechanisms such as CRLs or OCSP in accordance with certificate validation policy. Trust anchor management ensures only authorized roots are accepted.

Conformance To PCA Credential Requirements. Acceptance and use of PCA-rooted, RSA-compatible credentials is enforced consistent with the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy. Self-signed certificates are not used for communications traversing the ESInet or NGCS, ensuring compliance with NG911 PKI requirements.

TLS And Mutual TLS Enforcement Across NGCS And ESInet Interfaces. TLS or mutual TLS is enforced at NGCS and ESInet interfaces, including SIP signaling, HTTPS-based services, APIs, and management interfaces. Asymmetric certificate-based authentication is used during session establishment, and symmetric cryptography protects data for the duration of the session. Enforcement is applied consistently across the ESInet and NGCS to maintain confidentiality, integrity, and authenticated communications.

Operational Governance And Documentation. Documentation describes PKI trust architecture, ICA operations, certificate lifecycle processes, certificate profiles, example validation chains, revocation handling, and enforcement points for TLS and mutual TLS. This documentation supports auditability, governance, and ongoing alignment with Nebraska's NG911 security and trust requirements.

5.4.5.1. CRYPTOGRAPHIC KEYS

Cryptographic keys underpin identity and data protection in NG911. Keys are algorithm-specific and generated by approved processes. For asymmetric key pairs, the public key is submitted to a CA for inclusion in an X.509 certificate and the private key is securely stored. Private and symmetric keys must be protected against loss, corruption, and unauthorized access, with periodic access reviews. Private keys should be classified as 'Sensitive (Most Sensitive Information)' in alignment with NENA-STA-040.2-§4.2.2.1.4, or at a comparable level that aligns with the contractor's existing data classification schema.

Private keys must be revoked and reissued if compromised, or if compromised is suspected. Cryptographic key implementations must adhere to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy and align with the NENA i3 Standard (NENA-STA-010.3) and NIST SP 800-57 Part 2 Rev. 1 (Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Key generation & issuance procedures: how keys are generated, how public keys are submitted to the CA, and where/how private keys are stored.*
- *A classification statement designating private keys as 'Sensitive (Most Sensitive Information),' or similar, and the technical/administrative controls that enforce this classification.*
- *Access control & periodic review: who/what can access keys, authentication required, separation of duties, and the cadence/mechanics of access recertification.*
- *Key protection measures for storage/backup/restore, including protections at rest and in use, and configuration practices consistent with current TLS guidance.*
- *A compromise response plan detailing detection, revocation, re-issuance, distribution, and restoration steps when keys are, or suspected to be, compromised.*
- *Lifecycle management covering creation, distribution, rotation, archival and destruction, with logging/audit trails sufficient for compliance and forensics.*
- *Conformance attestations to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy.*

LUMEN RESPONSE:

Lumen implements cryptographic key management practices for Nebraska's NG911 environment that secure asymmetric and symmetric keys used across NGCS and the ESInet and align with NIOC PCA policies, NENA i3 requirements, and applicable NIST guidance. The approach ensures that key generation, protection, lifecycle operations, and compromise response preserve the confidentiality and integrity required for NG911 operations.

Key Generation And Issuance Procedures. Cryptographic keys are generated using approved, standards-based processes appropriate to the algorithm and intended use. For asymmetric key pairs, public keys are submitted to an authorized Certificate Authority for inclusion in X.509 certificates, while private keys are generated and retained within controlled environments designed to prevent unauthorized access, loss, or corruption. Key generation, submission, and issuance activities are documented and auditable as part of NG911 security operations.

Private Key Classification And Enforcement. Private keys are classified as Sensitive, consistent with NENA expectations and enterprise data classification practices. Technical controls enforcing this classification include restricted access, encrypted storage, and prevention of unauthorized export. Administrative controls include policy-based handling requirements, personnel training, and documented acknowledgment of responsibilities associated with sensitive key material.

Access Control And Periodic Review. Access to asymmetric and symmetric keys is limited to authorized systems and personnel with defined operational need, enforced through

role-based access control, strong authentication, and separation of duties. Periodic access reviews are conducted on a defined cadence to recertify continued authorization and remove access that is no longer required.

Key Protection Measures For Storage, Backup, And Use. Private and symmetric keys are protected at rest using encryption and controlled storage mechanisms and are protected in use through secure execution environments. Backup and restore processes preserve key confidentiality and integrity throughout the lifecycle. Configuration practices align with current TLS guidance to prevent weak key usage or exposure during operation.

Compromise Detection And Response. Documented procedures address suspected or confirmed key compromise, including detection and validation steps, immediate revocation, controlled reissuance of replacement keys and certificates, secure distribution, and restoration of affected services. All compromise response actions are logged and reviewed to support compliance and forensic analysis.

Key Lifecycle Management And Auditability. Cryptographic keys are managed through their full lifecycle, including creation, distribution, rotation, archival, and secure destruction. Rotation schedules and destruction criteria are defined to limit exposure and reduce risk. Comprehensive logging and audit trails are maintained to support regulatory compliance, operational oversight, and forensic investigations.

Conformance Attestation And Documentation. Lumen conforms and attests our solution aligns with the applicable NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy governing NG911 PKI. Supporting documentation, including key management practices and evidence of policy adherence, is maintained to demonstrate standards conformance and trust-architecture alignment.

5.4.5.2. USE OF SELF-SIGNED CERTIFICATES

Self-signed certificates MUST NOT be used for any NG911 communications that traverse an ESInet. All communications must use certificates traceable to the PCA root. External entities that are not in the PCA-traceable PKI must present certificated issued by a reputable public Certificate Authority. This ensures peer identity is validated through a recognized trust chain and prevents unauthenticated endpoints from participating in NG911 exchanges.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A certificate policy and enforcement plan affirming no self-signed certificates within or between ESInets and that NGCS/PSAP elements use PCA-anchored certificates.*
- *External entity onboarding requirements stating non-PCA participants must use Public CA certificates, and how this is verified during trust establishment.*
- *Trust store and path-validation configuration for SIP, HTTPS, APIs, and management interfaces, accepting only PCA-anchored chains (or approved public CA chains) with CRL/OSCP checks.*
- *An asset/certificate inventory and automated detection controls to identify and block self-signed or untrusted certs.*

- *An exception policy confirming there are no exceptions for self-signed certificates on ESInet-traversing communication, including test and non-production environments.*

LUMEN RESPONSE:

Lumen enforces a certificate policy for Nebraska's NG911 environment that explicitly prohibits the use of self-signed certificates for any communications traversing the ESInet. All NGCS, ESInet, and PSAP-facing elements are required to use PCA-anchored certificates, and trust is validated at every applicable interface so that only authenticated and authorized endpoints participate in NG911 exchanges.

Certificate Policy And Enforcement. A formal certificate policy is maintained that prohibits self-signed certificates within or between ESInets. All NGCS, ESInet, and PSAP elements authenticate using PCA-anchored X.509 certificates for NG911 communications. Enforcement is applied at all TLS and mutual-TLS termination points, including SIP signaling, application interfaces, APIs, and management interfaces, so non-compliant certificates are rejected automatically.

External Entity Certificate Requirements. External entities that are not participants in the PCA-traceable PKI are required to present certificates issued by a reputable public Certificate Authority. Certificate issuer, chain validity, key usage, and revocation status are verified during onboarding and trust establishment. External connectivity is not enabled until successful validation of a recognized trust chain is completed and documented.

Trust Store Configuration And Path Validation. Trust stores for SIP, HTTPS, APIs, and management interfaces are configured to accept only PCA-anchored certificate chains or explicitly approved public CA chains for vetted external entities. Certificate path validation and revocation checking are enforced as part of session establishment. Connections presenting self-signed, expired, revoked, or otherwise untrusted certificates are denied by default.

Certificate Inventory And Detection Controls. An inventory of certificates and certificate-using assets is maintained across NGCS and ESInet environments. Automated detection controls identify and block the presence or attempted use of self-signed or untrusted certificates. Inventory and detection outputs support continuous monitoring, auditability, and rapid remediation.

No-Exception Policy For Self-Signed Certificates. No exceptions are permitted for the use of self-signed certificates on any communications traversing the ESInet. This prohibition applies uniformly to production, test, staging, and non-production environments, ensuring consistent enforcement of NG911 trust requirements.

5.4.6. Integrity Protection

All NG 911 protocol operations must be integrity-protected with TLS, using SHA-256 or stronger (FIPS PUB 180-4); SHA-256 must be supported by all implementations. These controls make messages and media tamper-evident end-to-end.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *An integrity protection design confirming TLS deployment on all NGCS/ESInet protocol exchanges with SHA-256, and network-wide support for SHA-256.*

- *Cipher/algorithm policy and configuration artifacts proving acceptance of SHA-256 and procedures to prevent/detect downgrades.*
- *Verification & monitoring: evidence that interfaces negotiate required integrity algorithms; ongoing checks to prevent regression.*
- *Exception handling for legacy interoperability (where deployed), with compensating controls and a timeline to reach full SHA-256 compliance.*

LUMEN RESPONSE:

Lumen enforces integrity protection for all NG911 protocol exchanges within Nebraska's NG911 environment by requiring the use of TLS with SHA-256 or stronger algorithms across all NGCS and ESInet interfaces. All signaling, media negotiation, and related protocol operations are protected end to end so that only authenticated, tamper-evident communications are permitted, and all participating systems support SHA-256 system-wide in alignment with NG911 cryptographic expectations.

Integrity Protection Design. A consistent TLS-based integrity protection model is deployed across all NGCS and ESInet protocol exchanges. TLS configurations enforce the use of SHA-256 or stronger integrity algorithms and apply uniformly across signaling, data services, APIs, and management interfaces. Network-wide configurations ensure that all participating components support SHA-256 as the minimum integrity mechanism, providing end-to-end protection for NG911 communications.

Cipher And Algorithm Policy. Lumen maintains a formal cipher and algorithm policy that explicitly permits SHA-256 or stronger integrity algorithms and prohibits the use of weaker options. Configuration standards prevent protocol or cipher downgrade during session negotiation. Policy-driven controls are implemented to detect and block attempts to negotiate non-compliant integrity algorithms, ensuring cryptographic consistency across the environment.

Verification And Monitoring. All NGCS and ESInet interfaces are verified to successfully negotiate required integrity algorithms during TLS session establishment. Continuous monitoring is used to detect deviations, misconfigurations, or regressions from approved integrity standards. Integrity-related events and configuration changes are logged to support operational oversight, auditability, and rapid remediation.

Exception Handling For Legacy Interoperability. Where temporary legacy interoperability is required, Lumen documents compensating controls designed to preserve integrity protections. These accommodations are time-bounded and managed through formal risk review and approval processes. A defined timeline is maintained to achieve full SHA-256 compliance, with progress tracked and reported until all exceptions are retired.

5.4.6.1. JSON WEB SIGNATURES (JWS)

The contractor must implement JWS exactly as specified in the NENA i3 Standard (NENA-STA-010.3 §5.10), including, but not limited to, serialization, algorithm, discovery, certificate/chain handling, and Logging Service provisions defined therein. This RFP does not restate i3's normative details; Respondents must conform to i3 requirements as currently defined.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A statement of conformance to JWS requirements of NENA-STA-010.3 §5.10, plus a clause-by-clause matrix mapping the implementation to each i3 requirement.*
- *Operational policies reflecting i3 requirements and certificate/chain handling with long-term stability where applicable.*
- *Test/validation evidence showing interoperability and conformance with i3 JWS processing & verification across relevant services.*

LUMEN RESPONSE:

Lumen implements JSON Web Signatures (JWS) in full conformance with the requirements defined in NENA i3, including all serialization, algorithm, certificate handling, discovery, and Logging Service provisions referenced in NENA STA 010.3 §5.10. The implementation follows the normative i3 specifications without deviation and applies stable operational practices that support long-term integrity, verification, and interoperability of signed objects across NGCS and ESInet functions within Nebraska's NG911 environment.

Statement Of Conformance And Clause-By-Clause Mapping. Lumen maintains a formal statement of conformance affirming full compliance with all JWS requirements specified in NENA STA 010.3 §5.10. A clause-by-clause mapping matrix aligns each i3 JWS requirement with the corresponding implementation component, demonstrating compliance across serialization formats, approved algorithms, JWS discovery behaviors, certificate and chain handling, and logging requirements. The conformance statement and mapping matrix are provided as ATTACHMENT X.

Operational Policies For JWS And Certificate Handling. Lumen maintains operational policies governing JWS creation, verification, and validation in accordance with NENA i3 requirements. These policies define required serialization methods, approved cryptographic algorithms, JWS discovery processes, and certificate and trust chain handling practices that ensure long-term stability and continuity of signed data across NGCS and ESInet services. Policy controls ensure JWS signing and verification behaviors remain consistent during system upgrades, configuration changes, and ongoing operations.

Test And Validation Evidence. Lumen maintains test and validation evidence demonstrating interoperable JWS processing and verification across applicable NGCS and ESInet services. Testing confirms correct signature generation, validation, error handling, and standards-compliant behavior under both normal and adverse conditions. Validation artifacts supporting interoperability and ongoing conformance with NENA i3 JWS requirements are included as **Attachment 7**.

5.4.7. Information Privacy

All NG911 protocol operations must be privacy-protected in transit with TLS, and confidential data must be encrypted at rest, in conformance with the NENA i3 Standard and NG-SEC (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22). Implementations must support AES-256 (or stronger equivalent). Algorithms and key lengths must be chosen to protect data for the full retention period. Encryption keys must never be stored in plaintext; with access following a documented management policy - including strong passwords and multifactor authentication required for access. Alternative algorithms are acceptable only if cryptographically equivalent to, or stronger than, AES-256 with end-to-end interoperability support. The contractor should prepare for the ability to upgrade or

replace encryption algorithms and parameters to ensure continued conformance with future updates to the NENA i3 and NG-SEC Standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to NENA i3 and NG-SEC privacy & encryption requirements (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22).*
- An architecture/configuration overview showing TLS everywhere in transit and encryption at rest for stored confidential data, with cipher/algorithm policies and downgrade protections.*
- A cryptographic longevity rationale demonstrating algorithms and key lengths cover the full data lifecycle.*
- Key management policy: generation, storage, access control, rotation, backup/restore, and revocation; identification of key custodians and audit practices.*
- Operations evidence proving only approved algorithms are enabled and weaker ones disabled; include exception handling and a migration plan for any legacy endpoints.*
- If proposing alternates, a strength & interoperability justification confirming parity with AES-256 and end-to-end support across all impacted components.*

LUMEN RESPONSE:

Lumen provides privacy and encryption controls that conform to NENA i3 and NG-SEC requirements for protecting NG911 protocol operations and stored confidential information within Nebraska's NG911 environment. The design enforces TLS for all NGCS and ESInet traffic in transit and applies AES-256, or a cryptographically stronger equivalent, for data at rest. Encryption keys are protected in accordance with documented key management policies, and the architecture supports algorithm and parameter updates as NENA standards evolve to maintain long-term security.

Statement Of Conformance. Lumen affirms conformance with the privacy and encryption requirements defined in NENA STA 010.3 §5.8 and NENA STA 040.2 §6.22 for the protection of NG911 data in transit and at rest. All NGCS and ESInet implementations apply encryption controls consistent with required NG911 privacy protections. This conformance statement is provided as part of ATTACHMENT X.

Encryption Architecture And Configuration. Lumen enforces TLS across all NGCS and ESInet interfaces to ensure confidentiality and integrity end to end for data in transit. Confidential data stored within NGCS and ESInet components is encrypted at rest using AES-256 or stronger algorithms. Cipher and algorithm policies are centrally defined and enforced, with technical controls in place to prevent protocol or algorithm downgrade. Architectural diagrams and representative configurations are included as ATTACHMENT X.

Cryptographic Longevity. Lumen selects encryption algorithms and key lengths designed to protect NG911 data for the full retention lifecycle, including long-term storage where applicable. Cryptographic strength is periodically reviewed to ensure continued adequacy against evolving threat models. The design anticipates future algorithm transitions without requiring disruptive re-architecture.

Key Management Policy. Lumen maintains a documented key management policy covering key generation, secure storage, access control, rotation, backup and restore, and revocation. Encryption keys are never stored in plaintext and are protected by technical controls and strong administrative safeguards. Access to key management functions is limited to designated key custodians and requires strong authentication, including multifactor authentication. All key management activities are logged and subject to audit review.

Approved Algorithm Operations And Exception Handling. Lumen enables only approved encryption algorithms across NGCS and ESInet components and disables weaker or non-compliant alternatives. Configuration reviews and monitoring detect and prevent the use of unauthorized algorithms. Where legacy endpoints require temporary accommodation, Lumen applies compensating controls and manages exceptions through formal approval and tracking processes. A defined migration plan is maintained to transition all components to fully compliant encryption configurations.

Alternate Algorithm Justification. If alternate algorithms are proposed, Lumen provides documentation demonstrating cryptographic strength equal to or greater than AES-256. Interoperability across all affected NGCS and ESInet components is validated prior to deployment.

5.4.8. Security Assessment and Audit

A cybersecurity assessment/audit verifies conformance/compliance with security requirements, controls, and standards. At a minimum, assessments/audits shall apply the impact categories (low, moderate, high) and security objectives (confidentiality, integrity, availability) defined in NIST FIPS 199 when assessing findings, and use those categories and objectives – together with vulnerability and threat information – to determine risk and remediation priority.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *An audit methodology that applies NIST FIPS 199 impact categories and security objectives and explains how impact × likelihood (or equivalent) drives risk ratings and prioritization.*
- *The proposed audit scope and cadence – initial baseline and periodic re-evaluation – including coverage of ESInet segments, NGCS components, PSAP-facing interfaces, and policy/procedure controls.*
- *A findings lifecycle including severity assignment using FIPS 199 impacts, remediation due dates, owner assignment, tracking to closure, and verification of issue remediation.*
- *Integration points with the Risk Management program and with continuous monitoring for follow-up testing of high-severity items.*

LUMEN RESPONSE:

Lumen maintains a cybersecurity assessment and audit program that verifies conformance with NG911 security requirements and evaluates findings using the NIST FIPS 199 impact categories of low, moderate, and high, in combination with the confidentiality, integrity, and availability security objectives. These categorizations, together with vulnerability characteristics and threat context, are used to determine risk levels, establish remediation

priorities, and drive corrective actions across the ESInet and NGCS within Nebraska's NG911 environment.

Audit Methodology. Lumen employs a formal cybersecurity assessment and audit methodology that applies NIST FIPS 199 impact categories and security objectives when evaluating all findings. Risk ratings are derived using an impact-and-likelihood model, or an equivalent approach, informed by vulnerability attributes and threat conditions. This methodology ensures consistent, repeatable scoring and prioritization across NGCS components, ESInet segments, and supporting control domains.

Audit Scope And Cadence. Lumen maintains an audit plan that defines scope and cadence for NG911 security assessments. The scope includes ESInet segments, NGCS functional components, PSAP-facing interfaces, and applicable policy and procedural controls. Assessments begin with an initial baseline audit and continue through periodic re-evaluations on a defined schedule and upon material system changes. Where appropriate, related components may be assessed collectively to reflect integrated NG911 operations.

Findings Lifecycle Management. Each audit finding is classified using the defined FIPS 199 impact categories and security objectives. Findings are assigned responsible owners, documented remediation actions, and defined due dates, and are tracked through closure using formal governance processes. Verification activities confirm remediation effectiveness prior to closure, ensuring that corrective actions fully address identified risks.

Integration With Risk Management And Continuous Monitoring. Audit outputs are integrated with Lumen's Risk Management program so that high-severity and time-sensitive findings receive appropriate oversight, escalation, and follow-up. Continuous monitoring capabilities support additional testing and validation of remediation actions, particularly for higher-risk items. Monitoring results are used to detect regression, validate control effectiveness, and inform future audit cycles.

5.4.8.1. ASSESSMENT AND AUDIT DOCUMENTATION

Security requirements and risk considerations must be built into development and delivery. Before deployment, every NG911 resource must complete a documented security assessment verifying conformance/compliance with applicable policies and/or requirements. Related components may be assessed as a group when appropriate. Assessment records must be retained as auditable evidence for future reviews.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A pre-deployment security assessment process covering all components with acceptance criteria, approvers, and required evidence.*
- *Templates and examples of deliverables (control test results, residual risk statements, exceptions & compensating controls, approval sign-off) mapped back to requirements.*
- *A documentation retention & evidence management plan supporting internal and third-party audits/assessments.*
- *Integration points with change management and release processes to ensure no promotion to production without a complete, approved assessment.*
- *A tracking mechanism linking assessment findings/exceptions to remediation or formal risk acceptance and verification of closure.*

LUMEN RESPONSE:

Lumen requires every NG911 resource to complete a documented security assessment prior to deployment, ensuring conformance with applicable security requirements and policies before promotion into production within Nebraska's NG911 environment. Related components may be assessed as a group when appropriate to reflect integrated NG911 operations, and all assessment artifacts are retained as auditable evidence to support internal and third-party reviews. The assessment process is integrated with change and release management so that no component is deployed without an approved security assessment.

Pre-Deployment Security Assessment Process. Lumen enforces a structured pre-deployment security assessment process for all NGCS and ESInet components. The process defines assessment scope, acceptance criteria, required evidence, and designated approvers with authority to authorize deployment. Each assessment verifies compliance with applicable security policies and requirements prior to release, and related components may be assessed together where appropriate to reflect system integration.

Assessment Templates And Evidence Artifacts. Lumen maintains standardized templates and example deliverables to ensure consistent documentation, traceability, and repeatability of security assessments. Required artifacts include control test results, residual risk statements, documented exceptions with compensating controls, and formal approval sign-off. Each template maps assessment outputs directly to governing security requirements to support auditability and review.

Documentation Retention And Evidence Management. Lumen maintains a documentation retention and evidence management plan that preserves security assessment records for the full retention period defined by NG911 governance requirements. Assessment documentation is stored in controlled, auditable repositories with access restrictions, version control, and integrity protections. The retention approach supports both internal oversight and external audits or assessments.

Integration With Change And Release Management. Lumen integrates security assessment requirements into change management and release processes. No NGCS or ESInet component is promoted to production without a complete and approved security assessment package. Assessment status is verified at release authorization checkpoints to prevent unauthorized or non-compliant deployment.

Findings Tracking And Closure Verification. Lumen maintains a tracking mechanism that links assessment findings and approved exceptions to remediation actions or formal risk acceptance. Each finding or exception is assigned an owner, tracked through resolution, and verified prior to closure. Closure verification confirms that remediation actions or accepted risks align with documented approvals and defined assessment criteria.

5.4.9. Security Monitoring, Detection, and Alerting**5.4.9.1. SECURITY EVENT LOGGING AND CONTINUOUS MONITORING**

Security event logging is essential for early detection, scoping, and investigation of cybersecurity incidents. Logging should be centralized and standardized, tuned to capture only what is necessary, and informed by a baseline of "normal" activity so anomalies can be detected. While "Security Event Logging" objects for the NG911 Logging Service are not yet defined, the contractor's proposed solution must be ready to adopt them when published and leverage current standardized log retrieval functions.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time synchronization controls proving all logging applications and device clocks align to the time server requirements from NENA-STA-040.2 §5.6.1, enabling cross-system correlation.
- A centralized logging architecture (collection, transport, storage) with coverage to trace and correlate events end-to-end across ESInet/NGCS; include any additional logging for administrative accounts.
- A review/monitoring cadence: at minimum weekly human review, plus a plan to reach near real-time visibility via automation (e.g., SIEM).
- Log integrity & access protections: controls preventing deletion/modification, role-based access, retention periods, and storage locations that satisfy retention requirements.
- Tuning & performance practices showing log scopes/levels calibrated for detection without degrading performance; include the method to establish and update behavioral baselines.
- Forward-compatibility commitment to adopt forthcoming NG911 Security Event Logging specifications on release, including mapping/schema updates for integration with the NG911 Logging Service.

LUMEN RESPONSE:

Lumen maintains centralized, standardized security event logging across the ESInet and NGCS to support early detection, scoping, and investigation of cybersecurity incidents within Nebraska's NG911 environment. Logged events rely on synchronized timestamps, protected storage, calibrated log levels, and structured review and monitoring processes. The logging design aligns with NG911 time synchronization and retention expectations and is architected for forward compatibility with forthcoming NG911 Security Event Logging specifications.

Time Synchronization Controls. Lumen ensures that all NGCS and ESInet components synchronize system and application clocks to authoritative, resilient time sources. Time synchronization is enforced across logging platforms, network devices, servers, and applications to enable accurate cross-system event correlation. Drift monitoring and alerting detect and correct time discrepancies that could impact forensic analysis.

Centralized Logging Architecture. Lumen implements a centralized logging architecture that collects, transports, and stores security and operational events from NGCS applications, ESInet infrastructure, and supporting services. The architecture supports end-to-end traceability across call ingress, routing, delivery, and termination functions. Administrative and privileged account activity is logged alongside system and network events to support accountability and investigation.

Review And Monitoring Cadence. Lumen conducts at least weekly human review of logged security events to identify anomalies, trends, and indicators of compromise. Automated monitoring capabilities are employed to progress toward near-real-time visibility and alerting for high-risk or time-sensitive events. Monitoring outputs support incident response, investigative activities, and continuous improvement.

Log Integrity And Access Protections. Lumen applies controls to prevent unauthorized deletion, modification, or tampering of log data. Role-based access controls restrict log access to authorized personnel with defined operational need. Log retention periods and

storage locations are defined to meet NG911 operational, regulatory, and audit requirements.

Tuning And Performance Practices. Logging scopes and verbosity levels are calibrated to capture security-relevant activity without degrading NGCS or ESInet performance. Baselines of normal system and network behavior are established to support anomaly detection. Tuning practices are periodically reviewed and updated to reflect evolving traffic patterns, operational changes, and threat conditions.

Forward Compatibility With NG911 Security Event Logging. Lumen commits to adopting NG911 Security Event Logging specifications upon publication. The logging architecture is designed to support mapping and schema updates required for integration with the NG911 Logging Service. Forward-compatibility planning ensures that new standardized logging objects can be incorporated without disruptive redesign.

5.4.9.1.1. Time Synchronization

Accurate, consistent time underpins authentication, logging/correlation, troubleshooting, and continuous monitoring across the ESInet & NGCS. All elements must implement NTP (RFC 5905) and synchronize to a common, resilient time source consistent with NENA-STA-010.3 ('Time' §2.2 & 'Time Server' §4.17). The ESInet must provide an authoritative NTP service backed by a hardware clock or synchronized to external sources with sufficient redundancy to maintain local time during isolation. Service accuracy must be $\pm 1\text{ms}$ from true time, and the absolute time difference between any two elements within the ESInet/NGCS must be ≤ 0.1 second.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Time architecture showing the ESInet NTP service, upstream sources/hardware clocks, and redundancy/backup design.*
- *Element compliance evidence that all ESInet/NGCS elements support NTP (RFC 5905) and are configured to the designated time sources*
- *Accuracy & drift SLAs proving $\pm 1\text{ms}$ at the ESInet time service, and 0.1 second max element-to-element skew; include monitoring and alerting for out-of-tolerance conditions.*
- *Isolation resilience procedures to maintain accurate local time if upstream is unreachable.*
- *Operational controls: change management for time sources, certificate/time coupling checks, log/time baseline verification, and periodic audits of time-sync configuration and performance.*

LUMEN RESPONSE:

Lumen implements a unified time synchronization architecture that ensures accurate, consistent time across all ESInet and NGCS elements in accordance with Network Time Protocol (NTP) as defined in RFC 5905 and applicable NENA time requirements. The design provides an authoritative ESInet NTP service backed by redundant upstream time sources or hardware reference clocks and maintains accuracy within ± 1 millisecond of true time, with no more than 0.1 seconds of skew between any ESInet or NGCS element. This approach ensures precise, resilient time alignment across Nebraska's NG911 infrastructure.

Time Architecture. Lumen provides an authoritative ESInet NTP service delivered through a redundant and resilient architecture. The time service synchronizes to resilient upstream time sources and hardware-based reference clocks to maintain stability during upstream isolation events. Redundant and backup components ensure continued availability of accurate time services for NGCS components, ESInet infrastructure, PSAPs, and authorized agencies.

Element Compliance. All ESInet and NGCS elements are configured as NTP clients using the designated ESInet NTP service in accordance with RFC 5905. Compliance covers core NGCS functional elements, boundary devices, logging platforms, and PSAP-facing interfaces. Configuration standards ensure consistent time alignment across all components to support authentication, cryptographic operations, logging, event correlation, and troubleshooting.

Accuracy And Drift Service Levels. The ESInet NTP service is engineered to maintain time accuracy within ± 1 millisecond relative to true time. Absolute time skew between any two ESInet or NGCS elements is maintained at no greater than 0.1 seconds. Continuous monitoring measures clock offset, drift, and jitter, with alerting for out-of-tolerance conditions to enable rapid correction.

Isolation Resilience. Lumen maintains procedures to preserve accurate local time when upstream time sources become unavailable. During isolation, ESInet NTP servers rely on resilient internal references to maintain time stability within defined tolerances. These controls prevent loss of time coherence across NGCS and ESInet components during network disruptions or upstream failures.

Operational Controls. Lumen applies operational controls governing changes to time sources, NTP configurations, and related dependencies through formal change management processes. Certificate and time-coupling checks verify that time accuracy supports authentication, logging, and cryptographic operations. Log and time baseline verification processes confirm timestamp consistency across systems, and periodic audits validate time synchronization configuration and performance on an ongoing basis.

5.4.9.2. DENIAL OF SERVICE AND TELEPHONY DENIAL OF SERVICE (DoS/TDoS)

A DoS/TDoS attack attempts to render resources unavailable by overwhelming capacity or impeding traffic flow. ESInet providers must have plans and procedures to mitigate and manage DoS/TDoS events. An ESInet must be able to withstand the largest feasible Distributed Denial of Service (DDoS) or TDoS attack, which, as of the current version of NENA-STA-010.3, means $\approx \geq 1$ Tbps (terabit per second) of mitigation capacity. This can be achieved via a combination of network/BCF bandwidth and mitigation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *A DDoS/TDoS resilience architecture demonstrating $\approx \geq 1$ Tbps (terabit per second) effective mitigation capacity across ESInet ingress, BCF/SBC, upstream carriers, and contracted mitigation services (including how capacity is measured and assured).*
- *Traffic re-route capability design showing how private links and any Internet-based paths can be redirected to a mitigation service during events; include activation triggers, propagation steps, and rollback.*
- *Plans and procedures to mitigate and manage DoS/TDoS incidents.*

- *Operational testing evidence of re-route/mitigation cutovers and load exercises, with results demonstrating maintained call delivery and measured restoration times.*
- *Monitoring & detection of volumetric and signaling-layer abuse with alert thresholds and dashboards spanning network, BCF/SBC, and application layers.*
- *Configuration governance for temporary blocks/rate limits and rule updates during incidents, including audit trails and post-incident reviews.*

LUMEN RESPONSE:

Lumen implements DoS and TDoS resilience measures that enable Nebraska's ESInet to withstand large-scale volumetric and signaling-layer attacks consistent with NG911 mitigation expectations. The design delivers an effective mitigation capacity of approximately one Terabit per second (**1Tbps**) through a layered combination of ESInet backbone bandwidth, BCF and SBC capacity, upstream carrier protections, and contracted mitigation services. Lumen maintains the ability to dynamically re-route traffic to mitigation services when required and ensures call delivery remains stable during defensive actions.

DDoS/TDoS Resilience Architecture. Lumen employs a layered DoS/TDoS resilience architecture that distributes mitigation capacity across ESInet ingress points, BCF and SBC elements, upstream carrier networks, and contracted mitigation providers. The architecture supports an effective mitigation capacity of approximately 1Tbps using a combination of reserved bandwidth, scalable network resources, and on-demand mitigation services.

Traffic Re-Route Capability. Lumen supports dynamic traffic re-routing for both private links and Internet-based paths to divert attack traffic to mitigation services during DoS or TDoS events. The design defines activation triggers, routing propagation steps, coordination with upstream providers, and controlled rollback procedures once an event is resolved. Re-routing mechanisms are engineered to preserve call delivery and minimize service disruption.

DoS/TDoS Mitigation And Management Procedures. Lumen maintains documented plans and procedures to detect, mitigate, and manage DoS and TDoS incidents affecting NGCS and ESInet services, including volumetric and signaling-layer threats. Procedures define roles, escalation paths, coordination with mitigation providers, and communication protocols during incidents. Post-incident review processes capture lessons learned and identify improvement actions.

Operational Testing And Exercises. Lumen conducts operational testing and exercises to validate DoS/TDoS mitigation and traffic re-route capabilities. Testing includes cutover to mitigation services and load exercises designed to simulate volumetric and signaling-based attacks. Results demonstrate maintained call delivery and measured restoration times following simulated events.

Monitoring And Detection. Lumen monitors for volumetric attacks and signaling-layer abuse across network infrastructure, BCF and SBC components, and NGCS applications. Dashboards and alert thresholds provide visibility into abnormal traffic patterns and potential DoS/TDoS conditions, supporting rapid detection and initiation of mitigation actions.

Configuration Governance During Incidents. Lumen applies formal governance for temporary configuration changes during DoS/TDoS incidents, including traffic blocks, rate

limits, and rule updates. All changes are logged with audit trails and subject to review and rollback controls. Post-incident reviews assess effectiveness, validate service restoration, and document required policy or configuration updates.

5.4.9.3. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS/IPS)

The contractor must include intrusion detection to identify known threats and suspicious behavior across endpoints and networks, with alerts routed to a central monitoring function. Intrusion prevention adds automated blocking and must be carefully deployed to avoid disrupting 911 call handling; on segments carrying live call media and signaling, IPS should be avoided unless rigorously engineered, tested, and monitored. Controls must be tuned and maintained so detections remain accurate as the environment changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Architecture and placement: where IDS is deployed, where IPS (if any) is deployed, and how alerts flow to a central SIEM; include rationale for deployed controls - ensuring no impact to legitimate media/signaling.*
- *Content currency & tuning: processes to update signature content at least weekly and to review/update anomaly profiles at least annually and upon material changes; including tuning and drift management.*
- *Monitoring cadence: procedures for at least weekly human reviews, with staffing/tools that achieve daily or near real-time monitoring; escalation paths and on-call coverage.*
- *Configuration governance: annual configuration reviews, change controls, test/validation before enabling prevention actions, and rollback procedures.*
- *Quality management: metrics and methods to track and reduce false positives/negatives, periodic effectiveness reviews, and sample investigation records.*
- *Integration: how IDS/IPS telemetry correlates with firewalls, endpoint security, event logs, and SIEM; storage/retention aligned to logging requirements and protected against tampering.*

LUMEN RESPONSE:

Lumen deploys intrusion detection capabilities that identify known threats and suspicious behavior across ESInet and NGCS networks and endpoints, with all alerts routed to a centralized monitoring function. Intrusion prevention is applied only where it can be rigorously engineered and validated to avoid any disruption to live NG911 call media or signaling. Detection logic, signatures, and anomaly models are maintained and tuned to ensure continued accuracy as the NG911 environment evolves.

