



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

RFP #202691101

Technical Proposal REDACTED

April 15, 2026

Submitted to:



David Sankey
State 911 Director
Nebraska Public Service Commission
1200 N Street, Suite 300
Lincoln, NE 68508
402.471.3101
dave.sankey@nebraska.gov

Prepared by:



Seth Wold
Sales Director
NextGen Communications, Inc. ("Allerium, a Comtech segment")
2401 Elliott Avenue, Suite 100
Seattle, WA 98121-3311
435.231.3292
seth.wold@comtech.com

Notices

NextGen Communications, Inc. is a wholly owned subsidiary of TeleCommunication Systems, Inc. TeleCommunication Systems, Inc. is a wholly owned subsidiary of Comtech Telecommunications Corp. This proposal is being submitted by NextGen Communications, Inc. (using the Allerium brand). Throughout this proposal, the brand Allerium may be referenced. However, NextGen Communications, Inc. is the contracting entity for the delivery of our highly available Wireless E9-1-1, VoIP E9-1-1, VoWiFi E9-1-1 and NG9-1-1 i3 solutions and systems, and it is expected to be the contracting entity for the proposed system.

EMedia®, GEM9-1-1®, LivewirE9-1-1®, RAVE9-1-1®, SPATIAL MSAG®, and VoLTE9-1-1® are registered trademarks, and LocatE9-1-1™ is a trademark of TeleCommunication Systems, Inc. in the U.S. and certain other countries.

All other brand names and product names used in this document are trademarks, registered trademarks, or service marks of their respective holders.

Nasdaq GS: CMTL

Table of Contents

Executive Summary.....	1
1. Corporate Overview	8
1.1. Bidder Identification and Information [Proposal Instructions, Section A.1.a].....	8
1.2. Financial Statements [Proposal Instructions, Section A.1.b]	14
1.3. Change of Ownership [Proposal Instructions, Section A.1.c]	15
1.4. Office Location [Proposal Instructions, Section A.1.d]	15
1.5. Relationships with the State [Proposal Instructions, Section A.1.e]	16
1.6. Bidder's Employee Relations to State [Proposal Instructions, Section A.1.f]	16
1.7. Contract Performance [Proposal Instructions, Section A.1.g].....	16
1.8. Summary of Bidder's Corporate Experience [Proposal Instructions, Section A.1.h] ..	17
1.9. Summary of Bidder's Proposed Personnel/Management Approach [Proposal Instructions, Section A.1.i]	28
1.10. Subcontractors [Proposal Instructions, Section A.1.j]	50
2. Factors Used to Evaluate Corporate Overview [Proposal Instructions, Section A.2]	56
3. Response to Scope of Work [Proposal Instructions, Section A.3 / Project Requirements and Scope of Work, Section B]	57
3.1. Services to be Provided [Project Requirements and Scope of Work, Section B].....	57
3.1.1. ESInet Architecture and Design	57
3.1.2. NG911 Core Services (NGCS).....	62
3.1.3. GIS and Location-Based Routing	62
3.1.4. Call Flow and Media Session Handling.....	63
3.1.5. Security, Privacy, and Trust.....	64
3.1.6. Logging, Reporting, and Call Detail Records	66
3.1.7. Interoperability, Testing, Conformance, and System Acceptance.....	67
3.1.8. Operational Support and Service Level Agreements (SLAs).....	69
3.2. Applicable Standards	71
3.2.1. Federal Communications Commission Rules	73
3.2.2. Other Industry Standards	73
3.3. Conformance to Standards.....	75
3.3.1. Baseline Conformance	75
3.3.2. Gap Identification (Proposal Requirement)	76
3.3.3. Standards Updates (Post-Award).....	77

3.3.4.	Non-Disclosure and Breach	78
3.3.5.	Deviation Classification (Proposal Requirement).....	79
3.3.6.	Remediation Plan and Progress	80
3.3.7.	Interoperability	82
3.4.	NENA NG911 i3 Standard Conformance	84
4.	Response to Work Plan and Project Planning [Proposal Instructions, Section A.4 / Project Requirements and Scope of Work, Section C]]	97
4.1.	Project Management [Project Requirements and Scope of Work, Section C.1]	97
4.1.1.	Project Management Approach	97
4.1.2.	Project Manager.....	98
4.1.3.	Preliminary Plan (Project Management Plan [PMP])	99
4.2.	Staffing and Qualifications [Project Requirements and Scope of Work, Section C.2]	100
4.2.1.	Key Personnel.....	100
4.2.2.	Staff Qualifications	119
4.2.3.	Designations, Certifications, and Licenses.....	120
4.3.	Implementation [Project Requirements and Scope of Work, Section C.3]	120
4.3.1.	Implementation Approach.....	120
4.3.2.	Elements of Implementation	121
4.4.	Transition [Project Requirements and Scope of Work, Section C.4]	123
4.4.1.	Transition Plan: Current and Future	123
4.5.	Testing and Acceptance [Project Requirements and Scope of Work, Section C.3]..	130
4.5.1.	Testing (Comprehensive Test Plan).....	130
4.5.2.	Test Plan Methodology.....	131
4.5.3.	System Acceptance Testing	132
4.5.4.	Independent Validation and Verification (IV&V)	133
5.	Response to Technical Requirements [Proposal Instructions, Section A.5]	135
5.1.	ESInet Requirements [Project Requirements and Scope of Work, Section E.1]	135
5.1.1.	Architecture and Topology.....	154
5.1.2.	External and PSAP Connectivity.....	159
5.1.3.	Legacy Interoperability.....	163
5.1.4.	Network Behavior and Performance	172
5.1.5.	Resilience and Service Levels.....	184

5.1.6.	Operations and Management	191
5.1.7.	Implementation Details.....	197
5.2.	Next Generation Core Services (NGCS) Requirements [Project Requirements and Scope of Work, Section E.2].....	198
5.2.1.	Edge Security and Ingress.....	202
5.2.2.	Core Routing and Location	208
5.2.3.	Data and Enrichment	223
5.2.4.	Call Flow and Media Handling	224
5.2.5.	Egress and External Interfaces.....	232
5.3.	GIS and Database Services Requirements [Project Requirements and Scope of Work, Section E.3].....	233
5.3.1.	Data Management and Interfaces.....	234
5.3.2.	Core Data Services	241
5.3.3.	PSAP-Facing Services	244
5.3.4.	External Integrations	246
5.4.	Security Requirements [Project Requirements and Scope of Work, Section E.4]....	247
5.4.1.	Management and Process Control.....	247
5.4.2.	Information System Infrastructure and Management.....	260
5.4.3.	Authentication and Federated SSO.....	270
5.4.4.	Cryptography and Public Key Infrastructure	271
5.4.5.	Integrity Protection.....	273
5.4.6.	Information Privacy.....	274
5.4.7.	Security Assessment and Audit	275
5.4.8.	Security Monitoring, Detection, and Alerting.....	276
5.4.9.	Domain Name System (DNS).....	280
5.5.	Reporting Services Requirements [Project Requirements and Scope of Work, Section E.5] 281	
5.5.1.	Reporting and Data Collection Requirements.....	283
5.5.2.	Logging Service.....	284
5.5.3.	i3 Logging and Reporting Requirements	285
5.5.4.	Functional Element Reporting	285
5.5.5.	Monitoring, Outages, Failover, Trouble Tickets, and Escalation	288
5.5.6.	Maintenance and Configuration Reports.....	291
5.5.7.	Discrepancy Reporting.....	294

5.6. Installation Requirements [Project Requirements and Scope of Work, Section E.6]	317
5.6.1. Installation Services.....	317
5.6.2. Wiring and Cabling.....	321
5.6.3. Grounding	322
5.7. Training [Project Requirements and Scope of Work, Section E.7]	322
5.7.1. Audiences and Scope	323
5.7.2. Training Elements	324
5.7.3. Technical Assistance	325
5.7.4. Schedule and Locations.....	325
5.7.5. Training Materials.....	326
5.7.6. Post-Deployment Training and Costs (Proposal Requirement)	326
5.7.7. Comprehension, Testing, and Certification	327
5.7.8. Training Plan and Samples (Proposal Requirement)	328
5.8. Operations and Service Management Requirements [Project Requirements and Scope of Work, Section E.8].....	328
5.8.1. Service Management Framework.....	331
5.8.2. Continuity and Resilience.....	346
5.8.3. Operations Centers and Support	350
5.8.4. Monitoring and Event Management.....	369
5.8.5. Change, Maintenance, and Release Management.....	370
5.8.6. Spares and Inventory	384
5.9. Value Add and Optional Services [Project Requirements and Scope of Work, Section E.9]	387
5.9.1. Call Handling Equipment (CHE) Services	387
5.9.2. ESInet and NGCS Backup System.....	398
5.10. Use Case Examples for Use with Response [Project Requirements and Scope of Work, Section E.10]	400
5.10.1. Instructions	400
5.10.2. Additional Examples	411
6. Cost Proposal [Proposal Instructions, Section A.6]	413
7. Terms [Proposal Instructions, Section A.7]	414
8. Contractual Agreement Form [Proposal Instructions, Section A.8]	419

List of Figures and Tables

Table 1. Bidder Information	8
Figure 7. ISO/TL Certifications	10
Figure 8. Frost & Sullivan Awards	12

Table 6. Key Personnel Roster	32
Table 7. Key Personnel Resume: Aaron Demorow	33
Table 8. Key Personnel Resume: Ally Oughton	34
Table 9. Key Personnel Resume: Chris Hedges	35
Table 10. Key Personnel Resume: Dave Wiegel	36
Table 11. Key Personnel Resume: Elizabeth McMahon, PMP	37
Table 12. Key Personnel Resume: Eric Guerrero	38
Table 13. Key Personnel Resume: Greg Lathrop, PMP	39
Table 14. Key Personnel Resume: Jenn Richmond	40

Table 15. Key Personnel Resume: Kenneth Banville	41
Table 16. Key Personnel Resume: Matt Davis.....	42
Table 17. Key Personnel Resume: Matthew Mullins.....	43
Table 18. Key Personnel Resume: Melissa Liebert, ENP, PMP	44
Table 19. Key Personnel Resume: Mike Wolfe.....	45
Table 20. Key Personnel Resume: Neil Nyquist	46
Table 21. Key Personnel Resume: Patrick Hoover	47
Table 22. Key Personnel Resume: Patrick Melancon	48
Table 23. Key Personnel Resume: Seth Wold	49
Table 24. Subcontractor Inputs	51
Figure 9. Surviving Isolation of a Physical Site	59
Figure 10. Failure of a Single Element or Connection.....	61

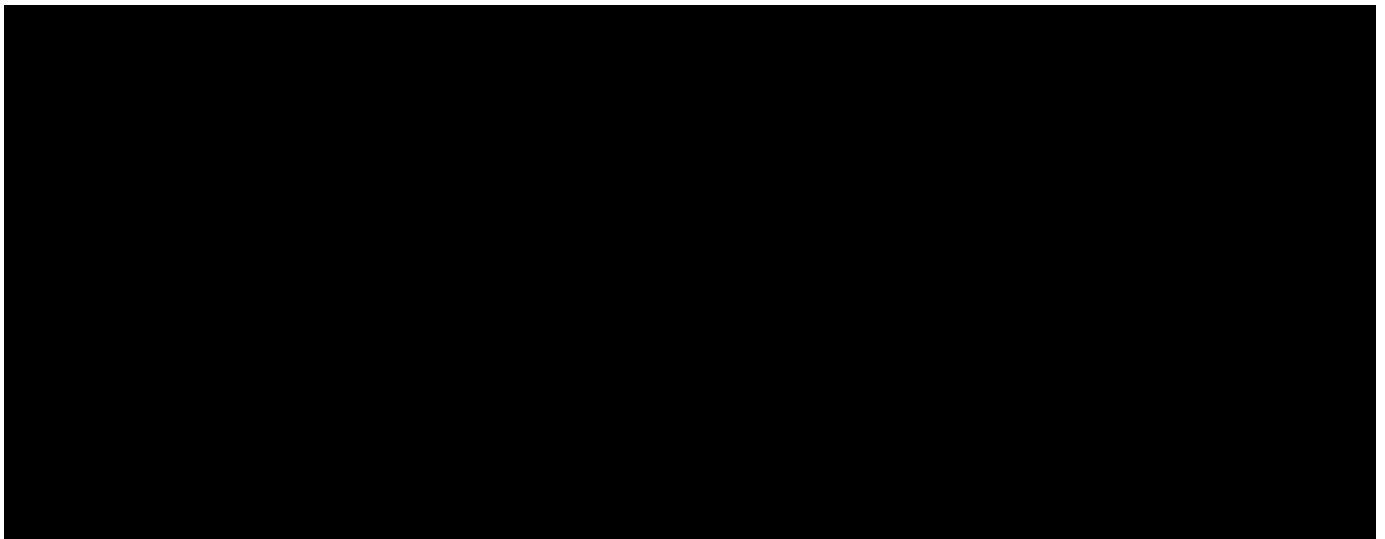


Figure 11. Overview of Allerium’s Standard Staffing Plan.....	99
Table 32. Key Personnel Roster	101
Table 7. Key Personnel Resume: Aaron Demorow	102
Table 8. Key Personnel Resume: Ally Oughton	103
Table 9. Key Personnel Resume: Chris Hedges	104
Table 10. Key Personnel Resume: Dave Wiegel.....	105
Table 11. Key Personnel Resume: Elizabeth McMahon, PMP.....	106
Table 12. Key Personnel Resume: Eric Guerrero	107
Table 13. Key Personnel Resume: Greg Lathrop, PMP.....	108
Table 14. Key Personnel Resume: Jenn Richmond.....	109

Table 15. Key Personnel Resume: Kenneth Banville	110
Table 16. Key Personnel Resume: Matt Davis.....	111
Table 17. Key Personnel Resume: Matthew Mullins.....	112
Table 18. Key Personnel Resume: Melissa Liebert, ENP, PMP	113
Table 19. Key Personnel Resume: Mike Wolfe.....	114
Table 20. Key Personnel Resume: Neil Nyquist	115
Table 21. Key Personnel Resume: Patrick Hoover	116
Table 22. Key Personnel Resume: Patrick Melancon	117
Table 23. Key Personnel Resume: Seth Wold	118
Figure 12. Overview of Allerium's Five Phased Migration Approach	121

Table 31. Critical Path Activities	122

Figure 15. National System Design View.....	137
Table 32. Levels of Assistance	138
Figure 16. All Active NOC/SOC Alerts Dashboard.....	140
Figure 17. Node Summary of an Active Alert	141
Figure 18. Major Backbone Network Connectivity Circuit Map	141
Figure 19. National System Design View.....	146
Figure 20. Failure of a Single Element or Connection	147

Table 33. Demonstrative PSAP-1 RTR-001 Route Table	149
Table 34. QoS Markings.....	152
Figure 22. National System Design View.....	157
Table 35. Bandwidth Details	163

Table 37. Levels of Assistance	185

Figure 25. Electrical Grid Interconnects	189
Figure 26. All Active NOC/SOC Alerts Dashboard	194
Figure 27. Node Summary of an Active Alert	194
Figure 28. Major Backbone Network Connectivity Circuit Map	195
Figure 29. Border Control Function	203
Table 57. Call Treatment of Malformed Messages	204
Figure 30. PRF Home Page.....	212
Figure 31. PRF PSAP Shutdown Page	213
Figure 32. PRF Time of Day Page	213
Table 39. QoS Markings.....	227

Table 41. Strategic Capability Mapping	266
Figure 33. High-Level Incident Response and Notification Flow	293
Figure 34. Automated PSAP Network Events Incident Detection & Notification Flow	294
Figure 35. Auto Generated Discrepancy Report	296
Figure 36. Manually Generated Discrepancy Report.....	296
Figure 37. SpatialMSAG® Change Request	297
Figure 38. SpatialMSAG Change Request (Denied)	297
Figure 39. Auto Generated Discrepancy Report	301
Figure 40. Manually Generated Discrepancy Report.....	302
Figure 41. SpatialMSAG® Change Request	302
Figure 42. SpatialMSAG Change Request (Denied)	303
Figure 43. All Active NOC/SOC Alerts Dashboard.....	306
Figure 44. Node Summary of an Active Alert	307
Figure 45. Major Backbone Network Connectivity Circuit Map	307
Figure 46. Auto Generated Discrepancy Report	311
Figure 47. Manually Generated Discrepancy Report.....	311
Figure 48. SpatialMSAG® Change Request	312
Figure 49. SpatialMSAG Change Request (Denied)	312
Figure 50. Auto Generated Discrepancy Report	314
Figure 51. Manually Generated Discrepancy Report.....	315
Figure 52. SpatialMSAG® Change Request	315

Figure 53. SpatialMSAG Change Request (Denied)	316
Table 42. Levels of Assistance	337
Table 43. Mapped Severity Levels and Assistance.....	337
Table 44. SIL Levels	339
Figure 54. Progress against Open Tickets (via our Web Based Trouble Ticket Viewer [TTV]) ..	345
Figure 55. Planned Maintenance Activities	345
Figure 56. Service Performance/Compliance Levels	346
Figure 57. RCA/RFO Status and Corrective Actions	346
Figure 58. National System Design View.....	351
Figure 59. All Active NOC/SOC Alerts Dashboard.....	352
Figure 60. Node Summary of an Active Alert	353
Figure 61. Major Backbone Network Connectivity Circuit Map	353
Figure 62. High-Level Incident Response and Notification Flow	360
Figure 63. Automated PSAP Network Events Incident Detection & Notification Flow	361
Table 45. Incident Escalation Matrix	362
Figure 64. All Active NOC/SOC Alerts Dashboard.....	363
Figure 65. Node Summary of an Active Alert	363
Figure 66. Major Backbone Network Connectivity Circuit Map	364
Figure 67. Typical Hosted Guardian NG9-1-1 Solution (Single Location)	390
Figure 68. Standalone Guardian NG9-1-1 System.....	391
Figure 69. Typical Geo-Diverse Guardian NG9-1-1 System	392
Figure 70. Typical Hosted Guardian NG9-1-1 Solution (Geo-Diverse)	393
Figure 71. Typical Graphical User Interface Layouts (Sheet 1 of 2)	395
Figure 72. Typical Graphical User Interface Layouts (Sheet 2 of 2)	395
Figure 73. Map Display with Main Menu Opened	396
Figure 74. Sample Guardian Survivability Controller Design	399
Figure 75. High-Level Future Architecture	402

Figure 78. Terms Table (Page 1 of 3).....	415
Figure 79. Terms Table (Page 2 of 3).....	416

Figure 80. Terms Table (Page 3 of 3).....	417
Figure 81. Contractual Agreement Form.....	420

Executive Summary

Allerium's executive summary is included below and **ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION**.

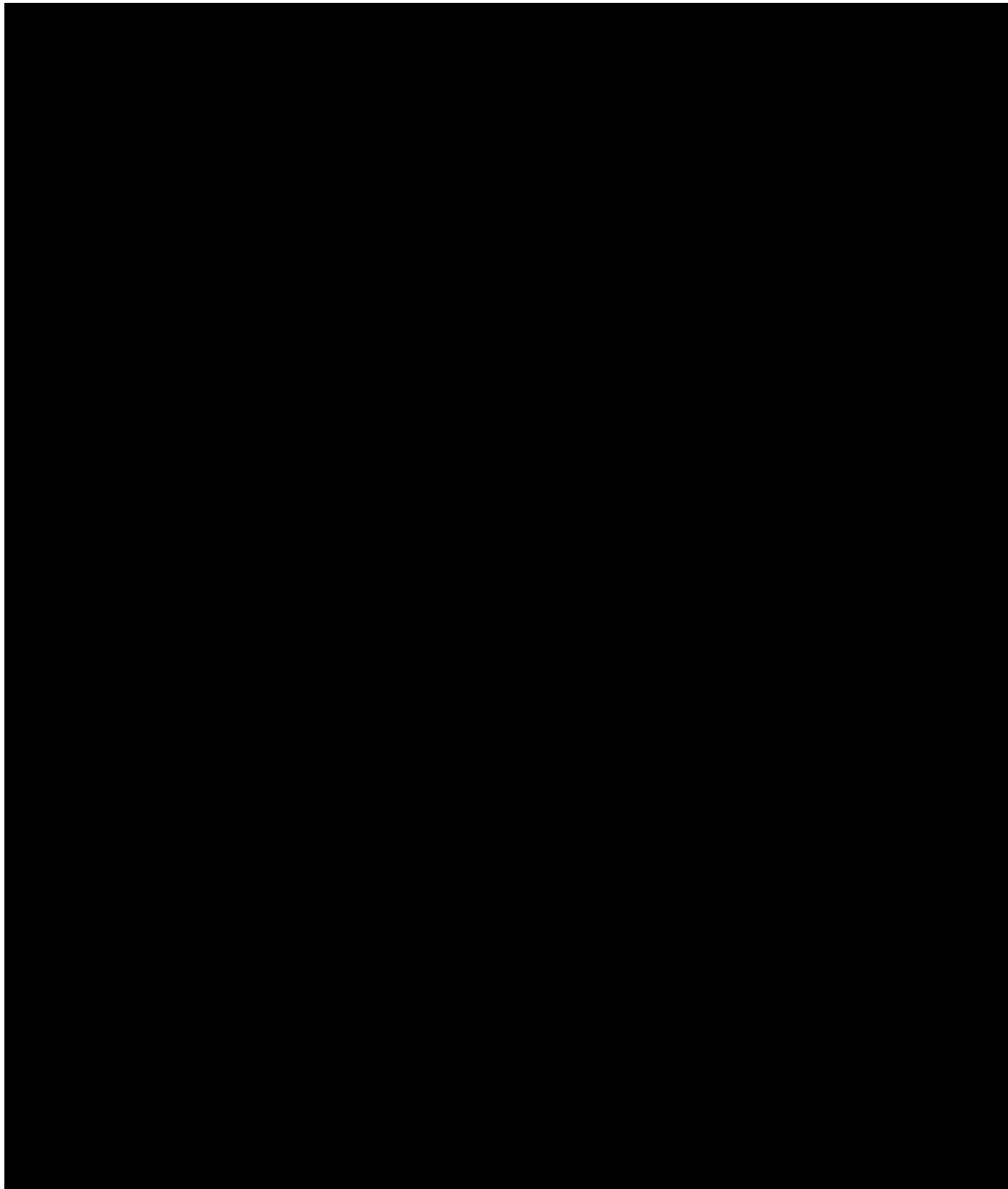


Figure 1. Executive Summary (Page 1 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

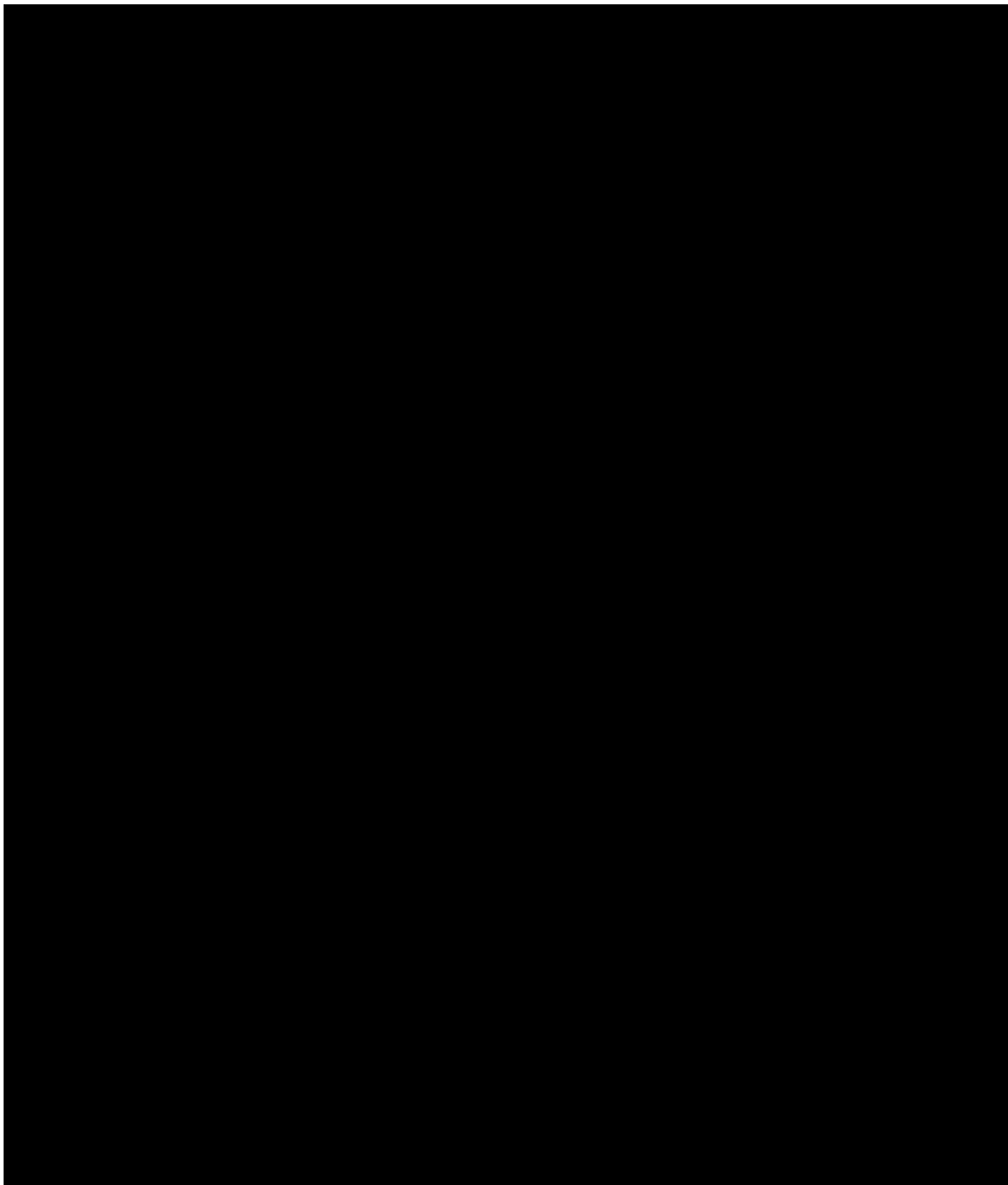


Figure 2. Executive Summary (Page 2 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

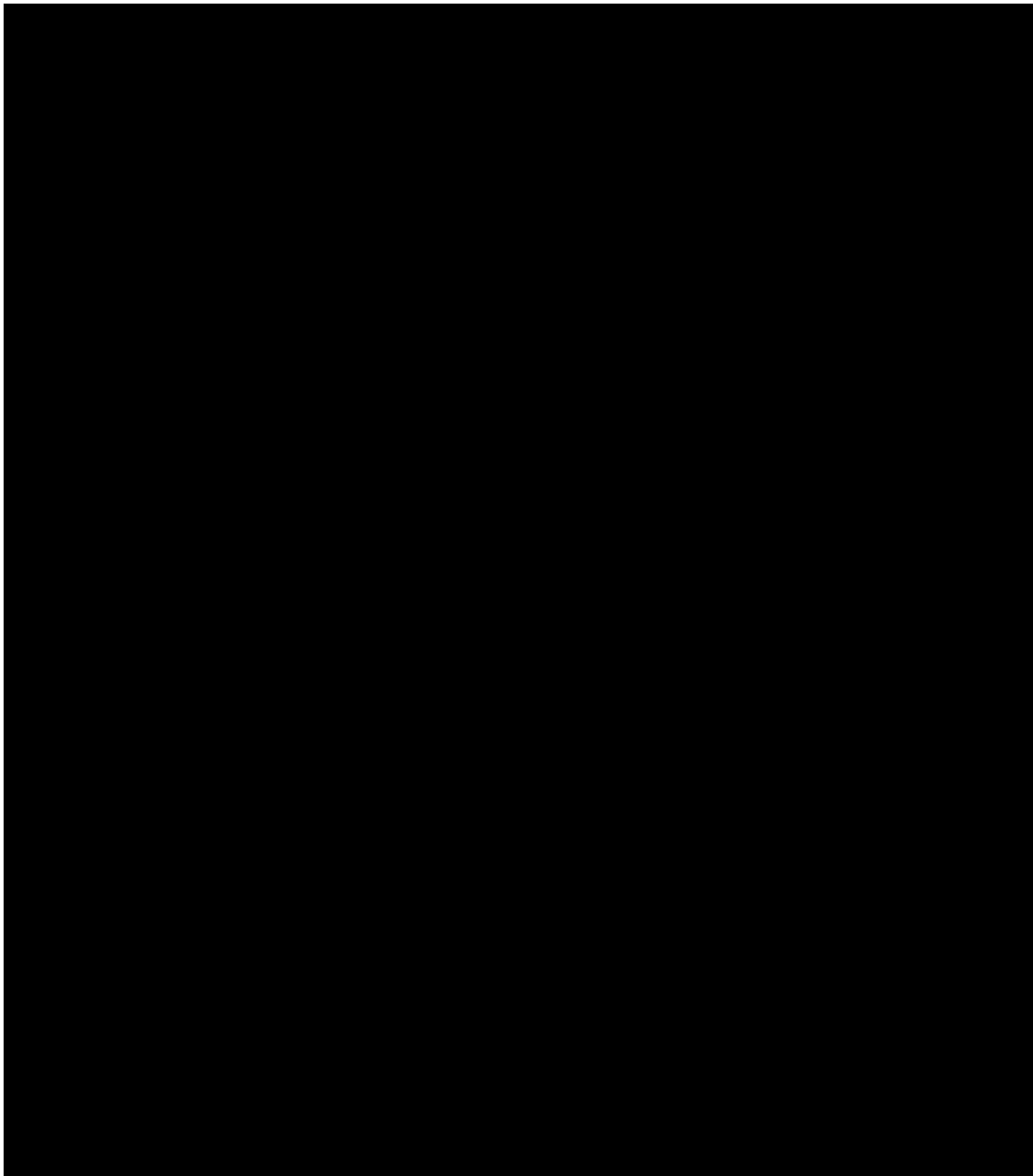


Figure 3. Executive Summary (Page 3 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

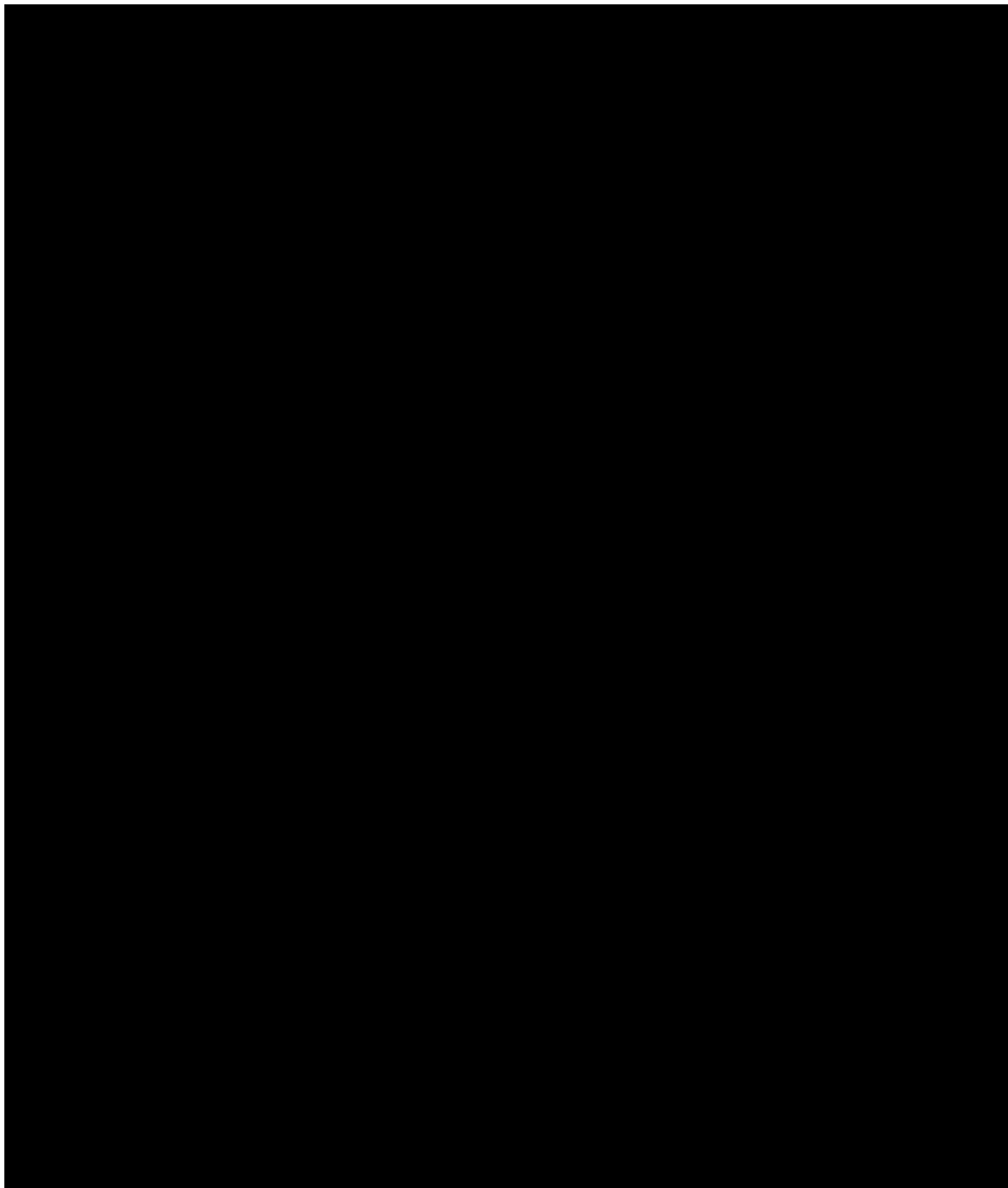


Figure 4. Executive Summary (Page 4 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

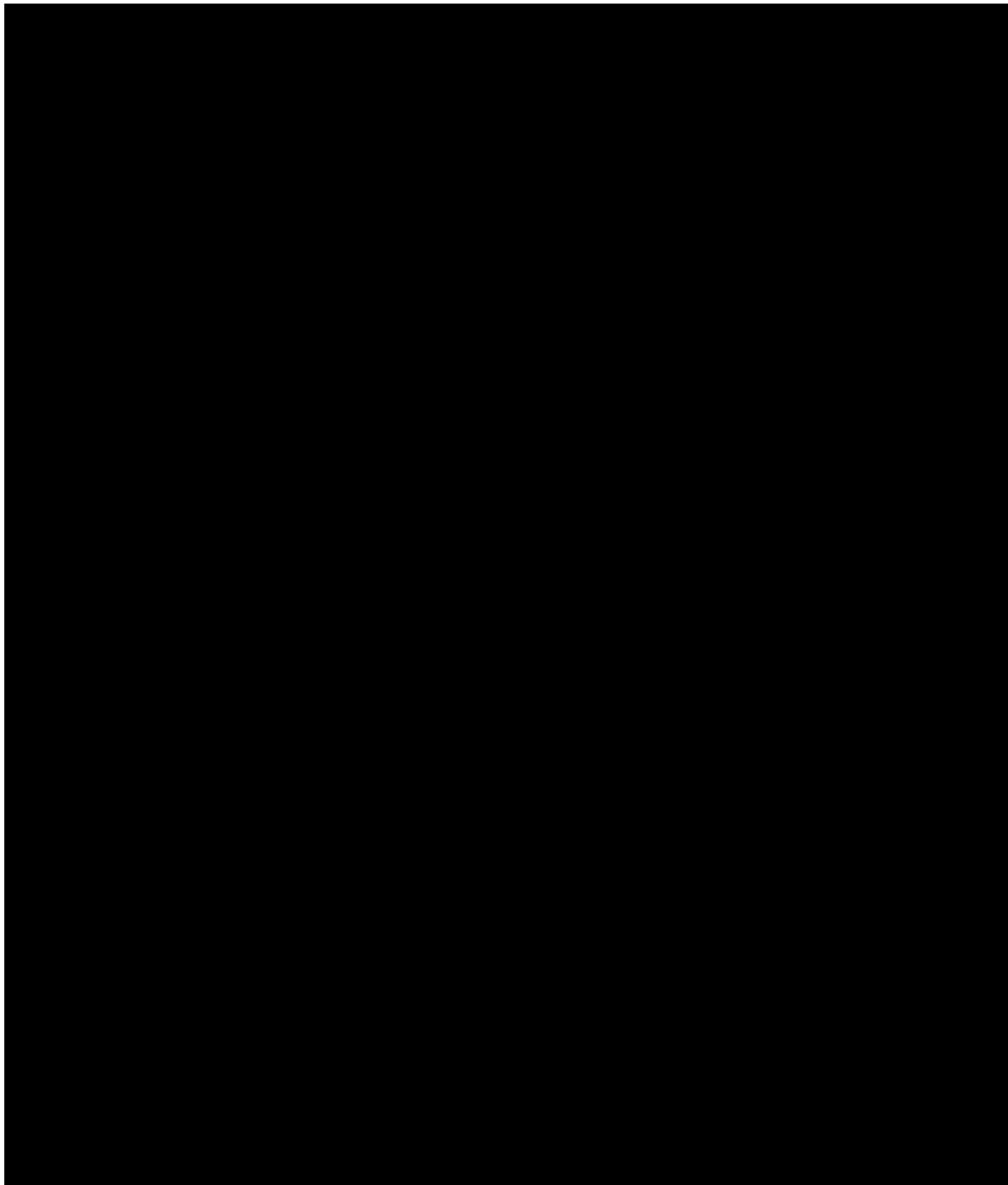


Figure 5. Executive Summary (Page 5 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

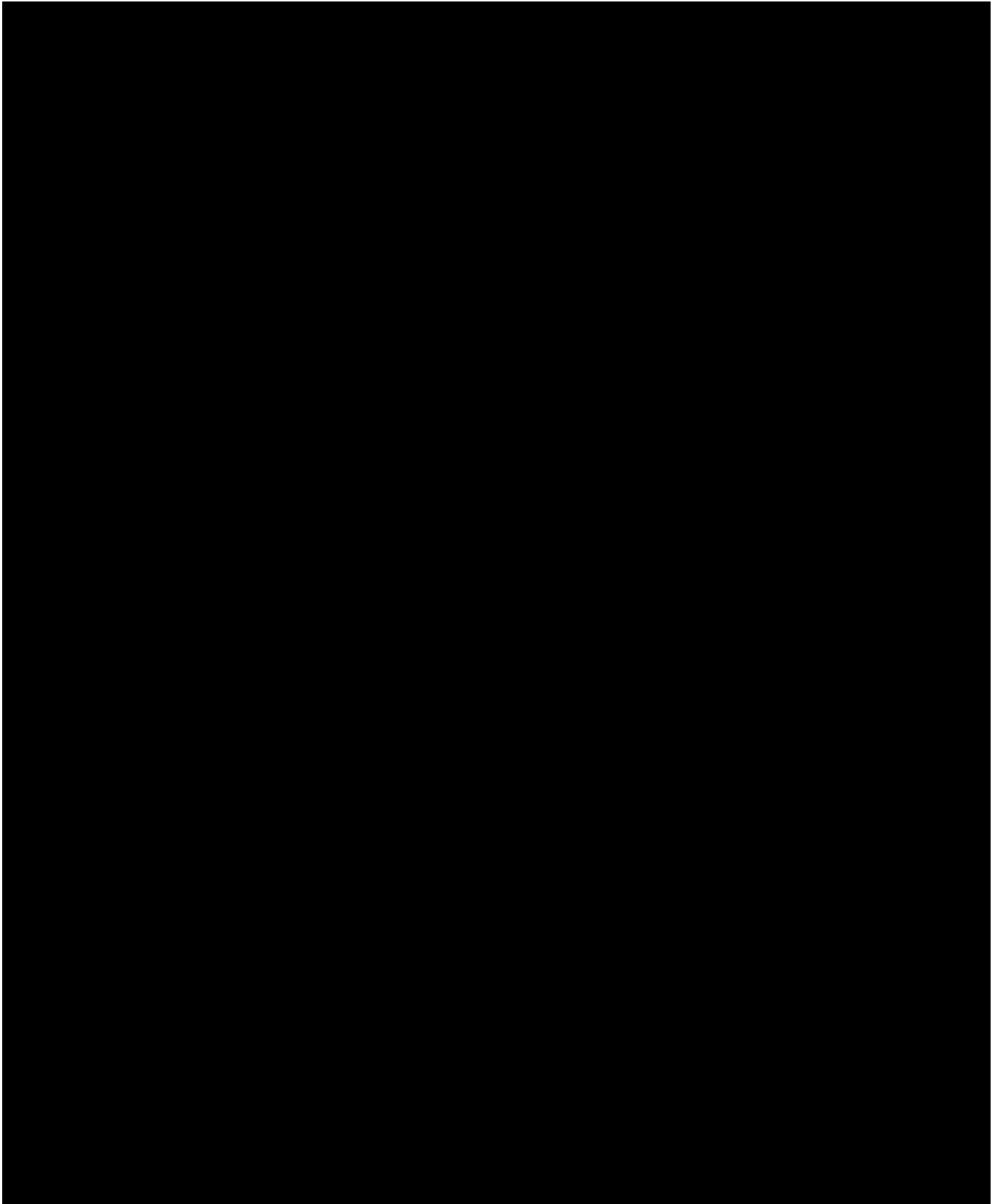


Figure 6. Executive Summary (Page 6 of 6) (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

1. Corporate Overview

Proposal Instructions

[...]