Architecture And Placement. Lumen deploys Intrusion Detection Systems (IDS) at strategic locations across ESInet ingress and egress points, core network segments, and NGCS application environments to identify known threats and suspicious activity. All IDS alerts are forwarded to a centralized monitoring and SIEM platform to support correlation and investigation across network, application, and endpoint layers. Intrusion Prevention Systems (IPS) are selectively deployed only on segments where prevention behavior can be validated as non-disruptive. On segments carrying live NG911 call media or signaling, IDS operates in detection-only mode unless prevention controls are proven safe for operational use.

Content Currency And Tuning. Lumen updates IDS and IPS signature content on a regular cadence of at least weekly to maintain protection against emerging threats. Anomaly detection profiles and behavioral baselines are reviewed at least annually and whenever material changes occur within the ESInet or NGCS environment. Formal tuning processes manage detection drift, reduce noise, and preserve sensitivity to relevant threat indicators.

Monitoring Cadence. Lumen conducts at least weekly human review of IDS and IPS alerts and trends to validate detections and identify emerging risks. Automated tools and staffing models support daily or near-real-time monitoring for high-severity or time-sensitive events. Defined escalation paths and on-call coverage ensure rapid response to confirmed or suspected intrusion activity.

Configuration Governance. IDS and IPS configurations are subject to formal annual reviews to confirm alignment with current architecture, traffic patterns, and threat conditions. All configuration changes follow controlled change management procedures, including testing and validation prior to enabling or modifying prevention actions. Rollback procedures are defined to quickly restore prior configurations if unintended impacts are detected.

Quality Management. Lumen tracks quality metrics such as false positives, false negatives, alert volumes, and response times to assess IDS and IPS effectiveness. Periodic effectiveness reviews are conducted to refine detection logic and improve accuracy. Investigation records are maintained to document how alerts are analyzed, validated, and resolved as part of the quality assurance process.

Integration. IDS and IPS telemetry is correlated with firewall events, endpoint security data, system logs, and other security signals through centralized monitoring and SIEM platforms. Integrated analysis provides end-to-end visibility across ESInet and NGCS environments. Detection records are stored in accordance with NG911 logging and retention requirements and are protected against unauthorized modification or deletion.

5.4.10. Domain Name System (DNS)

DNS is mission-critical for NG911 service reachability and must be engineered and operated to resist tampering and disruption (e.g., spoofing, cache poisoning, DoS on resolvers). The contractor shall implement defense-in-depth protections (DNSSEC validation/signing, logging, cache-locking, response-rate limiting), and align DNS administration with privileged account, patching, and change-management controls/requirements outlined elsewhere in this RFP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *DNSSEC is enabled on all deployed DNS servers, and clients are configured to request DNSSEC validation.*
- *DNS logging is enabled on all DNS servers with centralized collection and retention; describe log scopes and how performance impact is managed.*
- *Cache locking is enabled and set to 100% of TTL on recursive servers.*
- *Response rate/time limits are configured on name servers to mitigate DoS/TDoS effects.*
- *Administrative access controls to DNS infrastructure conform to requirements in NENA-STA-040.2 §6.2.1.3 'Administrator Accounts'.*

- *Patch and update compliance for all DNS components conforming to requirements in NENA-STA-040.2 §5.5 'Patching and Updating' including emergency update procedures for critical CVEs.*
- *Network placement & resilience: DNS architecture diagrams showing internal vs. external roles, inter-site redundancy, diverse upstream resolvers, and protections at network boundaries.*
- *Monitoring and alerting for DNS health and integrity (e.g., DNSSEC validation failures, abnormal NXDOMAIN spikes, RRL hits).*

LUMEN RESPONSE:

Lumen implements DNS services for Nebraska's NG911 environment with layered protections that prevent tampering, spoofing, cache poisoning, and resolver disruption. The DNS design applies defense-in-depth controls aligned with NG911 security expectations and maintains resilient internal and external resolution services to support availability, integrity, and reliable name resolution across ESInet and NGCS operations.

DNSSEC Enablement. Lumen enables DNSSEC signing and validation on all deployed authoritative and recursive DNS servers supporting the ESInet and NGCS. DNS clients are configured to request and validate DNSSEC records to ensure authenticated, tamper-evident DNS responses and to protect against spoofing and cache poisoning attacks. DNSSEC key management, rollover processes, and validation failures are monitored to ensure continued integrity of DNS operations.

DNS Logging And Centralized Collection. Lumen enables DNS logging on all DNS servers, capturing query, response, error, and security-relevant events. Logs are routed to centralized collection and retained in accordance with NG911 logging and retention requirements. Log scopes and verbosity are tuned to maintain required security visibility while managing performance impact on DNS resolution.

Cache Locking Configuration. Lumen configures recursive DNS servers with cache locking enabled at 100% of the time-to-live (TTL) to prevent cache overwrite and poisoning attempts. Cache locking behavior is monitored to ensure effectiveness without negatively impacting resolution performance.

Response Rate And Time Limiting. Lumen configures response rate limiting and time-based controls on authoritative DNS servers to mitigate DoS and TDoS amplification and abuse. Limits are tuned to protect DNS availability while preserving legitimate NG911 query traffic. Rate-limit policies and thresholds are periodically reviewed and adjusted based on observed traffic patterns and threat conditions.

Administrative Access Controls. Lumen restricts administrative access to DNS infrastructure using role-based access controls and strong authentication consistent with NG911 administrator account requirements. Privileged access activities are logged and subject to periodic review to ensure appropriate use and accountability.

Patch And Update Compliance. Lumen maintains patching and update practices for all DNS components, including routine maintenance updates and emergency patching procedures for critical vulnerabilities. Update processes are integrated with change management to ensure timely remediation without disrupting NG911 operations.

Network Placement And Resilience. Lumen's DNS architecture separates internal and external DNS roles and applies appropriate protections at network boundaries. The design

includes inter-site redundancy, diverse upstream resolvers, and resilient routing to maintain DNS availability during failures or attacks.

Figures 5.4.10-1 and **5.4.10-2** depict the redundant NGSC design, ensuring inter-site redundancy across the State of Nebraska NG911 enterprise.

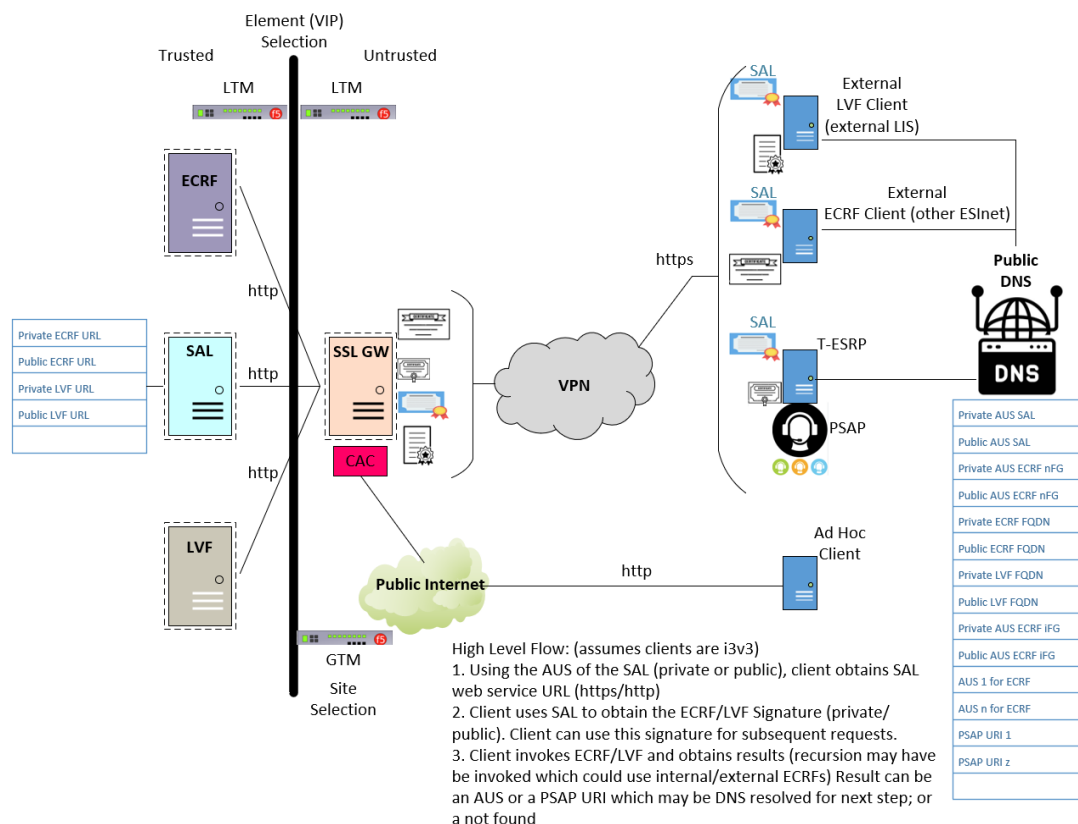


Figure 5.4.10-1. NGSC Core Redundant Design

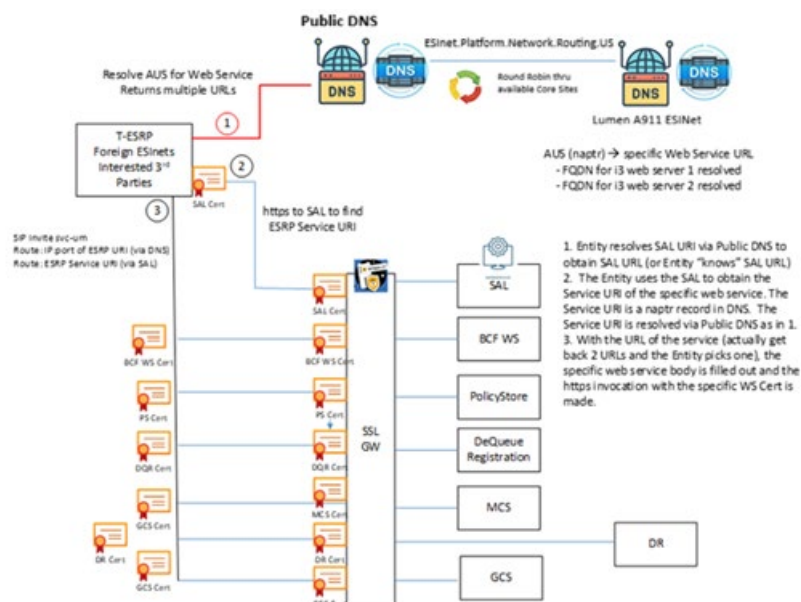


Figure 5.4.10-2. NGSC Core Redundant Design

Monitoring And Alerting. Lumen monitors DNS health and integrity indicators, including DNSSEC validation failures, abnormal NXDOMAIN behavior, cache anomalies, and response rate limiting activations. Dashboards and alerts provide visibility into DNS performance and security conditions across the ESInet and NGCS, supporting timely investigation and response to DNS-related incidents.

Deliverables - Security, Privacy, and Trust

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires a security architecture for NG911 that is standards-aligned, auditable, and demonstrably effective in protecting call handling, location data, and sensitive operational information. Lumen complies by providing comprehensive security architecture diagrams and supporting documentation, including PKI policies, role-based access control matrices, and access control configurations. These deliverables clearly define trust boundaries, identity management, encryption enforcement, and administrative authorization across the ESInet and NGCS environments.

Lumen further complies by providing recent third-party penetration test reports that assess the security posture of relevant systems and interfaces, along with documented service level commitments for vulnerability remediation and patching. These materials demonstrate disciplined security testing, transparent disclosure, and structured remediation processes aligned with NG911 operational risk management expectations.

In addition, Lumen demonstrates the active enforcement of security controls through evidence of mutual TLS authentication between NG911 functional elements, anomaly detection mechanisms used to identify and respond to abnormal behavior, and integration of security logs into a centralized SIEM platform. These demonstrations confirm that security events are detected, correlated, and acted upon without degrading NG911 service availability or performance. Collectively, these deliverables provide the State with verifiable assurance that the proposed solution enforces strong security, protects sensitive data, and maintains trust across all NG911 services.

5.5. Reporting Services Requirements

The contractor shall implement end-to-end logging for all call and transaction events across ESInet and NGCS components in RAW format. Logs must include ISO 8601 timestamps with time zone offset, unique correlation IDs, call identifiers, SIP message summaries (headers and SDP), PIDF-LO snapshots (privacy-redacted), routing decisions, ECRF/LVF responses, PSAP handoff timestamps, and error details. Logs shall be tamper-evident through cryptographic hashing or blockchain-like mechanisms and protected against unauthorized access.

The system shall generate CDRs for every emergency call, capturing fields such as calling line identifier, location used for routing, receiving PSAP ID, call start/answer/end

timestamps, media types negotiated, disposition codes, and any transfers. CDR format and fields must align with NENA specifications, supporting export in XML/JSON.

Logs and CDRs shall be retained for a minimum of 7 years (or per jurisdictional policy), with secure storage, searchable indexing (e.g., via Elasticsearch), and export in standard formats (CSV, JSON, PDF). Access must be role-based, with audit trails for queries.

The contractor shall provide data to the PSC data analytics platform to allow for pre-built reports on call volume, average answer time, transfer metrics, location validation failures, and outage incidents, along with ad-hoc querying tools.

The system must maintain auditable trails for all configuration changes, GIS updates, and policy modifications, recording user identity, timestamps, before/after values, and rationale.

LUMEN RESPONSE:

Lumen implements end-to-end logging and Call Detail Record (CDR) generation across the ESInet and NGCS so that all call and transaction events are captured in RAW format with the required technical detail, retention, and access controls. The design produces tamper-evident logs, standards-aligned CDRs, and searchable, exportable records that support Nebraska's operational, forensic, compliance, and analytic needs across the statewide NG911 environment.



Figure 5.5-1. Management Portal - Call Detail and Trace - Individual Messages Available

End-To-End Logging Content. Lumen logs all call and transaction events in RAW format with full technical fidelity. Logged elements include ISO 8601 timestamps with time-zone offset, unique correlation identifiers, call identifiers, SIP message summaries including headers and SDP, privacy-redacted PIDF-LO snapshots, routing decisions, ECRF and LVF query responses, PSAP handoff timestamps, and detailed error conditions. This content supports complete call reconstruction, troubleshooting, and forensic analysis.

Tamper-Evident Log Protection. Lumen applies cryptographic hashing or equivalent tamper-evident mechanisms to log records and protects log storage against unauthorized access. Controls ensure that any attempted modification, deletion, or corruption of log data is detectable and auditable, preserving evidentiary integrity throughout the retention period.

CDR Generation. Lumen generates a CDR for every emergency call. Each CDR captures the calling line identifier, the location used for routing, receiving PSAP identifier, call start, answer, and end timestamps, negotiated media types, disposition codes, and any call transfers. CDRs use a format and field set aligned with NENA specifications and support export in XML and JSON formats to enable downstream processing and analysis.

Retention, Storage, And Search. Lumen retains logs and CDRs for a minimum of seven years, or longer where jurisdictional policy requires. Records are stored in secure repositories with indexed search capabilities, such as an Elasticsearch-backed platform, enabling rapid retrieval and correlation. The solution supports export in CSV, JSON, and PDF formats to meet operational, audit, and reporting needs.

Role-Based Access And Auditing. Lumen enforces role-based access controls for all log and CDR queries, limiting access to authorized personnel with a defined operational or oversight need. Audit trails record access, queries, and exports to ensure accountability and support compliance reviews.

Analytics Integration. Lumen provides required log and CDR data to the PSC data analytics platform to support pre-built and ad-hoc reporting. Available metrics include call volume, average answer time, transfer activity, location validation failures, abandonment and backup routing, and outage-related incidents. The integration supports both statewide analytics and detailed operational insight. **Figure 5.5-2** depicts a system abandonment and backup routing report.

The screenshot displays the 'A9-1-1 Customer Management Portal' interface. On the left is a navigation menu with options like 'Select PSAP', 'All PSAP Operational States', 'All PSAP CDRs', 'All PSAP Call, IP Contact and Trunk Status', 'Call Status Display', 'Call Assurance Response Logger', 'ITG to PSAP Mapping', 'TDOs TNS', 'Agency Hierarchy', 'User Preferences', 'Douglas County 9-1-1 Communications Center', 'PSAP Contacts - Operational State - Subscribed Features', 'Route List', 'CDRs', and 'PSAP Call, IP Contact and Trunk Status'. The main content area shows several tables under the heading 'View Route Lists'. The first table is 'Abandonment Route List - DGLSNECC1abandon', followed by 'Backup Route List - DGLSNECC1backup', 'Wireline Transfer/Bridge Override Route List - DGLSNECC1default', 'Wireless Transfer/Bridge Override Route List - DGLSNECC1default', and 'VoIP Transfer/Bridge Override Route List - DGLSNECC1default'. Each table has columns for 'Dest. #', 'Destination Name', 'PSAP ID', 'Destination Type', 'TN', 'County', and 'State'. The 'County' and 'State' columns are consistently filled with 'Douglas' and 'NE' respectively.

Dest. #	Destination Name	PSAP ID	Destination Type	TN	County	State
1					Douglas	NE

Dest. #	Destination Name	PSAP ID	Destination Type	TN	County	State
1	Fast_Busy		Audio		Douglas	NE

Dest. #	Destination Name	PSAP ID	Destination Type	TN	County	State
1					Douglas	NE
2					Douglas	NE
3					Douglas	NE

Dest. #	Destination Name	PSAP ID	Destination Type	TN	County	State
1					Douglas	NE
2					Douglas	NE
3					Douglas	NE

Dest. #	Destination Name	PSAP ID	Destination Type	TN	County	State
1					Douglas	NE
2					Douglas	NE
3					Douglas	NE

Figure 5.5-2. Management Portal - Abandonment, Alternate, and Backup Routing

Configuration And Change Trails. Lumen maintains auditable records for configuration changes, GIS updates, and policy modifications. Change records include user identity, timestamps, before-and-after values, and stated rationale, enabling traceability and supporting governance, troubleshooting, and compliance validation.

5.5.1. Reporting and Data Collection Requirements

The State requires enterprise-wide reporting and data collection capabilities on all aspects of the proposed NG911 system.

This capability must be agnostic to provider, system or technology and must be able to collect reportable data on the operation, configuration, and maintenance of the NG911 system. This includes both the NG911 systemwide/statewide/enterprise wide and

local/PSAP specific data collection, logging and reporting necessary for the processing and documentation of 911.

LUMEN RESPONSE:

Lumen provides enterprise-wide reporting and data collection capabilities that span all aspects of Nebraska's NG911 system, from statewide ESInet and NGCS operations to PSAP-specific activity. The design is provider, system, and technology-agnostic and focuses on collecting, normalizing, and presenting operational, configuration, and maintenance data without requiring any specific vendor stack or toolset at the PSAP. This approach ensures consistent statewide visibility while supporting local operational needs.

Enterprise-Wide, Provider-Agnostic Data Collection. Lumen's NG911 solution is designed to collect, normalize, and correlate reportable data regardless of underlying provider, system, or technology. Data is captured across NGCS functional elements, ESInet infrastructure, and PSAP-facing interfaces, enabling consistent reporting in multi-vendor and hybrid operating environments. Normalization into a common schema ensures that statewide and PSAP-level reporting remains consistent and comparable across platforms.

Systemwide And PSAP-Level Logging. The solution supports both statewide and PSAP-specific data collection, logging, and reporting. Logged data includes NGCS and ESInet events across call ingress, routing, delivery, and termination; configuration and change management records for NGCS and network elements; and operational and maintenance records supporting troubleshooting, audits, and compliance. All records are time-synchronized and correlated to enable end-to-end traceability of 911 transactions. Logs are securely retained and protected to support integrity, auditability, and jurisdiction-specific retention requirements.

Reporting For Operations, Performance, And Compliance. Lumen enables enterprise and local stakeholders to access reporting required for operational oversight and documentation of NG911 services. Reporting includes statewide system health, availability, and performance views; PSAP-level operational views supporting local management and accountability; and historical reporting for incident analysis, service validation, and regulatory review. Secure access controls ensure users can view only authorized statewide or PSAP-specific data.

Statewide And PSAP-Specific Views. The reporting framework provides systemwide, statewide, and enterprise-level views that allow the State to analyze overall NG911 performance, trends, and incidents. In parallel, PSAP-specific views present local call handling activity, transfers, outages, and configuration changes. This dual-view approach supports centralized oversight while preserving local operational insight.

Query And Analytics Support. Reporting capabilities support both standardized and ad-hoc queries, enabling the State and PSAPs to analyze trends, validate performance, and document NG911 operations. Automated logging and structured configuration and maintenance records together provide a complete, end-to-end data foundation for operational analysis, audits, and long-term planning.

5.5.2. Logging Service

The State requires that there be a Logging Service conforming to NENA-STA-010.3. The logging service must be capable of logging all LogEvents defined in NENA-STA-010.3, including media, and all Functional Elements provided under the contract must generate such LogEvents and send them to the logging service.

The State desires that the Logging Service be made available to any PSAP that chooses to use it and implements the required i3 logging interfaces.

The Logging Service must support the query, retrieval, and log event replicator mechanisms described in NENA-STA-010.3.

*The Logging Service must support **ElementState** and **ServiceState** SUBSCRIBE/NOTIFY per NENA-STA-010. The State must be able to subscribe to ServiceState and receive the standard state changes.*

The proposal shall describe the Logging Service in detail.

LUMEN RESPONSE:

Lumen provides a Logging Service that conforms to NENA STA 010.3 and supports the generation, transport, storage, retrieval, and replication of all required LogEvents across the ESInet and NGCS. All Functional Elements in the solution generate NENA-compliant LogEvents, including media-related events, and transmit them to the Logging Service using the required i3 logging interfaces. The Logging Service is available to any PSAP that elects to use it, provided the PSAP implements the necessary i3 logging capabilities, enabling interoperable, statewide, and PSAP-accessible NG911 event logging.

NENA STA 010.3 Conformance. Lumen's Logging Service conforms fully to NENA STA 010.3 and supports all LogEvents defined by the standard, including signaling, media, routing, policy, and operational state events. All NGCS Functional Elements provided under this solution—including BCF, ESRP, ECRF/LVF, PRF, and associated services—generate required LogEvents and forward them to the Logging Service using standardized i3 logging interfaces.

Comprehensive LogEvent Capture. The Logging Service captures and correlates LogEvents across the complete lifecycle of a 911 interaction. Logged events include call ingress, routing, transfers, and termination; media handling and session events; Functional Element processing and decision points; and system, service, and network events affecting NG911 operations. Each LogEvent includes standardized timestamps and correlation identifiers, enabling end-to-end traceability across NGCS and ESInet components.

PSAP Availability And Provider-Agnostic Access. The Logging Service may be made available to any PSAP that elects to use it and implements NENA-compliant i3 logging interfaces. The service is provider-agnostic and does not require PSAPs to use a specific call-handling system or network provider, allowing jurisdictions to access standardized logging services regardless of local technology choices.

Query, Retrieval, And Replication Support. The Logging Service supports the query interface, LogEvent retrieval interface, and LogEvent replication mechanisms defined in NENA STA 010.3. These capabilities enable authorized users and systems to retrieve LogEvents for operational review and analysis, securely replicate LogEvents to State-designated or external systems, and integrate logging data with enterprise reporting, analytics, and archival platforms. This supports statewide oversight, PSAP-level review, and long-term record retention.

ServiceState And ElementState SUBSCRIBE/NOTIFY. The Logging Service supports ElementState and ServiceState SUBSCRIBE/NOTIFY mechanisms in accordance with NENA i3 specifications. The State may subscribe to ServiceState notifications and receive standardized

state-change events, including service availability, degradation, and recovery notifications, supporting real-time situational awareness and operational monitoring.

Security, Integrity, And Retention. LogEvents are stored in secure, access-controlled repositories designed to preserve data integrity and support audit and compliance requirements. Role-based access controls ensure that State and PSAP users can access only authorized data. Retention policies are configurable to meet State and jurisdiction-specific requirements.

Scalable, Standards-Based Architecture. The Logging Service is designed to scale as PSAPs, services, and call volumes increase without degradation of performance. Its standards-based implementation ensures compatibility with future NG911 capabilities and evolving NENA specifications.

5.5.3. i3 Logging and Reporting Requirements

The proposed solution's NG911 logging and reporting system must conform to NENA-SAT-010.3 i3 logging requirements, including functional element logging, data collection, and reporting.

LUMEN RESPONSE:

Lumen ensures the NG911 logging and reporting system conforms to NENA STA 010.3 and supports complete Functional Element logging, data collection, and report generation across all NGCS and ESInet components. All required LogEvents are generated, transported, stored, and made available for reporting in alignment with the i3 logging model. The solution provides standardized, provider-agnostic logging that supports statewide oversight and PSAP-level visibility into NG911 operations.

NENA STA 010.3 Conformance. Lumen complies with the State's i3 logging and reporting requirements by implementing a logging and reporting system that conforms to NENA STA 010.3. All NGCS Functional Elements provided under the contract generate and transmit required LogEvents using standardized i3 interfaces, ensuring consistent, interoperable logging across the ESInet and NGCS.

Functional Element Logging And Data Collection. Lumen's solution ensures that required Functional Element logging and data collection are performed consistently and in accordance with NENA i3 specifications. NGCS components generate LogEvents covering operational processing, routing decisions, media activity, and system state, enabling enterprise-wide and PSAP-level visibility into NG911 transactions and service behavior.

Reporting Support For Operations And Compliance. Collected log data supports operational monitoring, performance analysis, incident investigation, and compliance reporting for both statewide and local stakeholders. The reporting framework enables review of NG911 activity across ESInet and NGCS components, supporting accountability, troubleshooting, and regulatory validation.

Standards-Based, Scalable Reporting Framework. The logging and reporting framework is standards-based, provider-agnostic, and designed to scale as NG911 services, Functional Elements, and reporting needs evolve. This approach ensures long-term compatibility with NENA i3 standards while maintaining flexibility to support future NG911 capabilities.

5.5.4. Functional Element Reporting

All functional elements within the ESInet (e.g., ESRP, ECRF, LVF, LIS, BCF) MUST be capable of reporting their operational status, critical events, alarms, and other relevant data. This reporting is essential for system monitoring, troubleshooting, security analysis, and performance management. Reporting mechanisms shall conform to standard protocols to ensure interoperability with a centralized logging and monitoring infrastructure.

- *ESInet to PSAP Call Delivery transactions*
- *SIP Conference metrics*
- *PSAP Routing Duration Report*
- *Concurrent Calls*
- *BCF Session Reporting*
- *ESRP Session Reporting*
- *ESRP Queue State*
- *ECRF Session Reporting*
- *LVF Reporting*
- *LNG Session Reporting*

Respondents must describe the proposed enterprise-wide NG911 logging, data collection, and reporting system and the elements provided above.

LUMEN RESPONSE:

Lumen provides an enterprise-wide NG911 logging, data collection, and reporting system that delivers standardized operational visibility across all ESInet and NGCS Functional Elements. Each Functional Element generates operational status, critical events, alarms, and associated metrics using standard protocols so information can be consumed by centralized monitoring and reporting systems. The design ensures required reporting types, including call delivery, session behavior, routing duration, and queue state, are consistently produced and available to the State for system management and performance analysis across Nebraska's NG911 environment.

Functional Element Reporting. Lumen complies with the State's requirement for Functional Element reporting across the ESInet and NGCS. All NGCS and ESInet Functional Elements provided under the contract, including ESRP, ECRF, LVF, LIS, BCF, and related services—generate operational status, critical events, alarms, and relevant performance data using standardized formats that support centralized collection and monitoring.

Functional Element Status And Event Reporting. Each Functional Element continuously reports service and operational state, including normal, degraded, and unavailable conditions; critical events and alarms affecting call processing or availability; and session-level and transaction-level activity. This reporting supports real-time system monitoring, troubleshooting, security analysis, and performance management at both enterprise and PSAP levels.

Standards-Based Reporting And Interoperability. Reporting mechanisms conform to NENA i3 standards, including standardized logging, event generation, and state notification interfaces. This standards-based approach ensures interoperability with centralized logging and monitoring infrastructure and supports integration with State-designated reporting, analytics, and security platforms.

Enterprise-Wide NG911 Logging, Data Collection, And Reporting. Lumen's enterprise-wide framework aggregates and correlates data generated by all Functional Elements, enabling comprehensive visibility across the statewide NG911 system. Collected data supports operational oversight, performance analysis, incident investigation, and regulatory documentation while remaining provider- and technology-agnostic.

Supported Functional Element Reports And Metrics. The solution supports reporting for ESInet-to-PSAP call delivery transactions; SIP conference metrics; PSAP routing duration; concurrent call activity; BCF session behavior; ESRP session activity and queue state; ECRF session processing; LVF transactions and outcomes; and LNG session reporting where legacy interworking applies. These reports provide both real-time and historical insight into NG911 operations.

Secure Access And Scalability. Reporting data is protected through role-based access controls to ensure State and PSAP users access only authorized information. The reporting framework is scalable and designed to accommodate additional PSAPs, Functional Elements, and increased call volumes without degradation of performance.

5.5.5. Monitoring, Outages, Failover, Trouble Tickets, and Escalation

The State requires that there be a Network Operation Center (NOC) that monitors the ESInet, the NGCS, the gateways, and all the other elements provided under the Contract. Each element must be continuously monitored for correct operation, and any faults must cause alerts to the NOC.

Any element failure must be treated as an outage. Any service failure must be treated as a serious outage. The proposal must include a description of outage classifications with escalation processes and notification processes. A system outage must have an escalation process that escalates to the highest non-executive level within the committed SLA. For example, an outage on a service with a 5-nines (99.999% uptime) SLA must escalate to the highest non-executive level within five (5) minutes of the outage. In this context, non-executive means all the contractor and appropriate subcontractor technical staff is committed at the highest level, but not necessarily senior executives who could monitor, but not actually contribute to problem resolution. A single person must be designated the owner of such an outage, and that owner must be empowered to direct any available resources to assess, diagnose and repair the cause or effect of the outage. The owner of the outage must be reported to the State promptly.

Any outage visible to any PSAP must be reported to that PSAP and to the State. The proposal must include the available notification methods and timing of reports of outage, progress, and restoration.

Any outage which causes an SLA failure for the month in which the outage occurred must be investigated, the root cause(s) must be determined, and corrective actions must be undertaken. The State and affected PSAPs must receive a report with the root causes, corrective actions and with committed dates. Follow-up reports noting progress against the committed dates must be provided quarterly. The State expressly reserves the right to question the root cause determination and, if it determines that the proposed corrective action plan is deficient, the contractor and the State will negotiate in good faith to amend the root cause and form a corrective action plan that is mutually agreeable.

The State requires that the contractor provide a help desk, which may be the NOC or a different group. The help desk must be staffed 24/7/365 by staff qualified to solve the most common issues encountered by PSAPs. The help desk must have a ticketing system that accepts tickets submitted by website or telephone call. The help desk must be the exclusive mechanism used to report problems by PSAPs or State staff. Every problem report must generate a ticket.

For problem reports received by telephone, the call must be answered by a qualified technician within 60 seconds 90% of the time. For website entered tickets, an initial automated email must be generated immediately, and a follow up email or telephone call must be sent within 5 minutes 99% of the time. The technician first encountering a new issue must be able to solve the problem by taking whatever actions are required to close the ticket themselves 50% of the time. This should be included in a monthly report to offer KPIs.

The help desk must take ownership of all reported problems. Sustained effort must be maintained until the problem is solved and the ticket is cleared.

The State requires that the contractor integrate or “bond” the ticketing systems of each supplier or subcontractor which may be engaged by a ticket, so that the help desk is able to have full visibility and follow up as necessary with such suppliers and subcontractors. The help desk must maintain ownership of issues even if suppliers or subcontractors must solve all or part of the reported problems. However, while the help desk must maintain ownership of the issue, it is incumbent upon the contractor to keep the State informed and fully aware of progress during the effort to restore services. The State prefers that the reporting entity be able to converse with the people who can solve the problem, so if a contractor is solving the problem, the State desires the help desk to keep abreast, but not be in the middle of solving the problem.

When sustained outages (more than 15 minutes) occur, the contractor must investigate and initiate workarounds to bring the system back to at least partial operational state. Even if the actual problem source has been found, and repairs underway, workarounds must be devised to ameliorate the problem if the work arounds can be completed faster than the actual problem repair.

LUMEN RESPONSE:

Lumen operates a 24x7x365 Network Operations Center that continuously monitors the ESInet, the NGCS, all gateways, and every Functional Element provided under the Contract. All components are monitored for correct operation, and any element failure generates an immediate alert to the NOC. Failure of any individual element is treated as an outage, and any service failure is treated as a serious outage requiring rapid escalation and coordinated response. This approach ensures continuous visibility, rapid restoration, and transparent communication across Nebraska’s NG911 environment.

Outage Classification And Escalation. Lumen maintains defined outage classifications with associated escalation and notification processes. Any system-level outage affecting a service with a five nines service level agreement escalates to the highest non-executive technical level within five minutes. A single outage owner is assigned to every outage event and is empowered to direct all required resources for assessment, diagnosis, and repair. The assigned outage owner is promptly reported to the State to ensure clear accountability.

Notification To PSAPs And The State. Any outage visible to a PSAP is reported to the affected PSAP and to the State. Lumen maintains defined notification methods and timing requirements for initial outage alerts, progress updates, and restoration confirmation. Notifications provide timely, accurate status information throughout the lifecycle of the event.

Root Cause Analysis And Follow-Up. Any outage that results in a monthly service level agreement failure undergoes a formal root cause analysis. Lumen provides the State and affected PSAPs with a report detailing root causes, corrective actions, and committed completion dates. Quarterly follow-up reports document progress on corrective actions. If the State disagrees with the proposed root cause or corrective action plan, Lumen works in good faith with the State to revise the analysis and remediation plan.

Help Desk Operations. Lumen provides a 24x7x365 help desk staffed with technicians qualified to resolve the most common PSAP issues. All problem reports are submitted through the help desk, which generates a ticket for every issue. Calls are answered by a qualified technician within 60-seconds at least 90% of the time. Website-submitted tickets generate an immediate automated acknowledgment and a follow-up within five minutes at least 99% of the time. Technicians resolving new issues directly close at least half of tickets on first contact. These performance metrics are included in monthly key performance indicator reporting.

Ticket Ownership And Supplier Coordination. The help desk retains ownership of every issue from initiation through closure. Ticketing systems for suppliers and subcontractors involved in problem resolution are integrated so the help desk maintains full visibility and coordinated follow-up. While suppliers may perform technical remediation, Lumen ensures the State remains fully informed throughout investigation and restoration activities.