A. SOLICITATION RESPONSE SUBMISSION

1. CORPORATE OVERVIEW

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

1.1. Bidder Identification and Information [Proposal Instructions, Section A.1.a]

a. BIDDER IDENTIFICATION AND INFORMATION

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

Response:

Bidder Identification

This proposal is being submitted by NextGen Communications, Inc. (using the Allerium brand). NextGen Communications, Inc. is a wholly owned subsidiary of TeleCommunication Systems, Inc. and a registered CLEC in the State of Nebraska. TeleCommunication Systems, Inc. is a wholly owned subsidiary of Comtech Telecommunications Corp. Throughout this proposal, the brand Allerium may be referenced. However, NextGen Communications, Inc. is the contracting entity for the delivery of our highly available NG9-1-1 services described herein.

Table 1. Bidder Information

Requirement	Input
Full company or corporate name	NextGen Communications, Inc.
Nebraska SOS Account Number	10127497
Address of the company's headquarters	2401 Elliott Avenue, Suite 100, Seattle, WA 98121
Entity organization (corporation, partnership, proprietorship)	Corporation
State in which the bidder is incorporated or otherwise organized to do business	Incorporated in the State of Maryland
Year in which the bidder first organized to do business	Incorporated on October 27, 2008
Whether the name and form of organization has changed since first organized	No

Bidder Information: About Allerium

Built for What Matters Most

Allerium, a Comtech segment, is a trusted leader in mission-critical connections, backed by over 40 years of proven performance in public safety. We design technologies that connect calls, teams, and communities, quietly powering the moments where response starts.

From PSAPs to statewide networks, our solutions help agencies respond faster, route smarter, and adapt to the demands of modern emergency communication. Whether it's voice, text, video, or data, we help public safety teams stay focused and in control when every second counts.

Our platforms include intuitive tools like Guardian and Mira, anchored by a public safety-grade ESInet built to meet the demands of regional and statewide communities. Behind it all is a resilient, security-first foundation designed for uptime, scalability, and full NG9-1-1 readiness. From call handling to core systems, we give agencies the confidence to respond and evolve.

Allerium is the second-largest NGCS provider in North America and a leading operator of public safety-grade ESInets. Our networks support voice, text to 9-1-1, video, and data, delivering the flexibility PSAPs need as communication channels evolve. With dynamic location routing using enhanced geospatial data, we help agencies reach people faster, even in rural or complex environments. With security threats growing, our services are backed by a comprehensive cybersecurity program.

Our public safety and carrier capabilities include but are not limited to:

- **ESInet/NGCS Solutions:** Providing emergency call routing, location validation, policy-based routing rules, logging and security functionality, and network transport infrastructure for emergency services communications and support.
- **Short Message Service (SMS) Text to 9-1-1 Services:** Providing alternate paths for individuals who need to request assistance (via text messaging) as a method to reach PSAPs. Allerium is one of two nationwide TCC providers processing over 800,000 text sessions annually and delivering Text to 9-1-1 to more than 4,400 PSAPs, with additional PSAPs being deployed monthly.
- **Call Handling Equipment (CHE):** Providing a flexible multimedia emergency call management platform as well as heavily involved in testing other manufacturers' systems for interoperability compliance.
- **988 Solutions:** Connectivity and interworking between 988 agencies and other agencies in the public safety and behavioral health crisis continuum.
- **Situational Awareness:** Developing and evolving additional reporting.

Allerium's nationwide 9-1-1 experience, deployments, and knowledge are unparalleled. Unlike other vendors, we support 9-1-1 end-to-end: from the incident and user's device through the carrier's networks across an Emergency Services Internet Protocol (IP) network (ESInet) to the public safety answering point (PSAP). Collectively, Allerium is responsible for delivering hundreds of thousands of 9-1-1 calls per day for our clients.

A Rich Public Safety History

While the Allerium brand is relatively new to public safety, its core technologies and solutions portfolio have come through the acquisitions of highly regarded companies, each having decades of experience in emergency communications, including:

- **TeleCommunication Systems, Inc.:** A world leader in innovative, highly reliable, secure wireless communication technologies, software applications, and related services for carriers, defense and public safety government agencies, and enterprises founded in 1987.
- **Solacom Technologies, Inc.:** An NG9-1-1 call-handling solution and regional NG9-1-1 system provider (a call handling business originally founded in 1982 as CML Technologies).
- General Dynamics Information Technology (GDIT)'s state and local government NG9-1-1 business unit
- **microDATA GIS, Inc.:** An NG9-1-1 software and solutions provider founded in 1983.
- **XYPOINT Corporation:** A pioneer in wireless location-based service (LBS) and mobile positioning center (MPC) technology founded in 1993.

Dedicated Public Safety Personnel and Resources

Our highly dedicated and skilled public safety organization includes more than 450 experts, a seasoned team that supports the largest wireless and VoIP providers in the United States as well as provides cities, counties, states, and federal agencies with a variety of 9-1-1 services. The focus of Allerium's public safety division is 9-1-1. Our services are end-to-end and complementary, which allows us to work with carriers plus state and local governments to deliver 9-1-1 calls nationwide.

NOC/SOC Team

Allerium provides system monitoring, maintenance, incident management, and reporting services from our NG9-1-1 operations organization. This organization includes a NOC/SOC team with 24x7x365 public safety dedicated resources strategically dispersed across all U.S. time zones and working out of a centralized communications hub.

The Allerium NOC/SOC is unique because it is an in-house resource solely focused on 9-1-1 and staffed 24x7x365 by Allerium employees specifically trained on 9-1-1 services and applications. Many other organizations within the NG9-1-1 space use multipurpose personnel and facilities to "include" 9-1-1 or contract with generic, third-party help desk solutions providers.

ISO/TL Certifications

Allerium is committed to providing the highest quality products and services possible by meeting our clients' requirements and continually improving our business processes. Allerium is International Organization for Standardization (ISO) 9001/TL 9000 and ISO 27001 certified.



Figure 7. ISO/TL Certifications

We maintain an ISO 9001/TL 9000 certified NOC, requiring that our processes be well documented and audited, so that our customers can rely on a consistent level of service when they have an issue. Allerium offers the only TL 9000-certified non-carrier NOC for wireless and VoIP E9-1-1 services in the United States.

Standards Participation, Compliance & Commitment

Our employees were among the leading contributors during the initial development of the NENA i3 standard and continue to actively participate in NENA STA-010.3 working group (WG) activities as well as parallel updates to NENA standards. Allerium and its subcontractors maintain membership, committee participation, chair, board, and advisory positions in the leading industry SDOs involved with emergency services and other relevant organizations, including, but not limited to:

- NENA,
- 3rd Generation Partnership Project (3GPP),
- Association of Public-Safety Communications Officials (APCO),
- Alliance for Telecommunications Industry Solutions (ATIS),
- CTIA—The Wireless Association,
- Emergency Services Interconnection Forum (ESIF),
- Federal Communications Commission (FCC),
- Internet Engineering Task Force (IETF),
- NG9-1-1 Institute, and the
- Urban and Regional Information Systems Association (URISA).

Such widespread participation allows Allerium to align with current applicable industry standards as well as leverage a realistic adoption and implementation plan to accommodate future updates independent of individual vendor processes. As such, our solutions can evolve quickly as technologies and standards are developed. Allerium carefully considers the impact of each new standard as it is published, after which Allerium makes appropriate updates and/or adjustments to its solutions as required.

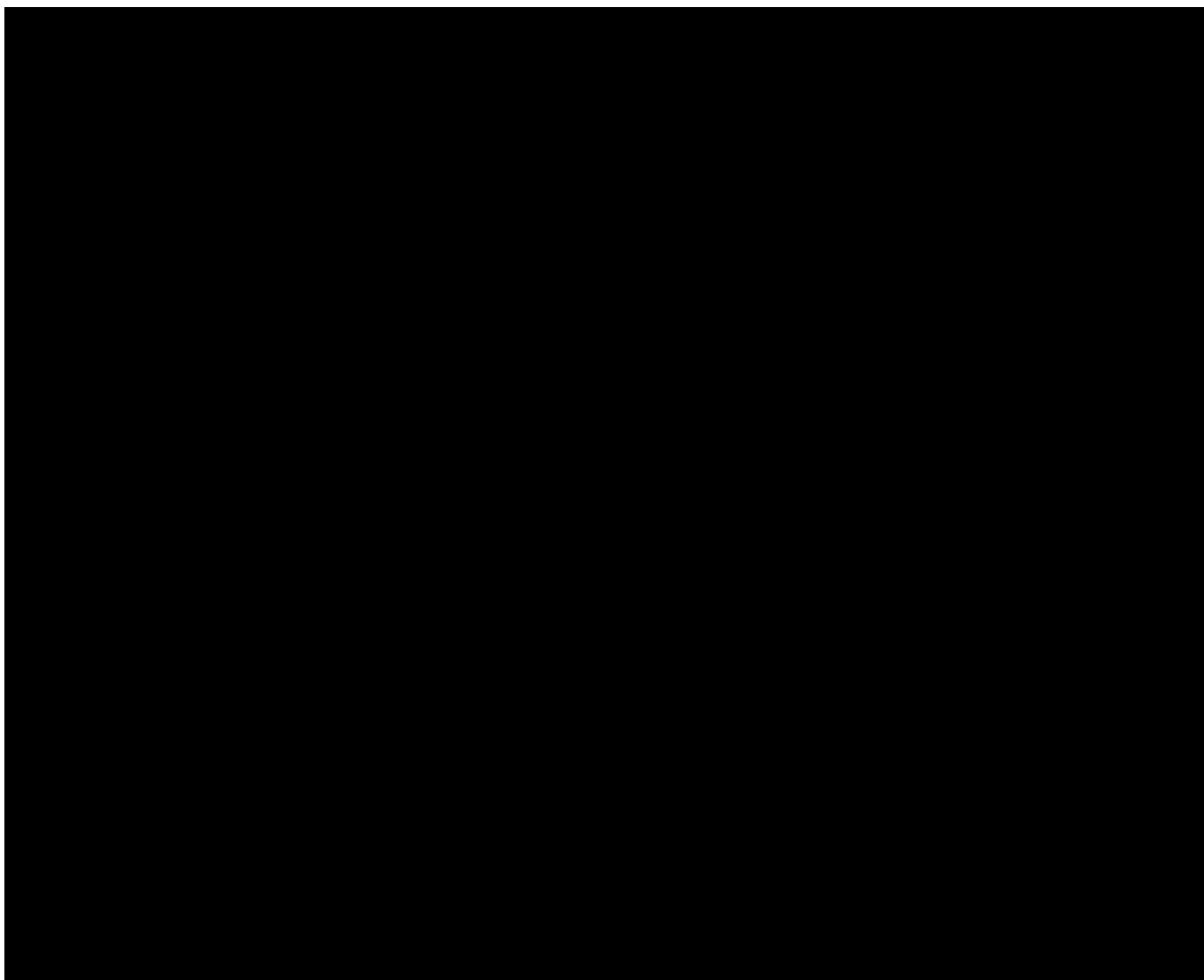
Technological Leadership Awards

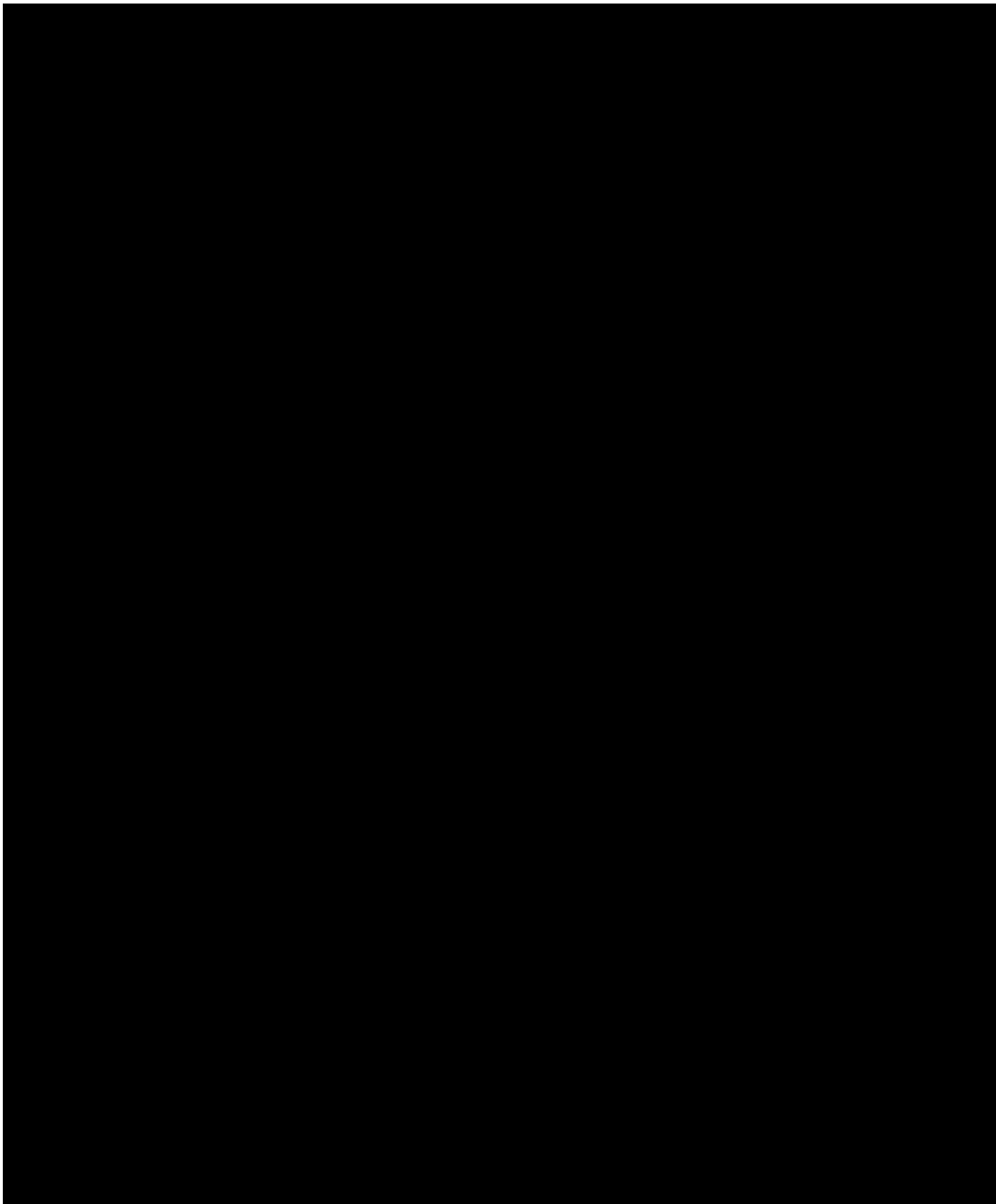
Allerium offers the most comprehensive NG9-1-1 end-to-end in-house technical capabilities in the market plus a full portfolio of service, system, and integration capabilities. This distinction, in combination with Allerium's significant NG9-1-1 market growth in 2020 and 2021, earned us the Frost & Sullivan (F&S) 2019 Best Practices Award for North American Next Generation 9-1-1 Product Line Strategy Leadership and 2021 Growth Leadership Award. These awards recognize the extent to which a company's product line meets its customers' basic demands as well as the overall impact it has in terms of customer value and increased market share.



Figure 8. Frost & Sullivan Awards

Bidder Information: Allerium's Proven Experience





1.2. Financial Statements [Proposal Instructions, Section A.1.b]

b. FINANCIAL STATEMENTS

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

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that 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.

Response:

Applicable Financial Statements

Bidder NextGen Communications, Inc. ("Allerium") does not generate financials separately from its ultimate parent company Comtech Telecommunications Corp. ("Comtech"). Comtech manages its business in two reportable segments:

- Allerium and
- Satellite & Space Communications.

The offeror is managed under the Allerium business segment.

Ultimately parent company Comtech is a publicly traded corporation listed on the NASDAQ under the symbol CMTL. Comtech makes its filings with the SEC—including annual, quarterly, and current reports as well as amendments to those filings—available on its corporate website (www.comtech.com), including the financial statements provided with this proposal. Comtech has been in continuous business since 1967.

Our most recent audited financial report / statement (FY2025 Form 10-K ending July 31, 2025) is included in Appendix 1: Financial Statements.

Financial/Banking Organization Contact Information

Disclosures

As a publicly traded company, any financial disclosures can be found in the most recent audited financial report / statement included in Appendix 1: Financial Statements.

1.3. Change of Ownership [Proposal Instructions, Section A.1.c]

c. *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.

Response:

No change of ownership is anticipated.

1.4. Office Location [Proposal Instructions, Section A.1.d]

d. *OFFICE LOCATION*

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

Response:

Allerium's primary office location responsible for the performance pursuant to a contract award is 2401 Elliott Avenue, Suite 100, Seattle, WA 98121.

The following offices will also support this NG9-1-1 project:

- 370 Interlocken Blvd, Suite 500, Broomfield, CO 80021
- 100 Technology Center Drive, Suite 400, Stoughton, MA 02072
- 450 Av des Entreprises, Unit 101, Gatineau, QC J8R 2X5

1.5. Relationships with the State [Proposal Instructions, Section A.1.e]

e. *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.

Response:

Bidder NextGen Communications, Inc. has no contracts with the State of Nebraska to declare. We do have Text to 9-1-1 agreements in place with some PSAPs and have contracted with the North Central Region to provide Guardian call handling.

Subcontractors Eonti and Equature Inc. have had no prior contracts with the State of Nebraska within the past ten (10) years.

Subcontractor GeoComm currently maintains the bulk of the locally authoritative NG9-1-1 GIS data in the State of Nebraska via its contracts with 82 of the 93 counties which are served by 58 of the 68 PSAPs.

1.6. Bidder's Employee Relations to State [Proposal Instructions, Section A.1.f]

f. *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.

Response:

Bidder NextGen Communications, Inc. has nothing to declare.

Subcontractors Eonti, Equature, and GeoComm have nothing to declare.

1.7. Contract Performance [Proposal Instructions, Section A.1.g]

g. *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.

Response:

Bidder NextGen Communications, Inc. has nothing to declare.

Subcontractors Eonti, Equature, and GeoComm have nothing to declare.

1.8. Summary of Bidder's Corporate Experience [Proposal Instructions, Section A.1.h]

h. 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.

Response:

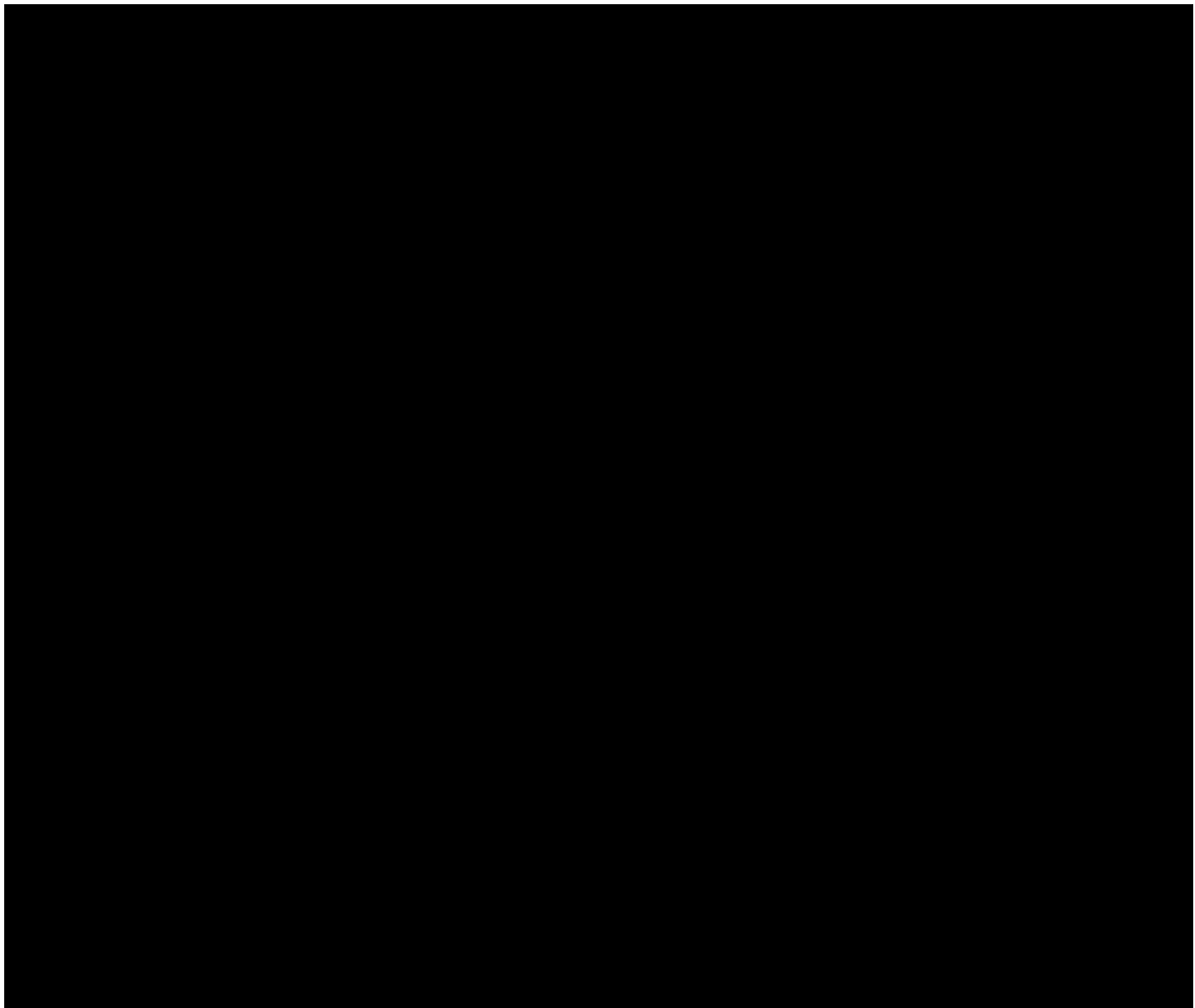
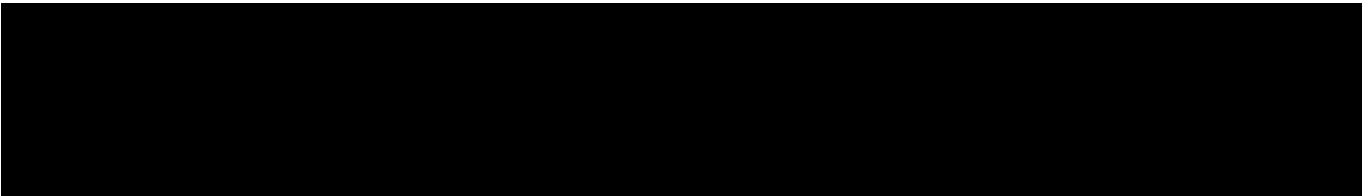
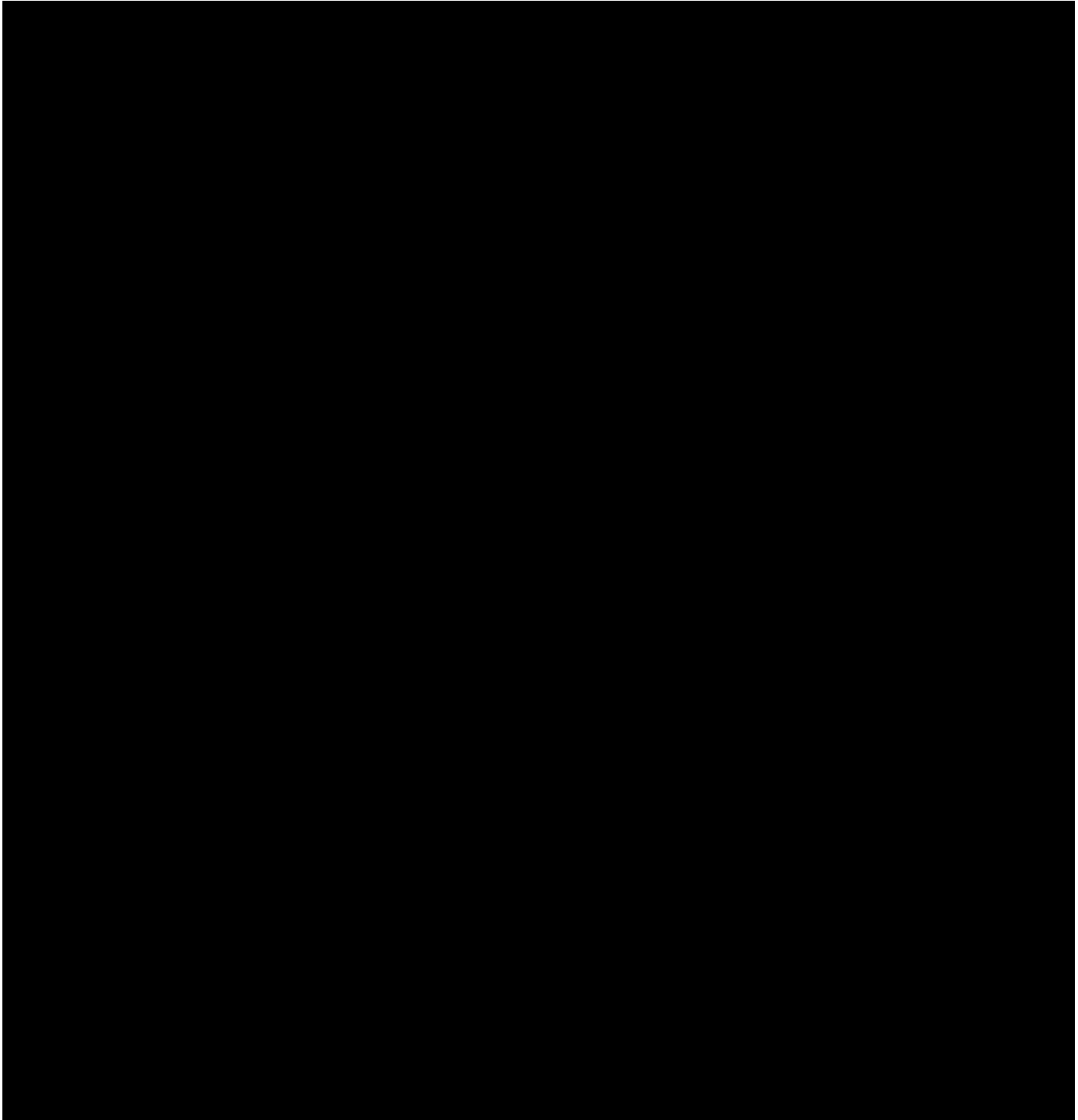
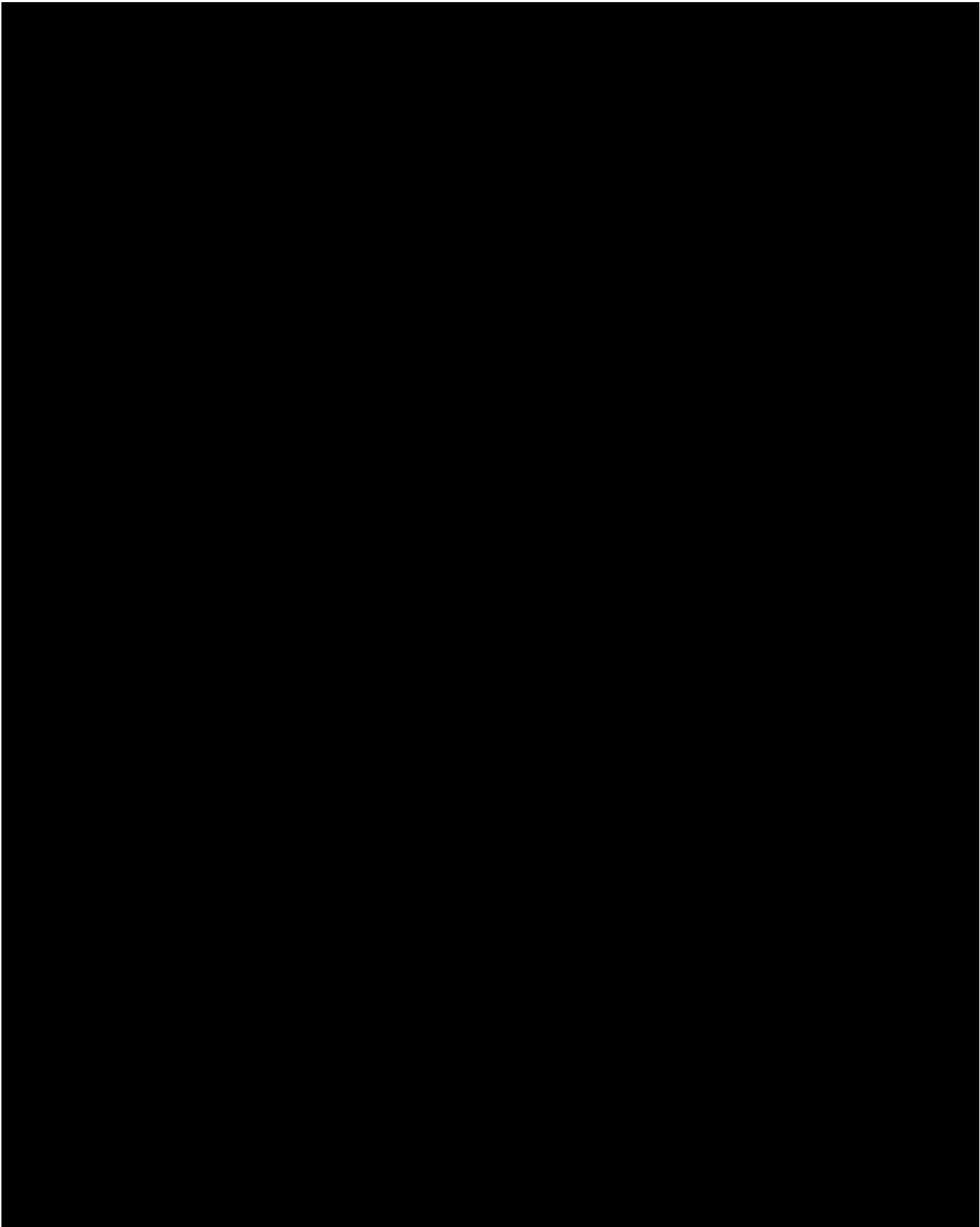
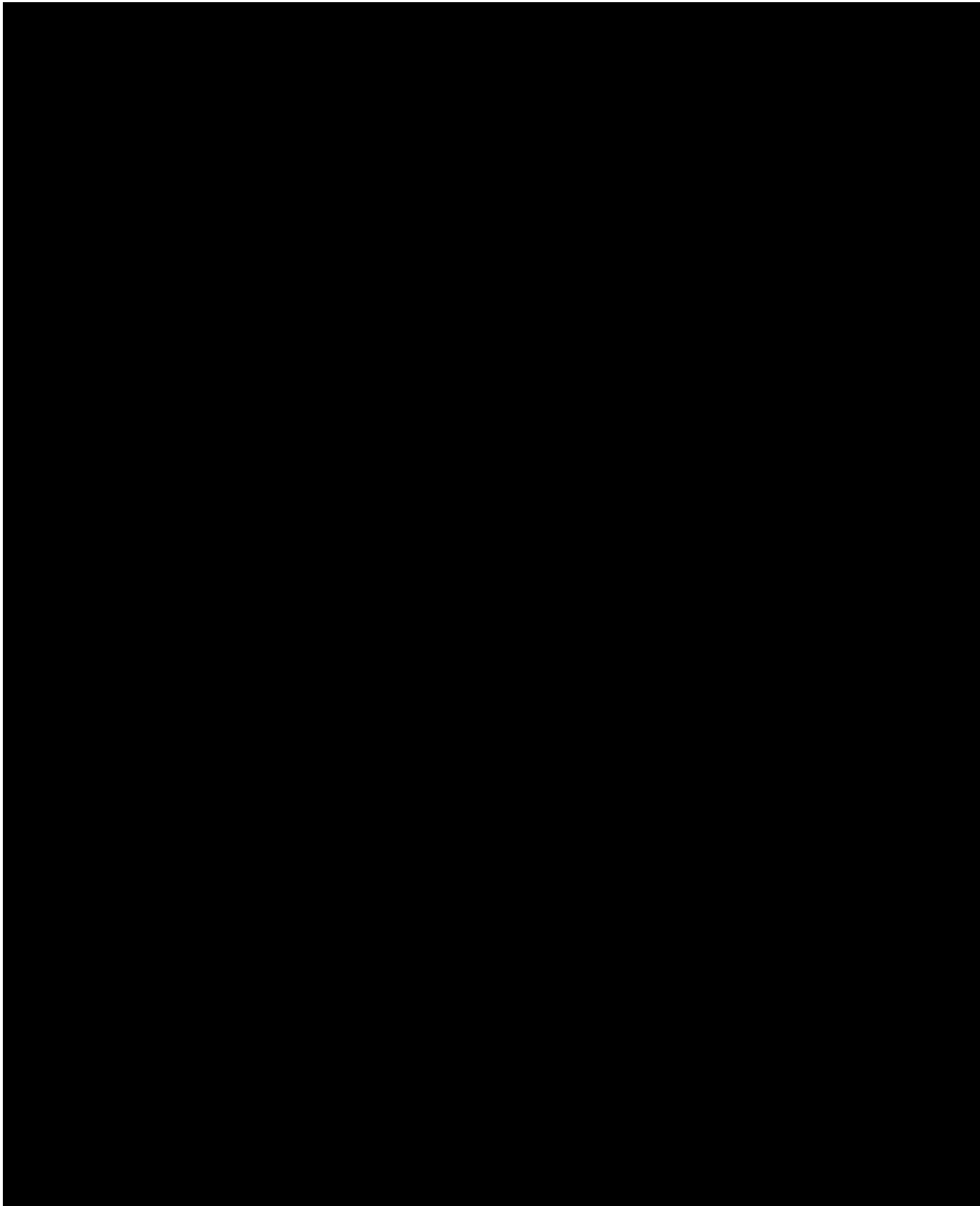
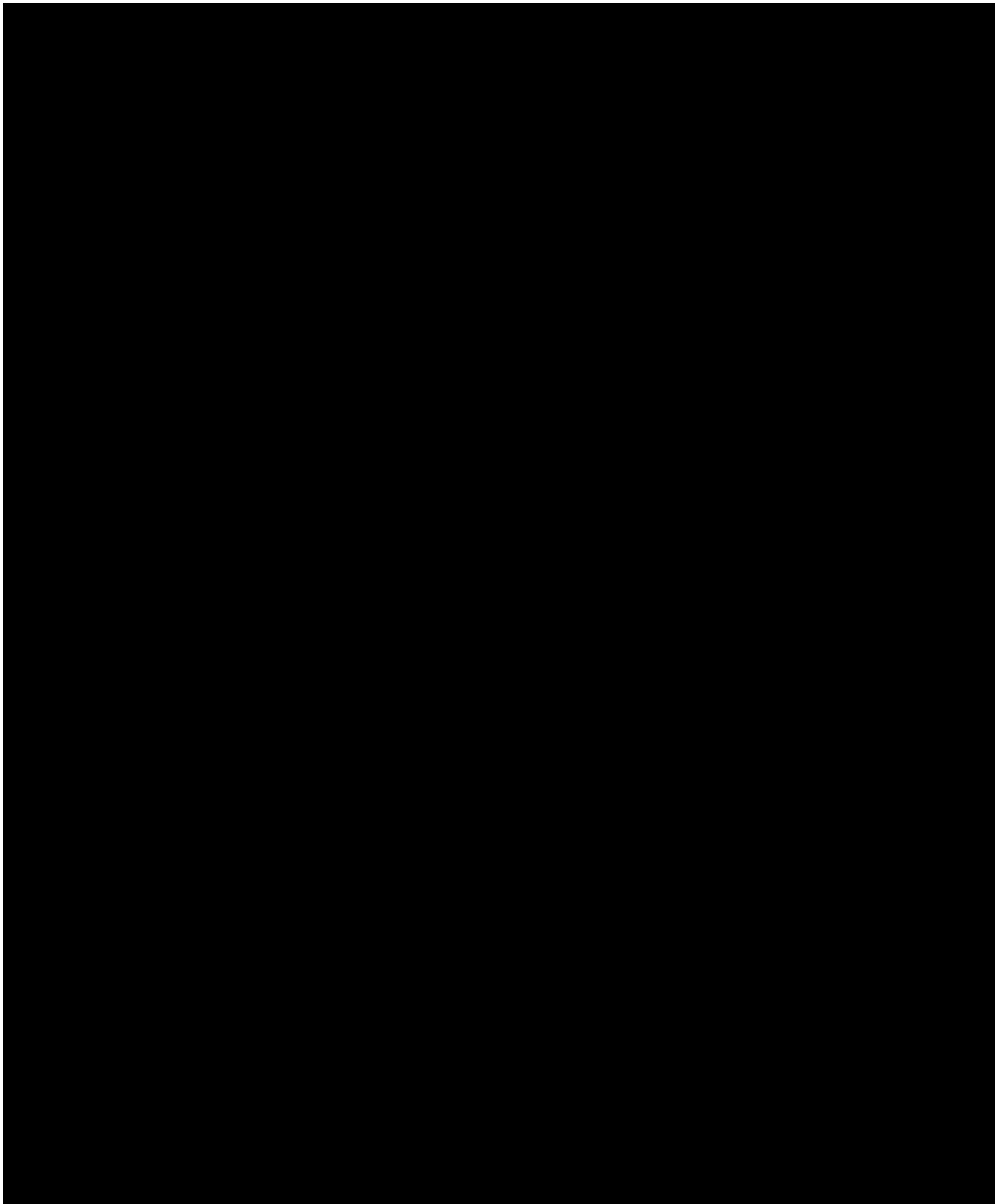


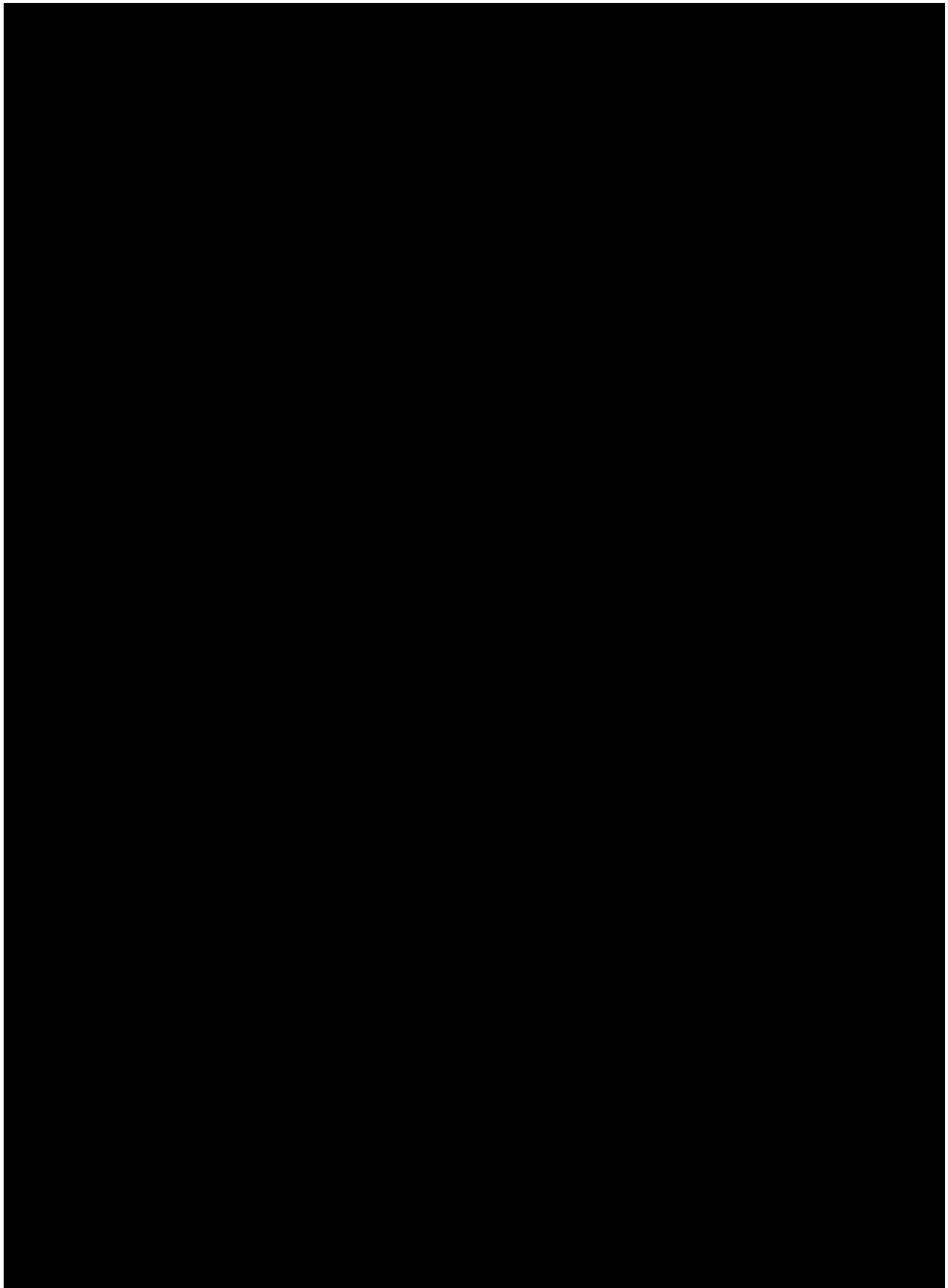
**Table 3. Previous Projects of Similar Size, Scope, and Complexity (ALLERIUM CONFIDENTIAL-
PROPRIETARY INFORMATION)**

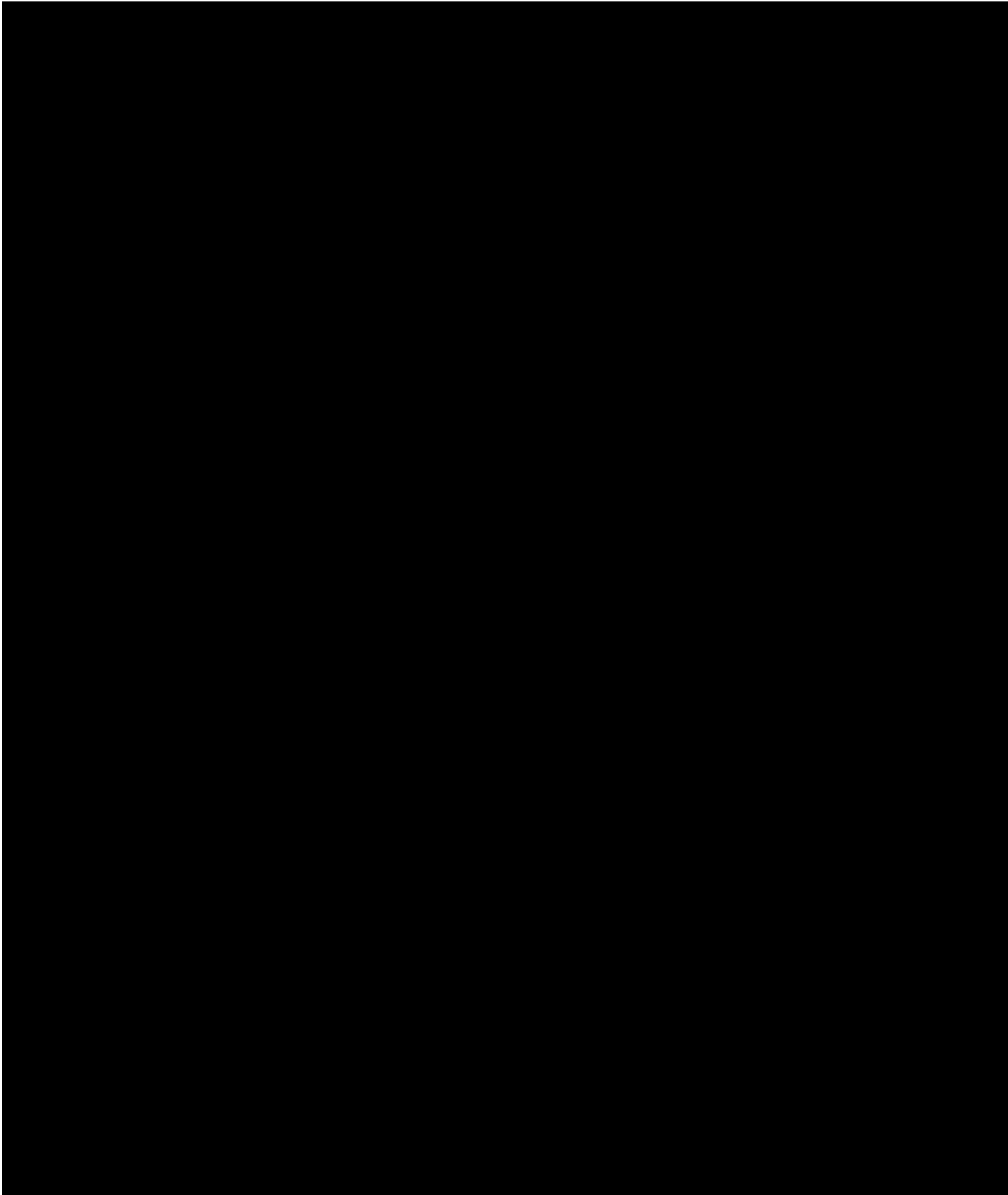


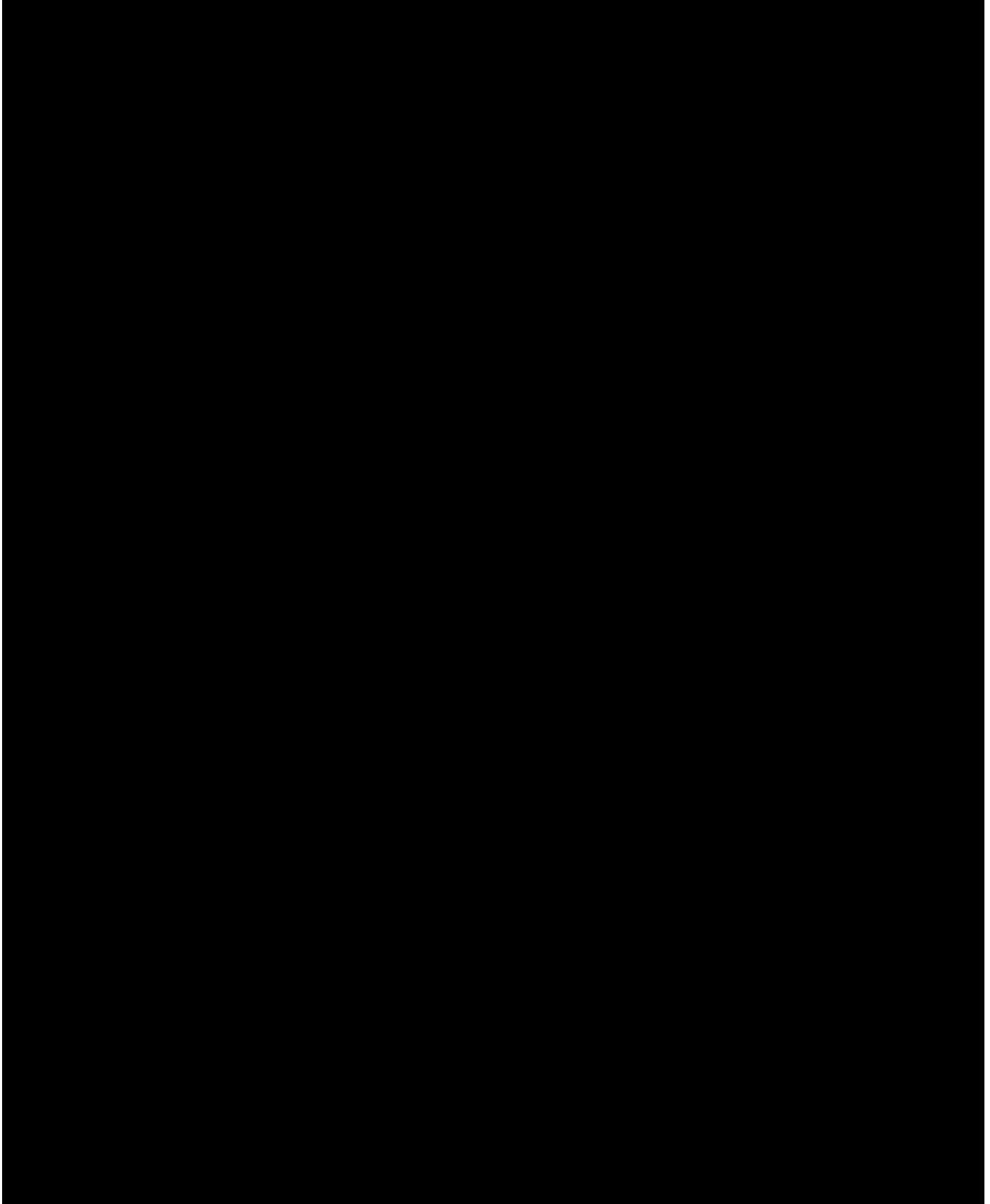


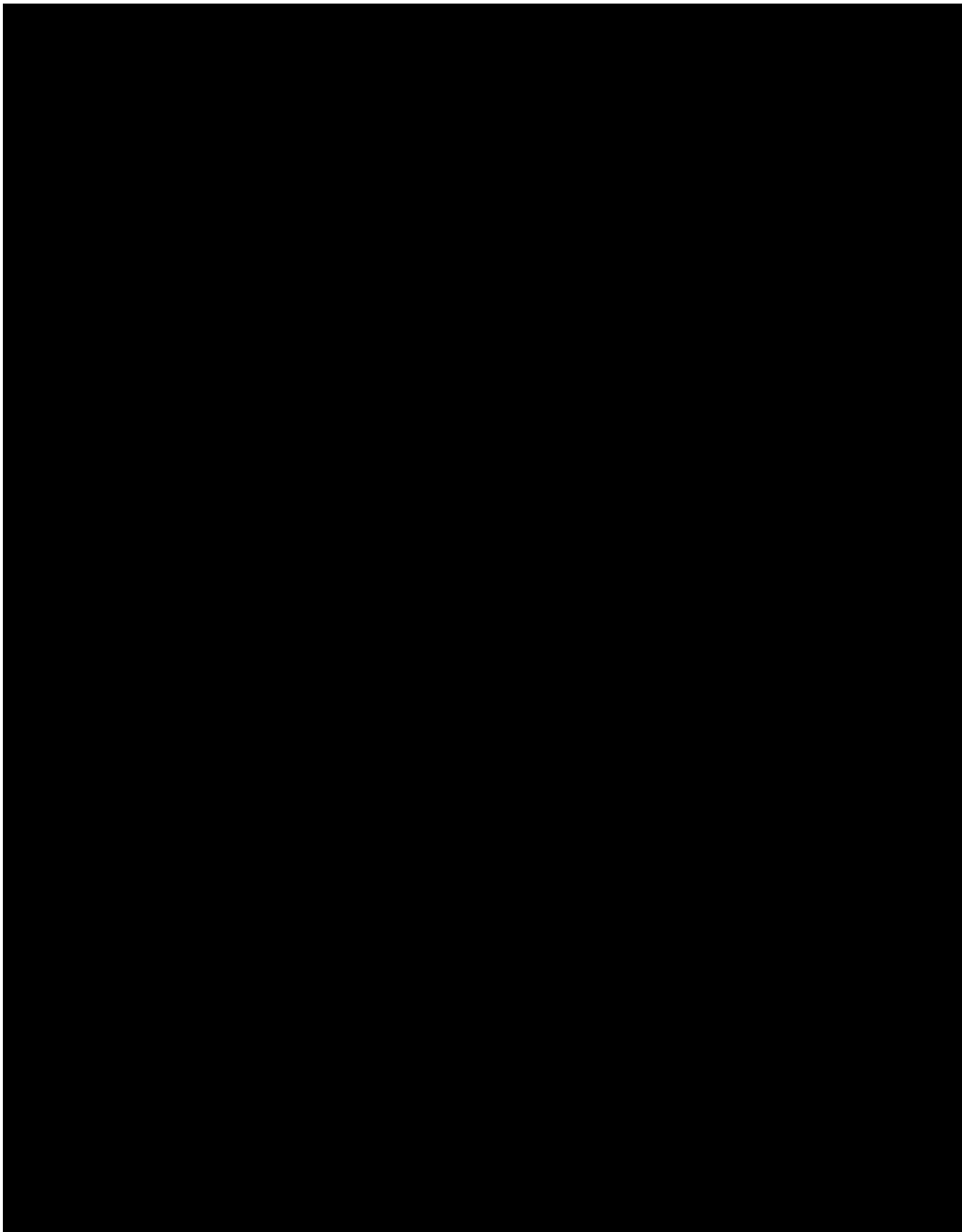


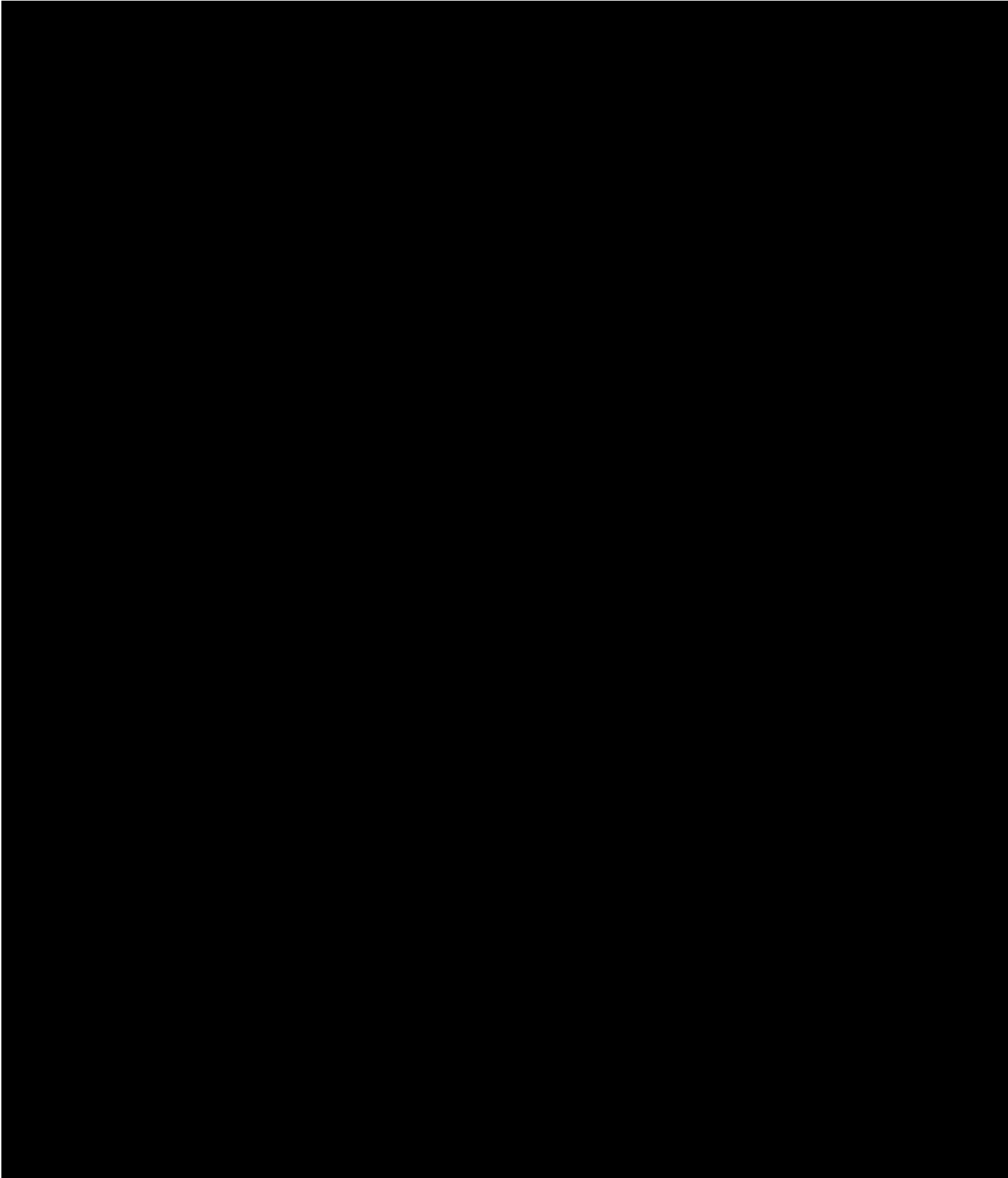












1.9. Summary of Bidder's Proposed Personnel/Management Approach [Proposal Instructions, Section A.1.i]

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

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

The bidder should identify the specific professionals who will work on the 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.

Response:**Proposed Approach to Managing the Project**Introduction

Allerium's Program/Project Manager (PM) will manage project planning and execution in accordance with the approved master project plan (MPP). The PM is the primary point of contact (POC) for the State and its PSAPs during the project life cycle. This individual oversees Allerium and subcontractor resource planning and assignments.

Allerium has a skilled and experienced core of employees and partners who make up the mobilization team for the initial service delivery to support the State NG9-1-1 service deployment. While this team will continue to support the State beyond the initial service delivery, Allerium will recruit any additional personnel required to provide a high quality of service.

Allerium NGCS business practice is based on providing and delivering a common, standards-based service through a repeatable process. Allerium has a core team of personnel who are part of a service organization supporting multiple customers. The Allerium employees and partners on this team include experts in all aspects of NG9-1-1 who have the technical understanding needed to ensure optimal project kick-off and progression. Members of this team were critical to the successful mobilization of NG9-1-1 deployments in Washington, Arizona, Massachusetts, Pennsylvania, South Carolina, and other locations. Their experience, and the lessons they learned, contributed to the evolution of our plans and procedures for deployment and testing. This team will remain intact for all phases of the system deployment and throughout the lifecycle of the service.

As the project moves forward, Allerium will continually evaluate resource demands and hire additional personnel as needed. Allerium will report any project staffing changes to the State administrator or assigned delegate. In the case of the person's resignation or the ceasing of his or her employment with Allerium, or in the case of a leave of absence due to medical or personal extenuating circumstances, Allerium will make a reasonable effort to give the State 30 calendar days' prior written notice of the removal.

Project and Program Experience

Allerium has extensive and diverse project and program experience managing large and complex NG9-1-1 projects since 2011, including:

- Performing multiple types of statewide deployments transitioning from legacy infrastructure to i3 solutions,
- Using regional/state sanctioned or owned networks in ESInet/NGCS deployments,
- Utilizing proven project/program management methodology based on ITIL, PMI, and industry best practices,
- Efficiently cutting over multiple PSAPs weekly (surge up to nine per week),
- Simultaneously conducting small and largescale NG9-1-1 deployment projects ranging from a dozen to 250 plus PSAPs supporting 15,000-13M population,
- Completing a 1.5M population deployment with 49 PSAPs six weeks ahead of schedule providing the customer both facilities costs and resource savings, and
- Interoperating and managed third party component solutions and vendors.

Complementary Program/Program Management Resources

Allerium uses a multi-team approach with a combination of project managers (PM) and a program/client services managers (CSM) to provide focal point management throughout the duration of the NG9-1-1 contract. We have standardized this approach across all our NG9-1-1 deployments based on our 15 years of experience in outfitting regions and states with this type of service. Our teams have found that deploying both large scale projects such as the Commonwealth of Massachusetts (211+ PSAPs) as well as other efforts like the state of Iowa (113 PSAPs), the Commonwealth of Pennsylvania (61 PSAPs), the state of South Carolina (80 PSAPs), and the state of Washington (65 PSAPs) is best managed by a combination of project and program managers. Allerium assigns these resources to the State's project, with primary responsibilities extending from project initiation through acceptance testing and transition and onward to operations and maintenance.

Initiating these two roles following contract signature and continuing to maintain them as described above (versus limiting the certified PM to leading the implementation and the CSM to post-implementation only) provides valuable project and program management continuity, critical deployment awareness for both resources, and a seamless transition between phases. This approach also enables each function to build relationships with critical stakeholders from day one.

Providing Sufficient Field and Technical Staff

Allerium employs over 450 team members dedicated to 9-1-1 services and operations. Most of these team members are technical in nature, and multiple SMEs from each technical area are assigned to a project of this size and scope. Our staffing plan includes SMEs performing the following functions:

- **Account Manager:** The account manager is primarily focused on helping to achieve customer goals and advocating within Allerium on the customer's behalf. The account manager channels new product and service offerings to our customers and handles service additions and contract extensions.
- **Project Manager:** The Allerium project manager is responsible for oversight, project management, staff supervision, and status reporting. The Allerium project manager is the focal point for project execution for the State, its jurisdictions, and associated PSAPs. The Allerium project manager works directly with the Allerium CSM, the State PM, PSC, and its jurisdictions to finalize a conversion plan that best fits the needs of key stakeholders and drives toward successful, on-time cutovers of PSAPs to the NG9-1-1 system.
- **Program Manager:** The Allerium program manager is responsible for onsite program management and serves as the primary POC for the term of the contract. The Allerium program manager collaborates with the project manager during the deployment phase and works directly with the State and its PSAPs to schedule and assist in PSAP migrations and onsite operations. The Allerium program manager attends all necessary meetings and visits PSAPs. Once a deployment is complete and accepted, the Allerium program manager is the focal point for all day-to-day interactions with the PSAPs unless there is a reason to contact the Allerium NOC/SOC.
- **Engineering:** The engineering department is solely dedicated to NG9-1-1 and comprised of staff members with direct experience in key subject matter areas (networking, security, computing systems, storage, SIP call processing, and legacy carrier routing) as well as

possessing intimate knowledge of our vendor's components as they apply directly to a NENA-compliant NG9-1-1 system. Engineering is responsible for all aspects of designing, integrating, and testing solution elements that integrate data centers, designated PSAPs, and OSPs. Engineering is also responsible for equipment staging (where PSAP configurations are configured and tested before shipment to the PSAPs), change/configuration management, and system security design and implementation. These same engineers then continue to support the service for the life of the contract, with activities ranging from performing routine maintenance related to patches and upgrading Allerium and third-party software to troubleshooting any incident that needs their depth and breadth of knowledge.

- **Business Management:** Allerium has staff dedicated to interfacing with the strategic partners, carriers, and telecommunications service providers necessary to implement an end-to-end NG9-1-1 system. This group's responsibilities include establishing the required performance, service delivery, interconnection agreements, and circuit orders/scheduling while also overseeing the service providers during provisioning, testing, and turn-up. Following cutover, this team ensures that these service providers are achieving applicable SLAs and managing and reporting on incidents as required by the contract.
- **Implementation and Testing:** Field technicians and installers are responsible for upfront site surveys to determine PSAP facility requirements and readiness, installation, and pre-cutover/cutover onsite testing during PSAP migration to the NG9-1-1 system.
- **Training:** The training coordinator works with the State's designated training lead as well as training content developers (OEMs and Allerium's in-house instructional systems designers) to finalize the proposed training curriculum and content. The training coordinator manages the training schedule, addresses customer satisfaction and feedback regarding training courses, and ensures that the instructors and materials being presented meet the State's training objectives.
- **Managed Network Services:** Post-conversion, Allerium provides system monitoring, maintenance, incident management and reporting, and service (help) desk services from our NG9-1-1 operations organization. This organization includes two redundant 24x7x365 public safety dedicated NOCs/SOCs with all the tools required to monitor and manage all components of the State's NG9-1-1 system. This team works with engineering closely, defining a Tier 1-Tier 4 structure and a clear triage and escalation path to ensure Allerium meets or exceeds the SLAs required for operating the State's NG9-1-1 system.
- **Field Operations:** Allerium maintains a pool of field technicians to support both project implementation and deployment, as well as post-conversion for operations and maintenance (both preventative and corrective action). In the post-conversion operations and maintenance phase, field technicians act as an extension of the Allerium NOC/SOC for local onsite activities. This team is comprised of qualified personnel knowledgeable and trained on the NG9-1-1 system and fully aware of the urgency required to maintain and adhere to SLA performance criteria.
- **Research and Development:** Allerium employs research and development staff with teams focused entirely on 9-1-1 solutions. Unlike many other companies providing NG9-1-1 services, Allerium not only develops NG9-1-1 solutions for states and local jurisdictions but also the 9-1-1 solutions used by OSPs that need to integrate with NG9-1-1. Our greater

understanding of the end-to-end 9-1-1 call flow allows us to avoid impairments related to certain predictable error scenarios such as intermittent bad locations or periods of missing location information.

- **Security:** Led by our Divisional Information Security Officer, the Allerium cybersecurity program instills a culture of security in support of our customers and business operations to lead the protection of and reduce risk for our information and information systems. We keep the trust of our customers and the communities they serve through the secure systems we develop and maintain using various tools and methods, including secure access and communication protocols, employee awareness and training, continuous assessment and corrective action planning, unabridged network and systems monitoring, responsive vulnerability management, and breach response and containment activities.

Specific Professionals

Allerium's key personnel roster below identifies key Allerium team members expected to support the State's ESInet/NGCS deployment. Allerium as prime contractor takes full responsibility for the project. All personnel report to the Vice President of Implementation & Customer Experience Greg Lathrop (aka project sponsor) and Senior Vice President/General Manager Eric Guerrero (aka executive sponsor).

Allerium's key personnel are trained on the proposed Allerium system(s) and services and have personal experience supporting ESInet/NGCS deployments of similar size, scope, and complexity. Allerium's key personnel resumes are included below and feature a list of the client projects supported by that individual. That list is provided for the purposes of illustrating their understanding of the process to NG9-1-1 as well as verifying experience, role/responsibility, and period of performance.

Table 7. Key Personnel Roster

Count	Name	Title	Project Role
1	Aaron Demorow	Vice President, Sys Engineering & Operations	Responsible for systems engineering & operations team
2	Ally Oughton	Senior Manager, Technical Communications	Training
3	Chris Hedges	Implementation & Support Manager	NOC, implementation management, PSAP deployments, cuts, and ATPs
4	Dave Wiegel	Senior Manager, Field Services	Field services
5	Elizabeth McMahon, PMP	Senior Project Manager	Project management
6	Eric Guerrero	Senior Vice President, General Manager	Executive sponsor
8	Greg Lathrop, PMP	Vice President, Implementation & Customer Experience	Program management

Count	Name	Title	Project Role
9	Jenn Richmond	Technical Program Manager	Coordinating data feeds to PSN Americas
10	Kenneth Banville	Divisional Information Security Officer	Security
11	Matt Davis	Technical Product Management Director	General NG9-1-1 standards support and product roadmap
12	Matthew Mullins	Principal Systems Engineer	Operational system design and engineering
13	Melissa Liebert, ENP, PMP	Manager, Geographic Information Systems	Responsible for GIS, sub DDTI, and providing DDTI training
14	Mike Wolfe	Program Manager	Program management
15	Neil Nyquist	Vice President, NOC & Field Services	Responsible for the NOC and field services teams
16	Patrick Hoover	Technical Program Manager	OSP migration
17	Patrick Melancon	Product Management Director	Overall product direction
18	Seth Wold	Sales Director	Sales management

Resumes

A sample of Allerium's key personnel resumes are included below. Each team member offers relevant project/program experience and has contributed to multiple Allerium ESInet/NGCS deployments.

Aaron Demorow, Vice President, Systems Engineering & Operations

Aaron Demorow has over 15 years of experience in public safety software development and engineering support and leads the systems engineering & operations team responsible for the State's project.

Table 8. Key Personnel Resume: Aaron Demorow

Resume: Aaron Demorow	
Title	Vice President, Systems Engineering & Operations: Responsible for leading our Systems Engineering & Operations teams to implement and support regional and statewide ESInet/NGCS implementations, including system deployment/testing, system upgrades/patches, system orchestration and deployment automation, systems engineering, telecom operations, interoperability testing, and RCA support.
Education	Associate degree, Network and Computing, National Institute of Technology, 1998-2000
Work Experience	Allerium/Comtech, Vice President, Systems Engineering & Operations, Aug 2025-Present

Resume: Aaron Demorow	
	- Comtech, Director, Operations, Aug 2021-Aug 2025 - Comtech/TeleCommunication Systems, Inc., Senior Manager, NG9-1-1 Operations, Mar 2016-Present - TeleCommunication Systems, Inc., QA Manager, Mar 2013-Mar 2016 - Christian Faith Center, IT Director, Jul 2007-Mar 2013 - TeleCommunication Systems, Inc., Lead QA Engineer, Jan 2004-Jul 2007
Relevant Certifications and Licenses	N/A.
Years Working with NG9-1-1 Systems and Technologies	- Since 2013. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, St. Louis County (Missouri), Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	- Gregory R. Kline, Deputy Director for 9-1-1, 9-1-1 Office, Pennsylvania Emergency Management Agency, 1310 Elmerton Avenue, Harrisburg, PA 17110, 717.651.2218, gregkline@pa.gov - Christy Williams, 9-1-1 Director, NCT9-1-1, 600 Six Flags Drive, Arlington, TX 76011, 817-695-9204 - Theresa Fazekas, Chief Financial Officer, Christian Faith Center, 33645 20th Ave S, Federal Way, WA 98003, 253-943-2400

Ally Oughton, Senior Manager, Technical Communications

Ally Oughton has over 19 years' experience in 9-1-1 technical communication and customer training and leads a team of technical writers, instructional designers, trainers, and document control experts to ensure the timely delivery of documentation and training for products and services under the wireless, VoIP, and NG9-1-1 product lines.

Table 9. Key Personnel Resume: Ally Oughton

Resume: Ally Oughton	
Title	Senior Manager, Technical Communications: Responsible for leading a Technical Communication program that provides mission-critical communication products and services for public safety, government entities, and carriers; and managing a team of technical writers, instructional designers, trainers, and document control experts to ensure the timely delivery of documentation and training for products and services under the wireless, VoIP, and NG9-1-1 product lines.
Education	Bachelor of Arts, English Major (writing concentration)/Computer Science Minor (technical writing and web development)
Work Experience	- Allerium/Comtech, Senior Manager, Technical Communications, Aug 2021-Present - Comtech, Technical Communications Manager, Apr 2015-Aug 2021

Resume: Ally Oughton	
	- Comtech/TeleCommunication Systems, Inc., Technical Communication Consultant, Next Generation Call Handling Division, Apr 2014-Apr 2015 - TeleCommunication Systems, Inc., Technical Communication Manager, Wireless Location and E9-1-1 Products & Services, Apr 2008-Apr 2012 - TeleCommunication Systems, Inc., Lead Technical Writer, Commercial Location Platforms, Dec 2002-2008 - Seattle Publishing, Inc., Technical Writer, 2002
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Since 2014. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.