Sustained Outage Workarounds. For outages lasting more than 15-minutes, Lumen investigates and implements workarounds to restore at least partial service, even when root cause repairs are already underway, provided the workaround can be completed more quickly. This approach prioritizes service continuity while permanent remediation is completed.

5.5.6. Maintenance and Configuration Reports

Respondents must provide maintenance and configuration reports once a maintenance issue has been completed or an issue requiring maintenance is resolved. This report shall include a description of the event and the corrective or preventative action taken.

- Lists events by date/time range
- Provides drill down to specific events

LUMEN RESPONSE:

Lumen provides maintenance and configuration reporting that documents every maintenance activity performed on ESInet or NGCS elements after an issue has been resolved. Each report provides a clear description of the event, the corrective or preventive actions taken, and a complete record of all events associated with the maintenance window. Reports are generated as part of Lumen's governed change and maintenance processes and are made available to the State upon completion of each activity, supporting transparency, verification, and auditability.

Maintenance And Configuration Reporting. Lumen provides a maintenance and configuration report following completion of any maintenance activity or resolution of an issue requiring maintenance. Each report includes a clear description of the event, the root cause when applicable, and the corrective or preventive actions taken to resolve the issue. Reports are generated through controlled change and maintenance workflows to ensure consistency and completeness.

Event Listing By Date And Time Range. Maintenance and configuration reports include a chronological listing of all relevant events within the applicable date and time range. Event listings identify impacted system components, affected ESInet or NGCS elements, and the timing of actions taken during the maintenance window. This structure enables the State to efficiently correlate maintenance activities with observed operational or performance conditions.

Drill-Down To Specific Events. Reports provide drill-down capability to individual maintenance or configuration events for detailed review. Drill-down details include specific changes performed, impacted components, validation steps completed, and confirmation of service restoration. Supporting artifacts, such as change records and configuration summaries, are included where applicable to provide traceability and verification.

5.5.7. Discrepancy Reporting

Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The functional elements and service will support the NENA-STA-010.3 discrepancy report (DR) function. The discrepancy report function is intended to be generated by any entity that is using the data and finds a problem.

- *The Discrepancy Reporting web service will be used by a reporting entity to initiate a Discrepancy Report per NENA-STA-010.3.*
- *Discrepancy Resolution will follow the NENA-STA-010.3 standard to request the resolution to the DR and sends the resolution to the Resolution Uri parameter in the report request.*
- *Entities will have access to discrepancy status updates.*
- *The Discrepancy Report (DR) function supports a phased response like the following:*
- *The reporting entity creates the DR and submits it to the responding entity.*
- *The responding entity acknowledges the DR and provides an estimate of when it will be resolved.*
- *The reporting entity may request a status update and receive a response.*
- *The responding entity resolves the DR and reports its resolution to the reporting agency.*

All DRs MUST contain common data elements (a prolog) that include:

- *Time Stamp of Discrepancy Submittal*
- *Discrepancy Report ID (a unique value generated by the reporting entity)*
- *Discrepancy reporting entity FQDN*
- *Discrepancy reporting agent user ID*
- *Discrepancy reporting contact info*
- *Service or Instance in which the discrepancy exists.*
- *Discrepancy Report type (from the list of DRs in this section)*

- *Additional notes/comments*
- *Reporting entity's assessment of severity*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Support for NENA-STA-010.3 DR function generated by data users.*
- *Discrepancy Reporting web service for initiating a DR.*
- *Resolution per standard to Resolution URI.*
- *Access to status updates.*
- *Phased response (create/submit, acknowledge/estimate, status update, resolve/report).*
- *Common prolog elements (timestamp, ID, FQDN, user ID, contact, service/instance, type, notes, severity).*

LUMEN RESPONSE:

Lumen supports the NENA STA 010.3 Discrepancy Reporting (DR) web service function across all NGCS and ESInet Functional Elements so that any authorized entity using NG911 data can initiate, track, and resolve discrepancies. The implementation supports the complete DR lifecycle, including report creation, acknowledgment, status updates, and final resolution, and includes all required common prolog data elements to ensure standardized processing and interoperability. This approach provides Nebraska with a complete, standards-aligned discrepancy reporting capability that supports timely identification and resolution of NG911 data issues.

Support For NENA STA 010.3 Discrepancy Reporting. Lumen supports the NENA i3 Discrepancy Report function and enables authorized data-consuming entities to generate discrepancy reports in accordance with NENA STA 010.3. All NGCS and ESInet Functional Elements required under the Contract support DR initiation, receipt, processing, and management. Discrepancy reporting is integrated with Lumen's operational and support workflows to ensure timely investigation and resolution.

Discrepancy Reporting Web Service. Lumen provides a standards-based Discrepancy Reporting web service that accepts new discrepancy submissions using the NENA-compliant interface model. The service processes each submission, validates required prolog elements and discrepancy details, and routes the report to the appropriate responding entity. Secure access controls ensure that only authorized entities can submit and view discrepancy reports. Web service interface descriptions are included as ATTACHMENT X.

Resolution To Resolution URI. Discrepancy resolution follows the NENA i3 phased response model. The responding entity submits resolution information to the Resolution URI included in the original discrepancy report. Resolution responses include the corrective actions taken and confirmation of issue closure, aligned with standard expectations.

Status Update Access. Authorized reporting entities are able to query discrepancy status throughout the lifecycle of the report. Status information includes acknowledgment, estimated resolution timelines, in-progress updates, and final resolution notification. This access supports transparency and coordination between reporting and responding entities.

Phased Discrepancy Response Workflow. Lumen supports the full phased DR workflow defined by NENA STA 010.3. The reporting entity creates and submits the discrepancy report. The responding entity acknowledges receipt and provides an estimated resolution

timeframe. The reporting entity may request and receive status updates as work progresses. The responding entity completes the resolution and sends the final result to the reporting entity. Each phase is tracked and documented to support auditability and operational accountability.

Common Discrepancy Report Prolog Elements. All discrepancy reports include the required common prolog elements. These elements include the timestamp of discrepancy submittal, a unique discrepancy report identifier generated by the reporting entity, the reporting entity fully qualified domain name, the reporting agent user identifier, reporting contact information, the service or instance where the discrepancy exists, the discrepancy report type, additional notes or comments, and the reporting entity's severity assessment.

5.5.7.1. POLICY AND CORE ROUTING

5.5.7.1.1. Policy Store Discrepancy Report

A client of a Policy Store may report a discrepancy. This type of DR most commonly arises when a Policy Query returns an invalid Policy from the Policy Store. A Policy Owner may retrieve a policy it previously stored to verify the query returns an exact match to the one that was stored; if not, then a DR should be filed against the Policy Store. A policy store may report a discrepancy against itself to raise an issue.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy Store DR against Policy Store

LUMEN RESPONSE:

Lumen supports the NENA STA 010.3 Policy Store Discrepancy Reporting (DR) model so that any authorized client of the Policy Store can initiate a DR when a stored policy does not match the policy returned by a Policy Query. The implementation supports full reporting, tracking, and resolution of Policy Store discrepancies using the standard DR workflow defined in the i3 architecture, ensuring consistent handling and traceability.

Support For Policy Store Discrepancy Reporting. Lumen enables Policy Store clients to generate a DR when a retrieved policy fails to match the originally stored version. The Policy Store also supports generation of self-reported discrepancy reports when internal inconsistencies are detected. All required Functional Elements support initiation, receipt, processing, and management of Policy Store discrepancy reports in accordance with NENA STA 010.3.

NENA STA 010.3 Policy Store Discrepancy Reporting. Lumen supports the Policy Store DR function as defined in the NENA i3 architecture, allowing any authorized Policy Store client to report discrepancies. Discrepancies may be generated when a Policy Query returns an invalid or unexpected policy, or when a Policy Owner retrieves a stored policy and identifies a mismatch with the submitted version. The Policy Store accepts discrepancy reports initiated by external reporting entities and supports self-reported discrepancies to flag internal issues.

Standard Discrepancy Workflow And Resolution. Policy Store discrepancy handling follows the standard phased DR workflow, including receipt, acknowledgement, investigation, and resolution reporting. Resolution details are returned to the reporting entity using the designated Resolution URI provided in the original discrepancy submission, ensuring traceability, closure, and alignment with NENA STA 010.3 expectations.

5.5.7.1.2. Policy Discrepancy Report

A Policy Discrepancy Report function will be implemented per NENA-STA-010.3. Any entity (such as an ESRP) using a policy (such as a routing policy) will be able to report a discrepancy against the owner of the policy (e.g., a PSAP or an ESRP).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy DR against policy owner (e.g., PSAP/ESRP).

LUMEN RESPONSE:

Lumen implements the Policy DR function in accordance with NENA STA 010.3 so that any Functional Element using a policy can report a discrepancy directly to the Policy Owner. This includes scenarios such as an ESRP applying a routing or call handling policy that behaves inconsistently with its defined intent. The implementation supports the full DR lifecycle, allowing reporting entities to initiate a Policy DR, transmit it to the designated Policy Owner, and receive acknowledgments, status updates, and final resolution consistent with the i3 architecture.

Support For Policy Discrepancy Reporting Against The Policy Owner. Lumen enables any NENA-compliant Functional Element that consumes a stored policy to generate a Policy DR when a discrepancy is detected. Reports are directed to the Policy Owner identified in the NENA STA 010.3 model, whether that owner is a PSAP, an ESRP, or another authorized entity. All Policy DRs are processed using the standard DR exchange defined by the i3 architecture.

NENA STA 010.3 Policy Discrepancy Reporting Against The Policy Owner. Lumen implements the Policy DR function in full alignment with the NENA i3 architecture. Any authorized entity that consumes a policy, such as an ESRP applying routing or call handling logic, may initiate a DR against the policy owner. Discrepancies may include policies that behave inconsistently with defined rules, produce unexpected outcomes, or do not align with the policy owner's intent.

Standard Discrepancy Workflow And Resolution. Policy DRs follow the standard phased workflow defined by NENA STA 010.3. This includes submission of the DR by the reporting entity, acknowledgment by the policy owner, investigation and corrective action, and final resolution reporting. Resolution information is returned to the reporting entity using the designated resolution mechanism to confirm corrective action and formal closure.

5.5.7.1.3. Emergency Services Routing Proxy (ESRP) Discrepancy Report

An ESRP Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP or other entity will be able to report a discrepancy against an ESRP when a call is received that should not have been routed to the PSAP, or the ESRP has one or more queues whose fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally be expected. A routing problem may be the result of incorrect data in the ECRF (GIS data). Calls are sent to PSAPs by ESRPs (Emergency Services Routing Proxy), so a PSAP should report a problem to the ESRP. The ESRP, in turn, reports any suspected GIS problems to the ECRF.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 ESRP DR for misrouted calls, queue fullness, low volume; ESRP reports GIS issues to ECRF.*

LUMEN RESPONSE:

Lumen supports the ESRP DR mechanism in full alignment with NENA STA 010.3 so that PSAPs and other authorized entities can report routing-related discrepancies to the ESRP, and the ESRP can report suspected GIS issues to the ECRF when appropriate. The implementation supports the standard DR workflow defined in the i3 architecture and ensures that misrouted calls, queue state issues, and abnormal call volume conditions are detected, reported, tracked, and resolved using standardized processes.

Support For ESRP Discrepancy Reporting. Lumen supports an ESRP DR function that conforms to the NENA i3 standard. A PSAP or other authorized entity may submit a DR against an ESRP when calls are received that should not have been routed to the PSAP, when ESRP queue fullness indicates abnormal or degraded conditions, or when call volumes are lower than expected. The ESRP supports receipt, acknowledgment, investigation, and management of these DRs using the standard workflow.

Misrouting, Queue State, And Low Call Volume Reporting. ESRP DRs capture conditions where routing behavior does not align with expected outcomes, including incorrect PSAP delivery, sustained queue fullness, or unexpected reductions in call volume. These reports enable timely identification of routing or capacity issues that may affect service performance or availability.

ESRP Reporting To ECRF For Suspected GIS Issues. When ESRP investigation indicates that a routing issue may be caused by incorrect, incomplete, or outdated GIS data, the ESRP generates a Dr to the ECRF. This enables the ECRF to analyze and correct GIS data issues that impact routing accuracy and service behavior.

Standard Discrepancy Workflow And Resolution. ESRP DRs follow the standard phased workflow defined by NENA STA 010.3. The ESRP acknowledges receipt of the report, conducts investigation, provides status updates, and completes resolution reporting. Resolution details are returned to the originating entity using the designated resolution mechanism, ensuring traceability, accountability, and formal closure.

Tracking And Auditability. DR handling includes auditable tracking, correlation to routing policies and call records, and documented resolution outcomes. This supports operational transparency, performance analysis, and compliance verification across the NG911 environment.

5.5.7.2. LOCATION AND GIS SOURCES

5.5.7.2.1. Location Information Server (LIS) Discrepancy Report

The contractor will include a LIS Discrepancy Report function per NENA-STA-010.3. Any client of a LIS will be able to report a discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 LIS DR for LIS clients.*

LUMEN RESPONSE:

Lumen supports the Location Information Server (LIS) DR function defined in NENA STA 010.3 so that any authorized LIS client can report discrepancies when incorrect, inconsistent, outdated, or unexpected location information is detected. The implementation ensures that LIS-related discrepancies follow the same standardized DR workflow used throughout the NG911 system, providing consistent handling, tracking, and resolution.

Support For LIS Discrepancy Reporting. Lumen enables any authorized LIS client to generate a DR when a location response appears incorrect or inconsistent with expected results. LIS-related DRs are processed using the NENA-compliant reporting and resolution exchange defined in the i3 architecture.

NENA STA 010.3 LIS Discrepancy Reporting. Lumen supports a LIS DR function that conforms to the NENA i3 architecture. Any authorized client of the LIS may initiate a DR when location information appears inaccurate, incomplete, outdated, or otherwise inconsistent with expected outcomes. Discrepancies may be reported for location delivered by value or by reference, including issues identified during dereferencing or validation.

Standard Discrepancy Workflow And Resolution. The LIS accepts, logs, and routes DRs through the standard phased workflow defined by NENA STA 010.3. This workflow includes report submission, acknowledgement, investigation, status updates, and final resolution. Investigation and resolution activities may include validation against authoritative GIS data and review of LIS processing logic, filters, and data sources. Resolution results are documented and communicated back to the reporting entity to confirm corrective action and closure.

5.5.7.2.2. GIS Discrepancy Report

The contractor will include a GIS Discrepancy Report function per NENA-STA-010.3. With this mechanism, the LoST server or other entity will be able to report a discrepancy report against GIS data.

Expected reports include: A gap or overlap discovered when data is coalesced.

- *Incorrect information (such as the LoST server to query for information about an area)*
- *Bad GIS data (such as bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an address range issue on centerline, a general provisioning failure, or a malformed URI).*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 GIS DR for gaps/overlaps, incorrect info, bad data (geometry, attributes, ranges, provisioning, URI).*

LUMEN RESPONSE:

Lumen supports a GIS Discrepancy Report function in accordance with NENA STA 010.3 so that any authorized entity, including a LoST server or other NGCS component, can report issues discovered in GIS data used for routing and validation. The implementation supports all discrepancy types defined by the standard and ensures that GIS-related discrepancies are

submitted, tracked, and resolved through the NENA-compliant Discrepancy Report exchange, enabling triage and remediation by the responsible GIS authority.

Support For GIS Discrepancy Reporting. Lumen enables the submission of GIS-related Discrepancy Reports when gaps or overlaps are detected in coalesced data, when incorrect information is returned, or when bad GIS data is identified. Authorized entities may initiate discrepancy reports for issues affecting routing accuracy or validation outcomes, and all reports are processed using the standard i3 Discrepancy Report workflow.

NENA STA 010.3 GIS Discrepancy Reporting. Lumen supports a GIS Discrepancy Report function that conforms to the NENA i3 architecture and allows authorized entities, including the LoST server, to report discrepancies against GIS data. Discrepancies may be generated for gaps or overlaps identified during data coalescence or boundary processing, incorrect GIS information such as misidentified LoST servers or incorrect service area associations, and bad GIS data. Supported issues include invalid or incorrect geometry, duplicate or conflicting attributes, missing mandatory data elements, incorrect data types, address range issues on centerlines, provisioning failures, and malformed URLs.

Standard Discrepancy Workflow And Resolution. Submitted GIS Discrepancy Reports are logged, categorized, and routed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and final resolution. Resolution activities include validation against authoritative GIS sources and correction or re-provisioning as required to restore accurate routing behavior. Resolution results are documented and communicated back to the reporting entity to ensure traceability and formal closure.

5.5.7.2.3. MSAG Conversion Service Discrepancy Report

A MSAG Conversion Service (MCS) Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. An LSRG or other entity will be able to report a discrepancy against the MSAG Conversion Service (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR may also be filed when the conversion succeeded but the returned location from the MCS is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to MSAG or MSAG to PIDF-LO).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 MCS DR for failed conversions or invalid returned locations (PIDF-LO/MSAG bidirectional).*

LUMEN RESPONSE:

Lumen supports the MSAG Conversion Service DR function in accordance with NENA STA 010.3 so that any authorized entity relying on MSAG conversion can report discrepancies when conversion behavior does not match expected results. The implementation supports discrepancy reporting for both conversion directions, from legacy MSAG to NG911 PIDF-LO and from PIDF-LO to MSAG, ensuring consistent identification, tracking, and resolution of translation issues across the NG911 environment.

Support For MSAG Conversion Service Discrepancy Reporting. Lumen enables an LSRG or other authorized entity to submit a DR when an MSAG conversion fails but should have succeeded, or when a conversion succeeds but returns an invalid or unexpected result. This

includes discrepancies identified during conversion from PIDF-LO to MSAG and from MSAG to PIDF-LO, in alignment with NENA STA 010.3 requirements.

NENA STA 010.3 MSAG Conversion Discrepancy Reporting. Lumen supports a MSAG Conversion Service DR function that conforms to the NENA i3 architecture. Authorized entities may initiate a DR when a conversion failure occurs under conditions where success is expected, or when a successful conversion produces a location that is not MSAG valid or LVF valid. The mechanism supports bidirectional discrepancy reporting to address errors in either conversion direction.

Standard Discrepancy Workflow And Resolution. Submitted MSAG Conversion Service DRs are logged, acknowledged, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes investigation, status updates, and documented resolution. Resolution activities may include validation against authoritative MSAG, LVF, and GIS data, as well as correction or re-provisioning of conversion logic or reference data as required. Resolution results are communicated back to the reporting entity to confirm corrective action and closure.

5.5.7.2.4. LoST Discrepancy Report

The contractor will include a mechanism for any client of an LVF/ECRF/LoST server to report a discrepancy per NENA-STA-010.3.

The expected reports are:

- *The LoST server reports a location as invalid when the client believes it is valid.*
- *A LIS MAY report a discrepancy against an LVF (as well as against an Originating Service Provider) if a civic address provisioned by an Originating Service Provider for a fixed device is reported invalid by an LVF.*
- *The LoST server returned an incorrect route in a `findServiceResponse`.*
- *The LoST server returned an incorrect error or warning regarding the location.*
- *The `getServiceBoundaryResponse` is incorrect.*
- *The `listServicesResponse` is incorrect.*
- *The `listServicesByLocationResponse` is incorrect.*

Other discrepancies may be reported but are expected to be less common. These include:

- *A client received an address reported as valid that it considers invalid.*
- *Multiple mappings were returned when only one was expected.*
- *Incorrect service number(s) returned.*
- *Expired data returned.*
- *An incorrect `<Uri>` element was returned.*

A DR against a LoST server must also support the ability of the LoST server to report a discrepancy against the GIS data.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Mechanism for LVF/ECRF/LoST client to report discrepancies (invalid location, incorrect route/error/warning, incorrect responses).*
- *Support for LIS reports against LVF/OSP.*

- *LoST server reports against GIS data.*

LUMEN RESPONSE:

Lumen supports a discrepancy reporting mechanism for LVF, ECRF, and LoST interactions in full conformance with NENA STA 010.3 so that any authorized client of these services can submit a DR when location validation, routing, or service discovery behavior does not match expected results. The implementation supports all discrepancy scenarios identified by the State and ensures that LoST servers may also file DRs against GIS data when routing issues appear to originate from underlying datasets.

Support For LVF, ECRF, And LoST Client Discrepancy Reporting. Lumen enables any authorized client of an LVF, ECRF, or LoST server to initiate a DR when a LoST server returns an invalid location unexpectedly, provides an incorrect route, generates an error or warning condition, or produces incorrect responses. Supported responses include `getServiceBoundaryResponse`, `listServicesResponse`, and `listServicesByLocationResponse`. All submitted DRs are processed using the NENA-compliant DR exchange.

Mechanism For Client-Initiated Discrepancy Reporting. Lumen supports a LoST DR mechanism that conforms to the NENA i3 architecture and allows authorized clients to report discrepancies related to invalid location determinations, incorrect routing results, or unexpected errors or warnings. The mechanism supports reporting of incorrect service boundaries, inaccurate service lists, or services returned by location. DR submissions are logged and processed through the standard phased workflow, including acknowledgement, investigation, status updates, and resolution. LoST discrepancy workflows and example message structures are provided as ATTACHMENT X.

Support For LIS-Generated Discrepancy Reports Against LVF Or OSP. Lumen enables a Location Information Server to submit a DR against an LVF or an Originating Service Provider when a civic address provisioned for a fixed device is reported as invalid. The discrepancy workflow captures the reported condition, supports investigation of validation logic and source data, and provides status updates to the reporting LIS. Resolution outcomes are communicated back to the reporting entity to confirm corrective action or data remediation.

LoST Server Discrepancy Reports Against GIS Data. Lumen supports the ability for a LoST server to initiate DRs against GIS data when routing behavior or service boundary determinations indicate potential data issues. These discrepancy reports are routed for validation and correction of underlying GIS data to restore accurate service determination. GIS-related LoST discrepancy reports follow the standard discrepancy lifecycle with auditable tracking and documented resolution.

5.5.7.3. SIGNALING AND EDGE

5.5.7.3.1. SIP Discrepancy Report

The contractor will have a NENA-STA-010.3 SIP Discrepancy Report function. Entities that encounter an error communicating with another entity via SIP (such as a PSAP) will be able to report a discrepancy.

The expected reports are:

- *An initial INVITE request failed.*
- *A MESSAGE request failed.*

- *An OPTIONS request failed.*
- *A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.*
- *Required media stream (audio, text, video) failed to be accepted.*
- *Media problems during a dialog.*
- *Signaling failure.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 SIP DR for comm errors (failed requests, media stream failures, media problems, signaling failure).*

LUMEN RESPONSE:

Lumen supports a SIP DR function in accordance with NENA STA 010.3 so that any authorized entity using SIP to communicate with another NG911 element can report signaling or media-related errors through the standard DR workflow. The implementation supports reporting of failed SIP requests, media stream acceptance issues, in-dialog signaling problems, and media failures, ensuring consistent tracking and resolution across the NG911 environment.

Support For SIP Discrepancy Reporting. Lumen enables authorized entities to generate SIP DRs when SIP communication behavior does not match expected results. Supported conditions include failure of initial SIP transactions such as INVITE, MESSAGE, or OPTIONS requests; failure of SIP requests sent within an active dialog such as re-INVITE or INFO; required audio, text, or video media streams not being accepted during session establishment; media issues occurring during an active dialog; and detected SIP signaling failures.

NENA STA 010.3 SIP Discrepancy Reporting. Lumen supports a SIP DR function that conforms to the NENA i3 architecture and enables authorized entities to report SIP communication issues. DRs may be initiated for failed initial requests, in-dialog request failures, rejected or unavailable media streams, media problems during established sessions, and signaling errors that impact call setup, modification, or continuity.

Standard Discrepancy Workflow And Resolution. Submitted SIP DRs are logged, acknowledged, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes investigation, status updates, and documented resolution reporting. SIP DRs are correlated with call signaling records and media telemetry to support efficient root cause analysis and remediation. Resolution outcomes are communicated back to the reporting entity to confirm corrective action and closure.

5.5.7.3.2. Border Control Function (BCF) Discrepancy Report

The contractor will have the BCF Discrepancy Report function as defined in NENA-STA-010.3. This function allows for an entity routing traffic through (to or from) a BCF to report a discrepancy.

The expected reports are:

- *Traffic incorrectly blocked before a dialog has been established (e.g., an INVITE, MESSAGE, or OPTIONS request, or response blocked).*
- *Traffic incorrectly blocked during a dialog.*

- *SIP signaling is inappropriately modified or dropped.*
- *Session Description Protocol (SDP) incorrectly regenerated during B2BUA/media anchoring.*
- *Media relayed with loss.*
- *Traffic permitted that should have been blocked because a designated bad actor generated it.*
- *Traffic permitted that should have been blocked for some other reason.*
- *QoS inconsistency.*
- *Invalid or improper Call Detail Recording.*
- *TTY to RTT transcoding errors.*
- *Firewall (non-SIP) errors.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 BCF DR for traffic routing issues (blocked/modified/dropped traffic, SDP regeneration, media loss, permitted bad actor traffic, QoS inconsistency, invalid CDR, TTY-RTT errors, firewall errors).*

LUMEN RESPONSE:

Lumen provides a Border Control Function (BCF) DR function in full conformance with NENA STA 010.3 so that any authorized entity sending or receiving SIP signaling or media through a BCF can report discrepancies related to traffic handling, signaling behavior, or media treatment. The implementation enables detection, tracking, and resolution of BCF-specific issues that may affect NG911 performance, routing accuracy, and media delivery using the standard Discrepancy Report workflow defined in the i3 architecture.

Support For BCF Discrepancy Reporting. Lumen enables authorized entities to submit DRs for BCF conditions defined in NENA STA 010.3. Supported discrepancy types include SIP requests or responses incorrectly blocked prior to dialog establishment, traffic blocked during an active dialog, improper modification or loss of SIP signaling, incorrect Session Description Protocol regeneration during B2BUA operation or media anchoring, and media relayed with loss or impairment.

NENA STA 010.3 BCF Discrepancy Reporting. Lumen supports a BCF DR mechanism that conforms to the NENA i3 architecture and allows any authorized entity routing traffic through a BCF to report discrepancies. DRs may be initiated for traffic incorrectly blocked before dialog establishment, including INVITE, MESSAGE, or OPTIONS requests or responses, as well as for traffic incorrectly blocked during an active dialog or SIP signaling that is modified or dropped inappropriately.

Supported BCF Discrepancy Conditions. The BCF DR function supports reporting of Session Description Protocol regeneration errors during B2BUA processing or media anchoring, media relayed with loss, and conditions where traffic generated by a designated bad actor is incorrectly permitted or traffic that should have been blocked for policy reasons is allowed. Additional supported discrepancy types include quality of service inconsistencies, invalid or improper call detail records, TTY to RTT transcoding errors, and firewall related errors that affect NG911 traffic handling.

Standard Discrepancy Workflow And Resolution. All BCF DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This

workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Discrepancy handling supports correlation to call signaling records, media telemetry, and BCF policy enforcement actions to enable efficient root cause analysis and remediation. Resolution outcomes are communicated back to the reporting entity to confirm corrective action and formal closure.

5.5.7.4. NETWORK AND INFRASTRUCTURE

5.5.7.4.1. Network Discrepancy Report

A Network Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. Any entity will be able to report a general networking discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 general networking DR.

LUMEN RESPONSE:

Lumen supports a general networking DR function in accordance with NENA STA 010.3 so that any authorized entity can report network-related issues affecting NG911 operations. The implementation enables submission of DRs for conditions that do not fall under a more specific DR category but still impact routing, connectivity, performance, or reliability of ESInet or NGCS services. All general networking discrepancies are handled through the standard i3 DR workflow to ensure consistent tracking, investigation, and resolution.

Support For General Networking Discrepancy Reporting. Lumen provides a standards-aligned mechanism for submitting NENA STA 010.3 general networking DRs. Authorized entities may record and escalate issues related to network behavior, connectivity anomalies, or unexpected operational conditions across the ESInet and NGCS. This capability ensures that network-level issues affecting NG911 service delivery are formally documented and addressed.

NENA STA 010.3 General Networking Discrepancy Reporting. Lumen supports a Network DR mechanism that conforms to the NENA i3 architecture and enables any authorized entity to report general networking issues. Discrepancy Reports may be initiated for conditions affecting network performance, availability, or behavior that do not align with another specific Functional Element DR type.

Standard Discrepancy Workflow And Resolution. General networking DRs are logged, categorized, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Network DR handling is integrated with Lumen's 24x7 monitoring and operational support processes to enable timely diagnosis and remediation. Resolution outcomes are documented and communicated back to the reporting entity to ensure transparency and formal closure.

5.5.7.5. SECURITY AND TRUST

5.5.7.5.1. Permissions/Security/Authentication Discrepancy Report

The contractor will deliver a Permissions/Security/Authentication Discrepancy Report function as defined by NENA-STA-010.3. Entities that identify a security issue or a

permissions or authentication error that is believed to be incorrect, will be capable of reporting a discrepancy using the DR interface of the entity or element believed to be responsible for the discrepancy.

The expected reports are:

- *Unable to authenticate.*
- *Unable to SUBSCRIBE to an event package.*
- *Permitted to SUBSCRIBE to an event package when it should have been denied.*
- *Unable to read a resource.*
- *Unable to write/modify a resource.*
- *Unable to delete a resource.*
- *Able to read a resource when it should have been denied.*
- *Able to write/modify a resource when it should have been denied.*
- *Able to delete a resource when it should have been denied.*
- *Unable to establish secure communication (e.g., TLS certificate is invalid or TLS failure).*
- *Unable to verify digital signature of a resource (e.g., a routing policy signature verification failed, or the certificate chain is invalid or contains an untrusted authority).*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Reports for security/permissions/auth errors (unable to auth/subscribe/read/write/delete, able when denied, TLS/certificate/signature failures).*

LUMEN RESPONSE:

Lumen supports a Permissions, Security, and Authentication DR function in accordance with NENA STA 010.3 so that any authorized NG911 entity can report errors involving authentication, authorization, or secure communications. The implementation ensures that failures in access control, permissions enforcement, or security validation are captured, tracked, and routed to the responsible Functional Element through the standard DR workflow defined in the i3 architecture.

Support For Security, Permissions, And Authentication Discrepancy Reporting. Lumen enables authorized entities to submit DRs when authentication fails, when authorization behavior is incorrect, or when access control does not operate as expected. Supported conditions include inability to authenticate, incorrect permission grants or denials, improper subscription handling for event packages, and situations where access to resources cannot be read, written, modified, or deleted as intended. DRs may also be submitted when a resource is accessible despite access being explicitly denied.

TLS And Certificate Related Discrepancy Reporting. Lumen supports DRs for failures to establish secure communications due to TLS or certificate issues. Supported conditions include invalid or expired certificates, TLS negotiation failures, untrusted or incomplete certificate chains, and failures in trust validation. The mechanism also supports reporting of digital signature verification failures, including invalid signatures or certificate authority trust issues.

NENA STA 010.3 Security And Authentication Discrepancy Reporting. Lumen supports a Permissions, Security, and Authentication DR function that conforms to the NENA i3 architecture. Authorized entities may initiate DRs for authentication failures, authorization errors, subscription anomalies, resource access discrepancies, and secure communication failures affecting NG911 operations.

Standard Discrepancy Workflow And Resolution. All Permissions, Security, and Authentication DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to confirm corrective action and formal closure, ensuring transparency and accountability across the NG911 environment.

5.5.7.5.2. Log Signature/Certificate Discrepancy Report

A Log Signature/Certificate Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the signature verification fails, it will be able to report the discrepancy to the entity that generated the LogEvent.

The expected cases for this Discrepancy Report are:

- *The certificate cannot be obtained (no “x5c” nor “x5u” field provided).*
- *The “x5u” field cannot be resolved or does not resolve to a valid certificate.*
- *The “x5u” field is present but the “x5t#256” field is missing, or the thumbprint specified does not match the certificate obtained from the “x5u” field.*
- *The signature of a LogEvent does not verify.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 report for certificate/signature issues (unobtainable/invalid cert, mismatched thumbprint, failed verification).*

LUMEN RESPONSE:

Lumen supports a Log Signature and Certificate DR function in accordance with NENA STA 010.3 so that any authorized entity verifying LogEvent signatures can report discrepancies related to certificate retrieval, certificate validity, thumbprint mismatches, or failed signature verification. The implementation ensures that integrity-related issues in logging workflows are captured, tracked, and routed to the originating Functional Element through the standard DR workflow defined in the i3 architecture.

Support For Log Signature And Certificate Discrepancy Reporting. Lumen enables authorized entities to submit DRs when LogEvent signature validation does not behave as expected. Supported conditions include cases where a certificate cannot be obtained because neither an x5c nor an x5u field is present, where an x5u field cannot be resolved or does not resolve to a valid certificate, and where an x5u field is present but the corresponding x5t#256 thumbprint is missing or does not match the retrieved certificate.

NENA STA 010.3 Log Signature And Certificate Discrepancy Reporting. Lumen supports a Log Signature and Certificate DR mechanism that conforms to the NENA i3 architecture.

DRs may be initiated for invalid, expired, or untrusted certificates; unresolved or incorrect certificate references; thumbprint mismatches; and LogEvents whose digital signatures fail verification. These reports enable consistent identification of integrity failures across NG911 logging workflows.

Standard Discrepancy Workflow And Resolution. All Log Signature and Certificate DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to confirm corrective action and formal closure, ensuring integrity assurance and auditability of NG911 logging operations.

5.5.7.6. DATA AND LOGGING

5.5.7.6.1. Logging Service Discrepancy Report

The contractor will have a Session Recording Client (SRC) or any entity generating logging events to, or retrieving logging records from, a Logging Service that may report a discrepancy.

The expected reports are:

- *An SRC encountered an error inviting the SRS.*
- *LogEvent returned an error when it should not have.*
- *RetrieveLogEvent returned an error when it should not have.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *SRC/entity reports for errors in inviting SRS, LogEvent, or RetrieveLogEvent.*

LUMEN RESPONSE:

Lumen supports a Session Recording Client DR function in accordance with NENA STA 010.3 so that any Session Recording Client, or any authorized entity generating or retrieving LogEvents from a Logging Service, can report errors encountered during recording or logging interactions. The implementation ensures that issues related to Session Recording Server invitations, LogEvent submission, and LogEvent retrieval are captured, tracked, and routed through the standard DR workflow defined in the i3 architecture.

Support For Session Recording Client And Logging Service Discrepancy Reporting.

Lumen enables a Session Recording Client or any authorized entity interacting with the Logging Service to submit a DR when recording or logging operations do not behave as expected. Supported conditions include errors encountered when inviting the Session Recording Server, LogEvent operations that return an error when successful processing is expected, and failures of RetrieveLogEvent operations.