Chris Hedges, Implementation & Support Manager, Allerium

Chris Hedges leads the end-to-end deployment of NG9-1-1 solutions—including call handling systems, CAD integrations, GIS components, and ESInet connectivity—for the State's project.

Table 10. Key Personnel Resume: Chris Hedges

Resume: Chris Hedges	
Title	Implementation & Support Manager: Responsible for leading the end-to-end deployment of NG9-1-1 solutions, including call handling systems, CAD integrations, GIS components and ESInet connectivity; coordinating project timelines, milestones, and resource planning across internal teams, vendors, and public safety agencies; translating PSAP operational needs into technical requirements and ensuring solutions meet state and national NG9-1-1 standards; overseeing system configuration, testing, validation, cutover planning, and go live support; and managing risk mitigation, change management, and quality assurance throughout all project phases. Also: - Serves as the primary escalation point for PSAPs and internal teams for technical or operational issues and ensures uptime, performance monitoring, and adherence to Service Level Agreements (SLAs). - Builds strong relationships with PSAP leadership, IT teams, emergency communications staff, and external partners. - Communicates project status, risks, and updates to managers, executives, and agency stakeholders. - Facilitates training and knowledge transfer for new deployments, upgrades, or major system changes.
Education	AS, Computer Science, ITT Technical Institute, 2010-2012
Work Experience	Allerium, Implementation and Support Manager, July 2025-Current

Resume: Chris Hedges	
	• Sky Unlimited, IT Administrator, May 2024-July 2025 • Camaro Central, IT Administrator, June 2021-May 2024 • AK Associates, 911 Engineer, May 2012-June 2021
Relevant Certifications and Licenses	N/A.
Years Working with NG9-1-1 Systems and Technologies	• Since 2012. • Regional 9-1-1 network deployments in Kentucky and Ohio. • Multiple Kentucky standalone CHE deployments. • Deployment of Allerium NG9-1-1 ESInet for Kentucky and South Carolina.
References	• Criss Chancellor, Service Manager, AK Associates, 7 Independence Ave, Derry, NH 03038, 603-490-5684 • Mark Greenthaner, Systems Integrations Engineering Manager, Axon, 640 Theresia Street, St. Marys, PA 15857, (814) 389-8584 • Chadd Friedman, PMO Coordinator, DATAMARK Technologies, 2323 W Fifth Ave, Ste 140, Columbus, OH 43204, 614-429-3384

Dave Wiegel, Senior Manager, Field Services, Allerium

Dave Wiegel is responsible for the management and oversight of the Allerium field organization, including both in-house field technicians as well as on-demand third party technicians through our partner program.

Table 11. Key Personnel Resume: Dave Wiegel

Resume: Dave Wiegel	
Title	Senior Manager, Field Services: Responsible for management and oversight of 21 field technicians supporting numerous NG911 programs. Technicians cover program items such as site surveys, installation / maintenance as well as 24/7/365 break-fix work.
Education	BS, Electrical Engineering – Milwaukee School of Engineering 1987-1991
Work Experience	• Allerium/Comtech, Senior Manager, Field Services, July 2022-Present • Understory, Field Operations Manager / Administration Lead, 2021-2022 • CivicSmart, Director of Operations, 2018-2021 • CenturyLink, Manager, Field Operations, 2012-2018 • CenturyLink, Sr / Central Office Engineer, 2006-2012 • AT&T Wireless, Transport Planner 4, 2004-2006 • TEKsystems, Transport Planner, 2003-2004 • AT&T Wireless, Network Engineering Manager, 2001-2002 • AT&T Wireless, Acting Operations Manager, 2000 • AT&T Wireless, Translations Engineer, 1996-2001

Resume: Dave Wiegel	
	360 Communications, Translations Engineer, 1994-1996 360 Communications, Cellular Engineer, 1992-1994
Relevant Certifications and Licenses	- Amateur Radio, Technician Class (N9KNX), 1990-Present - Amateur Radio Relay League, Emergency Coordinator, Washington County, WI, 2025-Present
Years Working with NG9-1-1 Systems and Technologies	- Since 2022. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, Commonwealth of Kentucky, Commonwealth of Massachusetts, St. Louis County (Missouri), State of Iowa, State of Ohio, and State of South Carolina projects.
References	- Molly Falls, Director of Partnerships, RapidSOS, 3 Park Ave, New York, NY 10016, 720-378-3930 - Michael Ball, NG9-1-1 Project Manager, SC Revenue and Fiscal Affairs Office, 1000 Assembly St, 4th Floor, Columbia, SC 29201, 803-734-2374 - Don Ehnert, Senior Network Engineer, Froedert Health, 8700 Watertown Plank Rd, Milwaukee, WI 53226, 262-993-0050

Elizabeth McMahon, Senior Project Manager, Allerium

Elizabeth McMahon, PMP leads the planning and execution of mission-critical public safety projects, including managing resources, schedules, budgets, and communications to ensure the successful delivery of NG9-1-1 programs.

Table 12. Key Personnel Resume: Elizabeth McMahon, PMP

Resume: Elizabeth McMahon, PMP	
Title	Senior Project Manager: Responsible for the planning, coordination, and execution of complex deployment activities for internal and external clients, ensuring alignment with scope, budget, and timeline objectives. Direct multiple concurrent projects facilitating customer-facing meetings and technical updates to drive transparency and accountability. Manage cross-functional initiatives by identifying risks, developing mitigation strategies, and aligning team efforts with strategic goals. Develop and maintain project documentation, including playbooks, dashboards, and ISO-compliant artifacts to ensure repeatable, high-quality delivery. Collaborate with customers and internal stakeholders to define requirements, establish incremental delivery plans, and track progress. Create and present executive-level project updates. Provide leadership to project teams, fostering continuous improvement through lessons learned and process enhancements. Support NG9-1-1 system integration efforts by coordinating with subcontractors and technical leads. Ensure adherence to quality standards while resolving issues efficiently to minimize impact on operations. Maintain strong stakeholder relationships through proactive communication, education, and engagement.
Education	BS, Chemistry, University at Buffalo, 1992-1997
Work Experience	Allerium/Comtech, Senior Project Manager, July 2025-Present

Resume: Elizabeth McMahon, PMP	
	- Windstream, Program Manager, Oct 2021-July 2025 - Windstream, Project Manager, April 2019-Oct 2021 - Xerox, Program Manager, July 2012-Dec 2018 - Xerox, Buyer/Planning, Jan 2005-July 2012
Relevant Certifications & Licenses	PMP certified in Mar 2024.
Years Working with NG9-1-1 Systems & Technologies	- Since 2019 beginning with in a supporting role on a Commonwealth of Massachusetts project while working at Windstream. - Supporting statewide NG9-1-1 projects in the Commonwealth of Kentucky and State of South Carolina, a Policy Store project for the State of Ohio, and the State of Iowa data center migration.
References	- Mike Mundorff, Senior Global Customer Relationship Manager, Uniti Group, 2101 Riverfront Drive, Little Rock, AK 72202, (585) 737-9098 - Candace Figueroa, Technical Project Manager, Cato Networks, 3031 Tisch Way, 110 Plaza West, San Jose, CA 95128, (860) 808-8326 - Ken Hunter, Lead Network Architect, Avis Budget Group, 6 Sylvan Way, Parsippany, NJ 07054, (516) 477-9572

Eric Guerrero, Senior Vice President, General Manager, Allerium

Eric Guerrero has over 20 years of experience starting as a first responder and dispatcher before serving in various leadership roles in public safety technology. Eric is the executive leader over the NGCS business at Allerium and will be the executive sponsor for the State's project.

Table 13. Key Personnel Resume: Eric Guerrero

Resume: Eric Guerrero	
Title	Senior Vice President, General Manager: Responsible for overall business performance and ownership of our E9-1-1 and NG9-1-1 call routing solutions and implementations for states, local jurisdictions and OSPs.
Education	- Master of Business Administration, Colorado State University, 2006-2008 - Bachelor of Science, Business Administration, Colorado Christian University, 2005
Work Experience	- Allerium/Comtech, Senior Vice President, General Manager, March 2025-Present - Comtech, VP, Program Management, Jan 2023-March 2025 - Comtech, Vice President, Service Delivery, May 2022-Jan 2023 - Enavate, Managing Director, Dec 2019-May 2022 - Cascade Healthcare Services, Chief Operating Officer, Mar 2017-Dec 2019 - Intrado, Vice President, Operations, Jun 2014-Mar 2017 - Intrado, Senior Director, Operations, Mar 2012-Jun 2014 - Intrado, Director, Account Management (Customer Team), May 2009-Mar 2012

Resume: Eric Guerrero	
	Intrado, Senior Program Manager, Sept 2006-May 2009
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	14 years. - Supporting multiple regional/statewide NG9-1-1 deployments, including Allerium's State of South Carolina, State of Iowa, Commonwealth of Kentucky, Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of Arizona, North Central Texas Region, State of Ohio, St Louis County, MO, and State of Washington projects.
References	- Paul Athey, Mapping & Operations Division Director, South Carolina Revenue and Fiscal Affairs (RFA) Office, 1000 Assembly St, 4th Floor, Columbia, SC 29201, 803.734.3789 - Greg Denton, 9-1-1 Program Administrator, Arizona Strategic Enterprise Technology (ASET) Public Safety State 9-1-1 Program, Arizona Department of Administration, 480.280.7171 - Christy Williams, 9-1-1 Director, NCT9-1-1, 600 Six Flags Drive, Arlington, TX 76011, 817-695-9204

Greg Lathrop, PMP, Vice President, Implementation & Customer Experience, Allerium

Greg Lathrop, PMP is responsible for the overall program management (e.g., project, deployment, ongoing lifecycle) for multiple states and well versed in Allerium's NG9-1-1 systems and services.

Table 14. Key Personnel Resume: Greg Lathrop, PMP

Resume: Greg Lathrop, PMP	
Title	Vice President, Implementation & Customer Experience: Responsible for the overall program management (e.g., project, deployment, ongoing lifecycle) for multiple Comtech clients, including the State of Arizona, State of Iowa, North Central Texas Emergency Communications District (NCT9-1-1), Commonwealth of Pennsylvania, and State of Washington.
Education	B.S., Business Administration, Central Washington University, 1996-2001
Work Experience	- Allerium/Comtech, Vice President, Implementation & Customer Experience, Apr 2026-Present - Allerium/Comtech, Senior Director, Programs, Aug 2025-Apr 2026 - Comtech, Director, Programs, Dec 2019-Aug 2025 - Comtech/TeleCommunication Systems, Inc., Senior Program Manager, Emerging Technologies, Aug 2017-Dec 2019 - TeleCommunication Systems, Inc., Program Manager, Emerging Technologies, Jun 2014-Aug 2017 - TeleCommunication Systems, Inc., Senior 9-1-1 Deployment Manager, Aug 2010-Jun 2014

Resume: Greg Lathrop, PMP	
	• TeleCommunication Systems, Inc., 9-1-1 Deployment Manager, Apr 2007-Aug 2010 • TeleCommunication Systems, Inc., Data Analyst, Feb 2004-Apr 2007 • Northwest Embroidery, Office Manager, Feb 2002-Feb 2004
Relevant Certifications and Licenses	PMP certified.
Years Working with NG9-1-1 Systems and Technologies	• Since 2019. • Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, North Central Texas Emergency Communications District (NCT9-1-1), Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	• Greg Denton, 9-1-1 Program Administrator, Arizona Strategic Enterprise Technology (ASET) Public Safety State 9-1-1 Program, Arizona Department of Administration, 480.280.7171, greg.denton@azdoa.gov • Gregory R. Kline, Deputy Director for 9-1-1, 9-1-1 Office, Pennsylvania Emergency Management Agency, 1310 Elmerton Avenue, Harrisburg, PA 17110, 717.651.2218, gregkline@pa.gov • Jonathan H. Brock, Deputy State 911 Coordinator / ESF-2 Lead, Emergency Management Division, Washington State Military Department, 253.223.3971, jonathan.brock@mil.wa.gov

Jenn Richmond, Technical Program Manager, Allerium

Jenn Richmond has a background in ALI data and application management as well as Data Analytics and Reporting. She works closely with the State, vendors, and internal SMEs to support successful communication and completion of reporting deliverables and training.

Table 15. Key Personnel Resume: Jenn Richmond

Resume: Jenn Richmond	
Title	Technical Program Manager: Responsible for facilitating the data exchange, application installation and data validation as it relates to ALI and Reporting analytics platforms. Working with both internal and external resources to ensure processes are established for data delivery from the Call Handling vendor and the NGCS through to the Analytics and Reporting applications as appropriate.
Education	Associate's in business, Front Range Community College, 2005-2007
Work Experience	• Allerium/Comtech, Technical Program Manager, Jan 2023-Present • Juvare, Product Manager, Sept 2021-Jan 2023 • Juvare, Product Owner, Feb 2021-Sept 2021 • Corvena, Product Manager, Feb 2020-Feb 2021 • Corvena, Technical Project Manager, June 2017-Feb 2020

Resume: Jenn Richmond	
	- West Safety Services (Intrado), Quality Management Specialist, April 2016-Jun 2017 - West Safety Services (Intrado), Associate Quality Management Specialist, May 2013-April 2016 - Intrado, Senior Data Analyst, Dec 2010-May 2013 - Intrado Data Analyst, Dec 2006-Dec 2010
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	12 years working on NG9-1-1 products, projects, and deliverables. 13 years working in application management for emergency management reporting and 9-1-1 data management, reporting, and analytics. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, Commonwealth of Massachusetts, North Central Texas Emergency Communication District, State of Ohio, Commonwealth of Pennsylvania, State of South Carolina, St. Louis County, Missouri, and State of Washington projects.
References	- Molly Falls, Director of Partnerships, RapidSOS, 3 Park Ave, Floor 22, New York, NY 10016, 720-378-3930 - Jeff Telford, VP of Product Management, Juvare, 235 Peachtree Street NE, Suite 2300, Atlanta, GA, 30346, 678-773-2776 - Alexander Warner, Chief Operating Officer, PSN Americas, 3626 N Hall St, Ste 406, Dallas, TX 75219, alex@psnamerica.com, 305-496-5068

Kenneth Banville, Divisional Information Security Officer

Kenneth Banville has over 30 years' experience in information technology (IT), engineering, and security and oversees our security team responsible for supporting 9-1-1 customers.

Table 16. Key Personnel Resume: Kenneth Banville

Resume: Kenneth Banville	
Title	Divisional Information Security Officer: Responsible for Allerium's security policies, maintaining both physical and cyber security standards and policies, and overseeing our security team that supports our 9-1-1 customers.
Education	- Bachelor of Science, Business Administration, University of Phoenix, 2007-2009 - Associate of Information Technology, Western International University, 2005-2007 - Certificate in Computer Systems Specialist, Northeastern University
Work Experience	- Allerium/Comtech, Divisional Information Security Officer, Nov 2021-Present - Comtech, Senior Systems Architect, NG9-1-1 Systems, May 2019-Nov 2021 - GDIT, Systems Architect, Oct 2016-Apr 2019

Resume: Kenneth Banville	
	• GDIT, Senior Principal Engineer, Oct 2009-Oct 2016 • GD through Insight Global, Unix Consultant, Feb 2009-Oct 2009 • Anacomp, Senior System Engineer, Jun 2001-Feb 2009 • Integrated Network Technology, Unix Consultant, Mar 2000-Jun 2001 • Star Market Co., Unix Systems Administrator, Oct 1996-Mar 2000 • Star Market, In-Store Systems Analyst, Mar 1996-Oct 1996 • Marshalls, Programmer Analyst I, Apr 1995-Mar 1996 • Marshalls, Senior Helpdesk Analyst, Jun 1992-Apr 1995 • Marshalls, Computer Operator, May 1990-May 1992
Relevant Certifications & Licenses	Active DoD Top Secret security clearance.
Years Working with NG9-1-1 Systems & Technologies	• Since 2016. • Overseeing a security team that supports all 9-1-1 customers, including Allerium's State of Arizona, State of Iowa, Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	• Charles Ashworth, System Analyst, Massachusetts State 911 Department, 151 Campanelli Drive, Suite A, Middleborough, MA 02346, 774-210-0911, charles.ashworth@state.ma.us • Frank Loulourgas, Hoplite Tech, LLC, 3 Valley Road, Norfolk/Dover, MA 02030, 617-780-9406 • Oscar Marcia, Eonti, 1345 Plaza Court North, Suite 3A, Lafayette, CO 80026, 720-470-9294

Matt Davis, Technical Product Management Director, Allerium

Matt Davis has over 24 years of experience in the IT industry, with 16 years specifically dedicated to public safety and NG9-1-1. Matt has held roles within many Allerium functional departments, including NG9-1-1 Operations, Application Engineering Management, Quality Assurance, Systems Engineering, and Product Management. Matt has provided support for all of Allerium's NG9-1-1 solutions and currently serves as the Technical Product Management Director for Allerium's NGCS and NG9-1-1 location platforms.

Table 17. Key Personnel Resume: Matt Davis

Resume: Matt Davis	
Title	Technical Product Management Director: Responsible for technical platforms, including Allerium's NG Core Runtime (ESRP, Policy Routing Function [PRF], LNG/LSRG, LPG, etc.), NG Core Provisioning, Location Data Platform, i3 Policy Store, ECRF/LVF, and MCS.
Education	BS, Technical Communications, Clarkson University, 1997-2001

Resume: Matt Davis	
Work Experience	- Allerium/Comtech, Technical Product Management Director, Mar. 2025-Present - Comtech Telecommunications Corp., Senior Technical Product Manager, Feb. 2019-Mar. 2025 - Comtech Telecommunications Corp./TeleCommunication Systems, Inc., Systems Engineer, Mar 2013-Feb. 2019 - microDATA GIS Inc., Technical Support, Sep 2009-Mar 2013 - Mission Critical Systems, Information Technology Consultant, 2007-2009 - Delwest Homes, IT Manager, 2002-2007
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Since 2009. - Support for CHE implementations throughout various U.S. states. - NGCS and routing customer platform support for statewide and regional networks since 2012, including 911 Association of Central Oklahoma Governments (911 ACOG), State of Arizona, State of Connecticut, multiple Florida counties, State of Iowa, Commonwealth of Kentucky, NCT9-1-1, Pennsylvania Emergency Management Agency, State of South Carolina, State of Tennessee, and State of Washington projects. - NENA i3 Architecture Working Group Member

Matthew Mullins, Principal Systems Engineer, Allerium

Matthew Mullins brings over 15 years of NG9-1-1 engineering experience to the State's project.

Table 18. Key Personnel Resume: Matthew Mullins

Resume: Matthew Mullins	
Title	Principal Systems Engineer, Emergency Systems Routing Engineering: Responsible for the operational system design and architecture of Allerium's emergency routing solutions.
Education	US Army, Signal Corp, 1996-2000
Work Experience	- Allerium/Comtech, ESRE, Principal Systems Engineer, 2016-Present - TeleCommunication Systems, Inc./Comtech, VoIP Telecom Apps, Systems Engineer, 2012-2016 - TeleCommunication Systems, Inc., Advanced Technical Applications Center, VoIP & NG Tier 2 Support Engineer, 2010-2012 - TeleCommunication Systems, Inc., Network Operations Center, Tier 1 Support Engineer, 2009-2010 - T-Mobile, Network Operations Center, Cellular Technical Support Engineer, 2009 - AT&T Mobility, Network Operations Center, Lead Cellular Technical Support Eng, 2000-2009

Resume: Matthew Mullins	
	US Army, Signal Corp, 1996-2000
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Since 2010. - Designed, deployed, and maintained multiple regional/statewide NG9-1-1 systems, including Allerium's State of Arizona, State of Iowa, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.

Melissa Liebert, Manager, Geographic Information Systems, Allerium

Melissa Liebert, ENP, PMP brings an extensive background in GIS and ALI platforms to the team. She works closely with the State, vendors, and internal SMEs to support successful communication and completion of GIS deliverables and training.

Table 19. Key Personnel Resume: Melissa Liebert, ENP, PMP

Resume: Melissa Liebert, ENP, PMP	
Title	Senior Technical Program Manager: Responsible for developing and implementing PSAP GIS and location data management processes and procedures required to support the rollout and maintenance of NG9-1-1 services; coordinating internal and external resources in support of required project deliverables; identifying and implementing process innovations, programmatic improvements, and automation opportunities for better operational efficiency; facilitating risk mitigation as a part of service deployment oversight; driving alignment between product, operations, and service delivery to support business growth and efficiency; supporting the delivery of our contractually obligated services through deployment and maintenance phases; horizontally aligning and coordinating between operations and service delivery for implementation and maintenance of services/software; managing, coordinating, and providing oversight of our vendors and partners; reporting and presenting schedules, progress, and risks to senior leadership; and generating key performance indicators (KPIs) from data sources to identify areas of improvement.
Education	- Graduate Certificate, Geographic Information Science, Oregon State University, 2014-2015 - Bachelor of Arts, Anthropology, Oregon State University, 2008-2011
Work Experience	- Allerium/Comtech, Senior Technical Program Manager, Aug 2025-Present - Comtech, Technical Program Manager, Aug 2022-Aug 2025 - Comtech, Program Manager, NG Location Services, Mar 2021-Aug 2022 - Comtech, Program Manager, Mar 2020-Mar 2021 - Comtech, GIS Analyst, Apr 2019-Mar 2020 - Liebert's Guide Service, GIS Contractor, Freelance, Nov 2016-Present - Liebert's Guide Service, Transcriptionist, Freelance, Jun 2013-Mar 2019 - Wahkiakum County, Cartographer/GIS Analyst, Nov 2014-Apr 2019

Resume: Melissa Liebert, ENP, PMP	
	- Warm Springs Geo Visions, Review and Compliance Coordinator/Archaeologist, Jan 2014-Nov 2014 - Warm Springs Geo Visions, Archaeologist/GIS Analyst, Jun 2012-Jan 2014 - US Forest Service, Archaeological Technician, Jun 2010-Dec 2011
Relevant Certifications & Licenses	- PMP certified in Mar 2024. - ENP certified in Feb 2024, expiring Feb 2028.
Years Working with NG9-1-1 Systems & Technologies	10 years working with NG9-1-1 and GIS systems and technologies. - Member of APCO's Common Computer Aided Dispatch (CAD) Public Safety GIS Identifiers Document WG, NENA's Utilization of GIS Data in NGCS Document WG, and Urban and Regional Information Systems Association's (URISA's) NG9-1-1 Task Force (formerly served as chair). - Contributed to NENA's GIS Data Stewardship Document WG, NG9-1-1 Data Model Template WG, and NENA-ADM-008 References WG. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, St. Louis County (Missouri), NINGA (Illinois), State of South Carolina, and State of Washington projects.
References	- Deb Rozeboom, Client Success Manager, DATAMARK Technologies, deb.rozeboom@mbakerintl.com, 548 4th Ave SE, Albany, OR 97321, 320-761-9767 - Richard Kelly, Senior Solutions Manager, 1Spatial, Inc, richard.kelly@1spatial.com, 8614 Westwood Center Drive #350, Vienna, VA 22182, 512-590-2945 - Kyle Bodtorf, Application Developer Administrator, GIS Section Chief, Pennsylvania Emergency Management Agency, kbodtorf@pa.gov, 1310 Elmerton Ave, Harrisburg, PA 17110, 717-651-2701

Mike Wolfe, Program Manager, Allerium

Mike Wolfe is the initial escalation point for non-service impacting concerns related to the State's deployment while ensuring that all related projects align with the long-term goals, coordinating priorities, managing interdependencies, and ensuring resources are allocated effectively across the program.

Table 20. Key Personnel Resume: Mike Wolfe

Resume: Mike Wolfe	
Title	Program Manager: Responsible for all program management responsibilities related to ESInet/NGCS services.
Education	- Fairmont State University, 1999-2001 - PMP Prep Course, 35 Hours, 2023
Work Experience	Allerium/Comtech, Program Manager, July 2022-Present

Resume: Mike Wolfe	
	- Frontier Communications, National Director of 9-1-1/Public Safety Sales, Project Management & Sales Engineering, Mar 2020-July 2022 - Frontier Communications, 9-1-1/Public Safety Sales Account Manager, May 2016-Mar 2020 - Monongalia County Commission, Director, Homeland Security Emergency Management and 9-1-1, Nov 2011-May 2016 - Monongalia County Commission, Deputy Director, Homeland Security Emergency Management and 9-1-1, Apr 2009-Nov 2011 - Monongalia County Commission, 9-1-1 Telecommunicator/PIO/County NIMS Coordinator/Training Officer, Nov 2006-Apr 2009 - Barbour County Commission, 9-1-1 Telecommunicator/Shift Supervisor/CAD Administrator, Dec 2005-Nov 2006
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	10 years. - Four years selling NG9-1-1 systems & technology. - Four years managing sales/project management/engineering of NG9-1-1 systems & technology. - Four years of program management for ESInet/NG9-1-1 services in South Carolina.
References	- David Morrison, Program Manager, South Carolina Revenue and Fiscal Affairs Office, Rembert Dennis Bldg., 1000 Assembly St., Suite 420, Columbia, SC 29201, 803-734-3880, david.morrison@rfa.sc.gov - Shelly C. Clark, Administrator, 911 Services Board, Kentucky Office of Homeland Security, 200 Mero Street, Frankfort, KY 40622, 502-352-3684, shellyc.clark@ky.gov - Susan Gochenour, Senior Manager, Technical Support, Segra, 11215 N Community House Rd, Ste. 1000, Charlotte, NC 28277, 540-946-6921, Susan.Gochenour@segrafiber.com

Neil Nyquist, Vice President, NOC & Field Services, Allerium

Neil Nyquist leads the Allerium NOC and field services teams responsible for the State's project.

Table 21. Key Personnel Resume: Neil Nyquist

Resume: Neil Nyquist	
Title	Vice President, NOC & Field Services: Responsible for managing a 24x7x365 operations team that monitors phones, email, and various tools for internal and external events and creates, updates, escalates, and resolves incident tickets; facilitating incident management and change management bridges and notifications, working with vendors and partners as needed to resolve service impacting events; and focusing on continual service improvement for all processes followed.

Resume: Neil Nyquist	
Education	- BSIT, University of Phoenix, 2003-2006 - ITIL Foundations certified. - Cisco Certified Network Associate (CCNA) certified.
Work Experience	- Allerium/Comtech, Vice President, NOC & Field Services, Aug 2025-Present - Comtech, Senior Director, NOC, Sept 2022-Aug 2025 - Comtech, Senior Manager, Network Operations Center, July 2019-Sept 2022 - Amazon, Operations Manager, Prime Video Live Events, Oct 2018-July 2019 - Expedia, Inc., Senior Manager, Major Incident and Problem Management, Nov 2014-Apr 2018 - DaVita, Senior Manager, Infrastructure, NOC Operations and ITIL Process Manager, Nov 2011-Nov 2014 - DaVita, IT Infrastructure and Operations Project Manager, Nov 2009-Aug 2012 - DaVita Kidney Care, Data Center and NOC Operations Supervisor, Nov 2006-Sept 2009 - RealNetworks, Real Operations Support Lead, Feb 2004-Nov 2006 - US Army, SSG - E-6 - Information Systems Specialist (74B) – Airborne/Air Assault/Rappel Master Qualified, 1995-2003
Relevant Certifications & Licenses	- ITIL Foundations certified. - CCNA certified.
Years Working with NG9-1-1 Systems & Technologies	- Since 2019. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, Commonwealth of Kentucky, St. Louis County (Missouri), Commonwealth of Pennsylvania, and State of South Carolina projects.

Patrick Hoover, Technical Program Manager, Allerium

Patrick Hoover has worked in the 9-1-1 industry for over 25 years, with comprehensive experience in both legacy E9-1-1 and the transition to NG9-1-1 (i3) as well as in the wireline, wireless, and VoIP 9-1-1 call delivery systems. Additionally, Patrick has call handling experience from both a deployment and ongoing troubleshooting perspective.

Table 22. Key Personnel Resume: Patrick Hoover

Resume: Patrick Hoover	
Title	Technical Program Manager: Experienced leader in E9-1-1/NG9-1-1 operations, technology, and deployment. Currently responsible for managing OSP onboarding to Allerium's NG9-1-1 systems directly for i3 call delivery capabilities. Strong skill set in managing multiple concurrent projects, ensuring successful conclusions and stakeholder satisfaction. Key responsibilities include leading NG9-1-1 OSP onboarding efforts to Allerium's NG9-1-1 systems, including initial outreach, implementation, testing and turnup;

Resume: Patrick Hoover	
	engaging with internal and external teams, including OSPs, state agencies, vendors, and competitors to work towards project success; working with CalR project management on all active OSP onboarding projects to help ensure timelines are met and act as escalation point for any obstacles; serving as a SME for E9-1-1 and NG9-1-1 systems and processes; managing integration, testing, and troubleshooting of 9-1-1 technology solutions; developing project reporting dashboards for tracking key milestones and deliverables; and identifying project risks and working to resolve issues and overcome roadblocks.
Education	Bachelor's degree, Colorado State University, 1999
Work Experience	• Allerium/Comtech, Technical Program Manager, Oct. 2024-Present • Intrado Life & Safety, Sr. Customer Success Manager, 2013-Oct 2024 • Intrado Life & Safety, Implementation Project Manager, 2012-2013 • Intrado Life & Safety, Program Manager, 2006-2012 • Intrado Life & Safety, Project Manager, 2004-2006 • Intrado Life & Safety, Project Manager, 2003-2004 • Intrado Life & Safety, Quality Management Specialist, 2001-2003 • Intrado Life & Safety, Data Integrity Unit Analyst I/II/III, 1999-2001
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	• Over 25 years of combined E9-1-1 and NG9-1-1 experience. • Supporting multiple statewide NG9-1-1 projects, including the State of Arizona, NCT9-1-1, State of Ohio, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington.

Patrick Melancon, Product Management Director, Allerium

Patrick Melancon brings over 16 years of NG9-1-1 experience to the State's project.

Table 23. Key Personnel Resume: Patrick Melancon

Resume: Patrick Melancon	
Title	Product Management Director: Responsible for supporting NG9-1-1 location product lines and developing and managing industry relationships with third party solution providers.
Education	• Master of Business Administration (M.B.A.), Plymouth State University, Plymouth, NH (and the national award winner for Small Business Institute [SBI] competition) • Bachelor of Science (B.S.) in Business Management and IT Management, Magna Cum Laude, Granite State College, Concord, NH
Work Experience	• Allerium/Comtech, Product Management Director, Dec 2024-Present • Founder and Principal Consultant, Circle M Innovations, Oct 2023-Present • Senior Product Manager, GeoComm, Nov 2014-Oct 2023

Resume: Patrick Melancon	
	- Vice President, Product Management, GIS Data Resources Inc., Aug 2013-Nov 2014 - Public Safety GIS Manager, State of Tennessee, Feb 2009-Aug 2013
Relevant Certifications & Licenses	- Five Forces Analysis Specialist, Advanced Innovation Group Pro Excellence (AIGPE™) - GISP, GIS Certification Institute (GISCI) (Issued Nov 2014) - Python, Visual Basic, SQL, C#, Agile Methodologies, Public Cloud Technologies, GIS Applications (ESRI)
Years Working with NG9-1-1 Systems & Technologies	- Since 2009. - Supported projects for the State of California, State of Maine, NCT9-1-1, New York City, State of North Carolina, Commonwealth of Pennsylvania, State of South Dakota, State of Tennessee, and the State of Washington prior to joining Allerium. - Involved in Allerium's ESInet/NGCS deployments. - Involved in multiple standards through the years, including the NENA GIS Data Model, NENA Data Stewardship, NENA i3 transition, and the APCO CAD GIS data requirements.
References	- Greg Spadorcio, Director of Sales, Smart Response Technologies, 7022 Singing Springs Ln, Evergreen, CO, 80439, 916-749-5010 - Tyler Thompson, Strategic Partnership Leader, GeoComm, 18215 Pine Vista Pl, Colorado Springs, CO 80908, 719-510-1649 - Deb Rozeboom, Client Success Manager, DATAMARK Technologies, 548 4th Ave SE, Albany, OR 97321, 320-761-9767

Seth Wold, Sales Director, Allerium

Seth Wold is the State's key point of contact (POC) for all questions related to the submitted offer. Seth serves as the sales lead for the State's NG9-1-1 project with an emphasis on helping to achieve the State's goals, handling account renewals, and presenting new product and service offerings to the State.

Table 24. Key Personnel Resume: Seth Wold

Resume: Seth Wold	
Title	Sales Director: Responsible for leading cross-functional teams to identify, capture, and implement new NG9-1-1 opportunities.
Education	- Bachelor's degree, Mathematics and Statistics, Utah State University, 2005-2008 - Bachelor's degree, History, Utah State University, 2005-2008 - Bachelor's degree, Polish Minor, University of Utah, 2005
Work Experience	- Allerium/Comtech, Sales Director, Apr 2025-Present - RapidSOS, Regional Manager, 2024-2025 - Utility, Inc., Business Manager, 2023-2024

Resume: Seth Wold	
	• Domo, Corporate Account Executive, 2021-2023 • Hexagon Geospatial, Regional Sales Manager, 2019-2021 • CentralSquare Technologies, Senior Sales Account Executive, 2017-2019 • Spillman Technologies, Field Sales Executive, 2015-2017 • iFIT, Vice President of Sales, 2014-2015 • Altra Running, National Sales Manager/Key Account Manager, 2011-2014
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	• Since 2015. • Worked on public safety projects in every state west of the Mississippi.
References	• Greg Denton, 9-1-1 Program Administrator, State of Arizona, 100 N, 15th Avenue, Suite 305, Phoenix, AZ 85007, 480-280-7171 • Adam Wasserman, State 911 Director, State of Washington, 1 Militia Drive, Camp Murray, WA 98430-5000, 253-512-7468 • Stacen Gross, President, GeoComm, 1100 W. Saint Germain St., Suite 300, Saint Cloud, MN 56301, 320-281-2186

1.10.Subcontractors [Proposal Instructions, Section A.1.j]

j.	SUBCONTRACTORS
<i>If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:</i>	
i.	<i>name, address, and telephone number of the subcontractor(s),</i>
ii.	<i>specific tasks for each subcontractor(s),</i>
iii.	<i>percentage of performance hours intended for each subcontract; and</i>
iv.	<i>total percentage of subcontractor(s) performance hours;</i>
v.	<i>whether the subcontractor is affiliated with the bidder or has common ownership. Please note the definition of "subcontractor" in the glossary in providing a proper response to this.</i>

Response:

Overview

Allerium's proposal includes four partners (subcontractors) whose capabilities meet or exceed the requirements of this RFP and address specific subtasks of the larger NG9-1-1 deployment. One subcontractor—GeoComm—already supports 58 of the 68 Nebraska PSAPs by maintaining most of the locally authoritative NG9-1-1 GIS data in the State while others collaborate with Allerium on multiple regional and statewide deployments in operation today.

Allerium's proposed subcontractors for the State's project are as follows:

- **CIS (CISSDM):** Providing SmartHands.
- **Eonti:** Providing the PKI lifecycle management services.

- **Equature:** Providing the logging service/servers.
- **GeoComm:** Providing the Spatial Interface (SI).

Allerium is providing all other solution components. All subcontractor personnel report to Allerium employees featured in the key personnel roster.

Table 25. Subcontractor Inputs

Requirement	CIS Inputs	Eonti Inputs	Equature Inputs	GeoComm Inputs
Name, address, and telephone number of the subcontractor(s)	CIS (CISSDM) 1023 Calle Sombra, Unit B San Clemente, CA 92673 949-297-3575	Eonti Inc. 1345 Plaza Court N., Ste 3A Lafayette, CO 80026 720-470-9294	Equature 18311 W. Ten Mile Road Southfield, MI 48075 858-768-2183	Geo-Comm, Inc. (GeoComm) 1100 West St. Germain Street, Suite 300 St. Cloud, MN 56301 320-281-2186
Specific tasks for each subcontractor(s)	SmartHands SmartHands is a colloquial term used to describe field engineers that support the move, add, change process as it relates to hardware and components that are not remotely accessible (e.g., a failed hardware component). CIS interfaces with our NOC/SOC and program teams to fulfill this function.	As the Registration Authority, Eonti provides PKI lifecycle management services such as vetting, certificate issuance, certificate revocation, etc.	Logging service/servers	SI The SI provides an interface between the jurisdiction level GIS data and the NGCS FEs.
Percentage of performance hours intended for each subcontract ¹	27%	51%	N/A	22%
Total percentage of subcontractor(s)	4%	7%	N/A	4%

¹ Calculation is the percentage of each subcontractor's "estimated" hours against all subcontractor hours.

Requirement	CIS Inputs	Eonti Inputs	Equature Inputs	GeoComm Inputs
performance hours ²				
Whether the subcontractor is affiliated with the bidder or has common ownership. Please note the definition of “subcontractor” in the glossary in providing a proper response to this.	No	No	No	No

Proposed Partners (Subcontractors)

CIS

Allerium has partnered with one of the industry’s premier field services companies to ensure any onsite needs—hardware, implementation support, troubleshooting—are quickly and professionally met with SmartHands.

In business since 2008, our partner CIS offers one of the most extensive field services footprints throughout North America with an industry-leading, massive network of over 42,000 local field service technicians who are insured, trained, vetted, and certified.

This subcontractor has a dedicated dispatch team and extensive experience having scheduled and completed over 200,000 onsite installations and repairs since 2008. Allerium’s program management and NOC/SOC staff work with their field service engineers to create customized, project-based statements of work (SOWs) to standardize even the most complex staging, structured cabling, or hardware installation projects.

All staging and deployment projects are deployed from the subcontractor’s 10,000 square foot Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and System and Organization Controls 2 (SOC 2)-compliant staging facility located in San Clemente, California. CIS’ ITIL-certified engagement managers ensure all dispatch requests are quickly fulfilled, project timelines are met, and field service technicians arrive on-time to properly complete installation tasks at hand.

Allerium and our subcontractor provide field technicians with the following certifications and expertise:

² Calculation is the percentage of each subcontractor’s “estimated” hours against all estimated performance hours.

- Averaging 50,000 hardware and local area network (LAN) elements staged, configured, and installed per year,
- Averaging 3,000 circuit installations, activations, and certifications per year provided by professionals with Certified Network Cable Installer (CNCI®), ETA® Fiber Optics, and Data Cabling certifications, and
- Averaging 23,000 site visits per year by our field technicians and fiber optics technicians (both inside-plant and outside-plant).

Importantly, Allerium and our subcontractor have experience working within PSAPs and the emergency services community at large. Technicians are properly credentialed and authorized to work within the public safety environment only after passing the appropriate screening and background checks.

The onsite support is end-to-end and includes staging, configuring, shipping, installing, and certifying all PSAP and data center hardware and circuits. Field technicians are ready for onsite installations and support 24/7, supporting after-hours maintenance windows as well as next day, weekend, and holiday onsite arrival times. Through this important partnership, Allerium provides installation, dispatch, and repair services paired with technical support and troubleshooting by the subcontractor's Technical Assistance Centers (TACs).

Allerium and CIS have worked together on the State of Arizona's NG9-1-1 project.

Eonti

Eonti provides consulting, strategy, governance, technology, and life cycle operations management for Public Key Infrastructures (PKIs). In addition, Eonti offers cyber security consultations and solutions for various industries. Eonti's security team has a proven record in providing:

- Customized implementations of PKI
- Digital credentials for cable devices worldwide
- Life cycle management of the Smart Grid, mobile, and communications trust infrastructures
- Prototyping trust infrastructure and other systems for customer testing and evaluation
- Cost effective solutions to various other security issues

Eonti had designed, implemented, and maintained complex ecosystems for multiple global leaders across the United States, Canada, Europe, and Asia.

The NG9-1-1 Interoperability Oversight Commission (NIOC) selected Eonti as the Public Key Infrastructure (PKI) service provider for the PSAP Credentialing Agency (PCA) to enable trust and interoperability in Next Generation 9-1-1 systems.

Equature

Founded in 1972 and formerly known as DSS Corp, Equature is the leading provider of audio and video recording and analytics software, including 9-1-1 dispatch recorders. For over 35 years, Equature has focused exclusively on public safety because excellent public safety is the foundation for safe neighborhoods, better education, and job growth. The company's long-standing commitment to innovation and excellence has established Equature as a trusted partner for public safety agencies across the country.

Equature specializes in providing comprehensive solutions tailored to the unique needs of public safety agencies, including:

- Recording systems
- Automated transcription and summarization
- Communication intelligence
- Video solutions
- Data analytics
- Quality assurance

Allerium and Equature have worked together on the Commonwealth of Massachusetts's NG9-1-1 project.

GeoComm

A longstanding Allerium partner, GeoComm was founded in Minnesota on May 18, 1995, to provide local governments with turnkey emergency 9-1-1 software and GIS services. Over the subsequent 30 years, the company has grown to serve emergency professionals in over 1,000 PSAPs throughout the United States, helping to keep more than 100 million people safe. Today, GeoComm has a national reputation as a leading provider of public safety GIS software solutions and services.

GeoComm has successfully completed numerous Address Conversion projects, assisting counties in transitioning from Rural Route and Box-style postal addresses to structured, locatable E9-1-1 addressing systems. These efforts have included in-depth on-site consulting to determine optimal addressing methodologies, comprehensive fieldwork to identify all addressable structures, and the development of Master Street Address Guide (MSAG) and Automatic Location Identification (ALI) databases. GeoComm's team manages the full lifecycle of address conversions—from legacy formats to fully standardized E9-1-1 address systems—ensuring accuracy, consistency, and operational readiness.

Over the years, GeoComm has evolved into a trusted leader in the delivery of public safety-grade GIS solutions. The company's service portfolio includes advanced data analysis, data remediation, and ongoing GIS maintenance. GeoComm also offers sophisticated mapping and dispatch applications, along with key NG9-1-1 core services, including the Emergency Call Routing Function (ECRF), Location Validation Function (LVF), Spatial Interface (SI), and comprehensive data validation tools. These capabilities are designed to strengthen emergency response systems and support a seamless transition to NG9-1-1.

GeoComm’s professional team brings decades of experience in the public safety sector, dating back to the earliest implementations of basic 9-1-1. This foundation has expanded significantly through the company’s work with hundreds of jurisdictions nationwide, supporting the deployment of Enhanced 9-1-1 (E9-1-1) solutions. Today, GeoComm’s expertise continues to grow through innovation, strategic customer partnerships, and active involvement in industry groups that are defining the future of NG9-1-1 across the United States.

Allerium and GeoComm have worked together on statewide NG9-1-1 projects for the State of Iowa, Commonwealth of Kentucky, Commonwealth of Pennsylvania, and State of Washington as well as regional deployments in Texas.

2. Factors Used to Evaluate Corporate Overview [Proposal Instructions, Section A.2]

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.

Response:

Allerium understands.

3. Response to Scope of Work [Proposal Instructions, Section A.3 / Project Requirements and Scope of Work, Section B]

3. RESPONSE TO SCOPE OF WORK

Bidder should read the Scope of Work Section of this RFP and provide a response as part of its proposal. This response should describe how the bidder will complete the scope of work, fill in any additional steps or details necessary, and demonstrate why the bidder is the most qualified or capable.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

Response:

Allerium understands and complies.

3.1. Services to be Provided [Project Requirements and Scope of Work, Section B]

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 SE (Technical Requirements) of this document.

Response:

Allerium has been designing, implementing, and operating NG9-1-1 systems and services for nearly 15 years. Prior to NG9-1-1, we built and supported some of the first wireless and VoIP E9-1-1 services, many of which are still in use today. Taken together, we route 9-1-1 calls and texts to nearly every PSAP in the country, including those in Nebraska. We understand what it takes to design and implement a NG9-1-1 service in your state, having taken on this exact challenge in Washington State 10 years ago. In both instances, an existing Lumen (then CenturyLink) 9-1-1 service (IP-based) was in place until we moved the State and PSAPs to our NG9-1-1 infrastructure. We've successfully managed the Washington State deployment through many challenges, including GIS migrations, rural PSAP ESInet connectivity, OSP ingress changes, and new technology integration.

We fully understand the technical requirements in this RFP and have the exact expertise needed to quickly and professionally move the State to a better solution.

3.1.1. ESInet Architecture and Design

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).

- 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).
- 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).
- 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).

Response:

Requirement Overview

Allerium designs every deployment for high availability, starting with a highly available architecture that leverages nearly two decades of providing 9-1-1 services in a similar fashion. Our architecture is built for active-active processing—no manual failover required to a standby system—with multiple layers of redundancy. Combining both local and geo-redundancy results in a six-core redundant service with each core capable of independently carrying the full load of traffic for the State. Coupled with multiple diverse and redundant network paths, fast convergence, prioritization, and call survivability, the NGCS and ESInet complement each other in delivering service across the State.

Built on top of the physical infrastructure, Allerium’s ESInet implements logical IP network concepts as described in RFC 3261 and other IP-related standards and best practices. Our network implements quality of service (QoS) to prioritize traffic, with our methodology described in detail in this RFP response. Similarly, we have provided bandwidth utilization metrics, showing typical bandwidth application usage as well as best practices design info. Allerium has provided ample bandwidth, per the RFP requirements, that will support the State well into the future.

While the ESInet is forward-leaning, the State recognizes (and we agree) that legacy interconnections will still exist between OSP networks and older CHE manufacturers. To overcome these challenges, Allerium has extensive experience deploying legacy gateways for OSPs, selective routers, and PSAPs. Our interface control documents (included with this response) outline all necessary procedures for interconnection to both legacy and NG9-1-1 capable networks provided by others, be they other ESInets or third-party providers in the ecosystem (such as CHE or ADR providers).

Additional Background Information

The following sections provide additional details regarding the ESInet design and architecture.

Surviving the Destruction of Any One Physical Site

Allerium’s active/active design ensures there are always redundant paths from the ingress service into the PSAP. These redundant paths connect the ingress service to each NGCS data center, thus connecting the ingress service through each NGCS data center to the egress ESInet such that the loss of an entire data center does not result in a loss of service.

In the Figure 9 scenario shown below (with the third data center omitted for clarity), the first data center is isolated from the ingress network and unable to process inbound calls. Given the redundancy between the ingress service and the NGCS data centers, an automatic reroute occurs to the remaining surviving data center site. The blue arrows illustrate both the failure and the alternate path. No manual intervention is required to maintain continuity of service in this event.

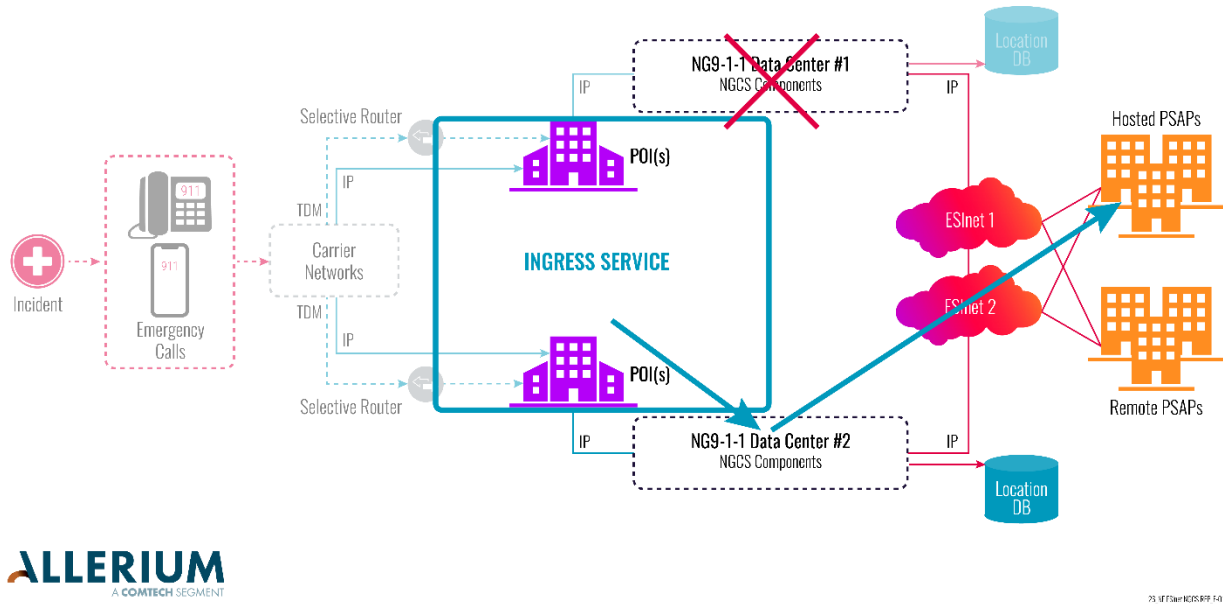


Figure 9. Surviving Isolation of a Physical Site

Overall Solution Performance

Allerium’s network- and systems-level devices and applications are designed and deployed in highly available pairs, ensuring that each device or system is fully capable of supporting 100 percent of call-routing volume should the other device or system fail.

Allerium designs its systems for high availability using a six-way-redundant approach for active/active call processing. We employ a load balancing methodology with each system being both locally and geographically redundant, resulting in each data center continually processing calls in an active/active manner. If any one element or physical connection is unavailable, the remaining elements or connections will handle the increased 9-1-1 traffic load rather than the system failing over. This methodology is extensible to the entire system so that any one element of the six available elements can handle the call volume.

Allerium’s design redundancy can be described by four primary categories of redundancy and failover:

- Applications & Functional Elements:** Each application and FE in the NG9-1-1 design performs tasks related to NG9-1-1 routing or services and is deployed in a high availability model within each data center. In this manner, each data center supports non-blocking availability for applications. The use of multiple data centers further enhances the reliability and availability model by enabling an active/active or active/standby model between data centers for each application as required to meet transactional vs. stateful applications. Therefore, application high availability is redundant both within a data center and across multiple data centers, resulting in a highly-redundant design.
- ESInet Design:** The ESInet design is a purpose-built unified communications infrastructure that leverages NENA standards and widely accepted best practices for delivering converged services. ESInet IP routing is designed to be fully redundant to support multiple interfaces and service-aware capabilities for failover. Routing across the network is highly

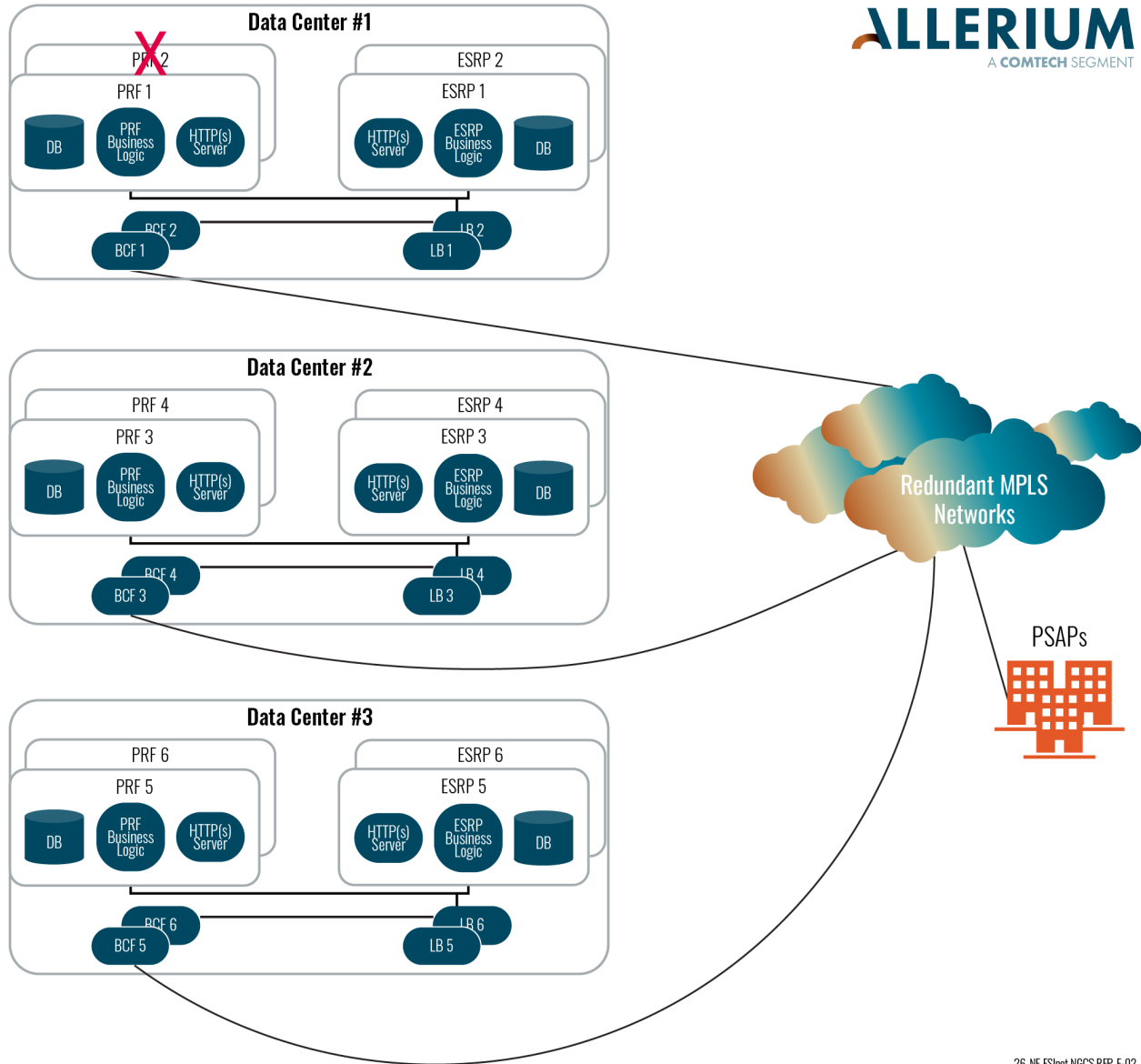
secure, leveraging encryption over virtual private network (VPN) tunnels. The QoS is highly deterministic, leveraging bandwidth analysis and traffic engineering using markings for DSCP. Coupled with diverse MPLS networks supporting the service, our ESInet offers the highest reliability available.

- **Telecommunication Circuits:** Allerium is circuit-agnostic, meaning we use the best available circuits regardless of underlying carrier (unlike existing telecom providers that show a strong proclivity to only use their own network infrastructure). Allerium's service incorporates a composite set of connectivity services that meets the performance requirements called out in the State's RFP for services transport. This design delivers exceptional flexibility by leveraging diverse carriers and network facilities. ESInet core IP routing provides a highly available and redundant solution accompanied by proven SLA management and compliance. Allerium will register circuits for 9-1-1 priority through telecommunications service priority (TSP) markings to further enhance the ESInet's survivability.
- **Management:** All elements of redundancy and availability are supported by a holistic approach to network management, where services are monitored on a 24x7x365 basis for KPIs to enhance survivability. This approach enables proactive maintenance to prevent failures as well as the flexibility to be reactive should a failure occur. The Allerium NSOC supports continuous monitoring. Allerium is very security conscious and provides additional SMEs in security operations to enhance cybersecurity. Finally, Allerium provides on-site "smart hands," vetted and approved for data center and PSAP access in advance to perform any needed onsite maintenance.

The key takeaways regarding Allerium's redundancy are:

1. Failure of any single instance of an element or physical connection will not impact the overall solution performance, and
2. No manual intervention is required to "failover" to the redundant system as all services are operating in parallel and surviving elements automatically assume any increased load due to element failure.

Figure 10 is a simplistic view of the designed redundancy methodology across the data center sites. We deploy each FE with both local and geographic redundancy as illustrated by the redundant ESRP and PRF deployment in Figure 10. We deploy all other elements in similar fashion. This redundancy results in a total of four elements being available for each function.



26_NE ESInet NGCS RFP_F-02

Figure 10. Failure of a Single Element or Connection

Redundant Network Interfaces

All Allerium’s network-connected elements support at least two redundant and physically diverse network interfaces. Allerium’s ESInet allows for interconnection to external networks. Interconnection to external networks is governed by an agreed upon network-to-network interface (NNI) document between all stakeholders. External network connections function in alignment with the core ESInet and include redundant, diversified paths to the external network. Fault of a single path results in automatic failover to surviving paths in an automated fashion.

Automatic Failover Mechanism

Allerium’s proposed solution is a NENA i3-compliant platform committed to the “five nines” standard (99.999 percent reliability) for providing the delivery and receipt of 9-1-1 calls. The

solution minimizes single points of failure and is composed of redundant central system components that provide load sharing and load balancing with failover capability. Manual intervention is not required since the solution is designed as a redundant system that employs automatic failover. We configure our routing protocols with appropriate timers to mitigate instability anomalies such as faulty devices or unstable connectivity.

3.1.2. NG911 Core Services (NGCS)

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.)

Response:

Allerium's proposed solution supports multiple regional and statewide deployments with NGCS functional elements as defined in the NENA i3 Standard.

Allerium implements each standards-based function with the products that are named after that function (e.g., the Allerium ECRF performs the ECRF function).

Allerium has been supporting NGCS interfaces within the core network of SIP and REST interfaces, including PIDF-LO in our deployments successfully with supporting documentation, schemas, and test harness endpoints.

Allerium has met acceptable latency and throughput SLAs for NGCS lookups and routing decisions with 99.999% uptime of our solution in all the markets we are deployed.

3.1.3. GIS and Location-Based Routing

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.

Response:

Accepting, Storing, and Using GIS Data

The State's requirement for GIS and location-based routing emphasizes the need for authoritative, standards-aligned spatial data to support accurate NG9-1-1 call handling. Allerium approaches GIS as a mission critical element within the NG9-1-1 environment, and our platform is designed to ingest, validate, store, and operationalize datasets consistent with the structure defined in NENA STA 006.2 2022. This includes all required layers, such as PSAP boundaries, Emergency Service Boundaries, address points, civic address attributes, emergency routing attributes, and road centerlines. When customer datasets arrive using alternative schemas, the platform translates them into the NENA GIS data model prior to use within the NGCS framework.

Once received, GIS data is processed through automated validation that examines topology, schema alignment, attribute completeness, and boundary consistency. This ensures datasets are prepared for provisioning into the Emergency Call Routing Function, Location Validation Function, and related geospatial services. If errors are identified, the submitting agency receives a clear, actionable report to support efficient correction and resubmission. This process maintains data integrity and provides the accuracy required for routing and validation.

Authoritative GIS Data

Allerium uses authoritative GIS data as the single source for routing decisions in the ECRF. The system accepts location information in PIDF LO format and processes both civic and geodetic inputs, normalizing location attributes when necessary to ensure routing decisions remain grounded in verified, governance-controlled information. This approach provides consistent interpretation of jurisdictional boundaries and helps ensure that calls are delivered to the correct responding agency.

GIS Data Versioning, Change Tracking, Import/Export, and Incremental Updates

To support agencies throughout the lifecycle of their spatial datasets, Allerium offers a complete framework for versioning, change tracking, import and export, and automated incremental updates. The platform accepts updates in NENA aligned formats and produces exports in schema compliant feature classes associated with NENA STA 006.2 2022. Differential update processing allows changes to be propagated to the ECRF and LVF without requiring full dataset reloads, reducing operational burden and preventing unnecessary service interruption. Historical datasets remain available for download, enabling local comparison, quality control, and rollback when required.

By combining authoritative data handling, structured validation, and a comprehensive lifecycle management approach, Allerium provides a GIS foundation that supports accurate, reliable, and operationally sustainable location-based routing across the NGCS environment.

3.1.4. Call Flow and Media Session Handling

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.

Response:

NENA i3 Call Flows, SIP Header Perseveration, and PIDF-LO Delivery

Allerium's NG9-1-1 platform is built around the full NENA i3 call flow model, ensuring that every call—beginning with the incoming SIP INVITE—progresses through ESRP/ECRF routing and on to the appropriate PSAP with accuracy, integrity, and transparency. This includes seamless support for integrated PSAP alternate routing.

In the end-state i3 environment, alternate routing relies on SIP SUBSCRIBE/NOTIFY queue subscription exchanges between the PSAP CHE and the ESRP. While CHE vendors across the U.S. continue building support for those capabilities, Allerium ensures uninterrupted operations today by embedding alternate routing logic directly within our NGCS. This approach allows each PSAP to benefit from resilient, standards-aligned routing while the broader ecosystem completes its adoption journey.

Throughout this call flow, Allerium preserves all required SIP signaling elements—including P-Asserted-Identity, Diversion, and History-Info—while ensuring PIDF-LO location information is delivered either by reference, by value, or both. Our NGCS also normalizes variations in incoming signaling from different service providers so that downstream PSAPs receive calls with clean, predictable, standards-compliant header values.

Real-Time Media and Supplemental Data Handling

Allerium supports the full suite of real-time media required for next-generation emergency communications, including voice, IP text-to-911, real-time text (RTT), and supplemental data. Our NG network performs media negotiation and fallback behaviors in accordance with NENA specifications, ensuring reliable delivery and consistent behavior across diverse endpoints and vendor implementations.

Looking forward, Allerium's product roadmap includes expanded support for live video and additional multimedia formats, aligning the platform with the evolving expectations of NG9-1-1 and the growing operational needs of PSAPs nationwide.

Call Transfer with Metadata and Location Preservation

PSAPs can rely on Allerium for smooth and standards-compliant call transfers—whether warm/attended transfers or blind transfers. When an i3 PSAP initiates a transfer via SIP REFER, Allerium's integrated conference and transfer engine adds the requested participant while preserving all call metadata, routing information, and the associated PIDF-LO location object. This ensures full continuity of context for the receiving agency and eliminates the data loss challenges common in legacy environments.

3.1.5. Security, Privacy, and Trust

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.

Response:

Allerium implements the NENA Emergency Services IP Network (ESInet) security and trust model with defined, implemented, and enforced Identity Access Controls across a managed IP network that carries 9-1-1 calls and data. The governing frameworks are the NENA i3 Standard (NENA-STA-010, now v3) and the NENA Security for NG9-1-1 Standard (NG-SEC, 75-001), with the PKI governed by the NG9-1-1 Interoperability Oversight Commission (NIOC).

Allerium follows the NENA ESInet layered Trust Model a defined hierarchy of Secure Boundary Elements.

1. **Network Segmentation and Boundary Control:** Enforced by the Border Control Function (BCF)
2. **Identity and Authentication:** Enforced by the PKI and mutual TLS
3. **Role-Based Access Control (RBAC):** Embedded in PKI certificates
4. **Inter-ESInet Routing Trust:** Enforced with PKI-verified participation
5. **Encryption of All Data in Transit and at Rest:** Mandatory per NENA NG-SEC

Allerium maintains an actionable Cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

The purpose of Incident Response (IR) policy is to establish a protocol to guide Allerium's response to a cyber-Cybersecurity incident.

- The Allerium Security Operations Center (SOC) operates both Endpoint Detection & Response (EDR) and Security Information & Event Management (SIEM) solutions to provide for broad infrastructure visibility and proactive protections of the digital infrastructure.
- The EDR solution provides for monitoring and response to threats on endpoints (e.g., laptops, servers, workstations, etc.).
- The SIEM solution allows for aggregating and analyzing security event data from various sources to provide for log management, event correlation, and threat detection.

Network vulnerability scans are performed monthly to determine existing vulnerabilities and to establish the current level of Cybersecurity risk associated with the environment and the technologies in use. The assessments employ external and internal vulnerability scanning techniques to provide customers with an understanding of the risks and Cybersecurity posture of their Allerium supported environment.

The scanning scope for this report includes the Allerium supported environment for XX customer. Scanning is performed using industry-standard vulnerability tools and frameworks.

- Vulnerabilities

- Cybersecurity Incidents
- Patching Status
- Scanning
- Compliance

Risk findings classification categories are used to determine appropriate and priority of remediation efforts:

- Critical
- High
- Moderate
- Low

3.1.6. Logging, Reporting, and Call Detail Records

6. *Logging, Reporting, and Call Detail Records*

- 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.*
- Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats.*
- Contractor shall provide operational reports (call volume, answer times, transfers, location failure rates, outage reports) and support ad-hoc queries.*

Response:

End-to-End Logging and CDR Production

Allerium approaches logging and call detail transparency as core pillars of a reliable NG9-1-1 environment. For every emergency transaction, Allerium generates full end-to-end logs and Call Detail Records (CDRs), capturing events at each functional element with precise timestamps. This comprehensive logging ensures that every component of the call path; routing, signaling, media, and metadata can be traced and correlated.

To support analytics, compliance, and operational insight, Allerium natively integrates with data analytics engines and includes all expected identifiers; correlation IDs, call identifiers, caller identity when available, location used for routing, destination PSAP, media types, and call disposition.

Because consistency is vital for downstream reporting, Allerium produces detailed data consumption guides and release-specific logging impact documents. These resources give analytics partners and state-selected vendors clear, predictable structures for ingesting Allerium logs and generating high-value insights for operational and administrative users.

Secure Storage, Role-Based Access, and Open-Format Export

Allerium ensures that all logs and CDRs are securely stored and accessible only through role-based access controls that align with industry best practices for identity and access management. Export capability is supported through open, standards-oriented formats, allowing seamless integration with the State's analytics environment and any preferred third-party tools.

This approach gives the State transparency, auditability, and secure control of all operational data without locking information into proprietary systems.

Operational Reporting and Ad-Hoc Query Support

Allerium supports the delivery of comprehensive operational reporting—call volumes, answer times, transfer activity, location success/failure metrics, and outage tracing—through established partnerships with analytics providers. In current NGCS markets, these capabilities are enabled through our long-standing collaboration with PSNA and their 911Logix platform.

For the State, Allerium would continue this model of seamless integration, supporting the selected analytics vendor and ensuring that all required reporting datasets and ad-hoc query capabilities are available. This approach preserves flexibility for the State while leveraging Allerium's proven interoperability with leading NG9-1-1 analytics solutions.

3.1.7. Interoperability, Testing, Conformance, and System Acceptance

7. *Interoperability, Testing, Conformance, and System Acceptance*
 - a. *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.*
 - b. *Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals.*

Response:

Allerium views interoperability of systems connect to the NG Core Services as essential. We have a history of ensuring solutions operate as expected for all expected parties and have also updated interfaces for conformance as necessary. Allerium intends to continue our focus on interoperability to ensure the State's solution remains reliable and operating as expected.

As service begins for the State, Allerium will review all parties connecting to the ESInet and NG Core. Connecting parties receive copies of Allerium's Interface Control Documents (ICDs) for review and discussion prior to connecting to the network. Allerium also maintains an interoperability lab leveraged to certify that the party meets expectations prior to connecting to production networks. Previously certified parties can leverage existing certifications while new parties enter a test cycle to confirm operation.

The interoperability testing process covers a range of parties including but not limited to OSPs, interconnected partners, third party service providers, and PSAP CHE. During interoperability sessions, Allerium works to validate the end-to-end call flow functions as expected, that signal paths look proper, and that media establishes as expected for all expected parties. Any conformance issues with interfaces discovered are remediated by the responsible party prior to test completion. Once all tests satisfy criteria, Allerium certifies the interface for the provider, and we proceed to connect to the production network.

The transition to live service also includes further validation that interoperability works as expected. Prior to turning service live, a pre-production acceptance test plan (ATP) is conducted to ensure all functions as expected.

Through our process of providing ICDs, interoperability certification, and acceptance testing, Allerium has successfully deployed and operated service for multiple NG Core networks. Production interoperability today includes interoperability between Allerium's solution and:

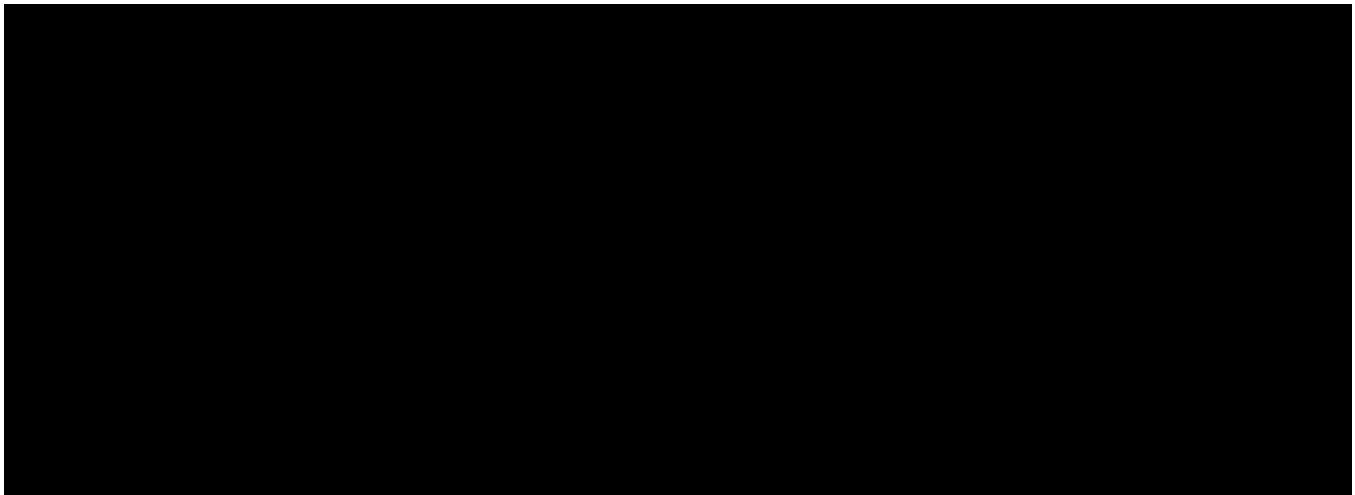
- OSPs,
- LDB providers,
- ECRF providers,
- LVF providers,
- LIS providers,
- ESInet to ESInet connectivity,
- Reporting / analytics providers,
- PSAP CHE providers.
- All aspects of the Allerium solution interoperate as expected. While all connected parties must interoperate as expected the PSAP CHE proves the most intricate due to PSAP data and integration demands.

Allerium has extensive experience interfacing with all types of CHE across its 1,000 plus PSAP deployments and has performed IOT with all major CHE manufacturers, including those deployed in the State:

- Allerium (Solacom),
- Intrado, and
- Motorola.

Allerium's systems have interfaced with the following CHE manufacturers and models in Table 26, all of which are currently operationally deployed within our NG9-1-1 deployments.

The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.



Allerium maintains a standing interoperability lab for testing our NGCS and ESInet solutions with other CHE manufacturers. The process for completing IOT with Allerium is as follows:

- Allerium provides an ICD, which details the needed network connection(s), SIP signaling commands, and general interaction through a variety of scenarios (e.g., call setup, call termination, call transfer, location queries, and associated functions).
- Allerium and the CHE manufacturer establish the needed network connection between the respective labs and schedule dedicated times for IOT with the CHE manufacturers.
- Allerium works with each manufacturer to define a mutually agreeable schedule and timeframe to conduct interoperability testing with all parties present.
- Allerium provides test result documentation to the CHE manufacturer at the conclusion of testing and works to resolve any discrepancies prior to certification.

As part of our normal installation process, we revalidate CHE functionalities checked in our interoperability lab to ensure no disruption of 9-1-1 service. After successful interoperability certification but prior to PSAP go live, Allerium conducts a PSAP-level final ATP to verify production configurations match test case scenarios. Our engineers validate expected call flows and features prior to migration of live traffic. Based on our experience, this additional process mitigates potential scheduling and operational impacts.

Allerium will participate in third party testing. The scope and additional costs are TBD.

Allerium provides the appropriate product and operational documentation as part of its ESInet/NGCS service.

3.1.8. Operational Support and Service Level Agreements (SLAs)

8. *Operational Support and Service Level Agreements (SLAs)*

- 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.*
- Contractor shall produce a rollback and contingency plan for major updates that affect routing/GIS or call handling.*

Response:

Allerium will partner closely with the PSC to collaboratively define, document, and implement Service Level Agreements (SLAs) that support operational stability, reliability, and the life-safety

mission of NG911 services. This process begins during onboarding and is refined through ongoing operational engagement.

SLA Definition and Governance

Allerium will work with the State to establish clear, measurable SLAs across key operational areas, including:

- Service availability and system uptime
- Incident response and notification timelines
- Escalation procedures and response thresholds
- Mean Time to Repair (MTTR) targets
- Change management processes and approval workflows
- Defined maintenance windows and notification requirements

These SLAs will be developed using Allerium's established best practices and informed by proven operational models currently in place across other NG911 markets. Allerium will ensure that all SLA definitions are realistic, measurable, and aligned with PSC expectations and operational priorities.

Once established, SLAs are formally documented and integrated into Allerium's operational processes, ITSM platform, and reporting structures to ensure consistent adherence and accountability.

SLA Adherence and Continuous Improvement

Allerium enforces SLA compliance through 24x7x365 NOC operations, structured incident management processes, and proactive monitoring and alerting systems. Performance against SLAs is continuously tracked and reported, with regular reviews conducted with the PSC to assess performance, identify trends, and implement improvements as needed.

This collaborative governance model ensures that SLAs remain aligned with evolving operational needs while maintaining high levels of service reliability.

Rollback and Contingency Planning

For all major updates—particularly those impacting routing, GIS, or call handling—Allerium develops and documents detailed rollback and contingency plans as part of the change management process.

These plans include:

- Defined backout procedures to restore prior system state
- Risk assessment and impact analysis
- Pre-change validation and testing requirements
- Post-change verification steps
- Clear decision points for rollback execution

All changes are governed through a formal Change Advisory Board (CAB) process, ensuring that rollback and contingency plans are reviewed, approved, and understood prior to implementation.

Through this structured, collaborative approach, Allerium ensures that SLAs are not only defined effectively but are consistently achieved, supporting the reliability and resilience required for public safety operations.

3.2. Applicable Standards

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.

Response:

Allerium and its subcontractors have proven experience with NG9-1-1 standards development organizations and professional organizations which are critical to NG9-1-1 understanding, solution design and development, and deployment execution.

Contributing to Industry Leading SDOs and Other Relevant Organizations

Our employees were among the leading contributors during the initial development of the NENA i3 standard and continue to actively participate in NENA STA-010.3 working group (WG) activities as well as parallel updates to NENA standards. Allerium and its subcontractors maintain membership, committee participation, chair, board, and advisory positions in the leading industry SDOs involved with emergency services and other relevant organizations, including, but not limited to:

- NENA,
- 3rd Generation Partnership Project (3GPP),
- Association of Public-Safety Communications Officials (APCO),
- Alliance for Telecommunications Industry Solutions (ATIS),
- CTIA—The Wireless Association,
- Emergency Services Interconnection Forum (ESIF),
- Federal Communications Commission (FCC),
- The Industry Council for Emergency Response Technologies (iCERT),
- Internet Engineering Task Force (IETF),
- NG9-1-1 Institute,
- The NG9-1-1 Interoperability Oversight Commission (NIOC), and the

- Urban and Regional Information Systems Association (URISA).