NENA STA 010.3 Logging Service Discrepancy Reporting. Lumen supports a Logging Service DR mechanism that conforms to the NENA i3 architecture. A Session Recording Client or any authorized entity generating LogEvents to, or retrieving LogEvents from, a Logging Service may initiate a DR for errors affecting recording, logging, or retrieval workflows. This includes discrepancies related to SRS invitation handling, LogEvent submission failures, and retrieval errors.

Standard Discrepancy Workflow And Resolution. All Session Recording Client and Logging Service DRs are logged, acknowledged, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to confirm corrective action and formal closure, ensuring integrity, traceability, and accountability for NG911 recording and logging operations.

5.5.7.6.2. ADR/IS-ADR Discrepancy Report

An ADR/IS-ADR Discrepancy Report mechanism per NENA-STA-010.3 will be provided. A PSAP, ESRP, ECRF, or other entity or function will be able to report a discrepancy against an ADR or IS ADR.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ADR/IS-ADR DR by PSAP/ESRP/ECRF/etc.

LUMEN RESPONSE:

Lumen supports an Additional Data Repository and Incident Specific Additional Data Repository DR function in accordance with NENA STA 010.3 so that any qualified NG911 element can report issues involving additional data used during call processing or routing workflows. This includes PSAPs, ESRPs, ECRFs, and other authorized entities that rely on ADR or IS ADR data. The implementation ensures that discrepancies related to additional data are captured, tracked, and resolved through the standard DR workflow defined in the i3 architecture.

Support For ADR And IS ADR Discrepancy Reporting. Lumen enables PSAPs, ESRPs, ECRFs, and other authorized entities to generate NENA STA 010.3 compliant DRs when ADR or IS ADR responses are incorrect, incomplete, inconsistent, unavailable, or otherwise invalid. This capability ensures that issues affecting the availability, accuracy, or integrity of additional data associated with an incident are formally documented and addressed.

NENA STA 010.3 ADR And IS ADR Discrepancy Reporting. Lumen supports an Additional Data Repository and Incident Specific Additional Data Repository DR mechanism that conforms to the NENA i3 architecture. Authorized entities, including PSAPs, ESRPs, ECRFs, and other NG911 Functional Elements, may initiate DRs when issues are identified with additional data referenced or retrieved from an ADR or IS ADR. Supported discrepancy conditions include problems related to data accessibility, correctness, completeness, or integrity.

Standard Discrepancy Workflow And Resolution. All ADR and IS ADR DRs are logged, categorized, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to confirm corrective action, data remediation, or final disposition, ensuring transparency and formal closure.

5.5.7.7. PSAP OPERATIONS AND TREATMENTS

5.5.7.7.1. PSAP Call Taker Discrepancy Report

The contractor will include the ability for a PSAP, downstream agency, or other entity to report a discrepancy against a PSAP Call Taker when a call is received that should not have been transferred to the reporting entity.

The resolution parameter in a DiscrepancyResolution report per NENA-STA-010.3 requires one of the following tokens:

- *CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)*
- *TransferCorrect (the transfer was correct)*
- *NoDiscrepancy*
- *OtherResponse*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Reports against PSAP Call Taker for erroneous transfers.*
- *Resolution tokens (CallTakerAdvised, TransferCorrect, NoDiscrepancy, OtherResponse).*

LUMEN RESPONSE:

Lumen supports a PSAP Call Taker DR function in accordance with NENA STA 010.3 so that a PSAP, downstream agency, or other authorized entity can report discrepancies when a call is transferred in error. The implementation enables authorized entities to submit a DR through the standard i3 interface when a call should not have been transferred to the receiving agency, ensuring that transfer issues are captured, reviewed, and resolved using a consistent, standards-based workflow.

Support For PSAP Call Taker Discrepancy Reporting. Lumen enables authorized reporting entities to generate a DR against a PSAP Call Taker when an erroneous transfer occurs. The DR captures transfer context and associated call information needed to support investigation, review, and determination of whether the transfer aligned with operational expectations.

NENA STA 010.3 PSAP Call Taker Discrepancy Reporting. Lumen supports a PSAP Call Taker DR mechanism that conforms to the NENA i3 architecture. A PSAP, downstream agency, or other authorized entity may initiate a DR when a call is received that should not have been transferred to the reporting entity. All DRs are processed using the standard i3 Discrepancy Report exchange.

Resolution Tokens And Standardized Outcomes. Lumen supports the required NENA resolution values for returning a DiscrepancyResolution. Supported resolution tokens include CallTakerAdvised, TransferCorrect, NoDiscrepancy, and OtherResponse. These standardized outcomes allow the responding entity to document the result of the investigation in a consistent and auditable manner.

Standard Discrepancy Workflow And Resolution. All PSAP Call Taker DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to

confirm corrective action, determination, or closure, supporting transparency and accountability across NG911 operations.

5.5.7.7.2. Call Transfer Failure Discrepancy Report

A Call Transfer Failure Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP, LSRG, or other entity will be able to report a discrepancy against a transfer entity when a transfer fails. The notification should be made to both the entity originating the transfer and the entity receiving the transfer.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 mechanism for transfer failures, notified to originating/receiving entities.*

LUMEN RESPONSE:

Lumen supports a Call Transfer Failure DR function in accordance with NENA STA 010.3 so that any PSAP, LSRG, or other authorized NG911 entity can report a discrepancy when a call transfer fails. The implementation ensures that discrepancy notifications are generated for both the originating entity and the intended receiving entity so that all parties are aware of the failure and can respond in a coordinated manner using the standard DR workflow defined in the i3 architecture.

Support For Call Transfer Failure Discrepancy Reporting. Lumen enables PSAPs, LSRGs, and other authorized entities to submit NENA STA 010.3 compliant DRs when a call transfer does not complete successfully. DRs may be initiated regardless of whether the failure occurs during transfer initiation, negotiation, or final handoff. This capability ensures that transfer failures impacting NG911 operations are formally captured and addressed.

NENA STA 010.3 Call Transfer Failure Discrepancy Reporting. Lumen supports a Call Transfer Failure Discrepancy Report mechanism that conforms to the NENA i3 architecture. The DR workflow captures relevant transfer context and associates the discrepancy with call signaling records and logging artifacts to support investigation, troubleshooting, and remediation.

Notification To Originating And Receiving Entities. When a Call Transfer Failure DR is generated, notification is provided to both the entity that initiated the transfer and the entity designated to receive the call. This dual notification ensures shared visibility, coordinated investigation, and consistent understanding of the failure across all involved parties.

Standard Discrepancy Workflow And Resolution. All Call Transfer Failure DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to all relevant entities to confirm corrective action and formal closure.

5.5.7.7.3. Interactive Media Response (IMR) Discrepancy Report

An Interactive Media Response (IMR) Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. Any entity aware of a discrepancy at an Interactive Media Response (IMR) will be able to report a discrepancy at it.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 IMR DR.

LUMEN RESPONSE:

Lumen supports an Interactive Media Response DR function in accordance with NENA STA 010.3 so that any authorized NG911 entity can report issues related to Interactive Media Response behavior through the standard DR workflow. The implementation ensures that discrepancies observed in IMR interactions are captured, routed, tracked, and resolved using the same interoperable processes applied to all other NENA-defined DR types.

Support For Interactive Media Response Discrepancy Reporting. Lumen enables any authorized entity interacting with an Interactive Media Response function to generate a NENA STA 010.3 compliant DR when IMR behavior is incorrect, unexpected, or erroneous. Supported conditions include IMR prompts, interaction flows, or media handling that negatively impact NG911 call processing or caller interaction.

NENA STA 010.3 Interactive Media Response Discrepancy Reporting. Lumen supports an Interactive Media Response DR mechanism that conforms to the NENA i3 architecture. Any authorized entity that becomes aware of an issue with IMR behavior may initiate a DR against the IMR. Discrepancies may be reported for IMR interactions, response logic, or media behavior that does not perform as expected within the call flow.

Standard Discrepancy Workflow And Resolution. All Interactive Media Response DRs are logged, categorized, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. IMR discrepancy handling integrates with Lumen's broader NG911 discrepancy management and operational processes to support efficient analysis, corrective action, and formal closure.

5.5.7.8. EXTERNAL PROVIDERS

5.5.7.8.1. Originating Service Provider Discrepancy Report

A mechanism for Originating Service Providers to file Discrepancy Reports will follow NENA-STA-010.3. The service allows an entity to create a discrepancy against an Originating Service Provider when a location provided by the Originating Service Provider fails validation.

- *An ECRF or ESRP or PRF or PSAP may report a discrepancy when a default location is used for routing because the location is missing or not usable.*
- *An LNG or other entity may report a call received without ANI.*
- *An LNG or ESRP or other entity may report that a badly formed PIDF-LO was received, or a location query timed out without receiving a PIDF-LO.*
- *An LSRG or other entity may report that a call was dropped or terminated without appropriate signaling.*
- *A PSAP may report a discrepancy when a civic location received with a fixed (wireline) call is incorrect.*
- *A BCF, ESRP, PSAP, or other entity may report an incorrectly formed call (e.g., a SIP INVITE that is badly formed, lacks certain header fields or body parts, etc.).*

- A BCF, ESRP, PSAP, or other entity, may report that an unusually large call volume (which might suggest a DoS or other attack) or an unusually low call volume is being generated by the Originating Service Provider.
- An Originating Service Provider may report a discrepancy against itself to raise an issue to be addressed.
- An entity may report a discrepancy when an Additional Data Reference included in the call is invalid.
- An entity may report a discrepancy when an Additional Data value is invalid.
- The Secure Telephone Identity-Verification Service (STIVS) FE may report a Secure Telephone Identity verification failure to an Originating Network.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism per NENA-STA-010.3 for OSP DRs (invalid/missing location, no ANI, bad PIDF-LO/query timeout, dropped call, incorrect civic, badly formed INVITE, unusual volume, invalid Additional Data, STIVS verification failure).
- Self-reports by OSP.

LUMEN RESPONSE:

Lumen supports an Originating Service Provider DR function in accordance with NENA STA 010.3 so that any authorized NG911 entity can report discrepancies related to OSP-supplied call, signaling, or location information. The implementation supports all discrepancy conditions identified by the State and ensures that issues involving missing or invalid data, malformed signaling, unexpected call behavior, and abnormal call volume patterns are captured, tracked, and resolved using the standard DR workflow. Lumen also supports self-reporting by an Originating Service Provider when issues are identified internally.

Support For Originating Service Provider Discrepancy Reporting. Lumen enables authorized entities, including the ECRF, ESRP, PRF, PSAP, LNG, LSRG, BCF, and other NG911 Functional Elements, to submit DRs when OSP-provided information or call behavior is incorrect, incomplete, or inconsistent with expected results. Supported scenarios include missing or unusable location information resulting in default routing, calls received without ANI, malformed or missing PIDF-LO, PIDF-LO query timeouts, calls dropped without appropriate signaling, incorrect civic location on fixed calls, and malformed SIP INVITE requests.

NENA STA 010.3 Originating Service Provider Discrepancy Reporting. Lumen supports an Originating Service Provider DR mechanism that conforms to the NENA i3 architecture. DRs may also be initiated for unusually high or unusually low call volume patterns that indicate abnormal or potentially malicious traffic conditions. Additional supported discrepancy types include invalid Additional Data References, invalid Additional Data values, and Secure Telephone Identity verification failures reported by the appropriate Functional Element to the originating network.

Support For Originating Service Provider Self-Reporting. Lumen supports the ability for an Originating Service Provider to generate a DR against itself in accordance with NENA STA 010.3 when an internal issue is identified. This capability allows OSPs to proactively document, investigate, and remediate issues that may impact NG911 call processing, routing accuracy, or data integrity.

Standard Discrepancy Workflow And Resolution. All Originating Service Provider DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity to confirm corrective action, disposition, and formal closure, ensuring transparency and accountability across NG911 operations.

5.5.7.9. TEST AND TOOLS

5.5.7.9.1. Test Call Generator Discrepancy Report

A Test Call Generator Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When a Test Call Generator encounters errors initiating or processing a test call, it reports the discrepancy to the PSAP that should have received the test call.

The expected cases for this Discrepancy Report are:

- *An initial INVITE request failed.*
- *A MESSAGE request failed.*
- *An OPTIONS request failed.*
- *A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.*
- *Loopback media stream (audio, text, video) failed to be accepted.*
- *Loopback media problems during the test dialog.*
- *Signaling failure.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *NENA-STA-010.3 Test Call Generator DR to PSAP for errors (failed requests, loopback failures, media/signaling issues).*

LUMEN RESPONSE:

Lumen supports a Test Call Generator DR function in accordance with NENA STA 010.3 so that any authorized entity performing NG911 test calls can report failures encountered during call initiation or processing. The implementation ensures that discrepancies identified through test call workflows are captured, tracked, and routed to the appropriate PSAP for review and correction using the standard Discrepancy Report workflow defined in the i3 architecture.

Support For Test Call Generator Discrepancy Reporting. Lumen enables a Test Call Generator to submit a NENA STA 010.3 compliant DR when test call behavior does not match expected results. Supported conditions include failure of initial SIP transactions such as INVITE, MESSAGE, or OPTIONS requests; failure of SIP requests within an active dialog such as re-INVITE or INFO; loopback audio, text, or video streams not being accepted; media problems occurring during a test dialog; and signaling failures that prevent proper execution of the test call.

NENA STA 010.3 Test Call Generator Discrepancy Reporting To PSAP. Lumen supports a Test Call Generator DR mechanism that conforms to the NENA i3 architecture. When a test call fails to initiate or process correctly, the Test Call Generator generates a DR and reports the issue to the PSAP that was intended to receive the test call. The DR captures relevant call context and associated signaling information to support investigation and remediation.

Standard Discrepancy Workflow And Resolution. All Test Call Generator DRs are logged, tracked, and processed through the standard phased workflow defined by NENA STA 010.3. This workflow includes acknowledgement, investigation, status updates, and documented resolution reporting. Resolution outcomes are communicated back to the reporting entity and the affected PSAP to confirm corrective action and formal closure, ensuring transparency and accountability for test call validation activities.

Deliverables - Logging, Reporting, and Call Detail Records

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires complete, auditable visibility into NG911 call processing, system behavior, and administrative activity to support operations, reporting, and compliance. Lumen complies by providing representative sample logs, Call Detail Record schemas, documented retention procedures, and role-based access control policies that define how logging data is generated, protected, accessed, and retained across the ESInet and NGCS environments.

Lumen further complies by demonstrating CDR generation and end-to-end reporting capabilities, including the ability to search, filter, and export records and to produce operational reports required for system oversight and performance monitoring. Demonstrations confirm that CDRs accurately reflect call processing activity, routing decisions, media handling, and call outcomes, and that reporting functions support both standardized and ad-hoc analysis without impacting NG911 service performance.

In addition, Lumen provides evidence of tamper-evident log storage and comprehensive audit trails for administrative actions and configuration changes. These controls ensure the integrity of logs and records, support forensic analysis, and enable traceability of privileged activity across NG911 systems. Collectively, these deliverables provide the State with verifiable assurance that logging and reporting mechanisms are accurate, secure, and operationally effective throughout the lifecycle of NG911 services.

5.6. Installation Requirements

Respondents are required to assume the primary project management and installation management role for their NG911 system. The State will aid and coordinate support for some aspects of the installation but will be looking for the Respondent (Contractor) to provide all installation services.*

Installation as defined in this RFP includes:

- Coordination with PSAPs
- System and service migration (i.e., logging, recording, CAD)
- Coordination with OSPs
 - Ingress
 - Core
 - Egress

- Coordination with current 911 system service provider
 - Ingress
 - Core
 - Egress
- Traffic migration
- Data migration
- Staging
- Testing
- Pre-cutover
- Cutover planning
- Training

The Respondent must, at a minimum, provide installation, maintenance, and support services for the duration of the contract period. Customer service support functions are identified below (§E-9, et seq.) and must be included in the Proposal to ensure that the network is fully supported.

LUMEN RESPONSE:

Lumen assumes primary project management and installation management responsibility for deployment of Nebraska's NG911 system. The approach includes direct coordination with PSAPs, Originating Service Providers, and the current 911 system provider, and spans all phases of installation, migration, staging, testing, cutover, and training. Lumen provides installation, maintenance, and support services for the full contract lifecycle, ensuring that the network and all components delivered under the Contract remain fully supported and operational.

Coordination With PSAPs. Lumen coordinates directly with PSAPs to schedule installation activities, gather required technical and operational information, and prepare for system transitions. Coordination activities support operational readiness throughout deployment and ensure PSAPs are informed and prepared for each phase of implementation.

System And Service Migration. Lumen manages migration of systems and services required for NG911 operations, including logging, recording, CAD, and other dependent platforms. Migration activities are planned and executed to maintain continuity of operations while services transition to the NG911 environment.

Coordination With OSPs And Current 911 Provider. Lumen coordinates ingress, core, and egress connectivity with Originating Service Providers and with the current 911 system service provider. This coordination supports traffic migration, interworking, and continuity during cutover and transition periods.

Traffic And Data Migration. Lumen supports migration of call traffic between legacy and NG911 components and manages required data migration to ensure operational readiness. Traffic and data migration activities are planned, executed, and validated to minimize risk and service disruption.

Staging, Testing, And Cutover. Lumen manages staging, testing, pre-cutover activities, and cutover planning to ensure accurate configuration and controlled transition into production. Cutover execution follows a well-sequenced approach designed to preserve service availability and reduce operational risk.

Training. Lumen provides training necessary to support State and PSAP operations during and after deployment. Training activities support operational readiness and successful adoption of the NG911 system.

Installation, Maintenance, And Support Services. Installation, maintenance, and support training is provided for the duration of the contract period. As the incumbent NG911 provider, Lumen brings continuity of operations and established knowledge of the existing network, interfaces, and service dependencies. This experience enables a controlled, well-sequenced migration that minimizes risk, avoids unnecessary rework, and supports a seamless transition while maintaining full 911 service availability. Ongoing maintenance, support, and customer service functions are integrated into Lumen's operational model to ensure continuous system availability, performance, and reliability throughout the contract term.

5.6.1. Installation Services

The Contractor is responsible for the installation of all requirements listed in the RFS and attachments and any other functional elements such as power and UPS as necessary to implement their NG911 solution. Devices that are installed at a PSAP may require analysis of the power and backup power supply at that PSAP. In some cases, the contractor may need to remediate issues to ensure their device has the resources needed. The State may aid coordination support for some aspects (such as approvals and scheduling) of the installation but is relying upon the Contractor to perform all installation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Methodology for installation of all NG911 system components and explain the approach to completing installation of the delivery of NG911 traffic. The methodology must include coordination with OSPs, PSAPs and other potential networks that can enhance the delivery of 911 traffic across the system.*
- *Coordination methodology to interconnect with all current telecommunication companies that are responsible for 911 call delivery and explain how these providers are accounted for during implementation.*
- *Plan to coordinate with all current 911 system service providers.*
- *Installation services to be provided and outline the roles and responsibilities of the Contractor and Subcontractor(s) during installation. Installation tasks as defined include, but may not be limited to:*
 - *Coordination with PSAPs*
 - *System and service migration (i.e., logging, recording, CAD)*
 - *UPS integration to support a minimum 3-hour backup validated with an MTTR / MTBF calculation*
 - *Coordination with OSPs*
 - *Coordination with current 911 system service provider*
- *Traffic migration*
- *Data migration*
- *Staging*
- *Acceptance testing*
- *Cutover planning*
- *Training*

LUMEN RESPONSE:

Lumen provides full installation management for all NG911 system components required under the RFS, including supporting Functional Elements such as power and uninterruptible power supply equipment necessary to ensure reliable system operation. The installation approach includes evaluation of PSAP power and backup power capabilities, coordination with all involved parties, and remediation where required so NG911 devices have appropriate resources. While the State may assist with coordination and scheduling, Lumen performs all installation services necessary to deliver NG911 traffic and transition Nebraska to the proposed solution.

Installation Methodology And NG911 Traffic Delivery. Lumen applies a structured, phased installation methodology that supports end-to-end deployment of all NG911 system components required for delivery of NG911 traffic. Installation activities are coordinated across ingress, core, and egress components to ensure continuity of service and controlled activation. The methodology includes direct coordination with PSAPs, Originating Service Providers, and interconnected networks to ensure all interconnections and dependencies are addressed as each component is deployed.

Coordination With Telecommunications Providers. Lumen coordinates directly with all current telecommunications providers responsible for 911 call delivery. Implementation planning incorporates each provider's ingress, core, and egress paths, provider-specific requirements, interface definitions, test plans, and cutover sequencing. Interconnections are validated prior to production traffic migration to ensure interoperability and continuity.

Coordination With Current 911 System Provider. Lumen leads coordination with the incumbent 911 system service provider to support seamless interworking and service continuity during migration and cutover activities. Coordination includes shared planning for traffic migration, data migration, testing, and cutover sequencing to minimize operational risk and maintain uninterrupted 911 services.

Installation Services, Roles, And Responsibilities. Lumen assumes overall responsibility for installation services, including project management, scheduling, and execution. Subcontractors, where used, operate under Lumen's direction and governance with clearly defined roles and responsibilities. Installation tasks include coordination with PSAPs for site readiness and scheduling, system and service migration such as logging, recording, CAD, and associated interfaces, integration of UPS and backup power to support a minimum three-hour backup capability validated using MTTR and MTBF considerations, coordination with Originating Service Providers, coordination with the current 911 system service provider, traffic migration, data migration, staging, acceptance testing, cutover planning, and training.

Traffic Migration. Lumen plans and executes traffic migration using controlled, staged approaches designed to minimize risk and service disruption. Migration activities include validation testing prior to live traffic cutover and defined rollback procedures as required to preserve service continuity.

Data Migration. Lumen manages data migration activities to ensure accuracy, integrity, and continuity of operational data. Data migration is validated prior to cutover to support uninterrupted NG911 operations.

Staging. Lumen performs staging activities to prepare systems, configurations, and integrations prior to deployment. Staging supports early validation of system readiness and reduces deployment risk.

Acceptance Testing. Lumen conducts acceptance testing in coordination with the State, PSAPs, and other stakeholders. Testing validates system functionality, interoperability, and readiness prior to cutover.

Cutover Planning. Lumen develops and executes detailed cutover plans that define sequencing, roles, communications, and contingency procedures. Cutover planning emphasizes continuity of service and rapid issue resolution.

Training. Lumen provides role-based training supporting NGCS and ESInet operations, administration, and support. Training covers architecture, Functional Elements, routing and policy management, security services, logging, monitoring, and interconnection across ingress, core, and egress. Instruction emphasizes hands-on, scenario-based training for technical and administrative staff, including normal and abnormal operations, failover scenarios, monitoring and alarms, troubleshooting workflows, and standards-aligned configuration and change management practices. Lumen delivers complete training materials and a train-the-trainer program to support initial instruction, refresher training, and onboarding throughout the contract term.

5.6.2. Wiring and Cabling

All interface connections and visible cables must use standard EIA connectors secured by wall plates where exposed. All cables must be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends. Any cables used must be plenum rated where required by local building or fire codes.

Respondents must ensure that all equipment is connected to emergency AC power and is configured to be supported by a UPS.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms must be installed in accordance with national standards and applicable local codes.

The minimum standards used in the installations shall include, but are not limited to, the following:

- ANSI/TIA/EIA-568 - Commercial Building Telecommunications Wiring Standard
- ANSI/TIA/EIA-569 - Commercial Building Standard for Telecommunications Pathways and Spaces
- ANSI/TIA/EIA-606 - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- ANSI/TIA/EIA-607 - Commercial Building Grounding and Bonding Requirements for Telecommunications
- Building Industry Consulting Service International, Telecommunications Distribution Methods Manual
- National Electrical Code (NFPA-70)
- FCC Rules and Regulations, Parts 68 and 15

LUMEN RESPONSE:

Lumen installs all interface connections and cabling in accordance with national standards and applicable local codes to ensure a safe, compliant, and fully supportable NG911 environment. All visible connections use standard EIA-compliant connectors secured by wall plates, and every cable is clearly marked or numbered at both ends with a unique identifier. Where required by building or fire code, all cable used will be plenum rated. Each installed device is connected to emergency AC power and integrated with UPS support to ensure continuity of operations during a commercial power failure.

All cabling, communications outlets, power wiring, grounding, conduit facilities, and equipment rooms are installed consistent with national standards and local regulations, including at a minimum:

- ANSI/TIA/EIA-568 Commercial Building Telecommunications Wiring Standard,
- ANSI/TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces,
- ANSI/TIA/EIA-606 Administration Standard for Telecommunications Infrastructure of Commercial Buildings,
- ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications,
- Building Industry Consulting Service International Telecommunications Distribution Methods Manual,
- National Electrical Code (NFPA-70), and
- FCC Rules and Regulations, Parts 68 and 15.

Lumen's approach ensures Nebraska's NG911 cabling and physical installation practices meet all applicable safety, reliability, and telecommunications infrastructure standards.

5.6.3. Grounding

The proposed system must provide surge and lightning protection for all connections to AC power and is required to meet the R-56 standard.

All hardware and peripheral devices must be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse.

Respondents must ground all equipment in compliance with manufacturer recommendations and applicable standards.

Respondents must furnish and install the required grounding and bonding conductors where necessary and complete the connections to the grounding system at all sites.

LUMEN RESPONSE:

Lumen provides surge and lightning protection for all NG911 system components deployed under the Contract, ensuring that every connection to AC power meets the R-56 standard. All hardware and peripheral devices are mechanically and electrically grounded to protect personnel safety and to prevent damage to equipment and data caused by external electrical impulse events. Grounding and bonding practices are implemented consistently across all sites to support system reliability, resiliency, and long-term operational stability.

Surge And Lightning Protection. Lumen installs appropriate surge and lightning protection on all NG911 system components and on all connections to AC power in compliance with the R 56 standard, applicable codes, and manufacturer recommendations. These protections mitigate the impact of lightning strikes, power surges, and other external electrical disturbances that could affect NG911 operations.

Grounding And Bonding Compliance. Lumen grounds all equipment in accordance with manufacturer specifications and applicable national and local standards. Where required, Lumen furnishes and installs all grounding and bonding conductors and completes connections to the site grounding system to ensure a compliant and safe electrical environment at each installation location.

Installation Responsibility And Validation. Lumen is responsible for furnishing and installing all grounding and bonding components necessary to support the proposed NG911 solution. Grounding connections are validated as part of installation activities to confirm proper continuity and effectiveness. These practices ensure protection of personnel, preservation of data integrity, and reliable operation of NG911 equipment under adverse electrical conditions.

Deliverables - Training

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

5.7. Training

The Respondent shall work cooperatively with the State and designated staff to deliver training for the proposed solution. Training shall be ongoing throughout the term of the contract, with the ability to provide on-demand sessions at the State's request. The Respondent must include a description and supporting documentation for all requirements in this section.

5.7.1. Audiences and Scope

PSAP Operations:

- Network status reports
- Help desk usage and processes
- Text-to-911 operations
- Text- from-911 operations
- Trouble Ticketing

State-Level Operations:

- Network status reports
- Help desk processes
- Trouble ticketing
- Root-cause analysis and review

LUMEN RESPONSE:

Lumen delivers a comprehensive training program that supports effective operation, oversight, and long-term sustainability of the State of Nebraska's NG911 environment. Training is provided throughout the contract term and is delivered collaboratively with the State to ensure that PSAP personnel and State staff are fully prepared to operate, support, and oversee NGCS and ESInet services. Training sessions are available on demand at the State's request and evolve as the NG911 environment matures.

PSAP Operations Training. The training program addresses both PSAP-level operational needs and State-level administrative, governance, and oversight functions. PSAP operations training focuses on day-to-day interaction with NGCS and ESInet support capabilities, enabling personnel to understand system health, recognize service impacts, and engage support processes efficiently. Topics include accessing and interpreting network status reports, understanding routing and alarm conditions, using help desk and escalation processes, supporting Text to 911 and Text from 911 operations, and submitting and tracking trouble tickets related to network, routing, logging, or media issues.

State-Level Operations Training. State-level operations training is tailored to oversight and analytical roles and supports effective statewide monitoring and governance of NG911 services. Training includes use of network status and performance reporting, coordination across PSAPs and service providers through help desk and escalation workflows, visibility into incident prioritization and resolution timelines, and review of root cause analysis documentation, including findings, corrective actions, and follow-up processes.

Training is delivered through instructor-led sessions and scenario-based instruction and is supported by comprehensive training materials, job aids, and reference documentation. All materials are maintained and updated as system capabilities evolve, ensuring that both PSAP personnel and State staff remain aligned with current operational practices and support procedures.

Our Training Plan and sample documentation are provided as **Attachment 8**.

5.7.2. Training Elements

The Respondent shall develop and deliver training to meet the following minimum requirements:

- *Login and logout procedures*
- *Password reset*
- *Equipment problem reporting*
- *Call transfer functionality*
- *Call conferencing functionality*
- *Discrepancy reporting*
- *Foreign language interpretation process*
- *Rebid/refresh of call information*
- *Instant recorder/playback*
- *Text-to-911*
- *Text-from-911*
- *Other solution features not otherwise listed*

LUMEN RESPONSE:

Lumen provides training that meets all required operational needs for PSAP personnel and State users, ensuring staff can successfully perform essential NG911 functions across the ESInet and NGCS. Training is delivered as part of Lumen's overall training program, coordinated with the State and designated staff, and provided prior to go-live with ongoing and on-demand availability throughout the contract term.

Core Operational Training Content. Training includes instruction on all operational capabilities required to support day-to-day PSAP and State operations. Topics include secure login and logout procedures for NG911 applications and interfaces; approved password reset procedures, including authentication steps and escalation paths; and equipment problem reporting, including recognition of issues and submission of detailed reports through the help desk ticketing system.

Training Content includes, but is not limited to, the following:

- **Login and Logout Procedures.** We train users on secure login and logout processes for all NG911 applications and interfaces.
- **Password Reset.** We provide instruction on approved password reset procedures, including authentication steps and escalation paths.
- **Equipment Problem Reporting.** We train users to recognize equipment issues and report them through the help desk ticketing system with the required detail.
- **Call Transfer Functionality.** We teach call takers how to perform NG911 call transfers, including blind, warm, and inter-PSAP transfers.
- **Call Conferencing Functionality.** We provide training on initiating, managing, and ending call conferences across supported media types.
- **Discrepancy Reporting.** We instruct staff on generating DRs using the NENA-STA-010.3 compliant discrepancy reporting functions.
- **Foreign Language Interpretation Process.** We provide guidance on invoking supported interpretation workflows when a caller requires language assistance.
- **Rebid/Refresh of Call Information.** We train call takers on requesting updated location or call metadata during active calls.
- **Instant Recorder/Playback.** We train users to access, retrieve, and review instant recall recordings as permitted.
- **Text-to-911.** We provide training on receiving, reading, responding to, and managing inbound text sessions.
- **Text-from-911.** We train personnel on initiating outbound text sessions to communicate with callers when appropriate.
- **Other Solution Features.** We deliver instruction on any additional capabilities required to support day-to-day PSAP and State operations.

Lumen's approach ensures all users receive complete and consistent training on the operational functions required to support Nebraska's NG911 system.

5.7.3. Technical Assistance

Upon request by the State, the Contractor shall provide technical assistance to PSAP personnel during training and testing.

LUMEN RESPONSE:

Lumen will provide technical assistance to PSAP personnel during training and testing whenever requested by the State. Our support includes access to qualified technical staff who can assist PSAP personnel in understanding NG911 system functions, validating operational readiness during testing activities, and addressing issues encountered while learning or exercising the system.

5.7.4. Schedule and Locations

No later than fourteen (14) calendar days before each PSAP cutover, train all PSAP personnel (including State and administrative personnel assigned to the PSAP) on the proper operation of all Contractor-supplied software and equipment. To maintain the deployment schedule and accommodate call-taker travel, the Contractor shall establish temporary training site(s) in Nebraska as needed and provide weekend and evening sessions when required.

LUMEN RESPONSE:

Lumen trains all PSAP personnel, including State and administrative staff assigned to each PSAP, no later than fourteen calendar days prior to cutover. Training covers the proper operation of all Lumen-supplied NG911 software and equipment to ensure personnel are fully prepared before transition to live service. Training schedules align with the overall deployment timeline and are coordinated collaboratively with the State to support operational readiness and call taker availability.

Flexible Training Delivery. To maintain the deployment schedule and accommodate PSAP staffing constraints, Lumen establishes temporary training sites within Nebraska when required and provides evening and weekend training sessions as needed. This approach ensures training can be completed without disrupting ongoing operations or delaying planned cutover activities.

Role-Appropriate Training Content. Lumen ensures that PSAP and State personnel receive timely, role-appropriate training on the systems required to support the Lumen ESInet and NGCS. Training content is sequenced deliberately to support readiness and a smooth transition. Core topics include GIS, LIS, reporting, dashboards, and trouble ticketing, along with other operational capabilities required to support NG911 services.

Training Sequencing and Readiness Alignment. Training topics are delivered in an order that supports effective system adoption and minimizes transition risk. For example, GIS training is conducted early in the deployment process to enable data loading through the Spatial Interface well in advance of PSAP cutover, reducing the potential for GIS-related delays. Other training areas, such as reporting and dashboard usage, are delivered closer to cutover to maximize knowledge retention and ensure personnel are prepared for go-live operations.

5.7.5. Training Materials

Provide all training materials and a Train-the-Trainer (TtT) curriculum for State approval. Maintain up-to-date training materials at the State for the duration of the contract.

LUMEN RESPONSE:

Upon award, Lumen will provide all required training materials and a Train-the-Trainer curriculum for State review and approval. Our materials cover all NG911 system functions delivered under the Contract and are maintained in updated form for the full duration of the agreement.

As the current provider, Lumen has provided the State with all necessary documentation and training. Updated versions are furnished to the State whenever system changes, enhancements, or procedural updates require revisions to ensure personnel always have access to current, accurate training content.

5.7.6. Post-Deployment Training and Costs (Proposal Requirement)

The Respondent shall, as part of their response:

- *Provide a proposed cost for post-deployment training for up to fourteen (14) students per class*
- *Provide a proposed cost for the post-deployment TtT course, including the maximum class size.*

LUMEN RESPONSE:

Lumen does not charge the State for training in support of the ESInet solution. There are no student class size limitations with Lumen provided training.

5.7.7. Comprehension, Testing, and Certification

Apply testing at intervals during initial and ongoing training and provide the State a final evaluation of each student's knowledge upon completion. Instructional methodologies shall include lectures, group discussions, audiovisual methods, and role-playing. Testing methodologies shall include written exams, oral exams, hands-on testing, and end-of-course certification.

LUMEN RESPONSE:

Lumen will incorporate testing into both initial and ongoing NG911 training so the State can verify that personnel understand and can correctly operate all required system functions. Testing is applied at defined intervals throughout training, and a final evaluation is provided to the State for each student upon completion. Our instructional approach uses multiple teaching modalities to support different learning styles and ensure operational readiness.