Such widespread participation allows Allerium to align with current applicable industry standards as well as leverage a realistic adoption and implementation plan to accommodate future updates independent of individual vendor processes. Our solutions can evolve quickly as technologies and standards are developed. Allerium carefully considers the impact of each new standard as it is published, after which Allerium makes appropriate updates and/or adjustments to its solutions as required.

Participating in and Reviewing Updated Standards

Because Allerium participates in the development of new NG9-1-1 standards, our solutions can evolve quickly as technologies and standards are developed. Allerium carefully considers the impact of each new standard as it is published, after which Allerium makes appropriate updates and/or adjustments to its solutions as required.

Once the Standards Development Organization (SDO) releases updated standards, our product and development teams start working towards inclusion of the required features if they do not exist. Generally, due to our active participation, we know about upcoming changes before the SDO releases an update and plan our development accordingly. We also work with industry partners to deliver updates to standards based functional elements (FEs). We address any new features for these FEs as the services are advanced from one NENA i3 version to the next.

Given that NENA, APCO, and other SDO standards are in a continuous state of update, refinement, and replacement, Allerium anticipates working with our customers on an ongoing basis to establish goals for adopting new NG9-1-1 standards and capabilities that may become the basis for future standards as they are incorporated within products from NG9-1-1 vendors, suppliers, and partners.

We believe maintaining standards compliance is imperative to ensuring and enabling support for full NG9-1-1 migration and the ever-advancing end state solution. This process includes inherent support for a wide array of existing and future technologies and services delivered within and outside of the ESInet, including video. This approach becomes even more important as interfaces extend beyond local, regional, and state jurisdictions to include interoperability and cooperation with regional and national agencies.

Testing, Implementing, and Migrating

As part of the capabilities of our NG9-1-1 solution and our ability to support evolving standards, Allerium operates multiple 9-1-1 research and development (R&D) and testing labs where our team deploys our equipment and software as well as those belonging to our industry partners to support a testing environment. We test new software, software updates, and functionality in these labs—as individual components and subsystems as well as the end-to-end solution—to ensure performance, reliability, and functionality.

Only after performing system engineering testing does Allerium recommend new software, hardware, services, and solutions to our customers. As updates are made to maintain industry standards compliance, Allerium's solution will support service or feature functionality in place at the time of the solution upgrade.

3.2.1. Federal Communications Commission Rules

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.

Response:

Allerium fully complies with all applicable Federal Communications Commission (FCC) rules governing 9-1-1, E9-1-1, Text to 911, and NG9-1-1 services, including those set forth in 47 CFR Part 9. These requirements form a foundational element of our NG9-1-1 design, implementation, and operational practices.

Our NGCS environment supports the FCC's expectations for:

- Transmission of all 911 calls,
- Delivery of caller identification (when available),
- Routing based on precise location information,
- Support for text and emerging multimedia communications, and
- Adherence to digital and IP-based system standards for reliability and public safety readiness.

Allerium's operational framework is built to align with FCC mandates for service continuity, network resiliency, and accurate location-based routing. These requirements are integral to our product development, system architecture, testing, and ongoing operational processes.

By maintaining this compliance posture, Allerium ensures that the State's NG9-1-1 ecosystem operates within the federal regulatory framework while supporting the level of reliability and service quality expected of public safety communications.

3.2.2. Other Industry Standards

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.*

Response:

Allerium's NG9-1-1 solution is designed and operated in alignment with the key industry standards and reference models identified by the State, including ANSI, EIA, IEEE, ISO, OSI, TIA, and UL. Allerium and its subcontractors have extensive experience working within NG9-1-1 standard development organizations and professional associations that are foundational to the design, implementation, and evolution of NG9-1-1 environments.

Participation in Industry-Leading Standards Organizations

Our employees were among the early contributors to the formation of the NENA i3 standard and remain active participants in the NENA STA-010.3 working groups and related standards updates. In addition, Allerium and its subcontractors maintain active membership, committee involvement, and advisory roles across the core industry bodies that directly influence emergency communications, including:

- NENA
- 3GPP
- APCO
- ATIS
- CTIA
- ESIF
- FCC
- iCERT
- IETF
- NG9-1-1 Institute
- NIOC
- URISA

This broad engagement keeps our teams closely connected to emerging changes in NG9-1-1 standards, technologies, and best practices.

Alignment With Open Standards Methodology

The Allerium NG9-1-1 solution utilizes an open standards methodology consistent with the RFP. Our system aligns with ITU frameworks, IEEE 802 specifications at OSI Layer 2, and the IETF-defined IP and TCP standards at OSI Layer 3 and above. These models are the foundation of the NGCS environment and guide our approach to design, integration, and interoperability.

If any components within the solution use proprietary methods, Allerium documents the scope and impact for customers, including any limitations that may result. This ensures transparency and helps partners understand how those components interoperate within the broader standards-based NG9-1-1 architecture.

Ongoing Standards Review and Adoption

Because Allerium participates directly in the development of new NG9-1-1 standards, our product and development teams begin evaluating upcoming requirements even before they are finalized by the standards bodies. As updated standards are released, Allerium reviews their impact, plans the necessary development work, and implements updates across the NGCS functional elements to ensure conformance.

We also work closely with our customers to define adoption strategies for new standards and capabilities as they become relevant across the NG9-1-1 ecosystem. This ensures agencies can plan transitions thoughtfully while maintaining operational continuity.

Testing, Implementation, and Migration Support

To ensure that solution updates remain aligned with evolving standards, Allerium maintains multiple 9-1-1 research, development, and testing lab environments. Within these labs, we deploy our NGCS equipment and software—as well as components from our partners—to validate new features, updates, and standards-driven changes both individually and across the full end-to-end solution.

Only after successful engineering testing does Allerium recommend the deployment of new software, hardware, or features. As standards evolve and systems mature, our customers can expect that upgrades will preserve existing service functionality while incorporating the required elements from updated standards.

3.3. Conformance to Standards

3.3.1. Baseline Conformance

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.

Response:

Allerium is fully committed to delivering a solution that meets the State's expectations for NENA standards adherence at System Acceptance. Our NG9-1-1 platform conforms with NENA-STA-010.3f for all interfaces facing PSAPs and originating service providers, and this level of conformance will be in place as system go-live.

Allerium also recognizes that full end-to-end compliance with STA-010.3f requires alignment across all notes in the call path, including PSAP's Call Handling Equipment (CHE) as outlined in section 4.6 of the Standard. In our nationwide deployments, we have seen the industry steadily advancing toward this end state - drive by the shared goal of improving interoperability and replacing legacy interfaces with true NG9-1-1 capabilities.

As the broader NG9-1-1 ecosystem continues to evolve, certain optional or emerging features (such as SIP SUBSCRIBE/NOTIFY - based events) are still maturing in the operational U.S. market. Allerium approaches these areas proactively and collaboratively. We have developed well-

established methods to ensure smooth ESInet and NGCS operations today, while maintaining full compatibility with the ultimate i3 architecture defined in STA-010.3f.

Our philosophy is simple: deliver full standards compliance where the ecosystem supports it today, while providing a clear, sustainable path that allows all partners - CHE vendors, PSAPs, Carriers and NGCS providers - to continue advancing toward complete i3 conformance together. This approach allows the State to move confidently into the NG9-1-1 operations without compromising on standards alignment, interoperability, or future readiness.

3.3.2. Gap Identification (Proposal Requirement)

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.

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.

Response:

In reviewing the requirement for gap identification against NENA STA 010.3, Allerium approaches this disclosure with the same transparency and rigor we apply to our standards work across the industry. While the standard represents an important end state for NG911, it continues to evolve, and many components remain in active development across the ecosystem. Within that context, our current implementation does not represent one hundred percent alignment with every element of STA 010.3. Instead, our focus has been on delivering functionality that supports reliable i3 aligned call routing today while preparing for the full capabilities defined in i3v3 as they mature.

Our platform has consistently operated in the spirit of the i3 architecture, and in several areas we have introduced practical enhancements that address real world gaps experienced by legacy and transition state OSPs and PSAPs. These solutions have allowed our customers to maintain operational continuity without waiting for broader ecosystem readiness. As the standard advances, we continue to adapt our capabilities so they reflect what the market can reasonably support while positioning our customers for long term architectural integrity.

Several elements of STA 010.3 remain dependent on external availability. Components such as the Forest Guide are not yet deployable in a production context, and other interfaces, including the Spatial Interface, are under active review across NENA working groups to determine the most efficient and sustainable path forward. Allerium tracks these developments closely through our staff who hold active roles in NENA, APCO, and other standards bodies. Their participation ensures our roadmap remains aligned with emerging requirements and industry direction.

As part of our commitment to the State, we will maintain regular roadmap review sessions to ensure ongoing visibility into progress and prioritization. These discussions provide a structured forum for continued collaboration as STA 010.3 capabilities mature and become achievable in a production environment.

The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.

3.3.3. Standards Updates (Post-Award)

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.

Response:

Allerium fully supports the State's requirement to adopt new or revised NENA standards and works proactively to ensure timely compliance with updates as they are finalized. In our experience, a nine-month window is generally sufficient for implementing minor version updates to relevant NENA standards. These types of revisions typically focus on incremental adjustments, clarifications, or refinements and can be incorporated into our development and testing cycles within the required timeframe.

For larger, more extensive standard revisions—such as transitions between major i3 versions (e.g., STA-010.3.x to STA-010.4)—Allerium conducts a structured evaluation of potential impacts before implementation. Major version updates may introduce significant changes that can affect backward compatibility, interface behavior, and end-to-end interoperability across the ecosystem. As part of our assessment, Allerium reviews:

- Potential risks to existing deployments,
- the degree of market adoption among connected systems,
- and the testing timelines required to confirm safe integration.

Allerium can begin development toward updated functionality within the nine-month window; however, successful, end-to-end adoption often depends on other systems connected to the ESInet—such as PSAP CHE, ADR interfaces, and other external components—also supporting the updated standard. We engage closely with partners and stakeholders to monitor readiness and coordinate transitions to ensure continuity for the State.

In keeping with the RFP, Allerium will provide regular progress reports as standards are revised so the State has clear visibility into timelines and development activity. If at any point we determine that a nine-month implementation window is not achievable due to the scope of the update or dependencies external to the NGCS, Allerium will promptly notify the State in writing and provide an adjusted schedule. Should circumstances require, Allerium will also submit a formal waiver request accompanied by an alternative approach and timeline for achieving full conformance.

Our commitment is to maintain a standards-aligned NG9-1-1 environment while ensuring that any transition to updated NENA requirements is executed with the care, testing, and transparency needed to support uninterrupted operations for the State's PSAPs.

3.3.4. Non-Disclosure and Breach

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.

Response:

Allerium accepts the non-disclosure and breach provisions as stated. Allerium has a strong track record of transparent communication with state and local government customers regarding conformance status and development timelines.

3.3.5. Deviation Classification (Proposal Requirement)

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 t/o the NENA-STA-010.3 feature may be proposed for State consideration.*

Response:

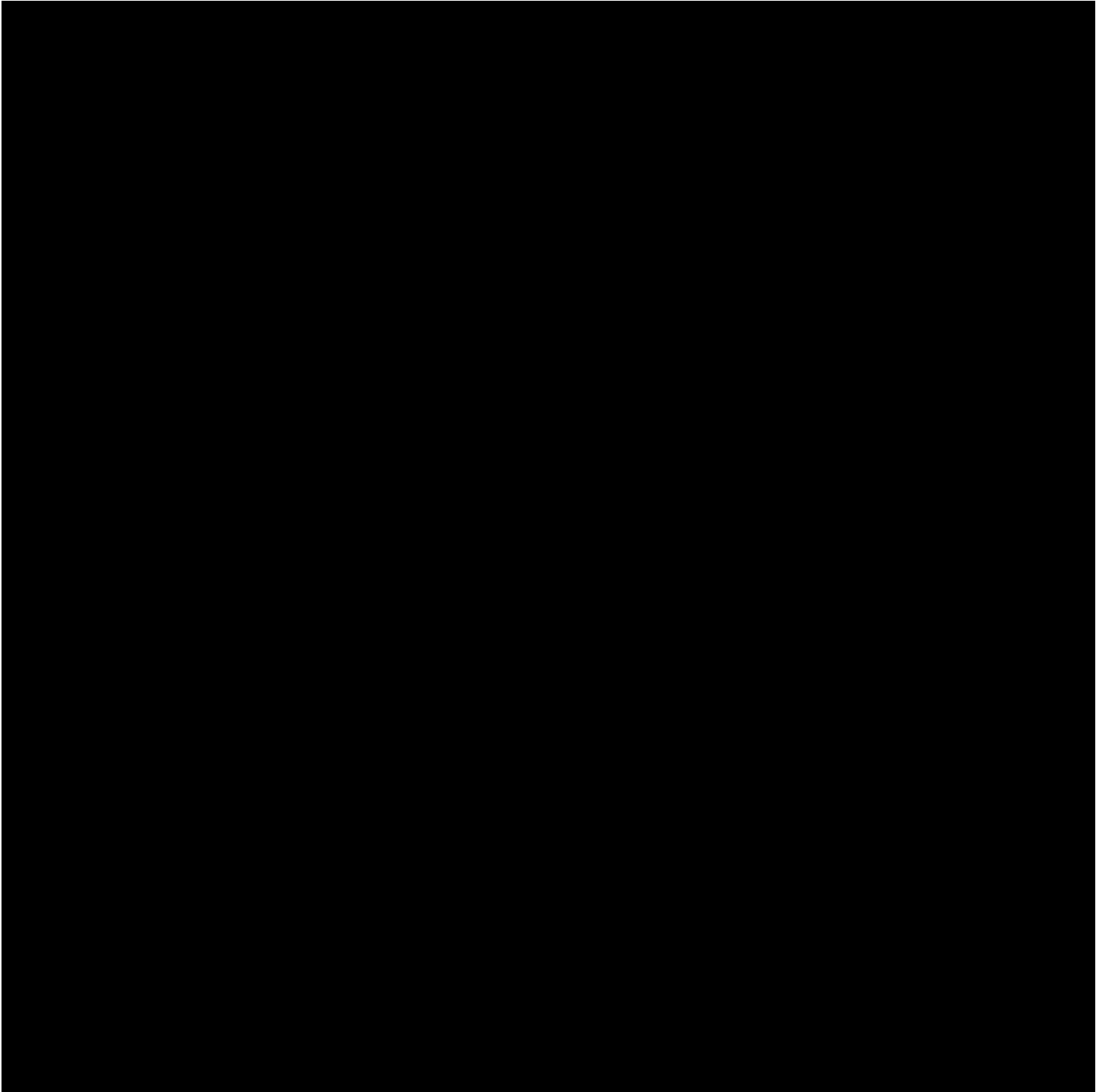
In reviewing the requirement for deviation classification against NENA STA 010.3, Allerium approaches this disclosure with the same transparency and rigor we apply to our standards work across the industry. While the standard represents an important end state for NG911, it continues to evolve, and many components remain in active development across the ecosystem. Within that context, our current implementation does not represent one hundred percent alignment with every element of STA 010.3. Instead, our focus has been on delivering functionality that supports reliable i3 aligned call routing today while preparing for the full capabilities defined in i3v3 as they mature.

Our platform has consistently operated in the spirit of the i3 architecture, and in several areas we have introduced practical enhancements that address real world gaps experienced by legacy and transition state OSPs and PSAPs. These solutions have allowed our customers to maintain operational continuity without waiting for broader ecosystem readiness. As the standard advances, we continue to adapt our capabilities so they reflect what the market can reasonably support while positioning our customers for long term architectural integrity.

Several elements of STA 010.3 remain dependent on external availability. Components such as the Forest Guide are not yet deployable in a production context, and other interfaces, including the Spatial Interface, are under active review across NENA working groups to determine the most efficient and sustainable path forward. Allerium tracks these developments closely through our staff who hold active roles in NENA, APCO, and other standards bodies. Their participation ensures our roadmap remains aligned with emerging requirements and industry direction.

As part of our commitment to the State, we will maintain regular roadmap review sessions to ensure ongoing visibility into progress and prioritization. These discussions provide a structured forum for continued collaboration as STA 010.3 capabilities mature and become achievable in a production environment.

The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.



3.3.6. Remediation Plan and Progress

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.

Response:

Allerium's remediation plan is included below. Allerium will provide:

- Quarterly updates to the remediation plan
- Continuous progress toward full NENA-STA-010.3 conformance
- Resolution of all identified gaps by end of Contract Year 2

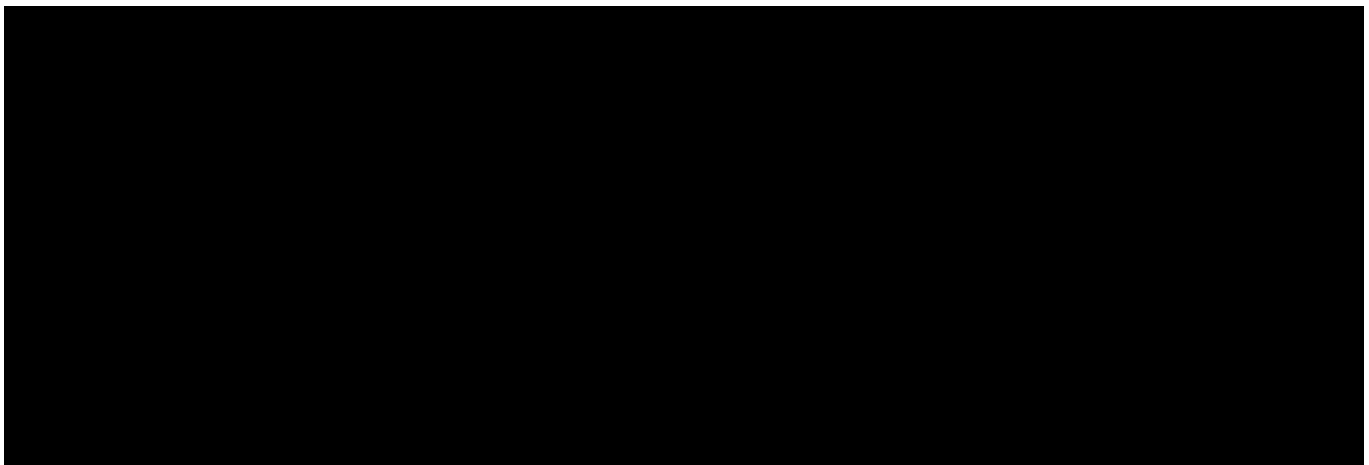
In reviewing the requirement for a remediation plan and progress against NENA STA 010.3, Allerium approaches this disclosure with the same transparency and rigor we apply to our standards work across the industry. While the standard represents an important end state for NG911, it continues to evolve, and many components remain in active development across the ecosystem. Within that context, our current implementation does not represent one hundred percent alignment with every element of STA 010.3. Instead, our focus has been on delivering functionality that supports reliable i3 aligned call routing today while preparing for the full capabilities defined in i3v3 as they mature.

Our platform has consistently operated in the spirit of the i3 architecture, and in several areas we have introduced practical enhancements that address real world gaps experienced by legacy and transition state OSPs and PSAPs. These solutions have allowed our customers to maintain operational continuity without waiting for broader ecosystem readiness. As the standard advances, we continue to adapt our capabilities so they reflect what the market can reasonably support while positioning our customers for long term architectural integrity.

Several elements of STA 010.3 remain dependent on external availability. Components such as the Forest Guide are not yet deployable in a production context, and other interfaces, including the Spatial Interface, are under active review across NENA working groups to determine the most efficient and sustainable path forward. Allerium tracks these developments closely through our staff who hold active roles in NENA, APCO, and other standards bodies. Their participation ensures our roadmap remains aligned with emerging requirements and industry direction.

As part of our commitment to the State, we will maintain regular roadmap review sessions to ensure ongoing visibility into progress and prioritization. These discussions provide a structured forum for continued collaboration as STA 010.3 capabilities mature and become achievable in a production environment.

The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.



3.3.7. Interoperability

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.*

Response:

Interoperability is a core principle of Allerium’s NG9-1-1 solution. Our NG Core Services are designed to interoperate with any system conforming to NENA-STA-010.3, and we treat interoperability assurance as essential to maintaining reliable end-to-end operations for all parties that connect to the State’s ESInet.

Allerium has a long history of validating interfaces, resolving conformance issues, and ensuring that systems from multiple vendors operate together as expected. As service begins for the State, Allerium will review all connecting parties and provide each with our Interface Control Documents (ICDs) for review prior to any integration work. These ICDs define signaling behaviors, call flows, and functional expectations that enable consistent, predictable interworking.

To support this process, Allerium maintains a dedicated interoperability lab used to certify compatibility before any system is allowed to connect to production networks. Previously certified partners can rely on existing certification records, while new parties enter a structured testing cycle where Allerium validates call flows, signaling paths, and media behavior across all required scenarios.

During interoperability sessions, Allerium confirms that end-to-end call handling functions correctly and that all relevant interfaces behave in accordance with the intent of NENA-STA-010.3. If interface issues arise, they are addressed by the responsible party before testing is finalized. Once a partner has met all test criteria, Allerium certifies the interface and supports its transition to the production environment.

Prior to live traffic, Allerium conducts a pre-production Acceptance Test Plan (ATP) to reconfirm interoperability and ensure production configurations match the certified behaviors. This process reduces operational risk and ensures PSAPs experience consistent performance on day one.

Allerium has successfully used this approach to establish interoperability across a wide range of partners, including:

- Originating service providers (OSPs),
- Location database and routing providers,
- ECRF and LVF providers,
- LIS providers,
- ESInet-to-ESInet connections,
- Reporting and analytics systems, and
- PSAP call handling equipment (CHE) vendors.

CHE interoperability is often the most complex area due to the depth of PSAP workflows and integration requirements. Allerium leverages its experience supporting more than 1,000 PSAP deployments and its ongoing CHE IOT efforts to validate call flows, transfers, location behavior, and associated functions across major CHE manufacturers.

The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.

Allerium's interoperability practices directly align with the RFP's expectations:

- If Allerium must make changes, we will provide the State with a proposed completion date.
- If the issue lies with the other vendor, Allerium will participate in testing but has no further responsibility.
- If the issue stems from 010.2 vs. 010.3 behavior outside backward-compatibility, Allerium is not required to make changes.

Through disciplined ICD management, structured certification, extensive IOT experience, and comprehensive pre-production testing, Allerium ensures that all connected components interoperate as expected and that the State's NG9-1-1 system maintains reliable, standards-aligned performance.

3.4. NENA NG911 i3 Standard Conformance

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

Remainder of page intentionally blank

Table 1: NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

		Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
v3 Standard Requirements	What Does It Do?	
<i>ElementState and ServiceState</i>	<i>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</i>	
<i>All i3v3 interfaces plus i3v2 for backwards compatibility</i>	<i>REST/JSON interfaces conforming to i3v3 standard YAML with backwards compatibility to the i3v2 SOAP/XML interfaces</i>	
<i>Security Posture</i>	<i>Allows routing rules to take security state (green/yellow/orange/red) into account</i>	
<i>IPv6</i>	<i>Allows every element to have a public address and get calls/data from modern nets (wireless) without translation</i>	
<i>DNS based redundancy model</i>	<i>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</i>	
<i>History Info/Reason</i>	<i>Provides a logged reason why a call was not delivered the "normal" way</i>	
<i>Video</i>	<i>Supports video calls to 911. Most importantly, allows deaf callers using VRS to be seen by call takers. Includes BCF, Bridge and logging service support</i>	

MSRP	Instant Messaging Service	
Non-Human Initiated Calls	Support for IoT devices, alarms, etc.	
TLS (Transport Layer Security) transport of SIP	Provides secure call signaling	
SRTP	Provides secure media (voice, video, text) for calls	
RTCP support on all SIP entities	Provides secure control of RTP (Real Time Transport Protocol) streams	
RTCP Extended Reports	Provides diagnostic information on media streams	
PSAP detection of loss of RTP vs silence	Differentiates silent calls from mechanical loss of audio media stream	
Element Overload (RFC 7339)	Graceful coping with too many SIP calls	
STUN/TURN/ICE	Standards based mechanisms for NAT Traversal	
NG-AACN Support	Update to Automatic Car Crash Notification standards	
SIP Presence for location	Allows OSPs to send location updates for mobile devices without manual rebid (requires OSP to implement also).	
Policy Store i3v3 interface	Interoperable policy repository that allows 3rd party editors/verifiers/etc.	
Multiple Geolocation	Accepts more than one location reported in a 911 call	
Discrepancy Reporting mechanism + i3v3 defined DRs (Discrepancy Report)	Standardized way to report discrepancies with standardized responses	
Bad Actor mechanism	Allows PSAP to stop repeated bad calls from a source	
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.)	
QueueState	Allows Policy routing based on queue congestion	
DequeueRegistration	Allows multiple PSAPs and other entities to dequeue from a queue	

ESRPnotify	Allows policy routing rule to notify some entity that a condition was encountered	
AbandonedCall	Standardized way to report a call that was hung up before PSAP got the call	
Service/Agency Locator	Service that allows discovery of things on any ESInet rather than provisioning it.	
XACML based data rights management	Standardized way to control who has access to what data	
EIDO on Transfer	Mehanism to transfer call state to a PSAP along with the call	
3rd Party Origination	Allows a 3rd party, like Video Relay Interpreter, to be automatically added to a call as a 3 way	
RTT	Real Time Text support, includes multiparty RTT (Real Time Text) support (RFC 9071) and mixer support for non-aware devices	
Resource Priority header	Allows SIP Resource Priority handling of SIP messages. All SIP entities support it, BCF polices/inserts it.	
Incoming Baudot is converted to RTT	TTY to/from OSP converted to Real Time Text by LNG (Legacy Network Gateway) (Baudot to RFC 4103)	
Outgoing Baudot is converted to RTT	TTY to/from PSAP converted to Real Time Text by LPG (Legacy PSAP Gateway) (Baudot to RFC 4103)	
Multipart MIME (BCF, bridge, media server)	Allows multiple SIP bodies. Typically, this is Location by Value plus SDP.	
SRV records for SIP interface resolution (BCF/ESRP and PSAP)	Standard mechanism to derive SIP connection address from a domain name	
Support for Outbound (RFC 5626)	SIP Protocol fixes for outbound calls	
i3v3 Syntax and Semantics for Policy Routing Rules	Standardized Syntax and Semantics for Policy Routing Rules	
SBC inserts NENA-Source parameter	Allows PSAP to identify which SBC (BCF component) handled a call. Used with Bad Actor	
ESRP supports AdditionalData dereference for PRR	Allows policy routing based on additional data	
ESRP handles incoming admin calls	Allows policy routing of admin calls	

ESRP policy routes calls to other agencies	Allows calls to other PSAPs, responders, to be policy routed. Includes extraction of location from an EIDO	
Support for incoming identity validation	STI-VS implemented to return STIR/SHAKEN validation on incoming calls.	
Gap/Overlap	Tells agencies about gap or overlap discovered by ECRF/LVF in GIS data	
ECRF handles any standard shape	Location can be specified by polygon, circle, ellipse, or arc band, in addition to point	
ECRF returns service boundary	ECRF can return a polygon, within which, the response will still be valid	
ECRF Supports lost-planned-changes	allows planned changes in GIS to occur on a schedule	
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	
i3v3 Appendix B/NG GIS implemented	Updated GIS provisioning data model	
Support CLDXF location	US profile of PIDF-LO, FGDC conformant.	
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	
ECRF/LVF replica support	Interface that allows an OSP or other entity to maintain a local copy of the ECRF/LVF	
Interconnected ESInet support	Allows neighboring ESInets to connect to the State ESInet. Supports bidirectional ECRF/LVF query, call transfer, etc.	
Forest Guide Support	Entry in FG for State ECRF/LVF, and recursive resolution of out of area queries via the FG	
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	

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	
MDS implemented	Map Database Service returns maps (as images) or features to support both local and out of area maps	
Spatial Interface is implemented	Standard was to provision ECRF/LVF/MDS/GCS/MCS	
Changes to PRR effective on next call	Update of PRR policy in Policy Store causes changes in routing immediately	
i3v3 DR interface and all defined DRs implemented	Automated Discrepancy Reporting mechanism and several standard DR formats	
i3v3 Test call is supported	Automated mechanism to test the call path. No human required. Includes media check (loopback)	
i3v3 Test Call Generator supported	Automated mechanism to generate test calls (can text PRR sets)	
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)	
humintlang tag supported	Signals request for language used on a call	
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	
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	
Media server supports i3v2 IMR	Standardized multimedia "Interactive Voice Response" unit (auto answer with menus). Includes audio, video, text, RTT. Includes VXML for control.	
Logging service supports all i3v3 LogEvents	Logging Service supports all i3 defined log events	
NGCS elements create the specified LogEvents	All NGCS elements generate all V3 standardized log events they should implement	
Logger logs media per the standard	Logging service logs all media per the standard	

Logger retrieval interface follows standard	Logging Service implements i3 standardized log retrieval interface	
Logger can be used as IRR (Instant Recall Recorder)	Logging Service implements the Instant Recall Recorder function	
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 Identity header	
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.	

Remainder of page intentionally blank

Response:

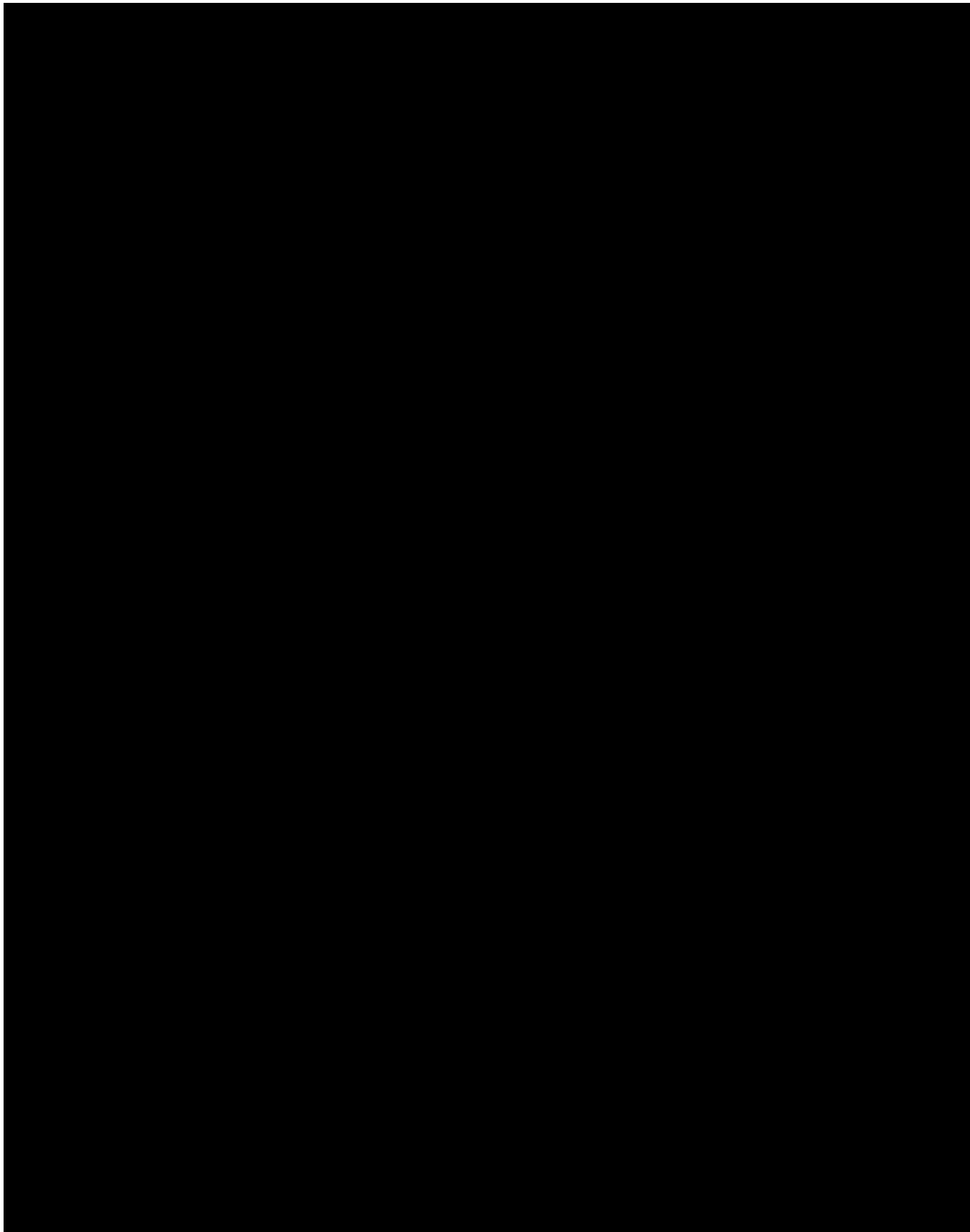
In reviewing the requirement for standard conformance against NENA STA 010.3, Allerium approaches this disclosure with the same transparency and rigor we apply to our standards work across the industry. While the standard represents an important end state for NG911, it continues to evolve, and many components remain in active development across the ecosystem. Within that context, our current implementation does not represent one hundred percent alignment with every element of STA 010.3. Instead, our focus has been on delivering functionality that supports reliable i3 aligned call routing today while preparing for the full capabilities defined in i3v3 as they mature.

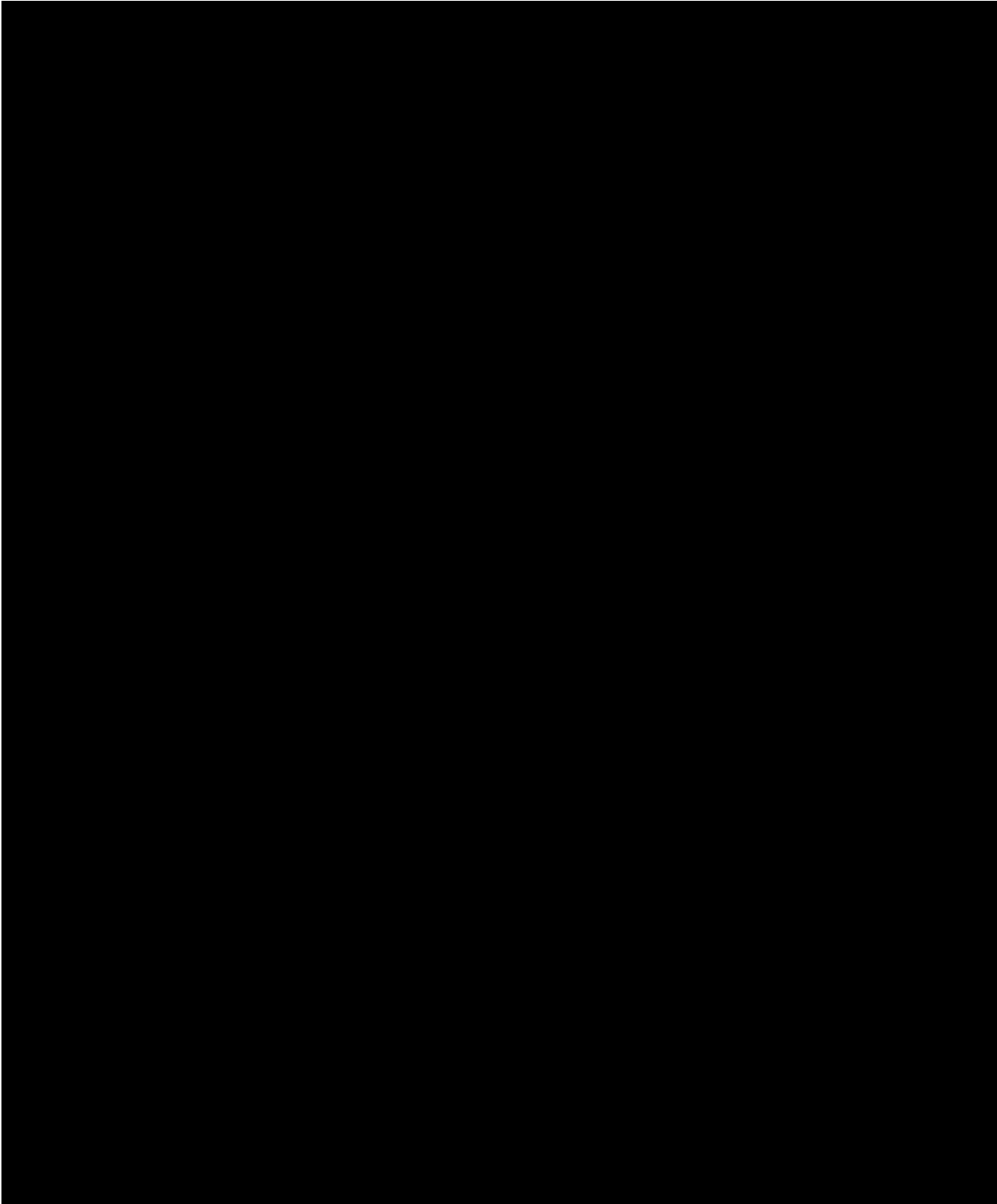
Our platform has consistently operated in the spirit of the i3 architecture, and in several areas we have introduced practical enhancements that address real world gaps experienced by legacy and transition state OSPs and PSAPs. These solutions have allowed our customers to maintain operational continuity without waiting for broader ecosystem readiness. As the standard advances, we continue to adapt our capabilities so they reflect what the market can reasonably support while positioning our customers for long term architectural integrity.