Instructional Methodologies. We deliver training using lectures, group discussions, audiovisual demonstrations, and role-playing exercises to reinforce system operation and real-world scenarios.

Testing Methodologies. We evaluate student comprehension through written examinations, oral examinations, hands-on operational testing, and end-of-course certification.

5.7.8. Training Plan and Samples (Proposal Requirement) The Respondent shall, as part of their response:

- *Provide a proposed training plan and sample documentation and/or materials covering the topics and audiences listed in §E-8.1 and §E-8.2, above.*

LUMEN RESPONSE:

Lumen will provide a proposed training plan along with sample documentation and materials that address the training topics and audiences defined in §E-8.1 and §E-8.2. Our training plan supports PSAP-level operational readiness and State-level administrative oversight, ensuring both groups receive instruction tailored to their responsibilities within the NG911 environment. Our Training Plan and sample documentation are provided as **Attachment 8**.

Training Plan. Our proposed plan outlines how training is delivered, refreshed, and supported throughout the contract term. It identifies required sessions, learning objectives for each audience, delivery formats, testing intervals, and on-demand availability. The plan also specifies how training is scheduled relative to deployment milestones, including pre-cutover requirements for PSAP personnel.

Sample Training Documentation and Materials. We provide representative examples of training content covering the topics listed in §E-8.1 and §E-8.2, including network status reporting, help desk usage and processes, Text-to-911 and Text-from-911 operations, trouble ticketing, call handling support functions, and State-level oversight activities such as root-cause review. These materials demonstrate the structure, depth, and clarity of the training that will be delivered.

Lumen's approach ensures Nebraska has complete visibility into the training curriculum, documentation quality, and instructional methods provided as part of the statewide NG911 implementation.

Deliverables - Interoperability, Testing, Conformance, and System Acceptance

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires structured, transparent testing and acceptance evidence to validate standards conformance, interoperability, and operational readiness prior to system acceptance. Lumen complies by providing comprehensive test plans, conformance matrices, and interoperability test schedules that document how ESInet and NGCS components are validated against applicable NENA i3 and solicitation requirements. These deliverables define test scope, success criteria, sequencing, and traceability to required functions and interfaces.

Lumen further complies by conducting and demonstrating pilot laboratory testing that validates end-to-end system behavior and performance. Pilot demonstrations include verification of key performance indicators, such as sustained system availability targets, call processing continuity, and failover behavior, providing the State with objective evidence that the proposed solution meets or exceeds required operational benchmarks prior to production acceptance.

In addition, Lumen provides complete user manuals, API specifications, and training curricula to support system operation, administration, and integration. These materials are designed

to enable State staff, PSAP personnel, and technical stakeholders to effectively operate, manage, and interface with the NG911 solution throughout its lifecycle. Collectively, these deliverables ensure that interoperability is proven, conformance is documented, and the system is fully prepared for formal acceptance and ongoing operations.

5.8. Operations and Service Management Requirements

The Contractor shall manage all service support for the NG911 system, including integration of service and support for all partners and Subcontractors delivering components to the State.

Service levels and escalation: The Contractor shall commit to 99.999% availability for core voice paths, MTTR < 2 hours for Priority 1 incidents, and defined response times (for example, 15-minute acknowledgment). Include documented escalation paths, root-cause analysis reports, and penalty provisions for SLA breaches.

Operations enablement:

Provide comprehensive training curricula (in-person and virtual), role-based certifications, and operational runbooks for common scenarios such as failover and GIS updates. Supply full technical documentation that uses NENA functional-element nomenclature and is tailored to PSAP operators, network administrators, and GIS staff.

Change management:

Establish documented change-control protocols, including scheduled maintenance windows during off-peak hours, rollback procedures, impact assessments, and at least 30 days' advance notice for changes that affect routing, GIS, or call handling.

Standards conformance and interoperability:

Demonstrate conformance to NENA i3 and NGCS standards through self-attestation and participation in multi-vendor interoperability events (for example, NENA ICE). Test plans shall include NENA-defined sequences, and the system shall interoperate with third-party equipment (for example, CHE from different vendors).

Testing program:

Execute a phased testing program covering unit tests, component integration, system integration, failover simulations, performance, and load testing (including 200% of peak capacity), and security validations using NENA test cases. Success criteria shall include 100% pass rates for critical flows.

Product documentation:

Provide thorough user manuals, API specifications (in OpenAPI format), and release notes, along with the training programs noted above, aligned with NENA terminology.

LUMEN RESPONSE:

Lumen will manage the service and support functions for Nebraska's NG911 system, integrating service delivery across all partners and subcontractors to ensure a unified operational model. Our service management approach aligns with required availability, escalation, training, change management, standards conformance, testing, and documentation expectations.

Service Levels and Escalation. We commit to 99.999% availability for core voice paths, maintain MTTR under two hours for Priority 1 incidents and meet defined response times such as a 15-minute acknowledgment. We maintain documented escalation paths, root-cause analysis reporting and processes to support corrective action, including provisions for SLA breach management and remediation.

Operations Enablement. We provide comprehensive in-person and virtual training curricula, role-based certifications and operational runbooks for common scenarios including failover and GIS updates. As the incumbent provider for the current NGCS solution, we have provided technical documentation using NENA functional element nomenclature for PSAP operators, network administrators and GIS personnel.

Change Management. We maintain documented change control protocols that include scheduled maintenance windows during off-peak hours, rollback procedures, impact assessments and at least thirty days' notice for changes affecting routing, GIS or call handling.

Operational Continuity and Performance Assurance

Lumen delivers operational continuity for Nebraska's NG911 environment through a carrier grade management framework that includes 24x7 NOC monitoring, predictive performance analytics, automated SLA and KPI reporting, and documented escalation and restoration procedures. This framework provides continuous verification of ESInet and NGCS performance, proactive fault detection and resolution, and enforcement of availability and recovery objectives for mission critical 9-1-1 call delivery and routing services.

Standards Conformance and Interoperability. We demonstrate conformance to NENA i3 and NGCS standards through self-attestation and participation in interoperability events. Our test plans include required NENA sequences, and we support interoperability with third-party equipment such as multi-vendor CHE.

Testing Program. We implement a phased testing program that includes unit testing, component and system integration testing, failover simulation, performance and load testing at up to 200% of peak capacity and security validation using NENA test cases. Critical flows are tested to a 100% pass rate.

Product Documentation. We provide user manuals, OpenAPI-formatted API specifications and release notes along with associated training programs using NENA terminology.

Lumen's approach delivers a unified, standards-based service and support model that fully addresses Nebraska's NG911 operational, performance and interoperability requirements.

5.8.1. Service Management Framework

5.8.1.1. SERVICE MANAGEMENT PLAN

Oversight of the NG911 system and services post implementation/transition is required. The preferred best practice is to utilize Information Technology Infrastructure Library (ITIL) as a guideline for how NG911 services are designed, implemented, managed, maintained, and improved within the term of the contract.

ITIL integrates five stages of service delivery into a comprehensive methodology for managing the lifecycle of services.

- Service Strategy
- Service Design
- Service Transition
- Service Operation

- *Continual Service Improvement*

Within these stages are specific areas relating to Information Technology Service Management.

At a high level, these areas reference how a service maintains availability, capability, capacity, security, manageability, and operability. Respondents must describe their approach to service management for the operation of the NG911 system. The NG911 service management approach shall incorporate components of ITIL or follow industry best practices for IT service management.

Respondents must provide a narrative of how their proposed service management approach is integrated into their project management activities. Respondents must discuss their ability to maintain consistent performance and the service levels of the network

Respondents must discuss their ability to maintain consistent performance and the service levels of the network to support the following framework:

- *Determination of the single point of contact*
- *Management of subcontracted support components*
- *Support personnel required and identification of Key Personnel*
- *Underpinning contract management*
- *Third-party support contracts*
- *Pre-emptive support*
- *Equipment refreshes*
- *Preventative maintenance*
- *Bug fixes*
- *Patching and upgrades*
- *Warranty*
- *Out of warranty items*
- *Service Level Agreements*

LUMEN RESPONSE:

Lumen will manage NG911 service operations using a service-management framework aligned with Information Technology Infrastructure Library (ITIL) and Project Management Institute (PMI) principles and industry best practices. Our approach supports the full lifecycle of NG911 services, from strategic planning through ongoing operations and continual improvement, and is integrated directly into our project management and operational governance processes to maintain consistent network performance and required service levels.

Service Management Approach. We incorporate ITIL concepts across Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. These principles guide how we maintain service availability, capability, capacity, security, manageability, and operability across the ESInet and NGCS.

Integration With PMI Best Practices. We embed our service-management practices into project management activities so that operational considerations, service-level expectations, change protocols, documentation, and support structures are accounted for from deployment through long-term operations. This integration supports predictable performance and consistent adherence to defined SLAs.

Framework Support. Our ability to maintain consistent performance and service levels across the NG911 network is supported by:

- **Determination of the Single Point of Contact.** We designate a single accountable point of contact to coordinate service operations and communication.
- **Management of Subcontracted Support Components.** We oversee all subcontractors and integrated solution partners to ensure seamless service delivery.
- **Support Personnel and Key Personnel Identification.** We assign qualified support staff and identify Key Personnel responsible for NG911 operations.
- **Underpinning Contract Management.** We manage underlying agreements with vendors and service providers to maintain continuity.
- **Third-Party Support Contracts.** We coordinate and govern external support arrangements required for NG911 service delivery.
- **Pre-Emptive Support.** We apply preventive monitoring and action to identify potential issues before they affect service.
- **Equipment Refreshes.** We manage lifecycle updates for equipment to maintain performance.
- **Preventative Maintenance.** We conduct scheduled maintenance aligned with operational needs and SLAs.
- **Bug Fixes.** We apply vendor-supplied fixes through controlled processes.
- **Patching and Upgrades.** We manage patches and upgrades using change-control protocols.
- **Warranty and Out-of-Warranty Items.** We maintain processes for both warranty and non-warranty equipment support.
- **Service Level Agreements.** We monitor SLA performance and take corrective action when service trends require intervention.

Lumen's approach provides Nebraska with a comprehensive NG911 service-management model that maintains operational consistency, supports service quality, and ensures continuous improvement throughout the contract term.

5.8.1.2. SERVICE LEVEL AGREEMENT (SLA)

The NG911 system will utilize the requirements outlined in this RFP to negotiate a Service Level Agreement (SLA) with the selected vendor. In preparation all Respondents must provide a description of their SLA performance measures and identify how the thresholds that are not met are recovered.

The Respondent shall negotiate a comprehensive Service Level Agreement (SLA) framework that defines specific, measurable, achievable, relevant, and time-bound (SMART) metrics for the performance, availability, and reliability of the ESInet and all its functional elements. This framework must detail the processes for monitoring, reporting, and reviewing SLA compliance. The approach should align with industry best practices for IT service management and project management to ensure consistent quality and continual improvement.

The State expects the Respondent to provide a description of how each of these components are met within their SLA.

The State recognizes the following categories as expectations for their SLA.
Critical - Network Outage

- *1st Level Support - Immediate*
- *Continuous problem resolution/workaround effort*
- *2nd Level Support - within 15 minutes*
- *3rd Level Support - within 30 minutes or upon Customer request.*

Major - Service effecting

- *1st Level Support - Within 5 minutes*
- *2nd Level Support - Within 30 minutes*
- *3rd Level Support - Within 2 Hours or upon Customer request.*

Minor - Non-service effecting

- *1st Level Support - Within 30 minutes*
- *2nd Level Support - Within 2 Hours*
- *3rd Level Support - Within 1 business day or upon Customer request.*

The Respondent must provide a description and/or documentation that supports the requirements in this section.

LUMEN RESPONSE:

Lumen will support Nebraska's NG911 environment with a comprehensive SLA framework that defines measurable performance, availability, and reliability expectations for all ESInet and NGCS components. Our SLAs are structured using SMART criteria and include monitoring, reporting, escalation, and remediation processes that align with IT service-management best practices and ensure continual service improvement throughout the contract term.

SLA Performance Measures and Recovery. Our SLAs specify the performance thresholds required for core voice paths, NGCS functions, and ESInet routing. When thresholds are not met, we apply defined restoration processes, root-cause analysis, and corrective actions to return the system to compliance and prevent recurrence.

SLA Framework. We negotiate a comprehensive SLA framework describing measurable performance, availability, and reliability requirements. The framework defines monitoring and reporting processes and includes regularly scheduled SLA reviews to validate service levels and drive continual improvement.

Critical Incident Response Expectations:

- **1st Level Support - Immediate.** We provide immediate first-level response for critical outages.
- **Continuous Resolution Effort.** We apply sustained remediation until service is restored.
- **2nd Level Support - Within 15 Minutes.** We escalate within fifteen minutes to second-level staff.
- **3rd Level Support - Within 30 Minutes or Upon Request.** We escalate to third-level support within thirty minutes or sooner at the State's request.

Major Incident Response Expectations:

- **1st Level Support - Within 5 Minutes.** We initiate support within five minutes of detection or reporting.
- **2nd Level Support - Within 30 Minutes.** We escalate within thirty minutes for deeper technical analysis.

- **3rd Level Support - Within 2 Hours or Upon Request.** We escalate to senior engineering within two hours or sooner as directed by the State.

Minor Incident Response Expectations:

- **1st Level Support - Within 30 Minutes.** Initial response occurs within thirty minutes.
- **2nd Level Support - Within 2 Hours.** Second-level support engages within two hours.
- **3rd Level Support - Within One Business Day or Upon Request.** Third-level escalation occurs within one business day unless the State requests immediate action.

Monitoring, Reporting, and Escalation. We continuously monitor ESInet and NGCS components for SLA compliance and generate automatic alarms for performance degradation. Our escalation model ensures that incident ownership, communication, and decision-making flow clearly through tiers of technical staff, reaching the highest non-executive technical level within required timelines when outages occur.

Service Management Integration. Our SLA processes align with ITIL-based operational practices, including incident, problem, change, and capacity management. SLA compliance data feeds into ongoing improvement processes, with trends analyzed to refine operations and performance targets.

Root-Cause Analysis and Corrective Action. For any incident that causes an SLA violation, we conduct root-cause analysis, identify corrective actions, provide the State and affected PSAPs with a written report containing committed remediation dates, and deliver quarterly follow-ups documenting progress.

This framework provides Nebraska with predictable service performance, transparent SLA governance, and rigorous recovery and corrective-action processes that ensure continued reliability of the NG911 system.

5.8.1.3. COMPLIANCE AND RISK MANAGEMENT

*The State requires the contractor to run a documented risk management program for all NGCS components and the ESInet. The program must identify assets, threats, and vulnerabilities; rate and rank risks by **likelihood** and **impact** on **call delivery, location accuracy, security, availability, latency, and resilience**; and select a treatment (reduce, avoid, transfer, or accept). Any non-compliance with security requirements, standards, procedures, or practices must be documented and submitted to the State for written approval, including criticality analysis and a corrective action and/or risk acceptance path.*

Each risk under the contractor's control or those outside of the contractor's span of control that will negatively impact the ESInet or NGCS must be recorded on a risk acceptance form and signed by a member of the contractor's senior leadership with the authority - and financial/legal responsibility - to accept that risk for the NGCS/ESInet scope.

All risks must be reassessed at least annually, and high/critical risks at least monthly. The method may use qualitative (very low ↔ very high) or numeric scales but must address both likelihood and impact.

Third-party risks (carriers, cloud providers, data suppliers, managed services, subcontractors) must be tracked and visible even when control is limited. Where a third-party risk could affect service to the State, the contractor must implement compensating controls and define escalation tied to SLA/SLOs (e.g., uptime, MTTR).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A documented Risk Management methodology covering asset identification, threat identification, vulnerability assessment, risk assessment and prioritization, and risk treatment selection (reduction, avoidance, transfer, acceptance). Include working definitions of threat, vulnerability, and risk, and show how business impact is mapped to NGCS/ESInet outcomes (call completion, routing location, latency, availability).
- A risk register template and sample entries showing fields for asset, threat, vulnerability, likelihood, impact, inherent and residual risk, selected treatment, owner, due dates, status, and verification of closure. Include examples for both NGCS applications and ESInet network elements.
- A risk acceptance form/template and completed examples that quantify or qualify likelihood and impact, reference the related non-compliance (if applicable), and record a senior leadership signature with authority to accept risk on behalf of the contractor for the NGCS/ESInet scope.
- Review cadence and triggers, showing at least annual reassessment of all risks and monthly reassessment of critical/high risks; include procedures to re-evaluate on material changes (e.g., carrier migrations, cloud region moves, software upgrades, configuration changes, new interconnections) or emerging threats.
- A third-party risk approach, including how contractor/subcontractor/carrier/cloud risks are tracked (e.g., supplier registers, attestations), how visibility is maintained when direct control is limited, required compensating controls, and escalation timelines aligned to SLAs/SLOs.
- Non-compliance linkage, showing how unresolved non-compliance (policy gaps, audit findings, penetration test results, vulnerability scans) is converted to corrective action or formal risk acceptance within the same process, with State notification/approval where required.

LUMEN RESPONSE:

Lumen will operate a documented risk-management program for all NGCS components and the ESInet that identifies assets, threats, and vulnerabilities; evaluates risks by likelihood and impact; assigns treatment strategies; and documents all non-compliance issues for State review and acceptance. Our approach aligns with the State's requirements for tracking contractor-controlled and third-party risks, applying compensating controls, and ensuring senior-leadership accountability for risk acceptance.

Risk-Management Methodology. Our methodology identifies NGCS and ESInet assets, associated threats, and vulnerabilities, and evaluates risk using likelihood and impact ratings. We apply treatments of reduction, avoidance, transfer, or acceptance and maintain working definitions of threat, vulnerability, and risk. Business impact is mapped to NGCS and ESInet outcomes such as call completion, routing accuracy, latency, availability, and system resilience.

Risk Register. We maintain a risk register that documents required fields, including asset, threat, vulnerability, likelihood, impact, inherent and residual risk, selected treatment, risk owner, due dates, status, and verification of closure. The risk register contains entries spanning NGCS applications and ESInet network components.

Risk Acceptance. We maintain a risk acceptance form that captures likelihood and impact ratings, references any associated non-compliance, and documents the signature of a senior leader authorized to accept the risk for NG911 operations. Each accepted risk is recorded and retained as part of the NG911 risk-management program.

Review Cadence. We reassess all risks at least annually and reassess high and critical risks monthly. Our review processes include triggers for reevaluation following material changes, including service provider migrations, cloud region changes, software upgrades, configuration modifications, new interconnections, or emerging threats.

Third-Party Risk Management. We track third-party risks for carriers, cloud providers, data suppliers, managed services, and subcontractors using supplier registers and attestations. When control is limited, we apply compensating controls and establish escalation paths aligned with SLA and SLO expectations.

Non-Compliance Linkage. We link unresolved non-compliance—including policy gaps, audit findings, penetration test results, and vulnerability-scan findings—to corrective action or formal risk acceptance, with notification to and approval by the State when required.

5.8.1.4. MONTHLY PROJECT REVIEW AND COMPLIANCE

The contractor shall meet with the PSC and any of the PSC designated resources at a minimum of monthly throughout the contract period. The frequency of these meetings may be adjusted by the PSC at any time based upon the project lifecycle. Additionally, the agenda of the meeting may be modified based upon any pressing issues that need attention.

The contractor is responsible for providing a report to the State each month that details:

- **Monthly Project review and timeline updates** to document a regular consistent path toward full implementation of the items within the contract
- **Regular Process Audits** to validate adherence to procedures, assess process maturity, and document any corrective actions.
- **Monthly System status and performance** summarizing the performance of the system with details such as utilization, packet success rate, call success rate, traffic path utilization, call transfer updates, database updates, and contract compliance
- **Monthly Service Level Agreement / and Service Level Objective** status vs the Key Performance Indicators in the SLA.
- **Monthly Risk Management Reports** providing updates to the risk register, risk response (impact and priority) to proactively communicate potential triggers that can cause the system harm.
- **Monthly Change Management Reports** summarizing all changes (planned, emergency, completed, deferred, and failed).
 - **Comprehensive Audit Trails** for all changes, retained for a minimum of three (3) years and available to the State upon request.

The contractors monthly project review process shall:

- Ensure the State is regularly informed of any roadblock or constraint in a proactive manner
- Address issues that arise before they become a barrier

- Regularly assess compliance with applicable **NENA i3** standards.
- Support compliance with **47 CFR Part 9, CJIS Security Policy, HIPAA** (where applicable), and State-level cybersecurity directives.
- Align with **PMI PMBOK** integrated principles.
- Conform to **ITIL v4** practices.
- Ensure traceability of all activities and all provisions of the contract to maintain expectations of the State of Nebraska.

LUMEN RESPONSE:

Lumen will meet with the PSC and designated State resources at least monthly throughout the contract period, with meeting frequency adjusted at the PSC's direction based on the project lifecycle. We support PSC-directed agenda changes and ensure that all operational, technical, and project-related matters are addressed proactively. As part of these engagements, we provide a full monthly report package that enables the State to monitor progress, validate compliance, and maintain full situational awareness of NG911 system performance and risks.

Monthly Project Review and Timeline Updates. We deliver monthly project status reports that document progress against the implementation plan, highlight upcoming milestones and identify any constraints or roadblocks requiring State engagement. These reviews maintain transparency and support consistent progress toward full contract delivery.

Process Audits. We perform regular process audits to validate adherence to documented procedures, assess operational and project process maturity, and identify required corrective actions.

System Status and Performance Reporting. We provide monthly summaries of ESInet and NGCS performance, including utilization, packet success rate, call success rate, traffic-path utilization, call transfer activity, database update status and compliance with contract performance requirements.

SLA and SLO Reporting. We report monthly on SLA and SLO compliance, comparing actual performance to KPI thresholds defined in the SLA and documenting any deviations requiring remediation.

Risk-Management Reporting. We deliver a monthly risk-management report that updates the risk register, identifies response actions, records impact and priority changes and highlights potential triggers that could affect system performance or stability. See **Section 4.1.3.3** for additional details on Lumen's approach to risk management.

Change-Management Reporting. We provide a monthly change-management report summarizing all planned, emergency, completed, deferred and failed changes. We maintain comprehensive audit trails for all changes for at least three (3) years and make them available to the State upon request.

Monthly Project Review Process. Our monthly review process ensures the State is informed proactively about constraints or risks, addresses emerging issues before they become barriers and validates compliance with NENA i3 standards. It supports alignment with applicable regulatory frameworks including 47 CFR Part 9, CJIS Security Policy and HIPAA when applicable. The process follows PMI PMBOK principles, conforms to ITIL v4 practices and maintains complete traceability to contract requirements.

Lumen's approach provides Nebraska with a structured, transparent and standards-aligned oversight model that ensures long-term operational stability and contract compliance across the NG911 system.

5.8.2. Continuity and Resilience

5.8.2.1. AVAILABILITY

The entire IP path, and call-related services, data transactions, and associated services will be available 99.999% of the time, end to end, with the appropriate caveat for PSAPs that do not have the necessary redundancy to maintain 99.999%. Provisioning services not related to call time, such as provisioning the location database in the LNG by legacy OSPs, will be available 99.9% of the time.

Availability is defined as:

MTBF / (MTBF+MTTR)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 99.999% availability for IP path/call services/data transactions end-to-end (with caveat for non-redundant PSAPs).
- 99.9% for non-call provisioning

LUMEN RESPONSE:

Lumen provides an availability architecture for the State of Nebraska's NG911 system that supports end-to-end performance expectations across all IP paths, call-related services, data transactions, and associated NGCS and ESInet functions. The design supports **99.999%** availability for the operational call path within the Lumen-managed network boundary. PSAP facilities that lack redundant local infrastructure may have availability limitations outside the ESInet and NGCS span of control. Non-call provisioning services, including legacy originating service provider location database provisioning through the LNG, operate at a minimum availability level of **99.9%**.

Availability Design and Measurement. NGCS and ESInet components are engineered using fault-tolerant design, geographic diversity, redundant instances, automated failover mechanisms, and diverse routing to sustain high availability. Availability calculations are applied end to end within the Lumen-managed environment using the required formula MTBF divided by the sum of MTBF and MTTR. These calculations encompass IP transport paths, call processing elements, signaling flows, and data transactions that support NG911 call delivery.

Network and Platform Resilience. Lumen deploys high-availability (HA) configurations across critical systems, including redundant hardware, diversified routing, automatic failover, and maintained spares to meet reliability and mean time between failure objectives. System configurations are backed up and maintained to support rapid restoration. Power infrastructure and environmental controls are designed so that commercial power failures do not result in service interruption.

Continuity of Operations Planning. Lumen maintains a comprehensive business and service continuity program designed to prevent or mitigate service disruptions and to support rapid response to loss or impairment of critical business functions or infrastructure.

NG911 operations can be shifted to alternate, secure NOCs within the same metropolitan area, ensuring uninterrupted monitoring and response. Continuity planning includes documented procedures, training, and periodic reviews to confirm ongoing effectiveness.

Disaster Recovery and Incident Management. Continuity planning addresses complex disaster and evacuation scenarios. Incident and event management procedures define response actions for varying severity levels and are executed through established escalation and coordination processes. Adequate hardware spares, geographically diverse deployments, and redundant operational facilities enable sustained operations during localized or regional disruptions.

Program Governance and State Alignment. The Lumen program management team supporting the State of Nebraska provides a comprehensive Project Development Plan that includes continuity of operations planning. Continuity measures, restoration procedures, and availability commitments are governed through formal documentation, periodic review, and coordination with the State to ensure alignment with Nebraska's operational expectations.

Security Operations Continuity. Details of Security Operations Center continuity planning are appropriately restricted due to the sensitivity of security operations. However, SOC continuity is supported through geographically distributed operations, including multiple CONUS facilities, providing resilience and sustained security monitoring during disruptive events.

5.8.2.2. CONTINUITY OF OPERATIONS PLAN (COOP)

The Continuity of Operations plan will include measures to account for common cyber security threats and "sunny day" outage vulnerabilities that could affect the normal operation of the NG911 system and cause an outage.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Measures for cyber threats/"sunny day" outages causing system disruptions.*

LUMEN RESPONSE:

Lumen will include Continuity of Operations (COOP) measures that address both cybersecurity threats and "sunny day" outage vulnerabilities to ensure NG911 services remain available despite conditions that could disrupt normal operations. Our plan identifies potential disruptions, defines protective and recovery measures for NGCS and ESInet components, and supports rapid stabilization of service when unexpected events occur.

Cybersecurity Threat Measures. We incorporate protections for conditions such as malware, ransomware, unauthorized access attempts, signaling manipulation, and disruption of certificate or identity services. These measures include endpoint hardening, boundary protections, continuous monitoring, detection and triage workflows, isolation procedures and defined recovery steps to maintain call delivery and critical NGCS functionality.

Sunny Day Outage Measures. We account for non-malicious operational disruptions such as hardware failures, facility power events, transport impairments, configuration errors and component misbehavior. Preventive measures include equipment redundancy, diverse routing, UPS-supported power, configuration validation, and health-check-driven failover.

Stabilization and Recovery. We maintain procedures to shift traffic to alternate paths, activate standby components and restore normal operations quickly after a disruption, regardless of whether the cause is malicious or accidental.

This configuration ensures Nebraska's NG911 system maintains dependable operations despite cybersecurity threats or everyday outage conditions.

5.8.2.3. DISASTER RECOVERY (DR)

The Disaster Recovery Plan will include the procedures for:

- *Activation procedures*
- *Recovery team identification*
- *Roles and responsibilities*
- *Recovery strategies and response*
- *Recovery management procedures*
- *Recovery cost procedures*
- *Recovery resources*
- *Recovery communications*
- *Stakeholder management*
- *Subcontractor, Supplier, Partner communication, and coordination*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *DR Plan with activation procedures, team ID/roles/responsibilities, strategies/response, management/cost/resources/communications, stakeholder/subcontractor coordination.*

LUMEN RESPONSE:

Lumen will maintain a Disaster Recovery (DR) Plan that meets the State's requirements and provides structured procedures for recovering NG911 operations following a disruption. Our DR Plan identifies activation steps, recovery roles, communication channels, required resources, and coordination with all parties involved in restoration, ensuring that NGCS and ESInet services return to service in a controlled and traceable manner.

Activation Procedures. We document the conditions that trigger DR activation, the authority required to declare activation and the process for initiating DR workflows.

Recovery Team Identification, Roles, and Responsibilities. We define the DR recovery team, identify responsible individuals and outline their roles and responsibilities during recovery operations.

Recovery Strategies and Response. We maintain DR strategies that describe how NGCS and ESInet functions are restored following various outage scenarios and provide guidance on executing recovery tasks.

Recovery Management Procedures. We include procedures for managing the overall DR effort, coordinating tasks, tracking progress and documenting actions taken.

Recovery Cost Procedures. We describe how costs associated with DR activities are identified, tracked and managed.

Recovery Resources. We specify the personnel, systems, tools and support elements required to execute DR activities effectively.

Recovery Communications. We document communication protocols for DR events, including internal coordination and external notifications to the State and PSAPs.

Stakeholder Management. We define how communications and coordination occur with stakeholders, including the State and operational partners, throughout the DR lifecycle.

Subcontractor, Supplier, and Partner Coordination. We include procedures for coordinating with subcontractors, suppliers and partners during recovery and ensuring their responsibilities are aligned with DR requirements.

Lumen's DR Plan ensures Nebraska receives a complete, standards-aligned DR Plan capable of supporting NG911 recovery across all required operational conditions.

5.8.3. Operations Centers and Support

5.8.3.1. NETWORK OPERATIONS CENTER (NOC)

The NOC must operate on a 24×7×365 basis for the duration of the contract. In addition, the NOC will include the capability to perform remote maintenance and restoration of alarms, as necessary.

The NOC will be the single point that performs continuous monitoring, maintenance, and network support services of the NG911 System. The NOC will interface with the help desk and the PSAPs or designated staff. The NOC will be staffed with appropriate technical resources to aid troubleshooting, diagnosis and recovery from issues related to the operation of the NG911 system.

The NOC will perform monitoring of the entire ESInet, all connections and functional components used in the routing of 911 calls. The NOC will be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure of the NG911 system.

- *The NMS will continuously monitor the performance and availability of all devices.*
- *The NMS will monitor network performance, including throughput, latency, jitter, packet loss, and other parameters deemed necessary by the State.*
- *The NMS will monitor the network for network intrusion attempts or security breaches and be capable of issuing security alerts when an event is recognized.*
- *The NMS will create alarms based on thresholds and parameters and distribute alarm notifications appropriately.*
- *The NMS will monitor the environment at all data centers or points of presence where critical network components are housed to ensure functionality.*
- *The NMS will monitor ancillary network components such as power utilization and backup power systems.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *24×7×365 NOC with remote maintenance/restoration.*
- *Single point for monitoring/maintenance/support.*
- *Interface with help desk/PSAPs.*
- *Staffed for troubleshooting/recovery.*

- *Monitoring of ESInet/connections/functional components.*
- *NMS for device performance/availability, network params (throughput/latency/jitter/packet loss), intrusion/breaches with alerts, threshold-based alarms/notifications, data center environment, power utilization/backup.*

LUMEN RESPONSE:

Lumen will operate a 24x7x365 NOC for the Nebraska NG911 system that functions as the single, authoritative point for continuous monitoring, remote maintenance, and restoration of the ESInet, NGCS, gateways, and all other contracted functional elements. The NOC uses an integrated Network Management System (NMS) and related tools to supervise the entire IP infrastructure that supports 911 call routing, with the ability to remotely diagnose issues, apply configuration changes, and restore service when alarms or degradations are detected.

NOC Operations And Interfaces. We staff the NOC around the clock with tiered technical resources who are trained on ESInet, NGCS, and PSAP connectivity. The NOC acts as the central coordination point for monitoring, ticket handling, and escalation, and it interfaces directly with the help desk system so incidents raised by PSAPs and State staff are correlated with network alarms and tracked through closure. Communication with PSAPs and designated State contacts follows documented notification and escalation procedures so that stakeholders receive timely status updates for alarms, incidents, and planned activities.

Remote Maintenance And Restoration. We perform remote maintenance and restoration through secured management channels that are logically separated from service traffic. The NOC uses hardened management jump hosts and out-of-band access where available to connect to routers, switches, firewalls, BCFs, NGCS servers, and other devices for configuration changes, log retrieval, and service restarts. Changes are executed under defined change-control procedures, and when alarms indicate a fault, NOC staff can remotely isolate impacted elements, reroute traffic, and restore normal operation without dispatching on-site personnel when feasible.

End-To-End ESInet And NGCS Monitoring. We monitor the entire ESInet, including all ingress and egress points, transport links, and functional components used in call routing. The NMS polls network and application elements using SNMPv3, API-based health checks, and system telemetry to track device state, interface status, and service availability. Logical call-path visibility is maintained so that issues affecting 911 call routing, such as link failure or degraded NGCS components, are quickly detected and surfaced to NOC operators.

Device Performance And Availability Monitoring. The NMS continuously monitors the performance and availability of all devices that participate in NG911 service delivery. This includes core and edge routers, switches, firewalls, BCFs, session border controllers, NGCS application servers, and key supporting systems. Per-device and per-interface metrics are collected at defined intervals, and hard thresholds for up/down status are combined with softer thresholds for warning conditions so that incipient problems are identified before they impact call delivery.

Network Performance Metrics. The NMS measures and reports network performance parameters including throughput, latency, jitter, packet loss, and any additional metrics the State deems necessary. Active and passive measurement techniques are used to validate end-to-end path quality. These metrics feed dashboards in the NOC for continuous visualization and drive alarms when service levels are approached or exceeded.

Security And Intrusion Monitoring. We integrate the NMS with security telemetry from boundary devices, IDS sensors, and host-based security agents so that network intrusion attempts, suspicious traffic patterns, and anomalous signaling are identified. Security-related events generate alerts in the NOC and can be forwarded to the State's security monitoring function as required. This supports detection of DoS, TDoS, scanning, and other malicious activity that could impact NG911 operations.

Threshold-Based Alarms And Notifications. We configure the NMS with threshold and state-based alarm rules that generate alerts when performance, availability, or security conditions deviate from expected baselines. Alarm routing rules ensure notifications are delivered to the appropriate NOC operators, on-call engineers, or escalation groups. Alarm severity levels are aligned with incident classification so critical events receive immediate attention and lower-severity issues are handled within defined response targets.

Environmental And Facility Monitoring. The NMS monitors environmental sensors at all data centers and points of presence where critical NG911 components are housed, including temperature, humidity, and other environmental conditions that could affect equipment operation. It also monitors alarms from facility systems, such as HVAC, to detect conditions that may require preemptive action to protect NG911 infrastructure.

Power Utilization And Backup Systems Monitoring. We track power utilization and status of UPS units and other backup power systems associated with NG911 equipment. The NMS collects status from power distribution units, UPS controllers, and, where available, generator interfaces, so the NOC can detect battery discharge events, degraded capacity, or failures in backup power infrastructure and coordinate remediation before call-handling capabilities are affected.

NOC Tools - Configuration Management, Backup, and Restoration. Lumen employs a comprehensive set of monitoring and management tools that enable continuous, 24x7x365 oversight of the NG911 environment by the NG911 NOC and SOC. These tools provide end-to-end visibility across the ESInet and NGCS and support timely detection, analysis, and response to service-affecting conditions.

Telemetry and Event Collection. Monitoring systems leverage syslog and SNMP traps for event and fault notification, SNMP polling for device and interface status, application health checks, and embedded host agents that communicate directly with Lumen's monitoring platforms. Together, these mechanisms provide real-time awareness of network, system, and application health and support automated alerting and correlation.

Foremost among Lumen's network and systems monitoring and management tools are the platforms described in the following sections.

Realtime Fault Manager (RFM). Lumen's Realtime Fault Manager (RFM) serves as the primary fault management and alarm generation platform for NG911 operations. RFM collects and correlates data using protocols including syslog, SNMP, CLI, CORBA, and TL1 and presents real-time fault and environmental alarms to Lumen operations centers. RFM also functions as an alarm aggregation platform, importing alerts from other monitoring systems into a single, unified operational view that supports automation and task execution. RFM is deployed in a highly available, geographically diverse configuration within CONUS to support mission-critical operations.

As shown in **Figure 5.8.3.1-1**, RFM receives data directly and indirectly from network elements across the solution, providing effectively end-to-end visibility. For the State of Nebraska, RFM visibility spans from the NGCS interface through the ESInet to the PSAP CHE. Outright failures generate immediate alarms to the NOC, while impaired or degraded conditions are conveyed through correlated alerts originating from performance and analytics platforms. In a high-availability architecture, failures typically indicate loss of protection rather than loss of service, allowing the NOC to initiate corrective actions proactively.

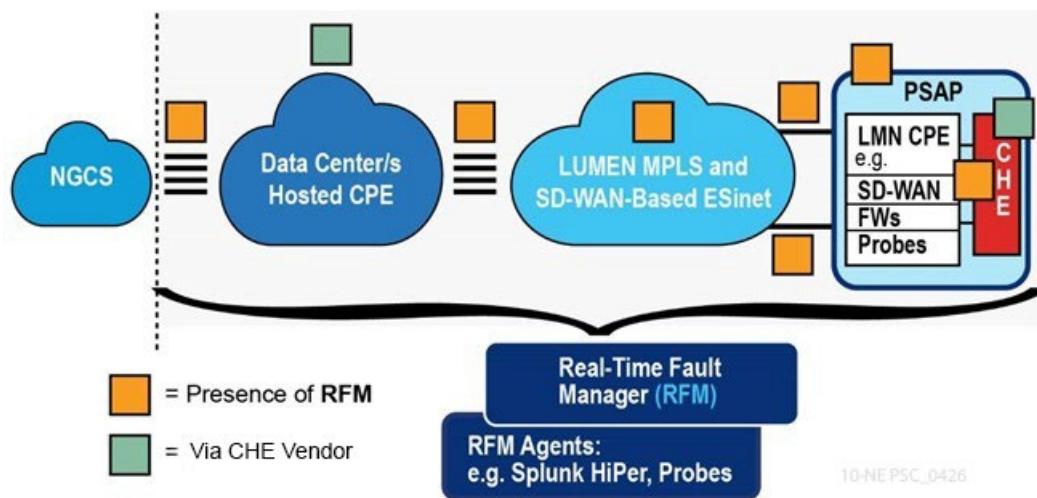


Figure 5.8.3.1-1. Visibility of Lumen's Realtime Fault Manager

Alarm Automation and Ticketing Integration. RFM incorporates Intelligent Alarm Automation, which automatically generates operational tickets when predefined conditions are met. These tickets are presented through the Operations Console, which integrates ticketing and change management functions. Tickets generated automatically or opened manually by Lumen or the State are visible through the State dashboard, ensuring shared situational awareness.

High Performance (HiPer) Telemetry and Analytics. HiPer is Lumen's primary performance monitoring and telemetry analytics platform. It collects near real-time network telemetry using distributed collectors and software probes that focus on active performance measurements, including latency, jitter, and packet loss. HiPer also collects SNMP data and NetFlow records from Layer 3 devices to support application visibility and performance analysis. Like RFM, HiPer is deployed in a highly available, geographically diverse configuration.

Alarm and ticket workflows are illustrated in **Figure 5.8.3.1-2**.

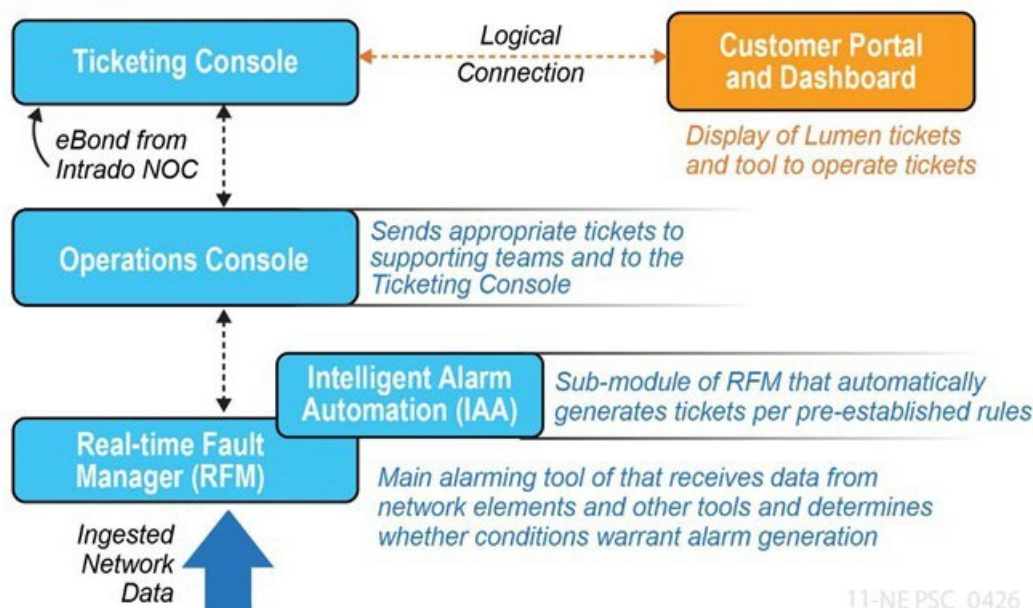


Figure 5.8.3.1-2. NG911 NOC Alarm Ticketing

As depicted in **Figure 5.8.3.1-3**, HiPer uses a layered architecture consisting of network elements, distributed collection, real-time analytics, and data access layers. HiPer's analytics engine processes telemetry in real time, generates Threshold Crossing Alerts, and stores aggregated data for reporting. In the NG911 environment, HiPer supports Quality of Service monitoring, including RTP and RTCP metrics such as packet loss, jitter, and latency. These metrics are used to calculate quality indicators, including MOS, and are aggregated for operational and external reporting.

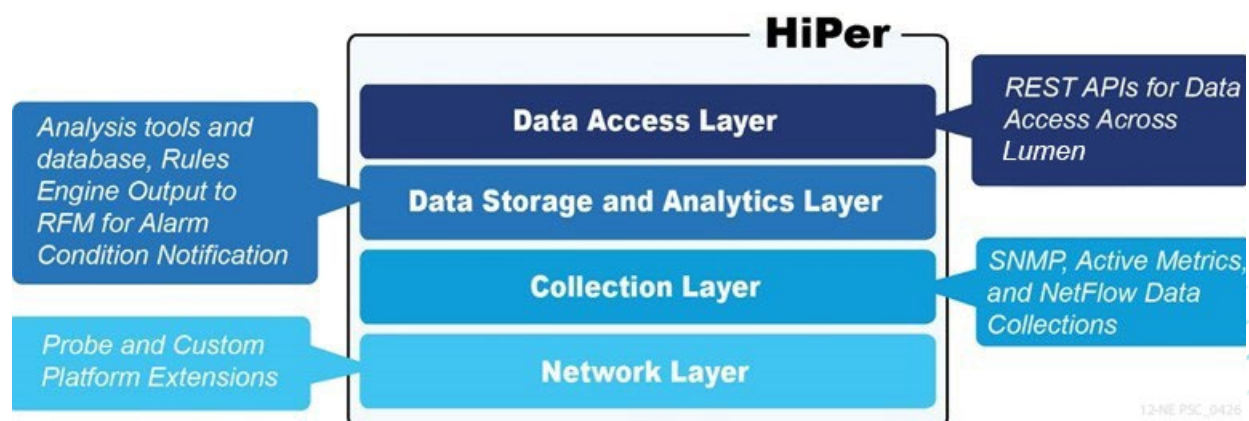


Figure 5.8.3.1-3. NG911 HiPer Architecture

Log Analytics and Event Correlation Using Splunk. Lumen uses Splunk to ingest and analyze large volumes of machine-generated data from applications, servers, databases, network devices, operating systems, and security platforms. Splunk correlates events in near real time to support troubleshooting, performance analysis, trend identification, malware signature searches, and alert generation. Custom dashboards and visualizations present operational data to multiple audiences.

Splunk serves as the primary platform for logging and analyzing all human and non-human login events. Log data is archived and available through dashboards and ad hoc queries,

supporting operational review, security investigations, and audit requirements. When Splunk identifies anomalous or threshold-based conditions, alerts are forwarded to RFM for alarm handling and NOC response.

Sentry Monitoring for Hosted CPE. Intrado Sentry provides centralized remote monitoring for hosted CPE located in data centers and PSAP CHE environments supporting the VIPER system. Sentry servers monitor VIPER components and associated equipment using embedded software and SNMP object identifiers, reaching PSAP equipment through the ESInet. Sentry operates continuously and generates notifications for fault conditions or performance threshold crossings. Selected alarms initiate tickets within both the Intrado Sentry NOC and the Lumen ticketing platform to ensure coordinated response.

Security Information and Event Management (SIEM). Lumen's Security Information and Event Management platform is integrated with ESInet monitoring and ingests logs and telemetry from network hosts, call processing elements, and security infrastructure. The SIEM performs real-time event correlation, predictive analysis, and automated threat detection across the NG911 environment. Security personnel continuously tune detection profiles to reduce false positives, prioritize meaningful alerts, and identify anomalous behavior efficiently.

Advanced heuristic analysis techniques are applied to detect previously unknown threats and assess system susceptibility to emerging risks. These analytics enhance the security posture of the NG911 environment by supporting early detection, rapid response, and continuous protection.

Lumen's approach provides Nebraska with a technically comprehensive NOC and NMS solution that delivers continuous visibility, proactive fault detection, and remote restoration capabilities across all ESInet and NGCS components.

Please see **Section 5.1.14.1** for a detailed description of our ESInet NGCS NOC solution.

5.8.3.2. SECURITY OPERATIONS CENTER (SOC)

The proposed solution requires the services of a Security Operations Center (SOC). The SOC (Security Operations Center) may be combined with the NOC and shares the overall requirements. The SOC must provide support for the following items:

- 24x7x365 operation.
- Capability to perform remote maintenance and restoration of security events.
- Single point that performs continuous monitoring, maintenance, and network support services of the NG911 System and identifies security faults.
- Interfaces with the help desk and the PSAPs or designated staff.
- Staffed with appropriate technical resources to aid troubleshooting, diagnosis, and recovery from security issues.
- Perform security monitoring of the entire NG911 system, all connections and functional components used in the routing of 911 calls.
- Security compliance testing, penetration testing, vulnerability testing, etc.
- Collection and monitoring security logs, and assist with incident response
- Operational security administration such as identity & access management, key management, firewall administration, etc.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24×7×365 SOC (possibly combined with NOC) with remote maintenance/restoration of security events.
- Single point for monitoring/maintenance/support identifying security faults.
- Interface with help desk/PSAPs.
- Staffed for security troubleshooting/recovery.
- Security monitoring of system/connections/components.

LUMEN RESPONSE:

Lumen operates a global Security Operations Center capability supported by eight physically diverse SOC locations that provide continuous, twenty-four by seven security monitoring and response for Lumen's managed security services. Four SOCs are located within the continental United States, including facilities in Colorado, Arizona, Minnesota, and additional geographically diverse locations. These SOCs operate using common tools, procedures, and staffing models and present to the State of Nebraska as a single, unified SOC. Physical diversity across multiple locations, combined with redundancy within individual SOCs, provides a highly available configuration and continuity of operations.

Staffing, Expertise, and Tiered Support. The SOC is staffed by more than one hundred security professionals providing Tier 1, Tier 2, and Tier 3 security support. Personnel bring deep experience in network security operations and hold a broad range of industry certifications covering security architecture, incident response, network defense, and secure operations. This staffing model ensures continuous coverage and rapid escalation when security events are detected.

Threat Visibility and Intelligence Advantage. Although Nebraska's ESInet operates on a secure, private MPLS network that is physically and logically separated from the public Internet, Lumen's position as one of the world's largest network operators provides exceptional visibility into the global threat landscape. Lumen's network platform incorporates intelligent, automated threat sensing, decision, and response tools that generate high-fidelity threat intelligence and support early detection of malicious activity before it can impact customer environments.

Black Lotus Labs Threat Research and Operations. Black Lotus Labs serves as Lumen's threat research and operations arm and is a foundational element of SOC operations. The team ingests and analyzes massive volumes of telemetry from across Lumen's global backbone to baseline normal network behavior and detect anomalies. Advanced analytics, machine learning, and automation are used to validate threats in near real time, reduce false positives, and prioritize response actions. Black Lotus Labs monitors and mitigates large-scale threats daily, tracks command-and-control infrastructure, and generates actionable intelligence that directly informs SOC detection, response, and prevention activities.

Black Lotus Labs also operates an extensive HoneyNet that captures attacker tactics, techniques, and procedures for analysis and intelligence development. In addition, Lumen's highly distributed network edge and deep peering enable detection and mitigation of malicious traffic closer to its source, including large-scale volumetric DDoS activity, reducing latency and improving mitigation effectiveness.

As presented in **Figure 5.8.3.2-1**, this team monitors more than 135 billion NetFlow sessions per day, and every day responds to and mitigates approximately 120 DDoS attacks. Command and Control (C2) networks or servers are the means through which an attacker communicates with and controls a compromised host. Overall, Lumen actively tracks more

than 18,000 C2 servers (C2s) per day, discovers some 680 new C2 networks per month, and proactively removes more than 60 C2s per month to help protect the global internet - all of which informs and strengthens our SOC operations.

Creating a Safer Internet Through Global Visibility

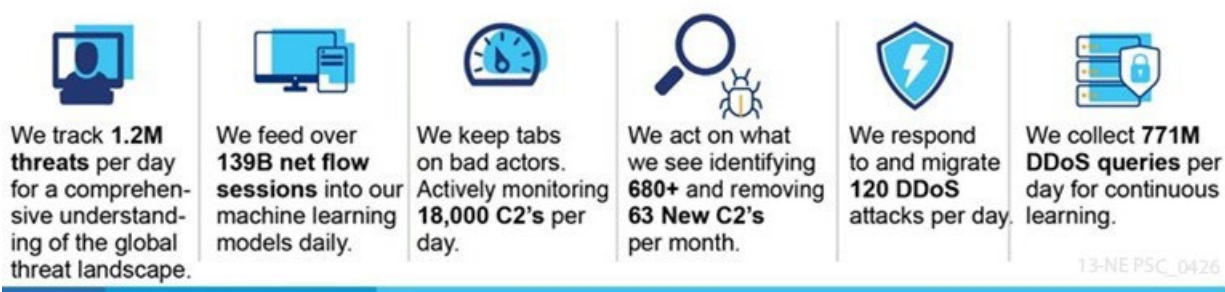


Figure 5.8.3.2-1. Lumen SOC Network Monitoring Capabilities

SOC Operations Model and Integration. The SOC operates as part of Lumen's broader security support infrastructure and works closely with the Cyber Incident Response Team and Security Architecture and Engineering teams. These teams design, build, and implement security environments that the SOC operates and protects. For NG911 environments, SOC-directed or supported services include advanced threat intelligence, rapid threat defense updates, DDoS mitigation support, continuous monitoring, incident response assistance, and security advisement.

Integrated SOC and NOC Operations. Lumen integrates SOC capabilities with its twenty-four by seven Network Operations Center operations to provide unified monitoring of performance, availability, and security conditions across the NG911 environment. Security events and operational events are monitored through coordinated processes with shared visibility and consolidated escalation paths. The integrated SOC/NOC model enables simultaneous detection, troubleshooting, and recovery for network faults and security incidents.

Security Monitoring and Incident Response. The integrated SOC/NOC provides continuous security monitoring across ESInet transport, NGCS functional components, gateways, and interconnection points. Monitoring includes analysis of IDS and IPS telemetry, firewall events, authentication and certificate failures, abnormal signaling behavior, endpoint security alerts, and other indicators of compromise. SOC and NOC personnel coordinate response actions, escalation, and remediation activities using defined operating agreements and bidirectional escalation paths.

Interfaces and Communication. Security-related alerts, investigations, and remediation activities are reflected in the same ticketing workflows used for operational events. The SOC/NOC interfaces directly with the help desk and State-designated staff to ensure that security incidents are tracked, communicated, and resolved with full visibility and coordination.

Security Administration and Compliance Support. As part of SOC operations, Lumen supports ongoing security compliance activities, including log collection and monitoring, vulnerability assessments, penetration testing support, and incident response coordination. The SOC also supports operational security administration functions such as identity and

access management, key management processes, and enforcement of firewall and border control policies.

5.8.3.3. HELP DESK

A help desk will be included with the NG911 system. The help desk(s) will operate on a 24x7x365 basis and be adequately staffed by resources who are trained and qualified in help desk and customer support services.

The help desk will serve as a single point of contact for all NG911 system and service matters, including without limitation, the NG911 system, all components of the NG911 system, and any additional system service providers delivering services or components for the NG911 ecosystem.

Only a fully staffed help desk will be considered. The help desk must not use an automated attendant or other automated means of answering a call.

The help desk must be accessible via various methods including voice, text, email, and other means as deemed appropriate or as directed by the State.

The help desk will have the ability to communicate directly and immediately with maintenance and support services for the NG911 system and all components of the system, including, without limitation, network troubles. This includes partner providers who are performing or supplying services within the system.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *24x7x365 staffed help desk trained in support.*
- *Single point for all system matters/components/providers.*
- *No automated attendant.*
- *Accessible via voice/text/email/etc.*
- *Direct/immediate communications with maintenance/support including network troubles/partners.*

LUMEN RESPONSE:

Lumen will provide a 24x7x365 fully staffed help desk for Nebraska's NG911 system, staffed by personnel trained and qualified in help desk and customer support services. Every incoming contact is answered by a live technician, and we do not use an automated attendant or any other automated means as the first response to a call. The help desk serves as the single point of contact for all NG911 system and service matters, including the ESInet, NGCS components, and any additional system service providers delivering services or components within the NG911 ecosystem.

We make the help desk accessible through multiple channels, including voice, text, email, and any additional mechanisms the State designates as appropriate. All problem reports received through these channels generate a ticket in the help desk system, which is used to track issues from initial report through diagnosis, remediation, and closure. The help desk maintains direct and immediate communication paths with the integrated SOC/NOC and all maintenance and support teams responsible for NG911 elements, including partner providers that perform or supply services within the system, so network troubles and other issues can be escalated and addressed without delay.

Lumen's approach ensures that Nebraska has a single, always-available help desk entry point with real-time access to technical support and partner providers for any NG911 system issue.

5.8.3.3.1. Trouble Handling and Ticketing Requirements

Trouble handling, and trouble ticket tracking services will be required for the successful operation of the NG911 system and services.

To ensure that all trouble tickets are resolved in a timely manner, The contractor will develop and maintain an escalation guideline document that describes the escalation procedure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Trouble handling/tracking.*
- *Escalation guideline document/procedure.*

LUMEN RESPONSE:

Lumen will provide trouble handling and tracking services that support timely identification, escalation, and resolution of issues across the NG911 system. All reported problems generate a unique trouble ticket, which is tracked from initial creation through diagnosis, remediation, and closure. Tickets originating from PSAPs, the State, or automated monitoring systems flow into a unified ticketing platform used by the help desk, integrated SOC/NOC, and all supporting subcontractors to ensure visibility and coordinated action.

Trouble Handling and Tracking. We document each problem report in the ticketing system with required details, assign an owner, track status through predefined stages and maintain audit history for all actions taken. Tickets are correlated with system alarms when appropriate so operational and security events feed directly into troubleshooting workflows.

Escalation Guideline and Procedure. We maintain a formal escalation guideline that defines how issues progress through technical tiers, including expected response intervals, communication requirements and criteria for increasing urgency. The procedure specifies escalation to specialized engineering teams, subcontracted support groups or leadership based on severity, impact or duration.

5.8.3.3.2. Monitoring of Applications and Equipment

Proactive monitoring of all NG911 system components for operation, performance, and fault conditions will be provided.

The contractor will ensure that all alarms including environmental status alarms are received and monitored in a Network Operations Center (NOC).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Proactive monitoring of components for operation/performance/faults.*
- *Receipt/monitoring of alarms including environmental in NOC.*

LUMEN RESPONSE:

Lumen will provide proactive monitoring of all NG911 system components to track operational status, performance, and fault conditions across the ESInet and NGCS. Our

proactive monitoring approach ensures that conditions affecting call routing, signaling, and supporting services are detected and surfaced in time to initiate corrective action before they impact service levels.

Proactive Component Monitoring. We continuously monitor NG911 devices and services for operation, performance, and fault conditions, including key indicators such as device reachability, interface status, utilization, and error conditions relevant to ESInet and NGCS call delivery paths.

Alarm Receipt and NOC Monitoring. We ensure that all alarms, including environmental status alarms from data centers and PSAP-facing sites, are received and monitored in the integrated NOC, where they are reviewed, correlated with other events, and used to initiate troubleshooting and recovery actions as required.

5.8.3.3.3. Root Cause Analysis

The contractor is required to provide a complete Root Cause Analysis (RCA) for any trouble with the system. The RCA process will follow a process like the following:

- *Following any critical event or major outage, the State/designated staff must receive a root cause analysis within five (5) business days.*
- *Immediately after a trouble has been identified the contractor will begin documenting the information as they complete the RCA. This documentation will be made available to the State via a shared online platform that will allow for constant tracking by the State as more information becomes available.*
- *The RCA format will include dates, times, and discoveries by the contractor as they investigate the trouble.*
- *Once the investigation has concluded the RCA must be submitted to the State for acceptance and approval that the trouble has been resolved.*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *RCA for troubles (within 5 business days for critical/outages).*
- *Immediate documentation shared online.*
- *Format with dates/times/discoveries.*
- *Final submission for State approval.*

LUMEN RESPONSE:

Lumen will provide a complete Root Cause Analysis (RCA) process for any trouble affecting the NG911 system, following the State's required timelines, documentation expectations, and approval workflow. Our RCA process begins immediately after trouble is identified and continues until the State has accepted the final RCA report.

RCA Delivery Timeline. We deliver a full RCA to the State or designated staff within five (5) business days following any critical event or major outage.

Immediate Documentation and Shared Access. As soon as a trouble condition is identified, we begin documenting all investigative actions, observations, and findings in real time. This documentation is posted to a shared online platform so the State can track progress continuously as additional information becomes available.

RCA Format and Required Details. The RCA includes all required data elements such as dates, times, investigative notes, discovered conditions, contributing factors, causal chains, and interim actions taken during the investigation.

Final Submission and Approval. Once the investigation is complete, we submit the final RCA to the State for review, acceptance, and verification that the issue has been properly resolved.

5.8.3.4. CUSTOMER SUPPORT SERVICES

The Respondent must provide a description and/or documentation that supports the requirements in this section, including SLA management (performance/monitoring/delivery/reporting/review); event/incident management; diagnostics/reporting; problem resolution/trouble handling; network fault monitoring; request fulfillment; access management; remote diagnostics; environmental requirements; capacity/change/configuration/transition management; training; commercial availability; all tied to SLOs for SLA measurement.

The contractor is required to provide monthly updates to the PSC regarding the performance of the system in the form of a Monthly Performance Review which is used to measure adherence to the contract elements, the performance measures, and Key Performance Indicators (KPIs). The KPIs are directly tied to the SLA.

Anticipated support services include:

- Service Level Agreement (SLA) management
 - Performance measurement and monitoring
 - Guaranteed delivery
 - SLA reporting and review
- Event management
- Incident management
- Diagnostics and reporting
- Problem resolution/trouble handling
- Network fault monitoring
- Request fulfillment
- Access management
- Remote diagnostics
- Environmental requirements
- Capacity management
- Change management
- Configuration management
- Transition management
- Training arrangements
- Commercial availability

Each of the items listed above are tied to Service Level Objectives (SLO) that the State measures against the Service Level Agreement (SLA).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *SLA management (performance/monitoring/delivery/reporting/review) on a monthly basis to the PSC.*
- *Event/incident management.*
- *Diagnostics/reporting.*
- *Problem resolution/trouble handling.*
- *Network fault monitoring.*
- *Request fulfillment.*
- *Access management.*
- *Remote diagnostics.*
- *Environmental requirements.*
- *Capacity/change/configuration/transition management; training.*
- *Commercial availability.*
- *All tied to SLOs for SLA measurement.*

LUMEN RESPONSE:

Lumen will provide a comprehensive service-support framework for Nebraska's NG911 system that aligns with the State's Service Level Objectives and supports ongoing SLA measurement. Our approach integrates SLA management, event and incident handling, diagnostics, fault monitoring, request fulfillment, access management, remote diagnostics, environmental oversight, and full lifecycle management of capacity, change, configuration, and transition activities. All functions are delivered within a structured operational model tied directly to the SLA and reviewed monthly with the PSC.

SLA Management. We maintain SLA management processes that include ongoing performance measurement, continuous monitoring of ESInet and NGCS components, documented delivery of contracted service levels, and formal SLA reporting and review. Each month, we provide the PSC with a Monthly Performance Review summarizing SLA status, KPI adherence, and trends requiring corrective action.

Event and Incident Management. We detect and classify events, escalate incidents according to priority and impact, and manage them to resolution. Incidents follow structured workflows supported by the help desk and integrated SOC/NOC so that all service disruptions or degradations are acted upon promptly and traceably.

Diagnostics and Reporting. We perform diagnostics across the ESInet and NGCS using telemetry, alarms, logs, and system health indicators. Diagnostic results feed into troubleshooting workflows and are included in monthly reporting to document system behavior.

Problem Resolution and Trouble Handling. We maintain processes that identify root causes, apply corrective actions, and track issues to closure. Trouble tickets record all activity, and the help desk maintains ownership from submission through resolution.

Network Fault Monitoring. We proactively monitor for network faults across all transport segments, interfaces, and functional elements. Faults generate alarms that feed directly into SOC/NOC workflows for triage and remediation.

Request Fulfillment. We execute operational requests such as provisioning changes, access requests, or configuration updates using documented procedures and standardized approval paths.

Access Management. We enforce identity-based access for all NG911 components, applying least-privilege controls and managing provisioning, modification, and de-provisioning through controlled workflows.

Remote Diagnostics. We perform secure remote diagnostics through the integrated SOC/NOC for rapid troubleshooting and resolution without requiring onsite presence when feasible.

Environmental Requirements. We monitor environmental conditions at all data centers and points of presence, ensuring that facilities supporting ESInet and NGCS components meet operational and environmental standards.

Capacity, Change, Configuration, and Transition Management. We maintain capacity management to ensure adequate resources for growth; change management to govern modifications, impact assessments, and rollback procedures; configuration management to track baselines and versions; and transition management to support deployment and lifecycle changes.

Training Arrangements. We provide training arrangements that align with operational roles and responsibilities, ensuring personnel understand workflows tied to SLA and SLO performance.

Commercial Availability. We ensure required NG911 components and services remain commercially available and supported across the contract period to maintain performance and lifecycle continuity.

Lumen's approach integrates all service-support functions with contractually defined SLOs and provides Nebraska with a unified operational model that supports measurable SLA performance and ongoing NG911 system reliability.

5.8.4. Monitoring and Event Management

5.8.4.1. ALARM CATEGORIES

Alarms by event types depending on the criticality of the event (i.e., critical, major, etc.) will be provided. Dynamic configuration of notification thresholds will be utilized to allow new alarm categories to be defined, as necessary.

The system will have automatic notification of the NOC when alarm conditions are detected. Different notification and escalation procedures may apply depending on the alarm category.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Alarms by criticality (critical/major/etc.).*
- *Dynamic notification thresholds for new categories; automatic NOC notification.*
- *Varying notification/escalation per category.*

LUMEN RESPONSE:

Lumen will provide alarm handling and notification capabilities that classify events by criticality, support dynamic threshold configuration, and automatically notify the integrated SOC/NOC when alarm conditions occur. Our alarm framework aligns with NG911

operational expectations and ensures that escalation and response behaviors match the severity of each event type.

Alarms By Criticality. We classify alarms into categories such as critical, major, and other defined severities. Each category is associated with predefined handling behavior so that critical conditions affecting call routing or service availability receive immediate attention, while lower-severity issues follow appropriate operational workflows.

Dynamic Notification Thresholds And Automatic NOC Notification. We support dynamic configuration of alarm thresholds so new alarm categories or modified conditions can be implemented without disruption. All alarms—regardless of type—initiate automatic notification to the SOC/NOC, where operators review and triage the condition.

Category-Based Notification And Escalation. We maintain differentiated notification and escalation processes based on alarm category. Critical alarms trigger immediate escalation to appropriate technical resources, while major and lower-severity events follow defined timelines consistent with operational priorities and SLA expectations.

5.8.5 Change, Maintenance, and Release Management

5.8.5.1. CHANGE MANAGEMENT REQUIREMENTS

*The Contractor shall ensure that all changes – planned or unplanned – are managed through a structured, documented, and auditable process that maintains service stability, security, and interoperability. The process shall conform to the principles of the **Project Management Institute (PMI)** and the **ITIL v4 Service Management Framework**.*

Objectives

The objectives of the Contractor's Change Management process shall be to:

- *Maintain a stable and secure NG911 operational environment.*
- *Minimize the impact of changes on system availability, reliability, and public safety operations.*
- *Provide transparency and accountability for all system modifications.*
- *Ensure that all stakeholders are informed, consulted, and prepared for any change that affects service delivery.*
- *Incorporate continuous improvement through post-implementation review and process enhancement.*

The Change Management process shall apply to all infrastructure, applications, systems, and interfaces under Contractor operational control, including but not limited to:

- **ESInet Infrastructure:** routers, firewalls, switches, circuits, transport paths, and interconnections.
- **NGCS Components:** ESRP, ECRF/LVF, PRF, BCF, LIS, logging, and policy routing elements.
- **Call Handling Systems:** software, hardware, operating systems, and integrations with CAD, logging, and recording systems.
- **Security Systems:** encryption, certificates, firewalls, intrusion detection/prevention, and access controls.
- **Support and Management Tools:** monitoring platforms, ticketing systems, and network management applications.

Change Classification

The Contractor shall classify all changes into the following categories:

- **Standard Change:** Pre-approved, low-risk, repeatable changes executed according to pre-established procedures (e.g., routine software patching).
- **Normal Change:** Planned changes that require full evaluation, testing, review, approval, and scheduling.
- **Emergency Change:** Unplanned changes necessary to restore service, mitigate critical vulnerabilities, or prevent imminent service degradation.

Each classification shall have documented criteria, approval authorities, and implementation procedures.

Process Requirements

The Contractor shall implement a formal Change Management process that includes the following elements:

- **Change Management Plan:** A documented process outlining governance, roles, responsibilities, and workflows aligned with PMI and ITIL best practices.
- **Change Advisory Board (CAB):** A standing review body, including State representation, responsible for evaluating and approving all Normal and Major Changes.
- **Change Request System:** A centralized, auditable tool for logging, tracking, and managing all changes from request through closure.
- **Risk and Impact Assessment:** An analysis of each proposed change to evaluate its impact on system performance, service continuity, interoperability, and cybersecurity.
- **Rollback and Contingency Plans:** Documented procedures for reverting or recovering from unsuccessful change implementations.
- **Change Scheduling and Coordination:** Change windows coordinated with the State and PSAPs to minimize service disruptions.
- **Notification Requirements:** Written notice to affected stakeholders no less than ten (10) business days prior to implementation of any planned change, unless otherwise authorized.
- **Post-Implementation Review (PIR):** A formal evaluation of significant or failed changes to identify root causes, corrective actions, and process improvements.

Emergency and Security Changes

- The Contractor shall maintain procedures for the execution of emergency changes required to restore service or address urgent security vulnerabilities.
- All emergency changes shall be documented and submitted for retrospective review by the CAB within five (5) business days.
- Security-related changes, including software updates, certificate renewals, or configuration modifications, shall comply with PMI and ITIL Change Enablement best practices.
- Security changes shall be tested in a controlled environment prior to production deployment whenever feasible.

- *The Contractor shall notify the State of any emergency or security change within twenty-four (24) hours of implementation.*

Integration with Other Service Management Processes

The Contractor shall integrate Change Management with the following processes:

- **Configuration Management:** *Each change shall be linked to affected Configuration Items (CIs) within the Configuration Management Database (CMDB).*
- **Incident Management:** *Changes shall be correlated with incident and problem records to support root cause analysis and continuous improvement.*
- **Release and Deployment Management:** *The Contractor shall coordinate releases to ensure version control and documentation integrity across environments.*

LUMEN RESPONSE:

Lumen implements a structured, documented, and auditable Change Management process for all NG911 infrastructure, applications, systems, and interfaces under Lumen's operational control. The process aligns with Project Management Institute (PMI) principles and the ITIL v4 Service Management Framework and is designed to maintain a stable, secure, and interoperable NG911 environment while minimizing risk to call delivery, public safety operations, and system availability.

Change Management Plan and Governance. Lumen maintains a documented Change Management Plan that defines governance, roles, responsibilities, workflows, approval requirements, and documentation standards. The plan applies to ESInet infrastructure, NGCS elements, call handling integrations, security systems, and supporting management tools. Any change to the Change Management process itself is communicated to the State within 30-days of implementation.

Change Classification and Approval. All changes are classified as Standard, Normal, or Emergency, with documented criteria and controls for each category. Standard changes follow predefined, low-risk procedures. Normal changes require full evaluation, testing, review, approval, and scheduled implementation. Emergency changes are executed only to restore service, mitigate critical vulnerabilities, or prevent imminent degradation. A Change Advisory Board with State representation reviews and approves all Normal and Major Changes, evaluating risk, impact, scheduling, and readiness prior to approval.