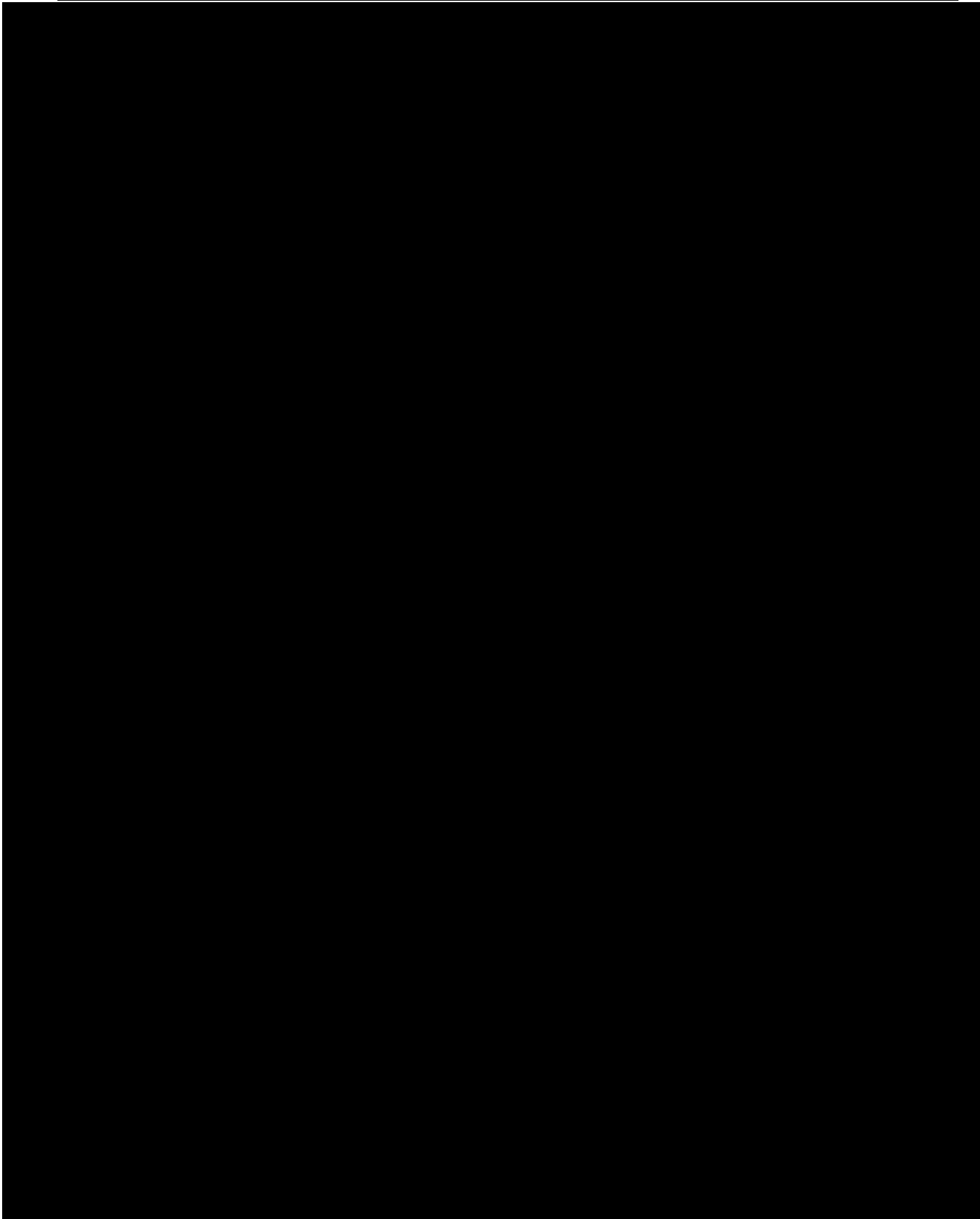
Several elements of STA 010.3 remain dependent on external availability. Components such as the Forest Guide are not yet deployable in a production context, and other interfaces, including the Spatial Interface, are under active review across NENA working groups to determine the most efficient and sustainable path forward. Allerium tracks these developments closely through our staff who hold active roles in NENA, APCO, and other standards bodies. Their participation ensures our roadmap remains aligned with emerging requirements and industry direction.

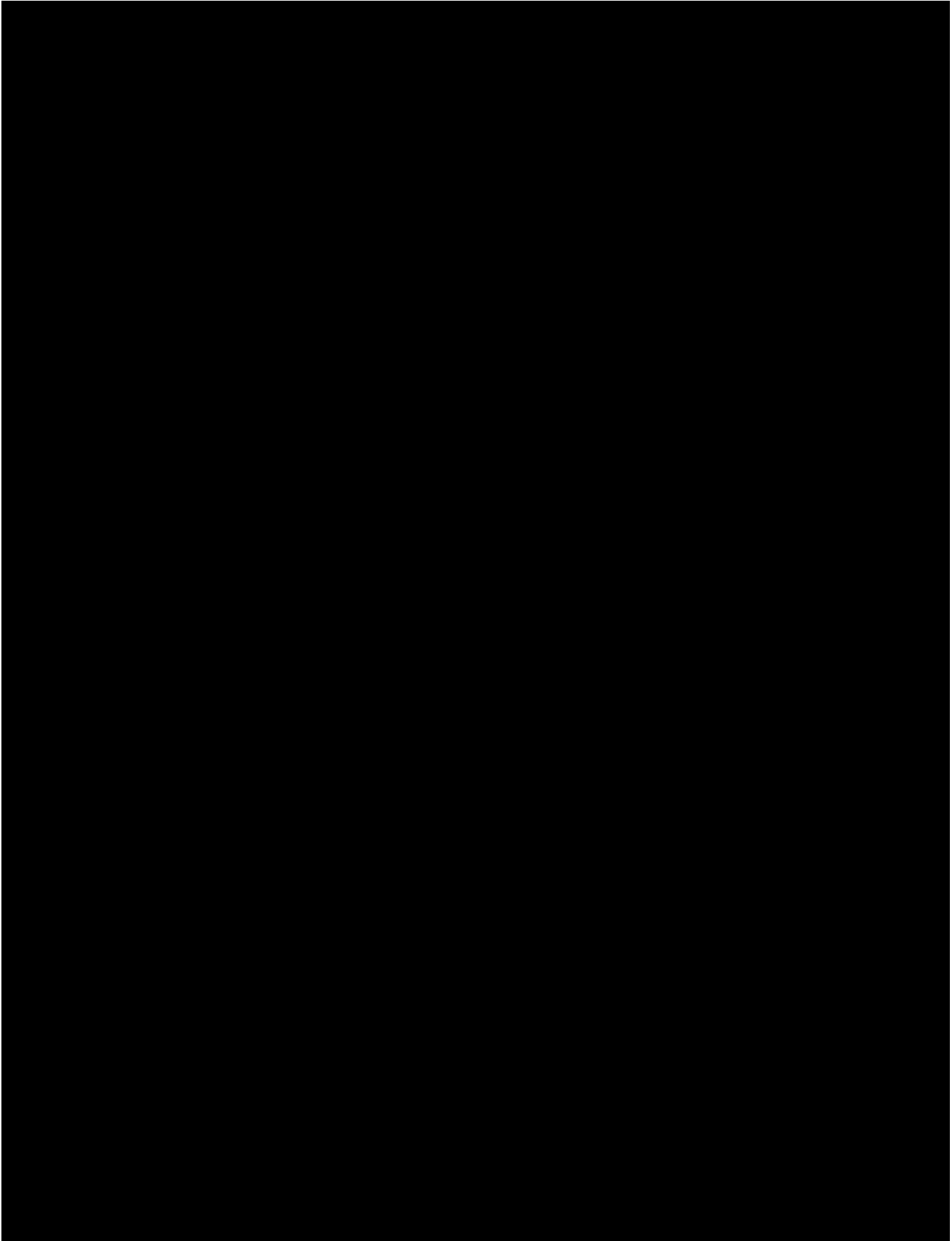
As part of our commitment to the State, we will maintain regular roadmap review sessions to ensure ongoing visibility into progress and prioritization. These discussions provide a structured forum for continued collaboration as STA 010.3 capabilities mature and become achievable in a production environment.

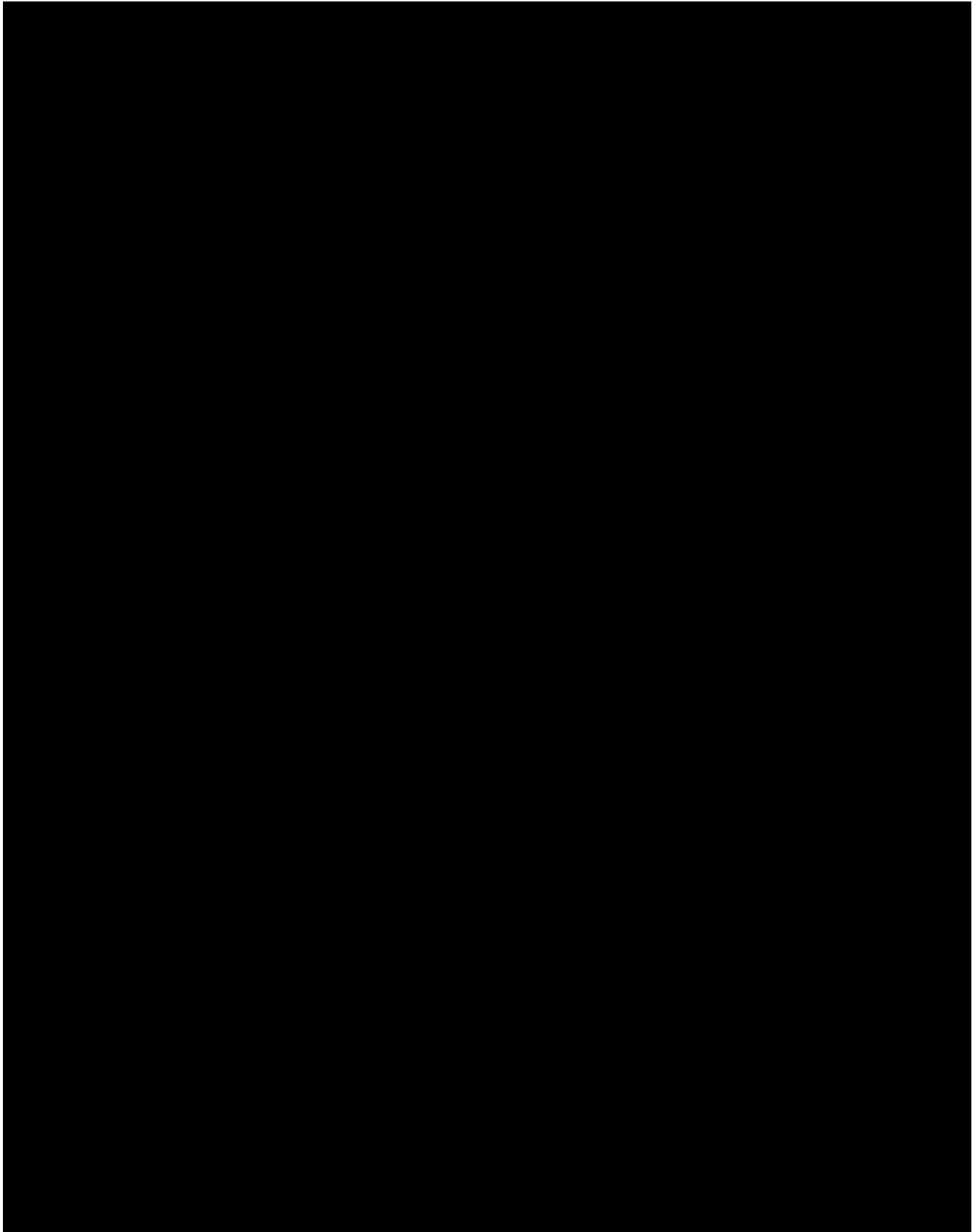
The following table is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.

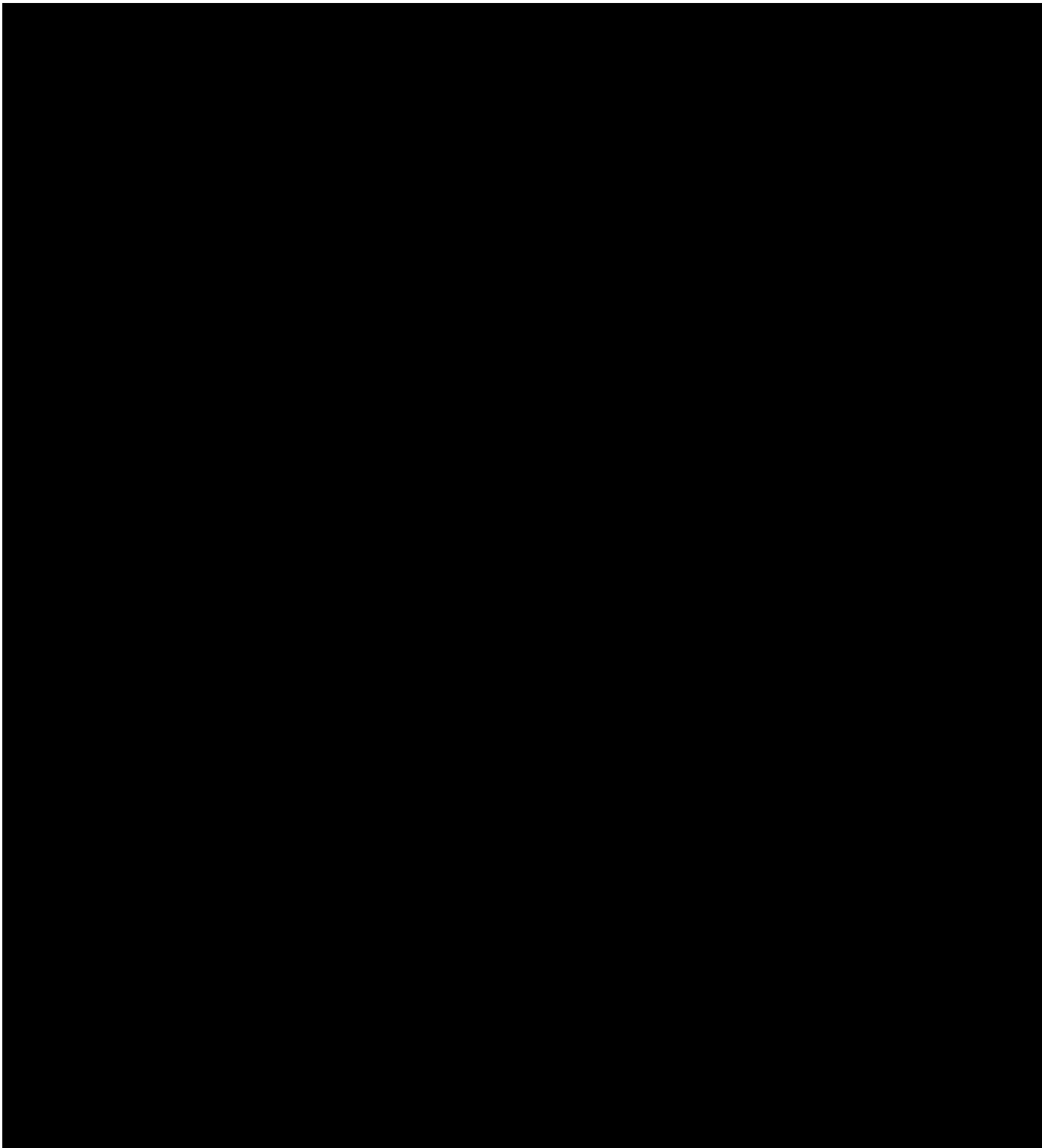












4. Response to Work Plan and Project Planning [Proposal Instructions, Section A.4 / Project Requirements and Scope of Work, Section C]]

4. RESPONSE TO WORK PLAN AND PROJECT PLANNING

Bidder should read the Work Plan and Project Planning Section of the RFP and provide a response as described in that section.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

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.

Response:

The following subsections describe the processes and documentation Allerium utilizes to communicate and execute the work plan for implementing NG9-1-1 services. Allerium delivers the work plan to the State in the form of Master Project Plan (MPP) document. The MPP is built specifically to each customer to meet the final negotiated Statement of Work (SOW) or scope of services. The MPP includes:

- Staffing models,
- Requirements/dependencies,
- Task lists,
- Project schedule,
- Testing methodologies, and
- Communication plans for project stakeholders.

4.1. Project Management [Project Requirements and Scope of Work, Section C.1]

4.1.1. Project Management Approach

1. Project Management

a. 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.

Response:

Allerium has extensive and diverse project and program experience managing large and complex NG9-1-1 projects since 2011, including:

- Performing multiple types of statewide deployments transitioning from legacy infrastructure to i3 solutions,
- Using regional/state sanctioned or owned networks in ESInet/NGCS deployments,
- Utilizing proven project/program management methodology based on ITIL, PMI, and industry best practices,
- Efficiently cutting over multiple PSAPs weekly (surge up to nine per week),
- Simultaneously conducting small and largescale NG9-1-1 deployment projects ranging from a dozen to 250 plus PSAPs supporting 15,000-13M population,
- Completing a 1.5M population deployment with 49 PSAPs six weeks ahead of schedule providing the customer with both facilities costs and resource savings, and
- Interoperating and managed third party component solutions and vendors.

Allerium adheres to rigorous project management, program management, and design planning methodologies to ensure smooth integration of the Next Generation 9-1-1 Services.

The Allerium Program Management Office utilizes rigorous and consistent methodologies across projects by following the Project Management Institute (PMI) standards as well as industry best practices.

Allerium documents project scope, schedule, and communications plans in a Master Project Plan (MPP) which is provided to the State for review and approval. Additional documentation such as Standard Operating Procedures (SOP), Change Management processes, user guides, and as built are provided to supplement the MPP where applicable.

4.1.2. Project Manager

b. 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.

Response:

Allerium provides four key points of contact for this project:

- **Program Manager:** Responsible for the overall program and contract deliverables for the duration of the service contract. The Program Manager serves as the primary point of contact for the State.

- **Program Director:** Leads the program management team in support of the State and serves as the Project Sponsor.
- **Project Manager:** Responsible for project planning, management, and Allerium resource coordination, throughout the project implementation.
- **NOC:** The Allerium NOC is available 24x7 for system monitoring and incident management throughout the life of the service.

The program manager is the primary single point of contact as that role stays with the customer for the life of the contract.

In addition to these contacts, Allerium provides resources with subject matter expertise in areas critical to project success. Functions supported by subject matter experts include:

- Implementation Management,
- GIS,
- Network Engineering,
- Systems Engineering,
- OSP migration,
- Reporting, and
- Training.

The following diagram provides an overview of Allerium's standard staffing plan.



Figure 11. Overview of Allerium's Standard Staffing Plan

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

c. 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. -*

Response:

As the contractor, Allerium provides a preliminary project plan in the form of an MPP. The MPP includes detailed project schedule which documents required tasks, ownership, deliverables, and acceptance criteria for all aspects of the implementation (e.g., PSAP-by-PSAP migration steps).

In addition to the project schedule, the MPP includes:

- Staffing models,
- Stakeholder communication plans,
- Risk management plans,
- Change management processes, and
- Additional materials to support a successful implementation.

The MPP and project schedule are updated throughout the project to reflect status, schedules, risks, and dependencies.

The project schedule is reviewed with the State on project status calls and available to the State via a secure document sharing portal.

4.2. Staffing and Qualifications [Project Requirements and Scope of Work, Section C.2]

4.2.1. Key Personnel

2. Staffing and Qualifications

a. 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.

Response:

Allerium has identified its key personnel for the State’s ESInet/NGCS project and provided resumes showing experience, qualifications, and relevant certifications.

Allerium’s key personnel are trained on the proposed Allerium system(s) and services and have personal experience supporting ESInet/NGCS deployments of similar size, scope, and complexity. Allerium’s key personnel resumes are included below and feature a list of the client projects supported by that individual. That list is provided for the purposes of illustrating their understanding of the process to NG9-1-1 as well as verifying experience, role/responsibility, and period of performance.

Allerium will collaborate with the State to review the list of key personnel and any subsequent changes. Allerium will provide 30 days’ written notice before a key person’s departure.

Table 32. Key Personnel Roster

Count	Name	Title	Project Role
1	Aaron Demorow	Vice President, Sys Engineering & Operations	Responsible for systems engineering & operations team
2	Ally Oughton	Senior Manager, Technical Communications	Training
3	Chris Hedges	Implementation & Support Manager	NOC, implementation management, PSAP deployments, cuts, and ATPs
4	Dave Wiegel	Senior Manager, Field Services	Field services
5	Elizabeth McMahon, PMP	Senior Project Manager	Project management
6	Eric Guerrero	Senior Vice President, General Manager	Executive sponsor
8	Greg Lathrop, PMP	Vice President, Implementation & Customer Experience	Program management
9	Jenn Richmond	Technical Program Manager	Coordinating data feeds to PSN Americas
10	Kenneth Banville	Divisional Information Security Officer	Security
11	Matt Davis	Technical Product Management Director	General NG9-1-1 standards support and product roadmap
12	Matthew Mullins	Principal Systems Engineer	Operational system design and engineering
13	Melissa Liebert, ENP, PMP	Manager, Geographic Information Systems	Responsible for GIS, sub DDTI, and providing DDTI training
14	Mike Wolfe	Program Manager	Program management

Count	Name	Title	Project Role
15	Neil Nyquist	Vice President, NOC & Field Services	Responsible for the NOC and field services teams
16	Patrick Hoover	Technical Program Manager	OSP migration
17	Patrick Melancon	Product Management Director	Overall product direction
18	Seth Wold	Sales Director	Sales management

Resumes

A sample of Allerium’s key personnel resumes are included below. Each team member offers relevant project/program experience and has contributed to multiple Allerium ESInet/NGCS deployments.

Aaron Demorow, Vice President, Systems Engineering & Operations

Aaron Demorow has over 15 years of experience in public safety software development and engineering support and leads the systems engineering & operations team responsible for the State’s project.

Table 33. Key Personnel Resume: Aaron Demorow

Resume: Aaron Demorow	
Title	Vice President, Systems Engineering & Operations: Responsible for leading our Systems Engineering & Operations teams to implement and support regional and statewide ESInet/NGCS implementations, including system deployment/testing, system upgrades/patches, system orchestration and deployment automation, systems engineering, telecom operations, interoperability testing, and RCA support.
Education	Associate degree, Network and Computing, National Institute of Technology, 1998-2000
Work Experience	- Allerium/Comtech, Vice President, Systems Engineering & Operations, Aug 2025-Present - Comtech, Director, Operations, Aug 2021-Aug 2025 - Comtech/TeleCommunication Systems, Inc., Senior Manager, NG9-1-1 Operations, Mar 2016-Present - TeleCommunication Systems, Inc., QA Manager, Mar 2013-Mar 2016 - Christian Faith Center, IT Director, Jul 2007-Mar 2013 - TeleCommunication Systems, Inc., Lead QA Engineer, Jan 2004-Jul 2007
Relevant Certifications and Licenses	N/A.
Years Working with NG9-1-1	Since 2013.

Resume: Aaron Demorow	
Systems and Technologies	Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, St. Louis County (Missouri), Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	- Gregory R. Kline, Deputy Director for 9-1-1, 9-1-1 Office, Pennsylvania Emergency Management Agency, 1310 Elmerton Avenue, Harrisburg, PA 17110, 717.651.2218, gregkline@pa.gov - Christy Williams, 9-1-1 Director, NCT9-1-1, 600 Six Flags Drive, Arlington, TX 76011, 817-695-9204 - Theresa Fazekas, Chief Financial Officer, Christian Faith Center, 33645 20th Ave S, Federal Way, WA 98003, 253-943-2400

Ally Oughton, Senior Manager, Technical Communications

Ally Oughton has over 19 years' experience in 9-1-1 technical communication and customer training and leads a team of technical writers, instructional designers, trainers, and document control experts to ensure the timely delivery of documentation and training for products and services under the wireless, VoIP, and NG9-1-1 product lines.

Table 34. Key Personnel Resume: Ally Oughton

Resume: Ally Oughton	
Title	Senior Manager, Technical Communications: Responsible for leading a Technical Communication program that provides mission-critical communication products and services for public safety, government entities, and carriers; and managing a team of technical writers, instructional designers, trainers, and document control experts to ensure the timely delivery of documentation and training for products and services under the wireless, VoIP, and NG9-1-1 product lines.
Education	Bachelor of Arts, English Major (writing concentration)/Computer Science Minor (technical writing and web development)
Work Experience	- Allerium/Comtech, Senior Manager, Technical Communications, Aug 2021-Present - Comtech, Technical Communications Manager, Apr 2015-Aug 2021 - Comtech/TeleCommunication Systems, Inc., Technical Communication Consultant, Next Generation Call Handling Division, Apr 2014-Apr 2015 - TeleCommunication Systems, Inc., Technical Communication Manager, Wireless Location and E9-1-1 Products & Services, Apr 2008-Apr 2012 - TeleCommunication Systems, Inc., Lead Technical Writer, Commercial Location Platforms, Dec 2002-2008 - Seattle Publishing, Inc., Technical Writer, 2002
Relevant Certifications & Licenses	N/A.

Resume: Ally Oughton	
Years Working with NG9-1-1 Systems & Technologies	• Since 2014. • Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium’s State of Arizona, State of Iowa, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.

Chris Hedges, Implementation & Support Manager, Allerium

Chris Hedges leads the end-to-end deployment of NG9-1-1 solutions—including call handling systems, CAD integrations, GIS components, and ESInet connectivity—for the State’s project.

Table 35. Key Personnel Resume: Chris Hedges

Resume: Chris Hedges	
Title	Implementation & Support Manager: Responsible for leading the end-to-end deployment of NG9-1-1 solutions, including call handling systems, CAD integrations, GIS components and ESInet connectivity; coordinating project timelines, milestones, and resource planning across internal teams, vendors, and public safety agencies; translating PSAP operational needs into technical requirements and ensuring solutions meet state and national NG9-1-1 standards; overseeing system configuration, testing, validation, cutover planning, and go live support; and managing risk mitigation, change management, and quality assurance throughout all project phases. Also: • Serves as the primary escalation point for PSAPs and internal teams for technical or operational issues and ensures uptime, performance monitoring, and adherence to Service Level Agreements (SLAs). • Builds strong relationships with PSAP leadership, IT teams, emergency communications staff, and external partners. • Communicates project status, risks, and updates to managers, executives, and agency stakeholders. • Facilitates training and knowledge transfer for new deployments, upgrades, or major system changes.
Education	AS, Computer Science, ITT Technical Institute, 2010-2012
Work Experience	• Allerium, Implementation and Support Manager, July 2025-Current • Sky Unlimited, IT Administrator, May 2024-July 2025 • Camaro Central, IT Administrator, June 2021-May 2024 • AK Associates, 911 Engineer, May 2012-June 2021
Relevant Certifications and Licenses	N/A.
Years Working with NG9-1-1 Systems and Technologies	• Since 2012. • Regional 9-1-1 network deployments in Kentucky and Ohio. • Multiple Kentucky standalone CHE deployments.

Resume: Chris Hedges	
	Deployment of Allerium NG9-1-1 ESInet for Kentucky and South Carolina.
References	- Criss Chancellor, Service Manager, AK Associates, 7 Independence Ave, Derry, NH 03038, 603-490-5684 - Mark Greenthaner, Systems Integrations Engineering Manager, Axon, 640 Theresia Street, St. Marys, PA 15857, (814) 389-8584 - Chadd Friedman, PMO Coordinator, DATAMARK Technologies, 2323 W Fifth Ave, Ste 140, Columbus, OH 43204, 614-429-3384

Dave Wiegel, Senior Manager, Field Services, Allerium

Dave Wiegel is responsible for the management and oversight of the Allerium field organization, including both in-house field technicians as well as on-demand third party technicians through our partner program.

Table 36. Key Personnel Resume: Dave Wiegel

Resume: Dave Wiegel	
Title	Senior Manager, Field Services: Responsible for management and oversight of 21 field technicians supporting numerous NG911 programs. Technicians cover program items such as site surveys, installation / maintenance as well as 24/7/365 break-fix work.
Education	BS, Electrical Engineering – Milwaukee School of Engineering 1987-1991
Work Experience	- Allerium/Comtech, Senior Manager, Field Services, July 2022-Present - Understory, Field Operations Manager / Administration Lead, 2021-2022 - CivicSmart, Director of Operations, 2018-2021 - CenturyLink, Manager, Field Operations, 2012-2018 - CenturyLink, Sr / Central Office Engineer, 2006-2012 - AT&T Wireless, Transport Planner 4, 2004-2006 - TEKsystems, Transport Planner, 2003-2004 - AT&T Wireless, Network Engineering Manager, 2001-2002 - AT&T Wireless, Acting Operations Manager, 2000 - AT&T Wireless, Translations Engineer, 1996-2001 360 Communications, Translations Engineer, 1994-1996 360 Communications, Cellular Engineer, 1992-1994
Relevant Certifications and Licenses	- Amateur Radio, Technician Class (N9KNX), 1990-Present - Amateur Radio Relay League, Emergency Coordinator, Washington County, WI, 2025-Present
Years Working with NG9-1-1 Systems and Technologies	- Since 2022. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium’s State of Arizona, Commonwealth of Kentucky,

Resume: Dave Wiegel	
	Commonwealth of Massachusetts, St. Louis County (Missouri), State of Iowa, State of Ohio, and State of South Carolina projects.
References	• Molly Falls, Director of Partnerships, RapidSOS, 3 Park Ave, New York, NY 10016, 720-378-3930 • Michael Ball, NG9-1-1 Project Manager, SC Revenue and Fiscal Affairs Office, 1000 Assembly St, 4th Floor, Columbia, SC 29201, 803-734-2374 • Don Ehnert, Senior Network Engineer, Froedert Health, 8700 Watertown Plank Rd, Milwaukee, WI 53226, 262-993-0050

Elizabeth McMahon, Senior Project Manager, Allerium

Elizabeth McMahon, PMP leads the planning and execution of mission-critical public safety projects, including managing resources, schedules, budgets, and communications to ensure the successful delivery of NG9-1-1 programs.

Table 37. Key Personnel Resume: Elizabeth McMahon, PMP

Resume: Elizabeth McMahon, PMP	
Title	Senior Project Manager: Responsible for the planning, coordination, and execution of complex deployment activities for internal and external clients, ensuring alignment with scope, budget, and timeline objectives. Direct multiple concurrent projects facilitating customer-facing meetings and technical updates to drive transparency and accountability. Manage cross-functional initiatives by identifying risks, developing mitigation strategies, and aligning team efforts with strategic goals. Develop and maintain project documentation, including playbooks, dashboards, and ISO-compliant artifacts to ensure repeatable, high-quality delivery. Collaborate with customers and internal stakeholders to define requirements, establish incremental delivery plans, and track progress. Create and present executive-level project updates. Provide leadership to project teams, fostering continuous improvement through lessons learned and process enhancements. Support NG9-1-1 system integration efforts by coordinating with subcontractors and technical leads. Ensure adherence to quality standards while resolving issues efficiently to minimize impact on operations. Maintain strong stakeholder relationships through proactive communication, education, and engagement.
Education	BS, Chemistry, University at Buffalo, 1992-1997
Work Experience	• Allerium/Comtech, Senior Project Manager, July 2025-Present • Windstream, Program Manager, Oct 2021-July 2025 • Windstream, Project Manager, April 2019-Oct 2021 • Xerox, Program Manager, July 2012-Dec 2018 • Xerox, Buyer/Planning, Jan 2005-July 2012
Relevant Certifications & Licenses	PMP certified in Mar 2024.

Resume: Elizabeth McMahon, PMP	
Years Working with NG9-1-1 Systems & Technologies	- Since 2019 beginning with in a supporting role on a Commonwealth of Massachusetts project while working at Windstream. - Supporting statewide NG9-1-1 projects in the Commonwealth of Kentucky and State of South Carolina, a Policy Store project for the State of Ohio, and the State of Iowa data center migration.
References	- Mike Mundorff, Senior Global Customer Relationship Manager, Uniti Group, 2101 Riverfront Drive, Little Rock, AK 72202, (585) 737-9098 - Candace Figueroa, Technical Project Manager, Cato Networks, 3031 Tisch Way, 110 Plaza West, San Jose, CA 95128, (860) 808-8326 - Ken Hunter, Lead Network Architect, Avis Budget Group, 6 Sylvan Way, Parsippany, NJ 07054, (516) 477-9572

Eric Guerrero, Senior Vice President, General Manager, Allerium

Eric Guerrero has over 20 years of experience starting as a first responder and dispatcher before serving in various leadership roles in public safety technology. Eric is the executive leader over the NGCS business at Allerium and will be the executive sponsor for the State's project.

Table 38. Key Personnel Resume: Eric Guerrero

Resume: Eric Guerrero	
Title	Senior Vice President, General Manager: Responsible for overall business performance and ownership of our E9-1-1 and NG9-1-1 call routing solutions and implementations for states, local jurisdictions and OSPs.
Education	- Master of Business Administration, Colorado State University, 2006-2008 - Bachelor of Science, Business Administration, Colorado Christian University, 2005
Work Experience	- Allerium/Comtech, Senior Vice President, General Manager, March 2025-Present - Comtech, VP, Program Management, Jan 2023-March 2025 - Comtech, Vice President, Service Delivery, May 2022-Jan 2023 - Enavate, Managing Director, Dec 2019-May 2022 - Cascade Healthcare Services, Chief Operating Officer, Mar 2017-Dec 2019 - Intrado, Vice President, Operations, Jun 2014-Mar 2017 - Intrado, Senior Director, Operations, Mar 2012-Jun 2014 - Intrado, Director, Account Management (Customer Team), May 2009-Mar 2012 - Intrado, Senior Program Manager, Sept 2006-May 2009
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1	14 years. - Supporting multiple regional/statewide NG9-1-1 deployments, including Allerium's State of South Carolina, State of Iowa, Commonwealth of Kentucky,

Resume: Eric Guerrero	
Systems & Technologies	Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of Arizona, North Central Texas Region, State of Ohio, St Louis County, MO, and State of Washington projects.
References	- Paul Athey, Mapping & Operations Division Director, South Carolina Revenue and Fiscal Affairs (RFA) Office, 1000 Assembly St, 4th Floor, Columbia, SC 29201, 803.734.3789 - Greg Denton, 9-1-1 Program Administrator, Arizona Strategic Enterprise Technology (ASET) Public Safety State 9-1-1 Program, Arizona Department of Administration, 480.280.7171 - Christy Williams, 9-1-1 Director, NCT9-1-1, 600 Six Flags Drive, Arlington, TX 76011, 817-695-9204

Greg Lathrop, PMP, Vice President, Implementation & Customer Experience, Allerium

Greg Lathrop, PMP is responsible for the overall program management (e.g., project, deployment, ongoing lifecycle) for multiple states and well versed in Allerium's NG9-1-1 systems and services.

Table 39. Key Personnel Resume: Greg Lathrop, PMP

Resume: Greg Lathrop, PMP	
Title	Vice President, Implementation & Customer Experience: Responsible for the overall program management (e.g., project, deployment, ongoing lifecycle) for multiple Comtech clients, including the State of Arizona, State of Iowa, North Central Texas Emergency Communications District (NCT9-1-1), Commonwealth of Pennsylvania, and State of Washington.
Education	B.S., Business Administration, Central Washington University, 1996-2001
Work Experience	- Allerium/Comtech, Vice President, Implementation & Customer Experience, Apr 2026-Present - Allerium/Comtech, Senior Director, Programs, Aug 2025-Apr 2026 - Comtech, Director, Programs, Dec 2019-Aug 2025 - Comtech/TeleCommunication Systems, Inc., Senior Program Manager, Emerging Technologies, Aug 2017-Dec 2019 - TeleCommunication Systems, Inc., Program Manager, Emerging Technologies, Jun 2014-Aug 2017 - TeleCommunication Systems, Inc., Senior 9-1-1 Deployment Manager, Aug 2010-Jun 2014 - TeleCommunication Systems, Inc., 9-1-1 Deployment Manager, Apr 2007-Aug 2010 - TeleCommunication Systems, Inc., Data Analyst, Feb 2004-Apr 2007 - Northwest Embroidery, Office Manager, Feb 2002-Feb 2004
Relevant Certifications and Licenses	PMP certified.

Resume: Greg Lathrop, PMP	
Years Working with NG9-1-1 Systems and Technologies	• Since 2019. • Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, North Central Texas Emergency Communications District (NCT9-1-1), Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	• Greg Denton, 9-1-1 Program Administrator, Arizona Strategic Enterprise Technology (ASET) Public Safety State 9-1-1 Program, Arizona Department of Administration, 480.280.7171, greg.denton@azdoa.gov • Gregory R. Kline, Deputy Director for 9-1-1, 9-1-1 Office, Pennsylvania Emergency Management Agency, 1310 Elmerton Avenue, Harrisburg, PA 17110, 717.651.2218, gregkline@pa.gov • Jonathan H. Brock, Deputy State 911 Coordinator / ESF-2 Lead, Emergency Management Division, Washington State Military Department, 253.223.3971, jonathan.brock@mil.wa.gov

Jenn Richmond, Technical Program Manager, Allerium

Jenn Richmond has a background in ALI data and application management as well as Data Analytics and Reporting. She works closely with the State, vendors, and internal SMEs to support successful communication and completion of reporting deliverables and training.