Centralized Change Tracking and Auditability. Lumen uses a centralized, auditable change request system to log, track, manage, and archive every change from initiation through closure. Each change record includes scope, impacted configuration items, risk and impact assessments, approvals, implementation details, rollback plans, and post-implementation outcomes. The State has visibility into change activity through reporting and dashboard access.

Risk Assessment and Contingency Planning. Every proposed change undergoes formal analysis to assess potential impacts on interoperability, performance, service continuity, routing accuracy, latency, and cybersecurity posture, with explicit linkage to NGCS and ESInet outcomes. All changes include documented rollback and contingency procedures to ensure rapid restoration if unexpected conditions occur.

Change Scheduling and Notification. Planned changes are scheduled within coordinated maintenance windows to minimize operational impact. The State receives written notice at least 10-business days in advance for planned changes affecting routing, GIS, or call handling behavior, unless an alternate timeline is authorized. Extraordinary maintenance outside standard windows requires additional State coordination. Emergency maintenance may be performed without prior notice when required, with immediate notification to the State.

Emergency and Security Changes. Emergency changes bypass normal approval only when necessary to restore service or mitigate urgent risk. All emergency changes are fully documented and submitted for retrospective Change Advisory Board (CAB) review within five (5) business days. Security-related changes follow the same governance framework and are tested in controlled environments whenever feasible. The State is notified within 24-hours of implementation.

Testing, Deployment, and Post-Implementation Review. All changes follow a structured lifecycle that includes pre-deployment testing, validation of rollback procedures, controlled deployment using staged execution, and post-deployment verification. Significant changes and all unsuccessful changes undergo post-implementation review to identify root causes, corrective actions, and opportunities for process improvement.

Configuration Management, Backup, and Restoration. Lumen employs automated configuration management tools to enforce policy compliance, detect configuration drift, and maintain consistent implementations across network elements. Configuration data is backed up on every commit and at least daily, with backups stored in secure, geographically diverse locations. Backups are performed prior to upgrades to ensure recovery capability and support restoration of known-good configurations without operational impact. For Nebraska NG911, backups include ESInet configurations stored in secure Lumen facilities, with NGCS-related backups coordinated with Intrado.

SD-WAN Configuration Control. ESInet SD-WAN configurations are managed centrally through the SD-WAN System Director rather than directly on appliances. Configuration changes are version-controlled and replicated to geographically diverse instances of the platform to support availability and continuity of operations. Configuration updates are pushed to appliances during approved change windows or automatically in the event of device replacement or failure.

Reporting and State Oversight. Lumen provides regular reporting on change activity, including changes opened, pending, completed, and closed. Backup and restoration reports are available on demand and on a scheduled basis. The Lumen Operations Service Manager provides copies of configuration data and change records to the State upon request, ensuring transparency, auditability, and continued alignment with State governance expectations.

5.8.5.1.1. Security Considerations in Change Management

*In conjunction with the change management processes defined in §E-9.5.2 (Scheduled Maintenance Process) and §E-9.5.3 (Software Update and Improvements) of this document, the contractor must evaluate the **security impact** and **operational risk** for all changes to NGCS elements and the ESInet - including equipment, software, and configurations. Every change requires **policy-compliant review and approval, a documented security review, and complete records**. If timing precludes standard*

pre-approval (Unplanned/Emergency [time-critical issues with expedited workflows] issues), all required reviews and documentation must be completed immediately after implementation. The contractor should utilize segregation of duties, maintain configuration baselines, and coordinate maintenance windows to protect call delivery, routing, location accuracy, latency, and availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Evidence that all changes are reviewed and approved per policy with a documented security review (threat/impact, affected NGCS/ESInet elements and services, potential customer impact, required controls and monitoring).*
- *An Unplanned/Emergency change process that documents expedited approvals and requires retroactive completion of all "SHALL" requirements and documentation identified in NENA-STA-040.2*
- *§4.4 (Change Management) within a defined timeframe.*

LUMEN RESPONSE:

Lumen will evaluate the security impact and operational risk for every change applied to NGCS elements and the ESInet, including changes to equipment, software, and configurations. All changes follow an established, policy-compliant review and approval process that incorporates a documented security review, risk evaluation, and full change record creation. This process applies to both planned and unplanned changes and is designed to protect call delivery, routing accuracy, latency, availability, and overall system integrity.

Policy-Compliant Review and Approval. We require every change to undergo documented review and approval before implementation. Each review includes a security assessment that evaluates threat exposure, operational impact, affected NGCS and ESInet components, potential service effects on routing or call handling, and required security controls and monitoring. Approval authorities follow the designated Change Management roles and workflows.

Documented Security Review. We document a formal security review for each change, including evaluation of vulnerabilities introduced or mitigated, dependency analysis, service-impact assessment, and validation that required protective controls are in place. All results are retained within the centralized change-request system as part of the permanent audit record.

Unplanned and Emergency Changes. We maintain an expedited Unplanned/Emergency change process for time-critical issues when pre-implementation approval is not feasible. Emergency changes follow immediate stabilization and restoration priorities and must undergo full retroactive documentation to complete all "shall" requirements defined in NENA-STA-040.2 §4.4 within the required timeframe. This includes retroactive security review, approval documentation, risk evaluation, and change record updates.

Segregation of Duties and Baseline Protection. We enforce segregation of duties during change request, approval, and implementation so no single individual controls the full process. Configuration baselines are maintained to ensure that changes are evaluated against known good states, and maintenance windows are coordinated with the State to minimize risk to call delivery and NG911 operations.

5.8.5.2. SCHEDULED MAINTENANCE PROCESS

A scheduled maintenance process document will be developed and maintained. The process must include a methodology for coordinating and scheduling preventative maintenance activities and how those events are executed as may be necessary during the operation of the NG911 system.

During scheduled maintenance activities the ESInet and NG911 system must maintain 99.999% availability. There must not be a substantial degradation or disruption caused by the maintenance activity. However, individual components may be taken down for maintenance if an alternate route or redundant system is used to maintain the 99.999% threshold.

If a partial or total outage occurs within hours of a maintenance activity, Contractor shall issue a report within 30 days to the State detailing:

- What occurred during the outage, including system elements that were impacted*
- Whether the outage was caused by, or influenced by, the maintenance activity*
- What corrective actions, specifically corrective actions to the change control process, will be implemented to avoid recurrence, not just to the specific problem but to similar problems*

Following any scheduled maintenance, a maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What are the results of the scheduled maintenance*
- What was done during the scheduled maintenance*
- How will such scheduled maintenance impact the services in operation*

Following any emergency maintenance, an emergency maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What caused the emergency maintenance*
- What was done during the emergency maintenance*
- How will such emergency maintenance be avoided in the future*

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Developed/maintained process document for coordinating/scheduling preventative maintenance.*
- No degradation/disruption during activities.*
- Allowance for individual component downtime with alternates/redundancy.*

LUMEN RESPONSE:

Lumen will maintain a scheduled maintenance process that coordinates, documents, and controls all preventative maintenance activities for NG911 components while preserving required service availability. The process ensures that maintenance tasks are planned, communicated, executed, and reviewed in a manner that maintains 99.999% availability for the ESInet and NGCS during maintenance windows.

Scheduled Maintenance Process. We develop and maintain a documented scheduled maintenance process describing how preventative maintenance is coordinated, approved, and executed. This includes maintenance-window planning, State coordination, notification

procedures, and verification steps before and after maintenance activities. The process ensures that maintenance is performed without disrupting NG911 call delivery, routing, or other critical NGCS functions.

Service Continuity During Maintenance. We ensure that scheduled maintenance does not cause degradation or disruption to ESInet or NGCS services. Individual components may be taken out of service for maintenance only when alternate routes or redundant systems are available to maintain 99.999% end-to-end availability. Maintenance windows are evaluated to confirm redundancy is active and monitored before any component is removed from service.

Outage Within Hours of Maintenance Reporting. If a partial or total outage occurs within hours of a maintenance activity, we prepare and submit a report to the State within thirty days. The report includes:

- A description of what occurred during the outage and which system elements were impacted,
- An analysis of whether the maintenance activity caused or contributed to the outage, and
- Corrective actions—including changes to the change-control process—required to prevent recurrence, addressing both the specific issue and similar failure modes.

Scheduled Maintenance Reporting. Within twenty-four hours of completing scheduled maintenance, we prepare and submit a scheduled maintenance report to the State that includes:

- The results of the maintenance,
- The activities performed, and
- Any effects the maintenance will have on operational services.

Emergency Maintenance Reporting. Within twenty-four hours of emergency maintenance, we provide an emergency maintenance report that includes:

- The cause of the emergency maintenance,
- The actions taken during emergency remediation, and
- Measures to avoid similar emergency events in the future.

Lumen's approach maintains NG911 service stability during maintenance, ensures full transparency to the State, and provides all required reporting and analysis to safeguard Nebraska's 911 operations.

5.8.5.3. SOFTWARE DEVELOPMENT PROCESS

The Contractor and all Subcontractors shall use a documented, modern software development lifecycle (SDLC) that produces high-quality code with minimal delay. At a minimum, the SDLC shall include secure coding standards, peer/code reviews, automated testing, version control, and controlled release management (CI/CD or equivalent).

For all software components directly in the NG911 call path, the Contractor and all Subcontractors shall have a process to evaluate, release, and deploy critical security patches within 72 hours of the patch's public availability. This process shall be rehearsed on a regular cadence, and rehearsal results shall be shared with the State.

When a trouble ticket or outage results in a software bug, a discrepancy report, or a required system change to prevent recurrence, the Contractor shall maintain an online, State-accessible log showing each item, severity, affected components, current status,

workaround (if any), and the target fix version and release date. This log shall also include items required to bring the system into conformance with standards such as NENA-STA-010.3(including the Discrepancy Reporting function).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Modern processes for high-quality code with minimal delay.*
- *72-hour release/install for critical security patches with rehearsal/results shared.*
- *Log of bugs/changes/estimated fixes available online.*
- *Updates for standards conformance.*

LUMEN RESPONSE:

Lumen employs a documented, modern software development lifecycle (SDLC) for all NG911 software developed or integrated for the State of Nebraska. This SDLC applies to all NGCS components and ESInet-related software under Lumen's control and is aligned with secure coding practices, controlled release management, and standards conformance. The lifecycle is designed to deliver high-quality software with minimal delay while protecting the integrity of the NG911 call path.

Modern Development and Release Practices. Lumen and its NGCS subcontractor, Intrado, apply mature, enterprise-grade SDLC practices that include secure coding standards aligned with industry best practices, peer and formal code reviews, automated unit, integration, and regression testing, version control with full change traceability, and controlled release management using Continuous Integration/Continuous Deliver (CI/CD) or equivalent gated deployment pipelines. Every change to NG911 software is version-controlled, reviewed, and validated prior to promotion into integration and production environments. Lumen applies comparable development and Change Management practices for Lumen-managed components, including the statewide trouble ticketing and service management platform.

Critical Security Patch Management. For software components that operate directly in the NG911 call path, Lumen and Intrado maintain a defined process to evaluate, approve, and deploy critical security patches within 72-hours of public availability when warranted by severity and risk. This process includes review of vendor advisories, risk and impact assessment, validation testing in a controlled environment, and promotion to production under emergency change procedures when required. The critical patch process is rehearsed on a regular cadence through planned exercises and simulated scenarios, with rehearsal results documented and shared with the State so Nebraska can verify that time-critical patching workflows operate as intended.

Trouble Ticketing, Discrepancy Tracking, and Change Transparency. Lumen provides and operates a State-accessible online trouble ticketing system that serves as the authoritative intake and tracking mechanism for incidents, outages, and service requests across the ESInet and NGCS environment. When a ticket identifies a software defect, discrepancy report, or required system change, Intrado performs root cause analysis, defect tracking, and remediation planning for NGCS software, while Lumen maintains coordination and visibility through the shared platform.

Online Bug and Change Log. Lumen maintains a State-accessible online log of software bugs, discrepancy-driven changes, and required system updates. For each entry, the log records, at a minimum, the item description or identifier, severity, affected components,

current status, any available workaround, the target fix version, and the planned release date. The same log includes work items required to bring the system into conformance with applicable standards, including NENA STA 010.3 and its Discrepancy Reporting requirements.

Standards Conformance and Governance. Intrado manages standards-related discrepancies and remediation activities for NGCS software, while Lumen ensures that conformance items impacting ESInet operations are tracked, coordinated, and communicated to the State. Progress updates, resolution status, and release alignment for standards conformance items are visible to the State through the shared logging and reporting process. Responsibilities between Lumen and Intrado are clearly defined to ensure effective coordination, transparency, and accountability across the NG911 environment.

5.8.5.4. SOFTWARE UPDATES AND IMPROVEMENTS

Updates, bug fixes, and patches must be classified by the contractor as normal or emergency. When any normal hardware or software changes are made to a site, there will be a minimum of 30 days before any hardware or software changes can be made to any other site. Where more than one instance of a function or service is provided on a site, only one instance can be changed at a time. Where there are both multiple sites and redundant instances per site, one instance may be changed at the first site, at least 30 days must elapse, one instance on another site can be made, at least two weeks must elapse, another instance can be updated, after which at least one week must elapse before the next change.

Emergency bug fixes/patches are not required to meet these minimum times. However, if the contractor determines that an emergency bug fix/patch is necessary, it will transmit a report to the State within 48 hours of such a determination, detailing the problem, the necessary fix, and a valid reason the fix could not be completed in regular software update or bug fix processes.

A prescheduled maintenance window will be negotiated between the contractor and the State. All normal maintenance will take place within that window. Extra-ordinary maintenance processes that require additional time may be scheduled with a minimum of 30 days' notice.

Emergency maintenance can be scheduled with no prior notice, but the State must be notified immediately that such an emergency maintenance is needed, what the estimated duration is and why the emergency maintenance is necessary.

The Respondent must provide a detailed methodology for managing all system updates, including software patches, security updates, configuration changes, and data updates (e.g., GIS data). The process must be structured to minimize service disruption, ensure system integrity, and maintain security. The update process must include procedures for testing, scheduling, deployment, and verification of all changes in the production environment.

A formal process for releasing software updates, bug fixes and improvements, and any changes to the process will be communicated to the State within 30 days of the change being put into practice.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *Formal process for updates/fixes/improvements with 30-day notice of changes.*
- *Classification as normal/emergency.*
- *Minimum 30-day spacing for normal changes across sites/instances.*
- *No minimum times for emergency but 48-hour report to State.*
- *Negotiated maintenance window.*
- *Extra-ordinary with 30-day notice.*
- *Immediate notification for emergency with duration/reason.*

LUMEN RESPONSE:

Lumen manages all NG911 updates through a formal, controlled, and auditable update methodology designed to maintain service stability, system integrity, and security across all ESInet and NGCS components. The methodology governs software updates, bug fixes, improvements, configuration changes, and data updates, and enforces classification, spacing, testing, scheduling, verification, and reporting requirements consistent with the State's expectations.

Formal Update, Fix, and Improvement Process. Lumen, as the Prime Contractor, and Intrado, as the NGCS software provider, maintain a documented process for managing all system updates across the NG911 environment. This process includes testing changes in controlled environments, coordinating deployment schedules with the State and PSAPs, verifying completion in production, and maintaining full documentation and traceability. Any change to the update methodology itself is communicated to the State within 30-days of implementation.

Update Classification and Governance. All updates, bug fixes, and patches are formally classified as either normal or emergency. Normal updates include planned software releases, enhancements, non-critical defect remediation, configuration changes, and scheduled data updates, including GIS-related changes. Emergency updates are limited to critical defects or security issues that present an immediate operational, safety, or security risk and cannot wait for the normal update cycle. Classification governs approval, scheduling, deployment sequencing, notification, and reporting requirements.

Normal Update Scheduling and Change Sequencing. For normal hardware or software changes, Lumen and Intrado adhere to strict spacing and sequencing controls to preserve redundancy and reduce operational risk. A minimum of 30-days elapses between a normal change at one site and the same change at another site. Where multiple redundant instances exist at a site, only one instance is updated at a time. When both multiple sites and redundant instances exist, one instance at the first site may be updated, followed by at least thirty days before updating one instance at another site, at least two additional weeks before updating the next instance, and at least one additional week before any subsequent change.

Emergency Update Procedures and Reporting. Emergency updates and patches are not subject to minimum spacing requirements. When an emergency update is required, the State is notified immediately of the issue, the reason emergency maintenance is necessary, and the estimated duration. Within 48-hours of the determination, Lumen provides the State with a written report describing the problem, the corrective action taken or required, and a valid justification for bypassing the normal update process. All emergency changes are fully documented retroactively and comply with all change management obligations.

Maintenance Windows and Extraordinary Maintenance. Lumen works with the State to establish a prescheduled maintenance window used for all normal maintenance activities.

Extraordinary maintenance requiring additional time or deviation from the standard window is scheduled with at least 30-days' notice and State coordination. Emergency maintenance may be performed without prior notice; however, the State receives immediate notification describing the reason, scope, and expected duration.

Testing, Deployment, and Verification. All updates undergo formal pre-deployment testing, including functional, regression, interoperability, and security validation where applicable. Deployment follows coordinated scheduling and staged, instance-by-instance execution. Post-deployment verification confirms system stability, redundancy, and service integrity and ensures that updates do not introduce degradation or unintended impacts. Intrado executes these processes for NGCS software components, while Lumen coordinates ESInet impacts, deployment timing, and State communication.

Process Transparency and State Oversight. Lumen and Intrado maintain comprehensive documentation describing update classification rules, scheduling requirements, testing procedures, deployment controls, and verification steps. This documentation is maintained and made available to the State upon request, ensuring transparency, auditability, and continued alignment with State governance expectations.

5.8.6. Spares and Inventory

5.8.6.1. SPARES

Respondents must describe their spares program, including stocking levels, storage locations, and the time required for an on-site field technician to obtain a spare. If the State has any role in spare stocking or access, explain that role.

A sufficient supply of spare parts shall be maintained at locations that enable immediate restoration of service. This requirement is tied to the Mean Time to Repair (MTTR) specified in §E-9 of this document. Where there are multiple connections, the Contractor shall provide multiple spare units staged in multiple locations.

Within the proposal response, explain how sparing strategies maintain both Mean Time Between Failures (MTBF) and MTTR at levels necessary to achieve 99.999% availability.

If malfunctions or failures recur, the State may require the Contractor to increase spare inventory to ensure adequate parts are available to address the repeated issue.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Describe the spares program, including stocking levels, locations, and technician access time
- Explain any State role in spare stocking or access
- Show how sparing maintains required MTBF/MTTR to achieve 99.999% availability

Operational Obligations (Post-Award):

- Maintain spare inventory at levels consistent with MTTR needs.
- Refresh replacement stock within twenty-four (24) hours after use
- Retain sole responsibility for restocking spare parts
- Track and report monthly on equipment failures requiring use of spare inventory
- Adjust inventory as needed and provide documentation to the State upon request
- Identify where spares are located and maintained

- *Use spare inventory to support the entire proposed system, adjusting as needed*
- *Replenish remote parts depots when their stock is depleted*
- *Increase spare inventory if repeated malfunctions occur.*

LUMEN RESPONSE:

Lumen will maintain a structured spare parts program designed to support immediate service restoration for the Nebraska NG911 ESInet and NGCS environment and to meet the Mean Time to Repair (MTTR) requirements specified in §E-9. We provision spare components for all critical NGCS and ESInet elements, including those required to support redundant and geographically diverse connections. Stocking levels are determined based on component criticality, historical failure patterns, vendor support models, and restoration objectives, and are maintained at levels sufficient to restore service without reliance on vendor shipping timelines.

Staged Spares Inventory. Spare inventory is staged in multiple secure locations to ensure rapid access by on-site or dispatched field technicians. These locations include regional depots serving Nebraska and, where applicable, controlled facilities associated with NG911 infrastructure locations. For elements deployed in multiple locations or supporting multiple connections, we stage multiple spare units across separate locations to avoid single points of failure. Our access and logistics procedures enable a qualified field technician to obtain and deploy a spare within the timeframes required to meet MTTR objectives and support immediate service restoration.

State of Nebraska Role. The State of Nebraska has no operational role in spare stocking, maintenance, or access. We retain sole responsibility for managing spare inventory, including storage, security, access control, deployment, and replenishment. Upon request, we provide documentation identifying spare locations, the classes of equipment supported, and confirmation that inventory levels align with contractual requirements.

Maintaining Performance. Our sparing strategy supports both MTBF and MTTR targets necessary to achieve 99.999% service availability. Redundant system design consistent with NENA i3 architecture limits the operational impact of individual component failures, while staged spare inventory enables rapid replacement and minimizes outage duration. We use failure trend analysis and lifecycle management practices to identify components requiring increased sparing or replacement, reducing the likelihood of repeat failures and sustaining required MTBF performance.

The following describes Lumen's spares approach:

- **Spares Program Description:** We maintain spare inventory for all critical NGCS and ESInet components, with stocking levels aligned to component criticality and MTTR requirements. Spares are stored in multiple secure locations and are accessible to field technicians within the time necessary to restore service.
- **State Role:** The State has no responsibility for spare stocking or access. We manage all aspects of spare inventory and deployment and provide documentation upon request.
- **MTBF/MTTR and Availability:** Redundant architecture combined with readily available spares enables rapid replacement of failed components, supporting MTBF and MTTR targets necessary to achieve **99.999%** availability.

Spares Inventory. We maintain spare inventory at levels consistent with MTTR requirements and refresh replacement stock within twenty-four (24) hours after a spare is used. We retain

sole responsibility for restocking spare parts and for replenishing remote depots when stock is depleted. For Nebraska NG911, Intrado-related spares are managed and staged through the Critical Spares organization, while ESInet-related spares are maintained locally in Buffalo County, Nebraska.

We track and report monthly on equipment failures requiring use of spare inventory and adjust inventory levels as needed based on observed failure trends. Documentation is provided to the State upon request. If repeated malfunctions or failures occur, we increase spare inventory as necessary to ensure adequate parts are available to maintain required service availability across the entire proposed system.

5.8.6.2. SPARE INVENTORY AT DATA CENTERS

In addition to the spare inventory maintained at Contractor locations, the Contractor must maintain critical spare inventory on-site at each data center location. The Contractor must:

- *Identify and provide documentation of critical spare inventory maintained on-site at each data center*
- *Add equipment to this list based on frequency and type of repair to ensure critical spare inventory is maintained on-site at all times*
- *Replenish spare parts inventory if required by the State in case of repeated malfunction or failure*

This on-site inventory ensures immediate access to critical components needed to maintain the required system availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- *On-site critical spare inventory at each data center.*
- *Identification/documentation of inventory.*
- *Additions based on repair frequency/type.*
- *Replenishment for repeated malfunctions/failures.*

LUMEN RESPONSE:

Lumen will maintain critical spare inventory on-site at each Nebraska NG911 data center location in addition to the spare inventory maintained at Lumen-controlled regional and depot locations. This on-site inventory is reserved for components designated as critical to the continuous operation of NGCS and ESInet services and is intended to ensure immediate access to replacement equipment required to maintain required system availability.

Documented Critical Spares. We identify and maintain a documented list of critical spare components stored on-site at each data center. This documentation specifies the classes of equipment supported and confirms that on-site inventory is sufficient to address failures that could otherwise impact service availability. The inventory list is reviewed and updated as part of our ongoing operational and maintenance practices and is made available to the State upon request.

Inventory Management. On-site critical spare inventory is adjusted and managed as needed based on the frequency and type of repairs observed within the operational environment. When failure trends or repair history indicate that additional components should be maintained on-site to reduce restoration time or mitigate recurring issues, we add those components to the on-site spare inventory to ensure they are available at all times.

If repeated malfunctions or failures occur, we replenish and, if required by the State, increase on-site spare parts inventory to ensure adequate components are immediately available to address the issue and maintain required system availability. We retain sole responsibility for managing, replenishing, and maintaining all on-site spare inventory, ensuring it remains aligned with MTTR requirements and overall system performance objectives.

This on-site sparing approach ensures that critical components are immediately accessible at each data center location, supports rapid service restoration, and contributes to sustaining the availability requirements of the Nebraska NG911 system.

Deliverables - Operational Support and Service Level Agreements (SLAs)

Deliverable Coordination, Schedule, and Format. Lumen has read, understands, and will comply with all State of Nebraska deliverable requirements. Post-award, Lumen will ensure that all required deliverables are provided to the State in accordance with the established deliverable schedule and in the format specified by the State. Lumen will coordinate closely with the State to confirm delivery expectations, acceptance criteria, and submission timing to support timely review, approval, and system acceptance.

Lumen understands that the State requires clearly defined operational commitments, enforceable service levels, and documented assurance that NG911 services will be continuously supported throughout the contract term. Lumen complies by providing comprehensive SLA documents, training curricula, sample operational runbooks, and a maintenance calendar that define availability targets, response and restoration commitments, escalation paths, and routine operational procedures supporting statewide NG911 operations.

Lumen further complies by providing references from three comparable NG911 deployments, including documented uptime and performance results, to demonstrate proven experience operating highly available, mission-critical NG911 environments. These references provide the State with objective evidence of Lumen's ability to meet sustained availability and service level commitments over time.

Lumen also acknowledges and complies with the State's requirement that the system and services be delivered conformant with applicable NENA standards at acceptance, unless mutually agreed-upon provisions are approved. In the event that any standards-related gaps are identified and accepted by the State, Lumen will provide a documented remediation plan and timeline and will communicate progress regularly with the State and the Advisory Committee until full conformance is achieved.

Finally, Lumen commits to maintaining ongoing conformance as NENA standards evolve. Lumen will implement new or revised standards within the State's nine-month guideline period and will proactively identify any areas where additional time may be required. In such cases, Lumen will provide a clear plan, schedule, and interim risk mitigation strategy to ensure transparency and continued alignment with State expectations. Collectively, these deliverables provide assurance that operational support, service levels, and standards conformance are sustained throughout the lifecycle of the NG911 solution.

5.9. Value Add and Optional Services

Respondents will describe any optional services that may enhance their product or the delivery of NG911 to the State. Particularly, this may mean the ability to deliver a hosted call handling system after the ESInet has been deployed and NG911 routing is being provided.

LUMEN RESPONSE:

Lumen offers optional services that enhance both the delivery and long-term evolution of NG911 services for the State of Nebraska. These optional capabilities are designed to integrate seamlessly with the deployed ESInet and NG911 routing environment without disrupting ongoing operations or requiring architectural changes. Please see the following sections for Lumen's optional Call Handling Equipment (CHE) services.

5.9.1. Call Handling Equipment (CHE) Services

The PSC would like to have insight into the options a vendor may provide for CHE. PSAPs in the State may want to move to a hosted solution or an approved solution at some point during the contract period. In order to determine the viability proposers may offer a CHE solution as an option, but it is not a firm requirement at this time.

Hosted CHE is preferred; to allow PSAPs an option of moving from an on-prem call handling system into the hosted CHE platform over time.

The Respondent may provide a Call Handling Equipment (CHE) solution that serves as the primary user interface for PSAP call takers and dispatchers. The CHE must be capable of receiving and managing emergency calls from the ESInet, including support for various media types such as voice, real-time text (RTT), and video. The solution must provide an intuitive graphical user interface (GUI) that displays all pertinent call information, including caller location on a map, and integrates seamlessly with other PSAP systems like Computer Aided Dispatch (CAD) and logging recorders.

Also, the signaling and media interface at the demarcation between the ESInet infrastructure and the PSAP will comply with standards-based NG911 requirements as stated in the NG911 services section and elsewhere within the technical and operational requirements. Solutions that utilize proprietary signaling and/or media across the Access Network to End Site demarcation point, or that otherwise do not comply with the technical or operational requirements specified for this demarcation point, will not be acceptable.

LUMEN RESPONSE:

Lumen offers CHE as an expanded service to support Public Safety Answering Points (PSAPs) in accepting Next Generation 9-1-1 (NG9-1-1) networks and services.

Where a PSAP elects to procure CHE under this contract, Lumen offers NENA i3-compliant wholesale replacement solutions, including both Motorola VESTA hosted and Intrado VIPER hosted, available statewide. Any CHE solution offered is provided as a complete replacement of the existing system. Each solution is hosted in Geodiverse data centers ensuring that there is no single point of failure (SPoF) for any PSAP within the system.

Lumen's CHE offerings are designed to integrate seamlessly with the proposed ESInet and NG911 Core Services, while providing PSAPs with flexible deployment choices, operational continuity, and enhanced call-handling capabilities.

Both Motorola VESTA and Intrado VIPER are based on NENA standards for emergency and non-emergency call processing, routing, and delivery, including text to 911. Each solution has the ability to interface with any combination of administrative lines including but not limited to Plain Old Telephone Service (POTS), Primary Rate Interface (PRI), Centrex, and Session Initiation Protocol (SIP).

Additional features include the ability to call back abandoned calls automatically, freeing up call taker time in the PSAP. Translation and transcription features are also available.

5.9.2. ESInet and NGCS backup system

The PSC would also like to understand the options a vendor may provide to increase the diversity and redundancy of the system. This may be a tertiary alternative that could be utilized in the event of the primary system or transport failure.

LUMEN RESPONSE:

Lumen is proposing two (2) optional items for tertiary connectivity to the PSAP. Dejero, in combination with Starlink will provide tertiary wireless and satellite connectivity to each host PSAP listed in this proposal.

Dejero is a small device placed at the PSAP that integrates with the SD-WAN. The SD-WAN will be connected to the traditional MPLS circuits as well as the Dejero device. The Dejero device will come with 2 SIM cards that are used to connect to wireless carriers with up to 600GB of data per month. As part of our implementation process, we will do testing at each CHE host site to see which wireless carriers have the best connectivity at each site. For example, Buffalo county may have better signal with AT&T and Verizon so those carriers will be used. In the event of a failure of the terrestrial MPLS circuits the SD-WAN will recognize the failure and will process the calls received through the wireless carrier/Dejero device.

To supplement the Dejero wireless connectivity, we are also including Starlink satellite connectivity in this proposal. Starlink gives the state another layer of redundancy ensuring that we meet **99.999%** reliability in the ESInet for this proposal. In the event of a failure of the terrestrial MPLS circuits and wireless carriers, PSAPs will still be able to receive calls through the Starlink satellite.

5.10. Use Case Examples for Use with Response

5.10.1. Instructions

The following diagrams depict the NG911 system from a functional view. These Use Case scenarios provide Respondents the opportunity to demonstrate the traffic flow and performance perspectives of their proposed system. The Use Cases are designed to present a basis for validation of responses to the requirements of the RFP and will be used as a basis for evaluation of the delivery of traffic from caller to PSAP.

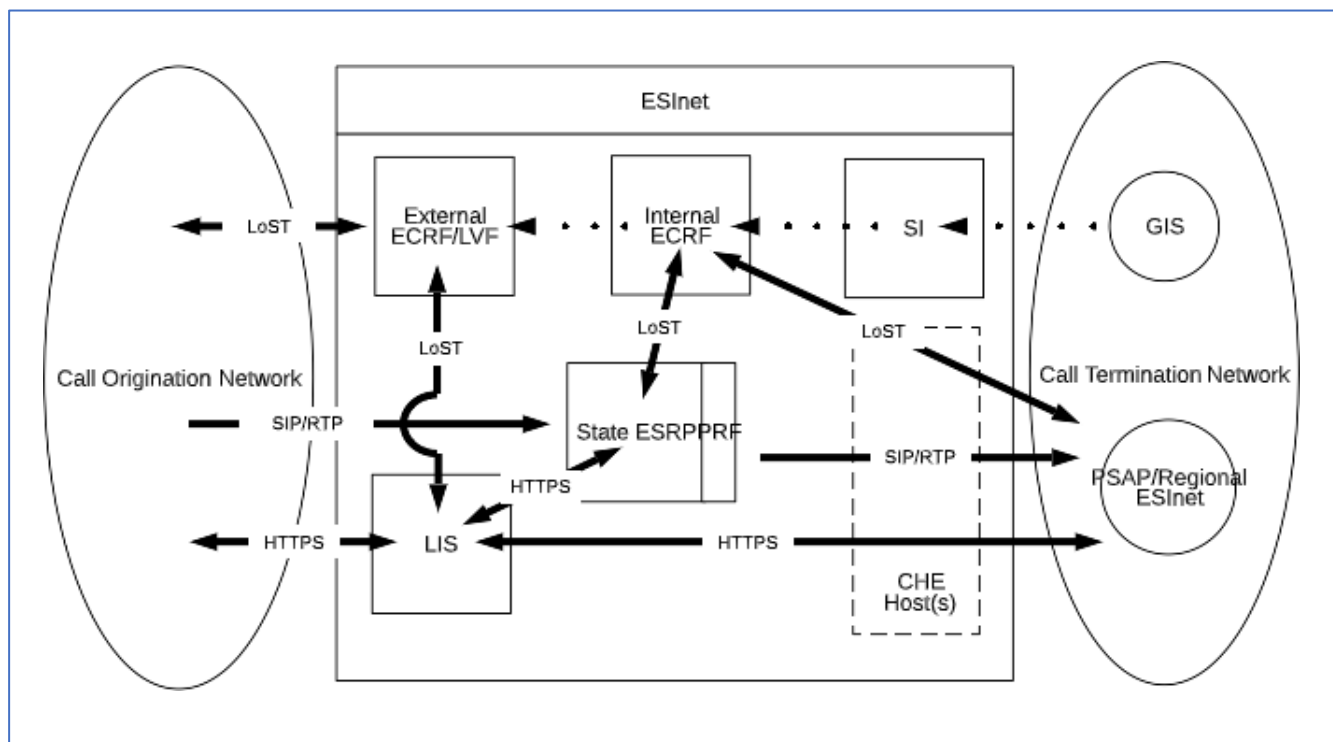


Figure 3: High-level NENA i3v3 Architecture

High-Level Use Case and Overall Expectation

The first expectation is for the Respondent to offer a narrative of how their proposed solution will meet the functionality depicted in the above diagram.

Respondents must:

- Describe how traffic flows from the call origination network, through the core to the PSAP in step-by-step fashion.
 - At each functional element, a description shall be provided to discuss how the traffic flow is being modified or adjusted due to additional data between functional elements.
 - At each functional element, a description shall be provided to identify how the system is managed and how alerts of disruptions or incidents will automatically notify the NOC.
 - At each functional element, a description of how the interface between the functional elements will be utilized.
 - Demonstrate how the system will handle the use case presented and discuss the operation, including which partner(s) (Prime or Subcontractor) would be responsible for ingress, core, and egress.
 - Identify the bandwidth available and options to manage and monitor bandwidth between functional elements and for the entire platform.
- Describe the performance expectations of the system and explain how performance is guaranteed for legacy 911 across the entire system to egress to a legacy PSAP.

- *Identify how systems operate in a “normal” state.*
- *Identify how systems operate in an “abnormal” condition.*
- *Demonstrate how the platform will operate in a “fail” condition.*
- *Describe how security is implemented across the system while maintaining the performance guarantees expected to egress to a legacy PSAP.*
 - *Identify how DDoS and TDoS events are mitigated.*
 - *Identify how security events are mitigated at each component throughout the system, including incidents that derive from the OSP, the PSAP and other ESInets.*
- *Describe how 911 data is delivered to the logging and reporting system to be accessed by a PSAP.*
 - *Identify how databases operate.*
 - *Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.*
 - *Explain how logging is collected and accessed for legacy CDR and i3 logging.*
- *Describe how calls may be transferred between NG PSAPs.*
 - *Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on the same NG911 system.*
 - *Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on a different NG911 system.*
 - *Describe how transfers are logged and how the data is logged.*
 - *Discuss the data that is transferred to the receiving PSAP.*
 - *Explain how logging is collected and accessed for legacy CDR and i3 logging.*
- *Describe any areas where the “span of control” on enforcement of diversity, redundancy, policies, procedures or any other automated or manual function that would limit the overall success of a call reaching a call taker is within the system.*
 - *Explain the limitations with the proposed system in a clear manner so that the evaluation team, and the State have a clear understanding of what is being proposed.*
 - *Gaps and limitations do not disqualify or eliminate a proposal; on the contrary an open and honest response will allow these types of issues to be documented and will lead to a collaborative plan to remediate.*

LUMEN RESPONSE:

High-Level NENA i3 Architecture and Traffic Flow - Use Cases. Lumen’s proposed NG911 solution for the State of Nebraska delivers a fully managed, standards based ESInet that conforms to the NENA i3 architecture and supports both NG911 and legacy 911 operations. The solution provides secure, resilient, and observable call routing from call origination through delivery to the appropriate PSAP, with clear operational ownership and continuous monitoring across all functional elements.

Step by Step Traffic Flow

1. Call Origination

Emergency calls originate from wireless, wireline, or VoIP service providers. Calls may include voice and associated data (e.g., location, call metadata) and are delivered toward the ESInet using SIP signaling consistent with NENA i3 requirements. Legacy 911 calls are supported through interworking functions to ensure continuity during transition periods.

2. Ingress to the ESInet

Calls enter the Lumen managed ESInet through secured ingress points. Border control and security functions enforce access control, protocol validation, and traffic inspection to protect the core network. At ingress, call signaling and associated data are normalized for processing within the i3 environment. Lumen is responsible for ingress network connectivity, security enforcement, and performance monitoring.

3. ESInet Core and i3 Functional Services

Within the ESInet core, i3 functional elements support policy based routing and call processing. Location information is evaluated using GIS driven routing functions to determine the appropriate destination PSAP. The ESInet core operates in a redundant, geographically diverse architecture to eliminate single points of failure and ensure rapid recovery from network events. All functional elements generate operational telemetry and alarms for real time visibility.

4. Egress and Policy Routing

Based on routing policy and location results, calls are delivered through the appropriate egress path. The ESInet supports delivery to NG911 capable PSAPs as well as legacy PSAPs, ensuring performance and service consistency across mixed environments. Traffic prioritization and QoS mechanisms are applied to maintain call quality under normal and peak conditions.

5. PSAP Delivery

Calls are delivered to the destination PSAP, including associated data required for call handling. The architecture ensures that both NG911 and legacy PSAPs receive calls with predictable performance, maintaining service continuity while supporting future migration to full i3 functionality.

Operations, Monitoring, and Incident Management. Lumen continuously monitors all ESInet functional elements through its NOC. Automated alarms notify operational staff of disruptions or performance degradation at any stage of the call flow. Incidents are managed through established operational procedures, with clear escalation, root cause analysis, and coordination with State stakeholders as required.

Performance and Bandwidth Management. The ESInet is engineered with scalable bandwidth and traffic management controls to support current and future call volumes. Performance expectations are enforced through network design, redundancy, and proactive monitoring. These measures ensure consistent call completion and quality for both NG911 and legacy 911 traffic across the entire call path.

Prime and Subcontractor Responsibilities:

- **Lumen (Prime):** ESInet design, ingress and egress connectivity, core network operations, security, monitoring, and performance assurance.
- **NG911 Application Providers (as applicable):** Call handling and application level services at the PSAP.

This division of responsibility ensures clear operational ownership while enabling seamless end to end service delivery.

Use Case Diagrams and Call Flow Scenarios. **Figure 5.10.1-1** depicts a scenario in which a Lumen-provided i3 OSP initiates an emergency call that is routed to an i3-compliant Terminating ESRP/PSAP. To expand on that depiction, the three diagrams below offer a high-level view of the end-to-end call flow, along with an illustration of how GIS data is provisioned through the Spatial Interface (SI) within the i3 architecture.

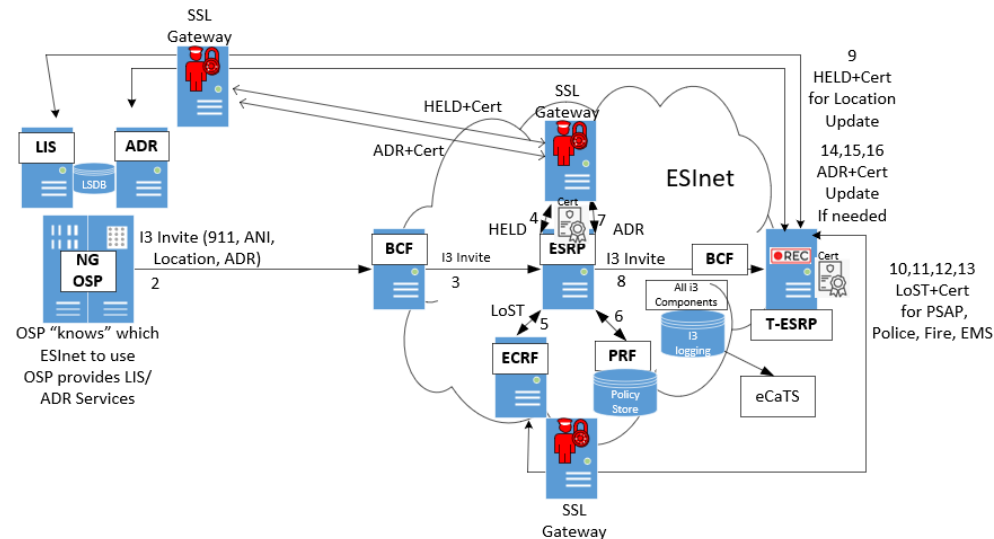


Figure 5.10.1-1. i3 OSP w/LIS/ADR not using NFG

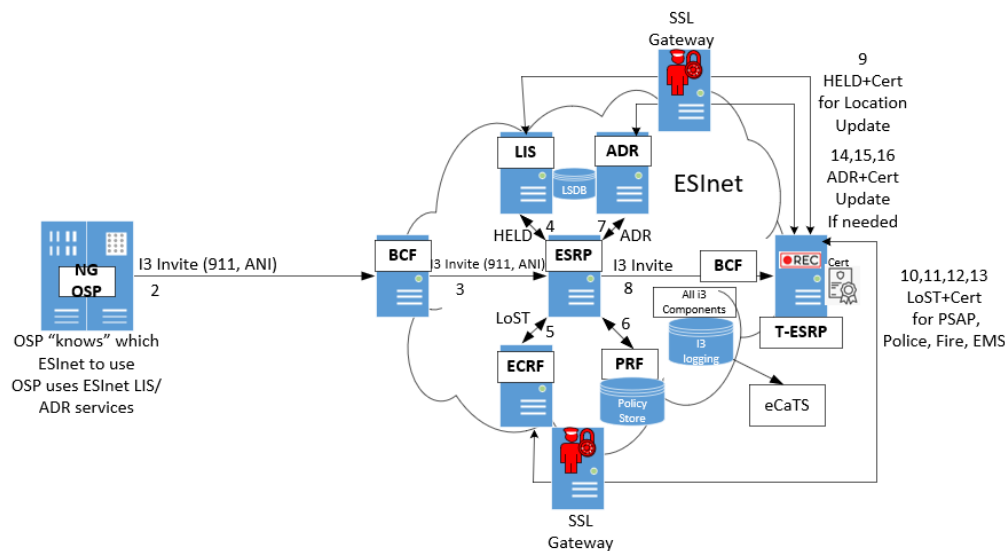


Figure 5.10.1-2. i3 OSP not using NFG using Lumen LIS/ADR

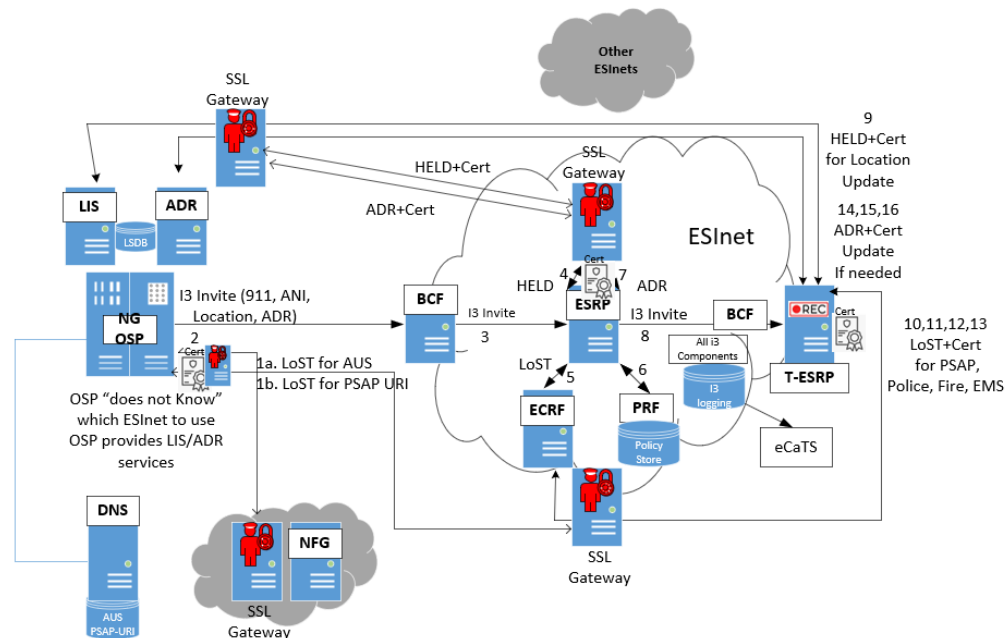


Figure 5.10.1-3. i3 OSP using NFG

Describe how traffic flows from the call origination network, through the core to the PSAP in step-by-step fashion.

- *At each functional element, a description shall be provided to discuss how the traffic flow is being modified or adjusted due to additional data between functional elements.*
- *At each functional element, a description shall be provided to identify how the system is managed and how alerts of disruptions or incidents will automatically notify the NOC.*
- *At each functional element, a description of how the interface between the functional elements will be utilized.*
- *Demonstrate how the system will handle the use case presented and discuss the operation, including which partner(s) (Prime or Subcontractor) would be responsible for ingress, core, and egress.*
- *Identify the bandwidth available and options to manage and monitor bandwidth between functional elements and for the entire platform.*

Functional Element. The attached Call Scenarios - Use Case document (**Attachment 10**) describes each functional element in detail. The document presents ladder-style diagrams to improve clarity and readability.

Incident Alerts. Lumen performs continuous remote monitoring of both network and system performance to collect statistical data on alarms by type and severity. A comprehensive set of monitoring tools is used to observe the full end-to-end service environment, including network infrastructure, data communications, compute platforms, databases, remote facilities, and application layers. These tools track metrics such as IP path availability, packet throughput, packet loss, retransmissions, and additional performance indicators. When thresholds are exceeded or service reliability is at risk, automated alarms are generated for operations personnel. NOC staff oversee the interdependencies across monitored elements and notify the appropriate teams for analysis and resolution. This monitoring and alerting

framework enables immediate notification of system faults or performance degradation and is implemented for each functional element throughout the call flow.

Functional Element Interfaces. **Attachment 10** further explains how interfaces between individual functional elements are intended to operate and interact within the overall architecture.

Use-Case Partner. The Lumen ESInet service is a Lumen-provided solution delivered in partnership with its NGCS provider. The Lumen ESInet solution is deployed as a two-core, with an optional 3rd, in-state NGCS core.

Bandwidth Management. Lumen has designed and engineered the platform to accommodate the entire country. Currently, including the production deployment of NE, the platform is at (roughly) 10% of its maximum capacity. To support this capacity, the following bandwidth and redundancy capabilities are currently in place:

- Core network components are equipped with dual 1-Gbps network interface cards (NICs) connected to redundant Gigabit switches, with 10-Gbps inter-switch links for cross-connectivity.
- Aggregation site networking similarly uses dual 1-Gbps NICs connected to redundant Gigabit switches, also cross-connected using 10-Gbps links.
- Aggregation sites are provisioned with redundant configurations and operate at 20-40 Mbps over 100-Mbps Ethernet circuits or 40 Mbps over 45-Mbps DS-3 circuits.
- Each core location maintains multiple redundant and diverse 1-Gbps connections to Lumen's MPLS backbone network.

Lumen continuously monitors both network utilization and server resource consumption. The Lumen NOC actively reviews utilization metrics and initiates troubleshooting procedures whenever predefined thresholds are exceeded. In addition, Lumen maintains internal reporting that includes backbone network capacity, aggregation site capacity, PSAP network capacity, and server resource utilization. These reports are used for trend analysis and to proactively augment network or system capacity as required.

Describe the performance expectations of the system and explain how performance is guaranteed for legacy 911 across the entire system to egress to a legacy PSAP.

- *Identify how systems operate in a "normal" state.*
- *Identify how systems operate in an "abnormal" condition.*
- *Demonstrate how the platform will operate in a "fail" condition.*

Attachment 10 details both steady-state ("sunny day") operations and failure or exception conditions. Section 2.2 outlines scenarios in which a legacy Originating Service Provider (OSP), operating within the Lumen environment, delivers a call to a legacy PSAP, covering both normal processing and abnormal conditions. In addition, Section 4 of **Attachment 10** expands on failure scenarios by describing the loss of RTP, providing further insight into abnormal or degraded operating conditions.

Describe how security is implemented across the system while maintaining the performance guarantees expected to egress to a legacy PSAP.

- *Identify how DDoS and TDoS events are mitigated.*
- *Identify how security events are mitigated at each component throughout the system, including incidents that derive from the OSP, the PSAP and other ESInets.*

Ingress Solution

The ingress connectivity between Originating Service Providers (OSPs) and Lumen ingress facilities is designed to operate within engineered capacity during normal conditions, while deliberately maintaining sufficient headroom to accommodate unexpected traffic surges. This capacity margin allows the network to respond effectively to demand spikes caused by emergency events or malicious TDoS/DDoS activity without negatively impacting service availability.

Lumen provisions ingress facilities based on anticipated busy-hour demand and leverages Call Admission Control (CAC) to regulate the number of concurrent sessions per customer. These controls ensure that traffic levels remain balanced across the shared infrastructure, preventing any single OSP from monopolizing resources and enabling temporary traffic expansion when demand increases.

Additional protections are implemented through the explicit authorization of customer source IP addresses within the Border Control Function (BCF). Only trusted and approved IP sources are permitted, blocking unrecognized or unauthorized traffic from accessing the network. The combined use of IP allow-listing and CAC policies ensures that malicious traffic cannot exhaust available resources or cause denial-of-service conditions for other authorized users.

During an active attack, Lumen network operations personnel can dynamically adjust CAC parameters in real time to temporarily increase a customer's available capacity, helping to mitigate service disruption. Once the threat subsides, CAC settings are restored to their standard configuration.

If an attack escalates beyond an isolated customer or impacts multiple ingress paths, Lumen works collaboratively with the affected OSPs and/or VSPs to rapidly identify attack vectors and block malicious traffic upstream. This coordinated response helps contain the event and prevents the attack from propagating into the Lumen ESInet or downstream emergency services.

Lumen additionally mitigates TDoS by utilizing automated detection and mitigation capabilities within the ESInet environment that continuously evaluate call behavior, signaling patterns, and call metadata in real time. When a potential TDoS condition is identified, the system applies progressive mitigation actions to contain the threat before it can impact PSAP operations. These actions may include controlled call rejection, caller interrogation, and pre-PSAP inhibition, allowing legitimate emergency calls to continue processing while malicious or nuisance calls are suppressed.

A key component of Lumen's TDoS mitigation strategy is the use of SWEEP (Software Event Evaluation Process). SWEEP enhances threat detection by analyzing patterns across multiple calls and dynamically querying available call data to identify potential threat actors early in an attack. By rotating through evaluation, interrogation, and inhibition techniques based on observed behavior, SWEEP helps distinguish malicious traffic from valid emergency calls, even when attackers attempt to evade controls using distributed or rapidly changing identifiers. This graduated mitigation approach reduces the risk of false positives, shortens response times, and limits disruption to PSAP operations during sustained or evolving attack scenarios.

Together, these network-level and application-level controls provide Lumen with a comprehensive, automated framework for detecting, mitigating, and managing both DDoS and TDoS events. This approach enables rapid containment of threats while preserving the integrity, availability, and reliability of emergency communications services.

Egress Solution

Lumen mitigates TDoS and DDoS threats impacting PSAP call delivery through both administrative controls and automated detection mechanisms.

First, PSAPs are provided with the ability to manually manage known threat sources. Through the Lumen management portal or resolution processes, an authorized PSAP may add a Telephone Number (TN) to a TDoS/DDoS mitigation list. This action immediately prevents calls from that source from being delivered to the PSAP.

Second, Lumen employs an automated mitigation capability known as SWEEP (Software Event Evaluation Process). SWEEP continuously analyzes calling behavior and signaling characteristics to identify patterns consistent with TDoS or DDoS activity. When a threat pattern is detected, the system automatically adds the associated TN to the mitigation list without requiring manual intervention. Entries in the mitigation list are temporary and are automatically removed after a defined aging period to prevent unnecessary long-term blocking of legitimate callers.

When an incoming call originates from a TN on the mitigation list, the call is rejected prior to PSAP delivery using a standard SIP 580 (Banished) response, which translates to an SS7 “not in service” indication. Experience has shown that this response is effective in deterring continued calling activity from the attacking source, resulting in rapid cessation of the attack traffic.

Lumen continues to enhance its mitigation capabilities. Planned and ongoing improvements include caller interrogation functions that require interaction before calls are permitted to proceed, helping differentiate malicious calls from legitimate emergency traffic. Additional support for post-event investigation is also provided, including dispatch-level location queries and auxiliary data requests to obtain information such as the originating carrier or number ownership, supporting identification of threat actors.

In addition to these specific TDoS/DDoS controls, Lumen applies security policies across all functional elements within the solution. Continuous monitoring and threat analysis are supported through a centralized Security Information and Event Management (SIEM) platform, providing real-time visibility, correlation of security events, and alerting across the network and service environment. SIEM-generated alerts are actively monitored and, when warranted, initiate formal security incident response procedures to investigate and remediate potential threats.

Describe how 911 data is delivered to the logging and reporting system to be accessed by a PSAP.

- *a. Identify how databases operate.*
- *b. Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.*
- *c. Explain how logging is collected and accessed for legacy CDR and i3 logging.*

How Databases Operate. Within the Emergency Call Management Complex (ECMC), also referred to as the NG9-1-1 Core Services (NGCS) sites, Lumen implements a resilient database architecture designed for high availability and data integrity. Each database tier is supported by a primary Common Support System (CSS) provisioning database that continuously synchronizes updates to corresponding target databases in near real time. The ECMC databases are deployed as two-node Oracle RAC clusters, enabling redundant operation and seamless failover in the event of a node failure. Application continuity between the primary and alternate CSS environments is maintained through Oracle Transparent Application Failover (TAF), which automatically redirects application connections using Oracle Transparent Network Substrate (TNS) services to ensure uninterrupted operation and five-nines availability.

Recording Systems. The Lumen ESInet solution supports media recording capabilities and provides authorized users with access to recordings through the Lumen Customer Management Portal. These recordings are primarily intended to support troubleshooting, diagnostics, and service assurance activities. Lumen also collaborates with PSAPs to assess existing local recording capabilities. While PSAP call recording falls outside the direct scope of the ESInet service, Lumen leverages its operational experience to assist PSAPs in transitioning from analog recording solutions to digital RTP-based recording environments where required.

Logging Collection and Access. Lumen's i3 logging framework captures operational and transactional logs from each functional element within the NG9-1-1 environment. These logs are centrally aggregated and retained within the Common Support Services (CSS) sites, which operate outside of the active 9-1-1 call path. In addition to log storage, CSS sites support system monitoring, Spatial Interface services, and management portals used for configuration and operational oversight. Lumen provides enhanced call analytics and troubleshooting support through its reporting tools, which compile i3 logs for authorized user access. Call Detail Records (CDRs) are also maintained within the CSS environment and are accessible through the Lumen Customer Management Portal for reporting and review purposes.

Describe how calls may be transferred between NG PSAPs.

- *Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on the same NG911 system.*
- *Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on a different NG911 system.*
- *Describe how transfers are logged and how the data is logged.*
- *Discuss the data that is transferred to the receiving PSAP.*
- *Explain how logging is collected and accessed for legacy CDR and i3 logging*

NG PSAP to NG PSAP Transfer. In an i3-enabled PSAP environment, call transfers are initiated through a SIP REFER message issued by the PSAP's Call Handling Equipment (CHE), replacing the star-code mechanisms used in legacy systems. The REFER request includes the destination PSAP's URI within the Refer-To header. Upon receipt, the Lumen ESInet evaluates the SIP URI and determines that the destination PSAP is located on the same ESInet. Lumen then generates a new SIP INVITE toward the receiving PSAP to complete the transfer. This INVITE includes references to the Location Information Service (LIS) and Additional Data Repository (ADR), allowing the receiving PSAP to retrieve current location and supplemental data. An updated History-Info header is also included to clearly identify the call as a transfer

rather than a new 9-1-1 call origination. When supported by the receiving CHE, this header prevents call looping by discouraging a return transfer to the originating PSAP. Section 3.1 of the attached Call Flow Scenarios document provides a detailed description of the PSAP-to-PSAP transfer process.

NG PSAP to NG PSAP Transfer - Different NG911. When an NG9-1-1 PSAP transfers a call to a PSAP that resides on a different ESInet, the transfer is initiated using the same SIP REFER method from the PSAP CHE. In this case, the Lumen ESInet recognizes the destination SIP URI as belonging to an off-net PSAP. Based on configured interconnection policies, Lumen identifies the appropriate external ESInet and performs the call handoff accordingly. Lumen supports ESInet-to-ESInet call transfers through defined Network-to-Network Interface (NNI) capabilities and provides detailed specifications describing signaling, routing, and data exchange requirements for these scenarios. Refer to the previously provided Lumen NNI specification for implementation details.

Transfer Logging. All call transfers are recorded within the ESRP i3 logging framework and reflected in the associated Call Detail Records (CDRs). Transfer events can be identified within the Lumen Customer Management Portal by reviewing the CDRs, where transferred calls are indicated by the “Bridge Field” being set to true.

Data Transfer. Lumen supports multiple mechanisms for delivering call-associated data to PSAPs. For i3 calls, data exchange follows NENA i3 standards, with the receiving PSAP using LIS and ADR references to obtain location and supplemental data. The PSAP CHE authenticates to these services using digital certificates. Inter-ESInet transfers can present challenges depending on the capabilities of the receiving ESInet. To address this, Lumen supports alternative methods for PSAPs located on ESInets that do not fully support i3 data exchange, including techniques such as dual provisioning of location services and No Record Found steering. While these approaches are not preferred, they provide a means to ensure PSAPs can still receive necessary data during call transfers.

Logging Collection and Accessed for Legacy CDR and i3 Logging. i3 loggers collect operational logs from each functional element across the system. These logs are centrally aggregated and stored within Lumen’s Common Support Services (CSS) sites, which are outside the active 9-1-1 call path. In addition to log storage, CSS sites host Spatial Interface services, monitoring systems, and management portals used for configuration and operational oversight. Lumen provides reporting capabilities that compile i3 logs and present them to authorized users. Call Detail Records are also retained within the CSS environment and are accessible through the Lumen Customer Management Portal for reporting and analysis purposes.

5.10.2. Additional Examples

The following diagrams serve as an example of how a Respondent shall answer the use case questions. Diagrams may be necessary with step-by-step demonstration callouts to document the overall traffic flow for the system. Respondents are encouraged to use their own diagram(s) to illustrate the traffic flow from end to end.

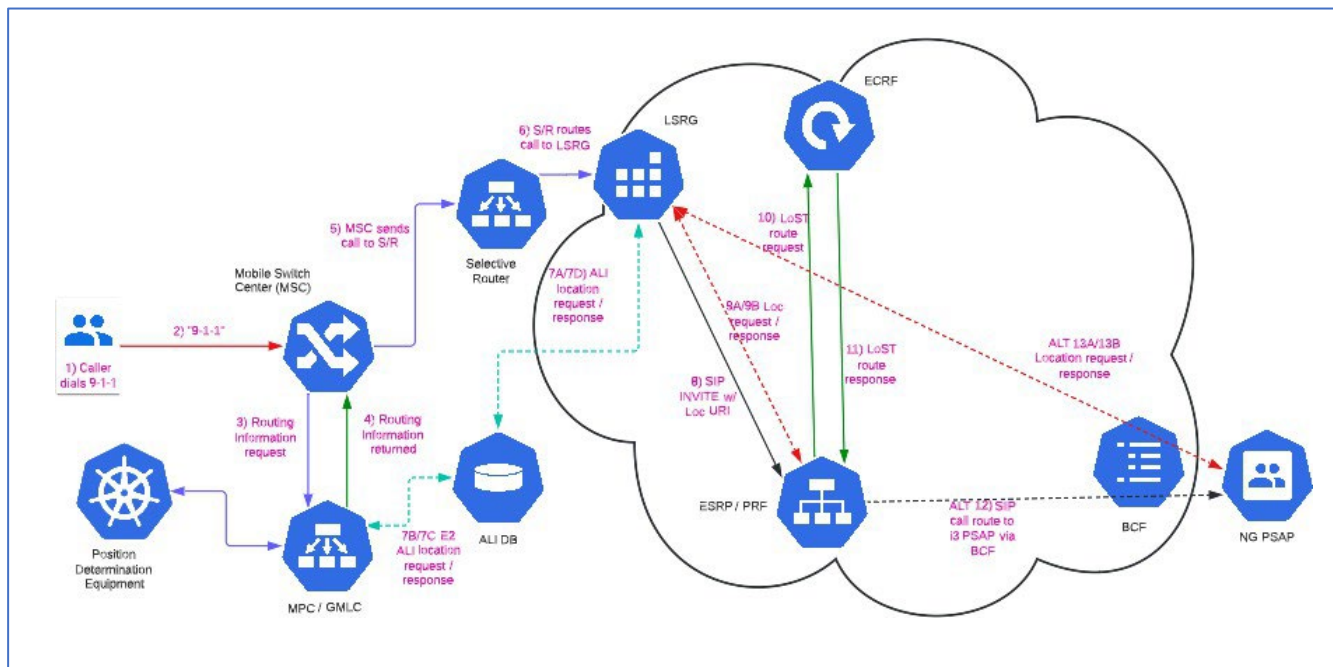


Figure 4: NENA Call Flow Scenario 1

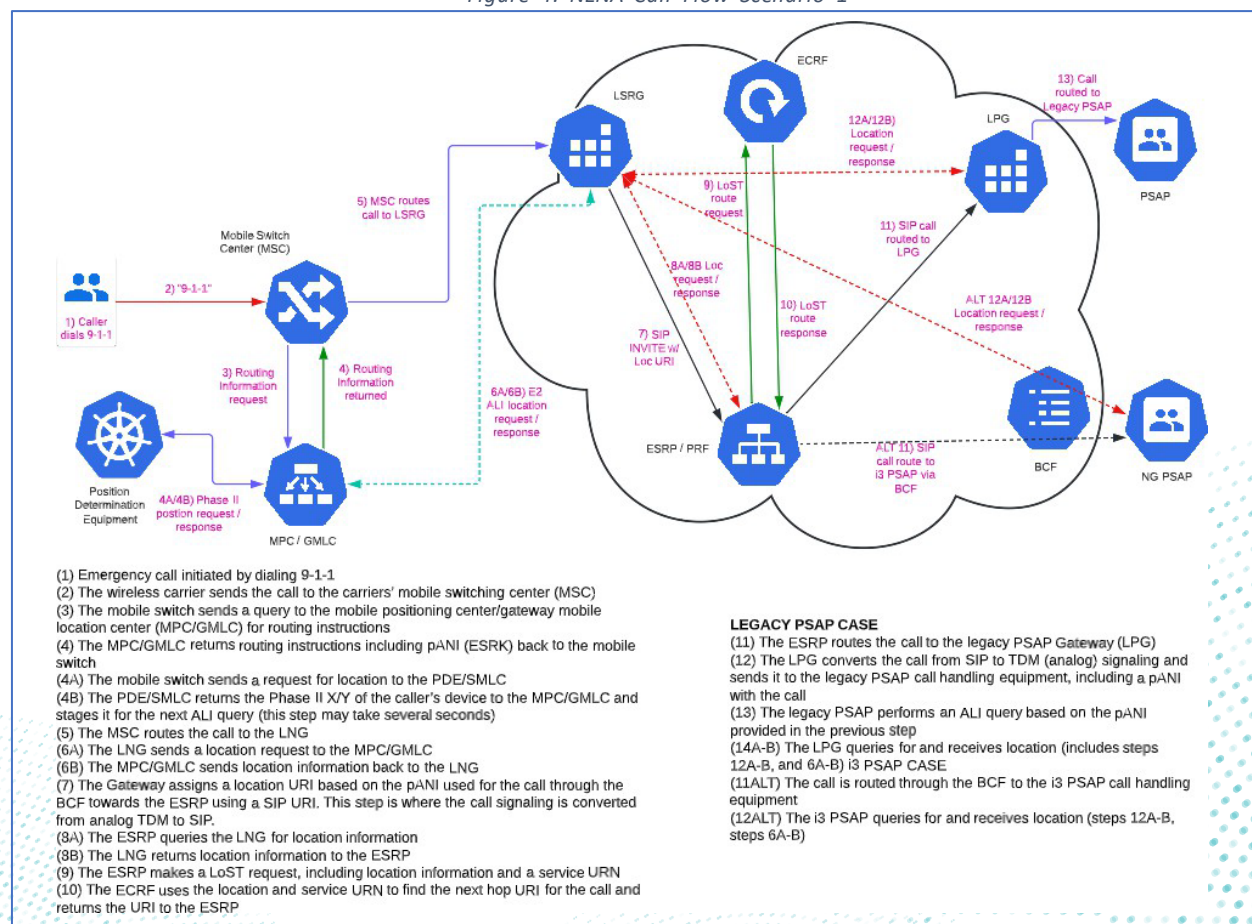


*Figure 5: NENA Call Flow Scenario 2***LUMEN RESPONSE:**

Lumen Response. Additional use case call flows and diagrams are found in the referenced Call Flow Scenarios – Use Case document provided as **Attachment 10**. Lumen understands that the State requires clear, end-to-end documentation of NG911 traffic flows to demonstrate how the proposed solution processes calls, signaling, media, and associated data across all functional elements. Lumen complies by providing detailed, respondent-developed diagrams that illustrate complete call flow behavior from origination through delivery, including step-by-step callouts that identify key processing points, decision logic, interfaces, and handoffs. These diagrams are purpose-built to demonstrate how the ESInet and NGCS operate together under normal, alternate, and exception conditions, and they align directly to the use case questions and scenarios defined by the State. Where appropriate, Lumen supplements diagrams with concise explanatory narrative to ensure that traffic flow, control paths, and system behavior are clear, traceable, and evaluator-friendly. This approach ensures the State has transparent, actionable insight into how the proposed solution functions in real-world operations and confirms full compliance with the requirement to document overall traffic flow using respondent-provided diagrams and step-by-step demonstrations.

6. COST PROPOSAL

Costs must be submitted as provided in the Cost Proposal (Appendix A). The Cost Proposal must include a complete response on all requested pricing information. Bidders may not take exception to any specific terms provided in the Cost Proposal.

The points awarded to a bidder will be determined by the following formula:

Points to Award = Lowest Bidder's Total Cost Submitted ÷ Bidder's Total Cost Submitted x Maximum Possible Points.

LUMEN RESPONSE:

Lumen has provided its Cost Proposal, which includes the completed Schedule 1 and Schedule 2 of the Cost template. Lumen has not taken any exception to specific terms in the Cost Proposal.

7. RESPONSE TO TERMS

Bidder should read the Terms provided with this RFP and must initial either "Accept All Terms and Conditions Within Section as Written" or "Exceptions Taken to Terms and Conditions Within Section as Written" in the table below (or include the same table in their solicitation response). If the bidder takes any exceptions, they must provide the following within the "Exceptions" field of the table; if an exception is not explicitly taken, it is deemed to be accepted as stated. The bidder may provide responses in separate attachment if multiple exceptions are taken. Exceptions must include:

1. The specific clause, including section reference, to which an exception has been taken;
2. An explanation of why the bidder took exception to the clause; and
3. Provide alternative language to the specific clause within the solicitation response.

Accept All Terms within Section as Written (initial)	Exceptions Taken to Terms Within Section as Written (Initial)	Exceptions: (Bidder must note the specific clause, including section reference, to which an exception has been taken, an explanation of why the bidder took exception to the clause, and provide alternative language to the specific clause within the solicitation response.)

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

LUMEN RESPONSE:

In accordance with Q&A # 15, 16 and 26, the State will present Terms and Conditions for a final contract between the parties post-award to Lumen. At that time Lumen will negotiate those Terms and Conditions in good faith in the context of an award. Lumen is confident that the parties will reach a definitive agreement in the context of an award. Lumen provides Service Schedules specific to the solution Lumen has proposed that it requests be attached to a final, negotiated contract between the parties. Those Schedules are in **Attachment 9** to this proposal.

8. CONTRACTUAL AGREEMENT FORM

The Contractual Agreement Form must be signed manually in ink, or by DocuSign or other electronic signature system, and returned by the opening date and time along with the bidder's solicitation. By signing the Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

CONTRACTUAL AGREEMENT FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

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 Vendors. This information is for statistical purposes only and will not be considered for contract award purposes.

 X NEBRASKA VENDOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Vendor. "Nebraska Vendor" 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. All vendors who are not a Nebraska Vendor are considered Foreign Vendors under Neb. Rev Stat § 73-603 (c).

 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. § 71-8511 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED MANUALLY IN INK OR BY DOCUSIGN

BIDDER:	CenturyLink Communications, LLC d/b/a Lumen Technologies Inc.
COMPLETE ADDRESS:	931 14th St., Denver, CO 80202
TELEPHONE NUMBER:	303-550-5653
FAX NUMBER:	
DATE:	April 14, 2026
SIGNATURE:	<i>Alex Khanin</i>
TYPED NAME & TITLE OF SIGNER:	Alexander Khanin, Manager, Offer Management