Table 40. Key Personnel Resume: Jenn Richmond

Resume: Jenn Richmond	
Title	Technical Program Manager: Responsible for facilitating the data exchange, application installation and data validation as it relates to ALI and Reporting analytics platforms. Working with both internal and external resources to ensure processes are established for data delivery from the Call Handling vendor and the NGCS through to the Analytics and Reporting applications as appropriate.
Education	Associate's in business, Front Range Community College, 2005-2007
Work Experience	• Allerium/Comtech, Technical Program Manager, Jan 2023-Present • Juvare, Product Manager, Sept 2021-Jan 2023 • Juvare, Product Owner, Feb 2021-Sept 2021 • Corvena, Product Manager, Feb 2020-Feb 2021 • Corvena, Technical Project Manager, June 2017-Feb 2020 • West Safety Services (Intrado), Quality Management Specialist, April 2016-Jun 2017 • West Safety Services (Intrado), Associate Quality Management Specialist, May 2013-April 2016 • Intrado, Senior Data Analyst, Dec 2010-May 2013 • Intrado Data Analyst, Dec 2006-Dec 2010

Resume: Jenn Richmond	
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	12 years working on NG9-1-1 products, projects, and deliverables. 13 years working in application management for emergency management reporting and 9-1-1 data management, reporting, and analytics. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, Commonwealth of Kentucky, Commonwealth of Massachusetts, North Central Texas Emergency Communication District, State of Ohio, Commonwealth of Pennsylvania, State of South Carolina, St. Louis County, Missouri, and State of Washington projects.
References	- Molly Falls, Director of Partnerships, RapidSOS, 3 Park Ave, Floor 22, New York, NY 10016, 720-378-3930 - Jeff Telford, VP of Product Management, Juvare, 235 Peachtree Street NE, Suite 2300, Atlanta, GA, 30346, 678-773-2776 - Alexander Warner, Chief Operating Officer, PSN Americas, 3626 N Hall St, Ste 406, Dallas, TX 75219, alex@psnamericas.com, 305-496-5068

Kenneth Banville, Divisional Information Security Officer

Kenneth Banville has over 30 years' experience in information technology (IT), engineering, and security and oversees our security team responsible for supporting 9-1-1 customers.

Table 41. Key Personnel Resume: Kenneth Banville

Resume: Kenneth Banville	
Title	Divisional Information Security Officer: Responsible for Allerium's security policies, maintaining both physical and cyber security standards and policies, and overseeing our security team that supports our 9-1-1 customers.
Education	- Bachelor of Science, Business Administration, University of Phoenix, 2007-2009 - Associate of Information Technology, Western International University, 2005-2007 - Certificate in Computer Systems Specialist, Northeastern University
Work Experience	- Allerium/Comtech, Divisional Information Security Officer, Nov 2021-Present - Comtech, Senior Systems Architect, NG9-1-1 Systems, May 2019-Nov 2021 - GDIT, Systems Architect, Oct 2016-Apr 2019 - GDIT, Senior Principal Engineer, Oct 2009-Oct 2016 - GD through Insight Global, Unix Consultant, Feb 2009-Oct 2009 - Anacomp, Senior System Engineer, Jun 2001-Feb 2009 - Integrated Network Technology, Unix Consultant, Mar 2000-Jun 2001 - Star Market Co., Unix Systems Administrator, Oct 1996-Mar 2000 - Star Market, In-Store Systems Analyst, Mar 1996-Oct 1996

Resume: Kenneth Banville	
	- Marshalls, Programmer Analyst I, Apr 1995-Mar 1996 - Marshalls, Senior Helpdesk Analyst, Jun 1992-Apr 1995 - Marshalls, Computer Operator, May 1990-May 1992
Relevant Certifications & Licenses	Active DoD Top Secret security clearance.
Years Working with NG9-1-1 Systems & Technologies	- Since 2016. - Overseeing a security team that supports all 9-1-1 customers, including Allerium's State of Arizona, State of Iowa, Commonwealth of Massachusetts, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.
References	- Charles Ashworth, System Analyst, Massachusetts State 911 Department, 151 Campanelli Drive, Suite A, Middleborough, MA 02346, 774-210-0911, charles.ashworth@state.ma.us - Frank Loulourgas, Hoplite Tech, LLC, 3 Valley Road, Norfolk/Dover, MA 02030, 617-780-9406 - Oscar Marcia, Eonti, 1345 Plaza Court North, Suite 3A, Lafayette, CO 80026, 720-470-9294

Matt Davis, Technical Product Management Director, Allerium

Matt Davis has over 24 years of experience in the IT industry, with 16 years specifically dedicated to public safety and NG9-1-1. Matt has held roles within many Allerium functional departments, including NG9-1-1 Operations, Application Engineering Management, Quality Assurance, Systems Engineering, and Product Management. Matt has provided support for all of Allerium's NG9-1-1 solutions and currently serves as the Technical Product Management Director for Allerium's NGCS and NG9-1-1 location platforms.

Table 42. Key Personnel Resume: Matt Davis

Resume: Matt Davis	
Title	Technical Product Management Director: Responsible for technical platforms, including Allerium's NG Core Runtime (ESRP, Policy Routing Function [PRF], LNG/LSRG, LPG, etc.), NG Core Provisioning, Location Data Platform, i3 Policy Store, ECRF/LVF, and MCS.
Education	BS, Technical Communications, Clarkson University, 1997-2001
Work Experience	- Allerium/Comtech, Technical Product Management Director, Mar. 2025-Present - Comtech Telecommunications Corp., Senior Technical Product Manager, Feb. 2019-Mar. 2025 - Comtech Telecommunications Corp./TeleCommunication Systems, Inc., Systems Engineer, Mar 2013-Feb. 2019 - microDATA GIS Inc., Technical Support, Sep 2009-Mar 2013 - Mission Critical Systems, Information Technology Consultant, 2007-2009

Resume: Matt Davis	
	Delwest Homes, IT Manager, 2002-2007
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Since 2009. - Support for CHE implementations throughout various U.S. states. - NGCS and routing customer platform support for statewide and regional networks since 2012, including 911 Association of Central Oklahoma Governments (911 ACOG), State of Arizona, State of Connecticut, multiple Florida counties, State of Iowa, Commonwealth of Kentucky, NCT9-1-1, Pennsylvania Emergency Management Agency, State of South Carolina, State of Tennessee, and State of Washington projects. - NENA i3 Architecture Working Group Member

Matthew Mullins, Principal Systems Engineer, Allerium

Matthew Mullins brings over 15 years of NG9-1-1 engineering experience to the State's project.

Table 43. Key Personnel Resume: Matthew Mullins

Resume: Matthew Mullins	
Title	Principal Systems Engineer, Emergency Systems Routing Engineering: Responsible for the operational system design and architecture of Allerium's emergency routing solutions.
Education	US Army, Signal Corp, 1996-2000
Work Experience	- Allerium/Comtech, ESRE, Principal Systems Engineer, 2016-Present - TeleCommunication Systems, Inc./Comtech, VoIP Telecom Apps, Systems Engineer, 2012-2016 - TeleCommunication Systems, Inc., Advanced Technical Applications Center, VoIP & NG Tier 2 Support Engineer, 2010-2012 - TeleCommunication Systems, Inc., Network Operations Center, Tier 1 Support Engineer, 2009-2010 - T-Mobile, Network Operations Center, Cellular Technical Support Engineer, 2009 - AT&T Mobility, Network Operations Center, Lead Cellular Technical Support Eng, 2000-2009 - US Army, Signal Corp, 1996-2000
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Since 2010. - Designed, deployed, and maintained multiple regional/statewide NG9-1-1 systems, including Allerium's State of Arizona, State of Iowa, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington projects.

Melissa Liebert, Manager, Geographic Information Systems, Allerium

Melissa Liebert, ENP, PMP brings an extensive background in GIS and ALI platforms to the team. She works closely with the State, vendors, and internal SMEs to support successful communication and completion of GIS deliverables and training.

Table 44. Key Personnel Resume: Melissa Liebert, ENP, PMP

Resume: Melissa Liebert, ENP, PMP	
Title	Senior Technical Program Manager: Responsible for developing and implementing PSAP GIS and location data management processes and procedures required to support the rollout and maintenance of NG9-1-1 services; coordinating internal and external resources in support of required project deliverables; identifying and implementing process innovations, programmatic improvements, and automation opportunities for better operational efficiency; facilitating risk mitigation as a part of service deployment oversight; driving alignment between product, operations, and service delivery to support business growth and efficiency; supporting the delivery of our contractually obligated services through deployment and maintenance phases; horizontally aligning and coordinating between operations and service delivery for implementation and maintenance of services/software; managing, coordinating, and providing oversight of our vendors and partners; reporting and presenting schedules, progress, and risks to senior leadership; and generating key performance indicators (KPIs) from data sources to identify areas of improvement.
Education	- Graduate Certificate, Geographic Information Science, Oregon State University, 2014-2015 - Bachelor of Arts, Anthropology, Oregon State University, 2008-2011
Work Experience	- Allerium/Comtech, Senior Technical Program Manager, Aug 2025-Present - Comtech, Technical Program Manager, Aug 2022-Aug 2025 - Comtech, Program Manager, NG Location Services, Mar 2021-Aug 2022 - Comtech, Program Manager, Mar 2020-Mar 2021 - Comtech, GIS Analyst, Apr 2019-Mar 2020 - Liebert's Guide Service, GIS Contractor, Freelance, Nov 2016-Present - Liebert's Guide Service, Transcriptionist, Freelance, Jun 2013-Mar 2019 - Wahkiakum County, Cartographer/GIS Analyst, Nov 2014-Apr 2019 - Warm Springs Geo Visions, Review and Compliance Coordinator/Archaeologist, Jan 2014-Nov 2014 - Warm Springs Geo Visions, Archaeologist/GIS Analyst, Jun 2012-Jan 2014 - US Forest Service, Archaeological Technician, Jun 2010-Dec 2011
Relevant Certifications & Licenses	- PMP certified in Mar 2024. - ENP certified in Feb 2024, expiring Feb 2028.
Years Working with NG9-1-1 Systems & Technologies	10 years working with NG9-1-1 and GIS systems and technologies. - Member of APCO's Common Computer Aided Dispatch (CAD) Public Safety GIS Identifiers Document WG, NENA's Utilization of GIS Data in NGCS Document

Resume: Melissa Liebert, ENP, PMP	
	WG, and Urban and Regional Information Systems Association's (URISA's) NG9-1-1 Task Force (formerly served as chair). - Contributed to NENA's GIS Data Stewardship Document WG, NG9-1-1 Data Model Template WG, and NENA-ADM-008 References WG. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium's State of Arizona, State of Iowa, St. Louis County (Missouri), NINGA (Illinois), State of South Carolina, and State of Washington projects.
References	- Deb Rozeboom, Client Success Manager, DATAMARK Technologies, deb.rozeboom@mbakerintl.com, 548 4th Ave SE, Albany, OR 97321, 320-761-9767 - Richard Kelly, Senior Solutions Manager, 1Spatial, Inc, richard.kelly@1spatial.com, 8614 Westwood Center Drive #350, Vienna, VA 22182, 512-590-2945 - Kyle Bodtorf, Application Developer Administrator, GIS Section Chief, Pennsylvania Emergency Management Agency, kbodtorf@pa.gov, 1310 Elmerton Ave, Harrisburg, PA 17110, 717-651-2701

Mike Wolfe, Program Manager, Allerium

Mike Wolfe is the initial escalation point for non-service impacting concerns related to the State's deployment while ensuring that all related projects align with the long-term goals, coordinating priorities, managing interdependencies, and ensuring resources are allocated effectively across the program.

Table 45. Key Personnel Resume: Mike Wolfe

Resume: Mike Wolfe	
Title	Program Manager: Responsible for all program management responsibilities related to ESInet/NGCS services.
Education	- Fairmont State University, 1999-2001 - PMP Prep Course, 35 Hours, 2023
Work Experience	- Allerium/Comtech, Program Manager, July 2022-Present - Frontier Communications, National Director of 9-1-1/Public Safety Sales, Project Management & Sales Engineering, Mar 2020-July 2022 - Frontier Communications, 9-1-1/Public Safety Sales Account Manager, May 2016-Mar 2020 - Monongalia County Commission, Director, Homeland Security Emergency Management and 9-1-1, Nov 2011-May 2016 - Monongalia County Commission, Deputy Director, Homeland Security Emergency Management and 9-1-1, Apr 2009-Nov 2011 - Monongalia County Commission, 9-1-1 Telecommunicator/PIO/County NIMS Coordinator/Training Officer, Nov 2006-Apr 2009

Resume: Mike Wolfe	
	Barbour County Commission, 9-1-1 Telecommunicator/Shift Supervisor/CAD Administrator, Dec 2005-Nov 2006
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	10 years. - Four years selling NG9-1-1 systems & technology. - Four years managing sales/project management/engineering of NG9-1-1 systems & technology. - Four years of program management for ESInet/NG9-1-1 services in South Carolina.
References	- David Morrison, Program Manager, South Carolina Revenue and Fiscal Affairs Office, Rembert Dennis Bldg., 1000 Assembly St., Suite 420, Columbia, SC 29201, 803-734-3880, david.morrison@rfa.sc.gov - Shelly C. Clark, Administrator, 911 Services Board, Kentucky Office of Homeland Security, 200 Mero Street, Frankfort, KY 40622, 502-352-3684, shellyc.clark@ky.gov - Susan Gochenour, Senior Manager, Technical Support, Segra, 11215 N Community House Rd, Ste. 1000, Charlotte, NC 28277, 540-946-6921, Susan.Gochenour@segrafiber.com

Neil Nyquist, Vice President, NOC & Field Services, Allerium

Neil Nyquist leads the Allerium NOC and field services teams responsible for the State's project.

Table 46. Key Personnel Resume: Neil Nyquist

Resume: Neil Nyquist	
Title	Vice President, NOC & Field Services: Responsible for managing a 24x7x365 operations team that monitors phones, email, and various tools for internal and external events and creates, updates, escalates, and resolves incident tickets; facilitating incident management and change management bridges and notifications, working with vendors and partners as needed to resolve service impacting events; and focusing on continual service improvement for all processes followed.
Education	- BSIT, University of Phoenix, 2003-2006 - ITIL Foundations certified. - Cisco Certified Network Associate (CCNA) certified.
Work Experience	- Allerium/Comtech, Vice President, NOC & Field Services, Aug 2025-Present - Comtech, Senior Director, NOC, Sept 2022-Aug 2025 - Comtech, Senior Manager, Network Operations Center, July 2019-Sept 2022 - Amazon, Operations Manager, Prime Video Live Events, Oct 2018-July 2019 - Expedia, Inc., Senior Manager, Major Incident and Problem Management, Nov 2014-Apr 2018

Resume: Neil Nyquist	
	- DaVita, Senior Manager, Infrastructure, NOC Operations and ITIL Process Manager, Nov 2011-Nov 2014 - DaVita, IT Infrastructure and Operations Project Manager, Nov 2009-Aug 2012 - DaVita Kidney Care, Data Center and NOC Operations Supervisor, Nov 2006-Sept 2009 - RealNetworks, Real Operations Support Lead, Feb 2004-Nov 2006 - US Army, SSG - E-6 - Information Systems Specialist (74B) – Airborne/Air Assault/Rappel Master Qualified, 1995-2003
Relevant Certifications & Licenses	- ITIL Foundations certified. - CCNA certified.
Years Working with NG9-1-1 Systems & Technologies	- Since 2019. - Supporting/supported multiple regional/statewide NG9-1-1 deployments, including Allerium’s State of Arizona, Commonwealth of Kentucky, St. Louis County (Missouri), Commonwealth of Pennsylvania, and State of South Carolina projects.

Patrick Hoover, Technical Program Manager, Allerium

Patrick Hoover has worked in the 9-1-1 industry for over 25 years, with comprehensive experience in both legacy E9-1-1 and the transition to NG9-1-1 (i3) as well as in the wireline, wireless, and VoIP 9-1-1 call delivery systems. Additionally, Patrick has call handling experience from both a deployment and ongoing troubleshooting perspective.

Table 47. Key Personnel Resume: Patrick Hoover

Resume: Patrick Hoover	
Title	Technical Program Manager: Experienced leader in E9-1-1/NG9-1-1 operations, technology, and deployment. Currently responsible for managing OSP onboarding to Allerium’s NG9-1-1 systems directly for i3 call delivery capabilities. Strong skill set in managing multiple concurrent projects, ensuring successful conclusions and stakeholder satisfaction. Key responsibilities include leading NG9-1-1 OSP onboarding efforts to Allerium’s NG9-1-1 systems, including initial outreach, implementation, testing and turnup; engaging with internal and external teams, including OSPs, state agencies, vendors, and competitors to work towards project success; working with CalR project management on all active OSP onboarding projects to help ensure timelines are met and act as escalation point for any obstacles; serving as a SME for E9-1-1 and NG9-1-1 systems and processes; managing integration, testing, and troubleshooting of 9-1-1 technology solutions; developing project reporting dashboards for tracking key milestones and deliverables; and identifying project risks and working to resolve issues and overcome roadblocks.
Education	Bachelor’s degree, Colorado State University, 1999
Work Experience	Allerium/Comtech, Technical Program Manager, Oct. 2024-Present

Resume: Patrick Hoover	
	- Intrado Life & Safety, Sr. Customer Success Manager, 2013-Oct 2024 - Intrado Life & Safety, Implementation Project Manager, 2012-2013 - Intrado Life & Safety, Program Manager, 2006-2012 - Intrado Life & Safety, Project Manager, 2004-2006 - Intrado Life & Safety, Project Manager, 2003-2004 - Intrado Life & Safety, Quality Management Specialist, 2001-2003 - Intrado Life & Safety, Data Integrity Unit Analyst I/II/III, 1999-2001
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	- Over 25 years of combined E9-1-1 and NG9-1-1 experience. - Supporting multiple statewide NG9-1-1 projects, including the State of Arizona, NCT9-1-1, State of Ohio, Commonwealth of Pennsylvania, State of South Carolina, and State of Washington.

Patrick Melancon, Product Management Director, Allerium

Patrick Melancon brings over 16 years of NG9-1-1 experience to the State's project.

Table 48. Key Personnel Resume: Patrick Melancon

Resume: Patrick Melancon	
Title	Product Management Director: Responsible for supporting NG9-1-1 location product lines and developing and managing industry relationships with third party solution providers.
Education	- Master of Business Administration (M.B.A.), Plymouth State University, Plymouth, NH (and the national award winner for Small Business Institute [SBI] competition) - Bachelor of Science (B.S.) in Business Management and IT Management, Magna Cum Laude, Granite State College, Concord, NH
Work Experience	- Allerium/Comtech, Product Management Director, Dec 2024-Present - Founder and Principal Consultant, Circle M Innovations, Oct 2023-Present - Senior Product Manager, GeoComm, Nov 2014-Oct 2023 - Vice President, Product Management, GIS Data Resources Inc., Aug 2013-Nov 2014 - Public Safety GIS Manager, State of Tennessee, Feb 2009-Aug 2013
Relevant Certifications & Licenses	- Five Forces Analysis Specialist, Advanced Innovation Group Pro Excellence (AIGPE™) - GISP, GIS Certification Institute (GISCI) (Issued Nov 2014) - Python, Visual Basic, SQL, C#, Agile Methodologies, Public Cloud Technologies, GIS Applications (ESRI)

Resume: Patrick Melancon	
Years Working with NG9-1-1 Systems & Technologies	• Since 2009. • Supported projects for the State of California, State of Maine, NCT9-1-1, New York City, State of North Carolina, Commonwealth of Pennsylvania, State of South Dakota, State of Tennessee, and the State of Washington prior to joining Allerium. • Involved in Allerium's ESInet/NGCS deployments. • Involved in multiple standards through the years, including the NENA GIS Data Model, NENA Data Stewardship, NENA i3 transition, and the APCO CAD GIS data requirements.
References	• Greg Spadorcio, Director of Sales, Smart Response Technologies, 7022 Singing Springs Ln, Evergreen, CO, 80439, 916-749-5010 • Tyler Thompson, Strategic Partnership Leader, GeoComm, 18215 Pine Vista Pl, Colorado Springs, CO 80908, 719-510-1649 • Deb Rozeboom, Client Success Manager, DATAMARK Technologies, 548 4th Ave SE, Albany, OR 97321, 320-761-9767

Seth Wold, Sales Director, Allerium

Seth Wold is the State's key point of contact (POC) for all questions related to the submitted offer. Seth serves as the sales lead for the State's NG9-1-1 project with an emphasis on helping to achieve the State's goals, handling account renewals, and presenting new product and service offerings to the State.

Table 49. Key Personnel Resume: Seth Wold

Resume: Seth Wold	
Title	Sales Director: Responsible for leading cross-functional teams to identify, capture, and implement new NG9-1-1 opportunities.
Education	• Bachelor's degree, Mathematics and Statistics, Utah State University, 2005-2008 • Bachelor's degree, History, Utah State University, 2005-2008 • Bachelor's degree, Polish Minor, University of Utah, 2005
Work Experience	• Allerium/Comtech, Sales Director, Apr 2025-Present • RapidSOS, Regional Manager, 2024-2025 • Utility, Inc., Business Manager, 2023-2024 • Domo, Corporate Account Executive, 2021-2023 • Hexagon Geospatial, Regional Sales Manager, 2019-2021 • CentralSquare Technologies, Senior Sales Account Executive, 2017-2019 • Spillman Technologies, Field Sales Executive, 2015-2017 • iFIT, Vice President of Sales, 2014-2015 • Altra Running, National Sales Manager/Key Account Manager, 2011-2014

Resume: Seth Wold	
Relevant Certifications & Licenses	N/A.
Years Working with NG9-1-1 Systems & Technologies	• Since 2015. • Worked on public safety projects in every state west of the Mississippi.
References	• Greg Denton, 9-1-1 Program Administrator, State of Arizona, 100 N, 15th Avenue, Suite 305, Phoenix, AZ 85007, 480-280-7171 • Adam Wasserman, State 911 Director, State of Washington, 1 Militia Drive, Camp Murray, WA 98430-5000, 253-512-7468 • Stacen Gross, President, GeoComm, 1100 W. Saint Germain St., Suite 300, Saint Cloud, MN 56301, 320-281-2186

4.2.2. Staff Qualifications

b. Staff Qualifications

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

Response:

Allerium has acquired extensive and diverse project and program experience managing large and complex NG9-1-1 projects since 2011, including:

- Performing multiple types of statewide deployments transitioning from legacy infrastructure to i3 solutions,
- Using regional/state sanctioned or owned networks in at least five ESInet/NGCS deployments,
- Utilizing proven project/program management methodology based on ITIL, PMI, and industry best practices,
- Efficiently cutting over multiple PSAPs weekly (surge up to nine per week),
- Simultaneously conducting small and largescale NG9-1-1 deployment projects ranging from a dozen to 250 plus PSAPs supporting 15,000-13M population,
- Completing a 1.5M population deployment with 49 PSAPs six weeks ahead of schedule providing the customer with both facilities costs and resource savings, and
- Interoperating and managed third party component solutions and vendors.

Allerium's personnel are highly qualified and experienced in designing, deploying, and operating ESInet/NGCS services of varying size and scope. They are devoted to successful contract performance and ensuring the utmost quality and customer experience in the industry.

Allerium will collaborate with the State to determine a course of action to resolve any such problems with key personnel working on the State's NG9-1-1 project.

4.2.3. Designations, Certifications, and Licenses

c. *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.

Response:

Allerium's personnel hold the professional designations, certifications, and licenses necessary to perform their roles on Allerium's regional and statewide NG9-1-1 projects as illustrated in the resumes provided herein.

4.3. Implementation [Project Requirements and Scope of Work, Section C.3]

4.3.1. Implementation Approach

3. *Implementation*

a. *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.

Response:

In addition to PMI standards and industry best practices, Allerium has applied lessons learned from our extensive experience implementing and supporting NG9-1-1 services to optimize implementation plans and operational support processes. The result is a proven methodology known as Allerium's Five Phased Migration approach.

Allerium's Five Phased Migration approach is designed to ensure a successful and timely implementation of NG9-1-1 services. More specifically, this methodology allows Allerium to accurately identify tasks, requirements and risks related to the implementation. This, in turn, allows us to build and maintain accurate project schedules, as well as communicate expectations to project stakeholders, throughout the implementation.

Additional objectives and benefits of this approach include establishing mutually agreed upon network and system designs, building and configuring systems to design, and executing applicable testing and signoff procedures.

Additional details on specific tasks and activities related to the implementation are provided as part of our sample implementation plan and implementation responses.

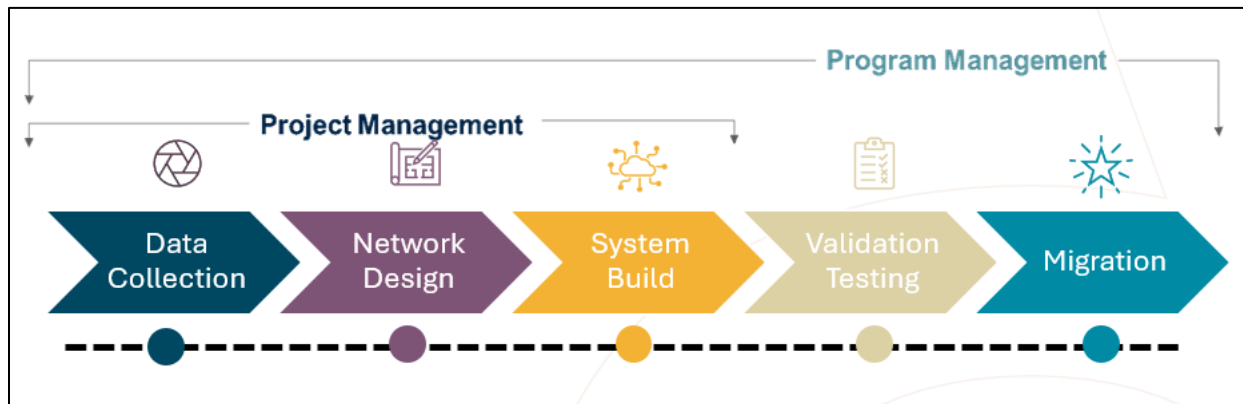


Figure 12. Overview of Allerium's Five Phased Migration Approach

4.3.2. Elements of Implementation

b. 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.

At a minimum, the implementation plan should address:

- Methodology for implementing the entire NG911 system, establishing call delivery from all OSPs to all PSAPs across the State of Nebraska
- Methodology for administering and operating the NG911 system for the contract term.
- IP routing plan, how requirements are met, and governance of routing changes and documentation.
- How NGCS will operate with the ESInet, and how each Functional Element will deliver required functionality.

Response:

Overview

Allerium develops a comprehensive implementation plan to address the full project lifecycle and all contracted services by following the five phased approach described above. Mutually agreed upon requirements and information gathered in the early stages of the project allow us to build an implementation plan and project schedule specific to the project needs.

The implementation plan and project schedule are documented via a Master Project Plan (MPP) document. The MPP is shared with the State and continuously updated throughout the implementation project. Following is a sample project schedule in the form of a Gantt chart, and a preview of critical path items from the implementation plan.

Sample Project Schedule

Allerium's sample project schedule is included below and **ALLERIUM CONFIDENTIAL- PROPRIETARY INFORMATION**. The x-axis represents anticipated calendar days from contract signing.

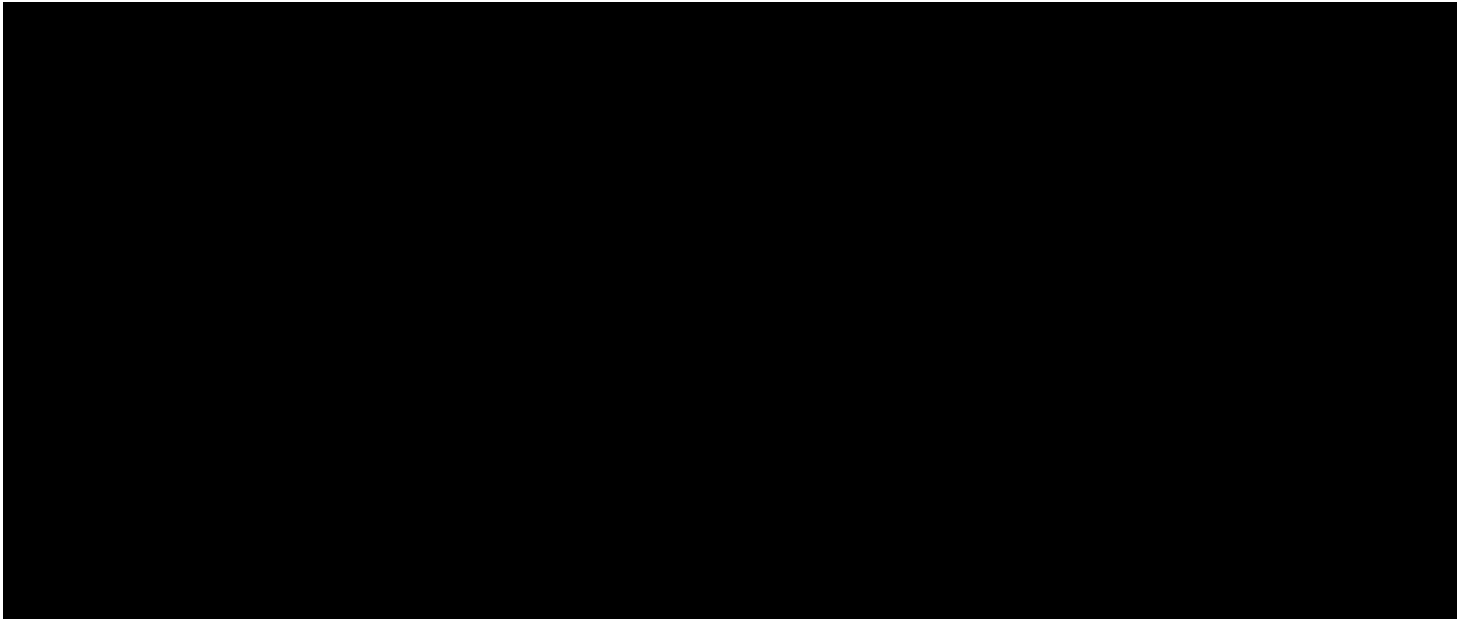


Figure 13. Sample Project Schedule (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

Critical Path Activities

Below are the critical path activities included in Allerium's implementation plan.

Table 50. Critical Path Activities

Data Collection	Design	System Build	Testing	Migration
- Requirements (Functionality, Resiliency, Capacity) - Data Center and OSP POI Locations - LSR Vendors and Locations - PSAP Site Surveys - PSAP CHE details (vendor, version, host/remote) - LOAs	- ESInet design - HW / SW Design - IP Routing Plan - LSR connectivity - PSAP/CHE HW/SW Readiness - NGCS-to-CHE interface specs - OSP Interface specs	- HW / SW install and config - Network install and config - ESInet Edge HW Install and Config - PSAP/CHE HW/SW upgrades (if needed) - CHE Interface config - OSP circuit orders - OSP/PSAP Dual ALI Provisioning	- NGCS Core ATP - Ingress POIs to NGCS connectivity - LSR to OSP Ingress POIs connectivity - ESInet Connectivity and Failover - CHE Host ATP - Individual PSAP ATP - OSP Voice and Location Delivery	- PSAP Migration Requirements Met - LSR vendor traffic reroute to Allerium - Voice and Text traffic routing through NGCS - OSP traffic reroute to Allerium

Sample Implementation Plan

A comprehensive Implementation Plan sample is included in Appendix 2: Sample Implementation Plan.

Administering & Operating the NG9-1-1 System for the Contract Term

Below are key elements of Allerium's methodology for administering and operating the NG911 system for the contract term:

- Service Review Meetings
- System Monitoring by Network Operations Center (NOC)/Security Operations Center (SOC)
- Incident Management and Triage
- Service Updates and Upgrades
- Scheduled Maintenance
- Change Management
- Root Cause Analysis (RCA)
- Service Level Agreement Compliance Reporting

Operational support processes are documented in Standard Operating Procedure (SOP) documents and shared with applicable stakeholders.

IP Routing Plan, Meeting Requirements, and Governance of Routing Changes and Documentation

The IP routing plan, including network protocols and subnets specific to the State ESInet, is established in the design phase of the implementation plan and documented in applicable design and as-built documents. The IP routing plan is communicated to PSAP and/or Call Handling vendors for interface configuration and integration. Additionally, the IP routing plan is communicated to OSPs for interface configuration and integration.

Governance of IP routing changes is managed through Allerium's change management process. This process defines communication/notification requirements for changes initiated by PSAPs, OSPs, or Allerium. Under the Allerium change management process, all IP routing changes are reviewed by the Allerium change control board, documented in a method of procedures (MOP) document and executed in a maintenance window that has been coordinated with applicable stakeholders.

4.4. Transition [Project Requirements and Scope of Work, Section C.4]

4.4.1. Transition Plan: Current and Future

4. Transition

a. 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.

Minimum topics:

- *Transition schedule with milestone dates for design, development, testing, implementation, and cutover to full operational readiness.*
- *System testing approach during transition.*
- *PSAP/site cutover approach, including phased migration and parallel operation with current systems.*
- *Contingency and rollback plan for implementation or integration failures.*
- *Risks, dependencies, and interdependencies affecting cutover.*
- *OSP interface transition and service migration to the NG911 system.*
- *Integration with other systems, services, and providers.*

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.

Response:

Experience Transitioning Away from a Lumen-Provided Solution

Allerium has valuable experience working with your current solution provider (Lumen/Intrado) and has successfully completed transitions away from that provider in previous statewide deployments. In the State of Washington, for example, Allerium successfully migrated from Lumen's (then CenturyLink's) IPSR solution and network to Allerium's NGCS and ESInet.

Lumen was using a non-NENA transitional IP solution based on Request for Assistance Interface (RFAl), making Allerium the first NG9-1-1 provider in the country to accomplish a successful move from a transitional IP service to full NENA i3 network. Allerium determined interconnection details regarding transfers as part of the workbook methodology we use for implementation planning. The resulting knowledge from the Washington deployment as well as many other locations where we have worked with Lumen (e.g., the State of Arizona) is directly applicable to the State's deployment.

Transition Plan: Current and Future

Allerium will develop a transition plan through coordination with the State, the incumbent provider, and other applicable stakeholders. The transition plan will be based on available support and technical capabilities of the incumbent provider, as well as technical capabilities of the PSAP call handling systems. Tasks, requirements and dependencies specific to transition activities will be incorporated into the implementation plan and project schedule detailed above. Incorporating transition-related activities into the implementation plan and project schedule allows for a single source to view status and updates on all implementation activities

Transition Schedule with Milestones

Allerium's sample project schedule is included below and **ALLERIUM CONFIDENTIAL- PROPRIETARY INFORMATION**. The x-axis represents anticipated calendar days from contract signing.

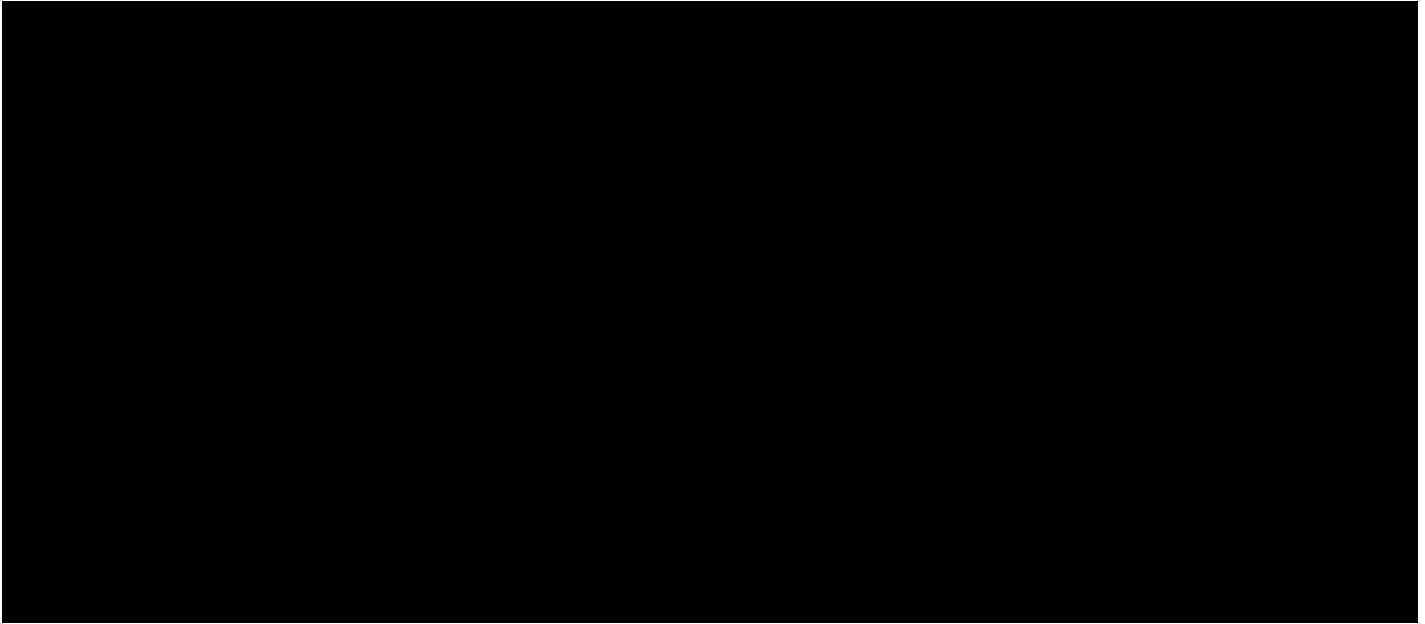


Figure 14. Sample Project Schedule (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

The sample project schedule shown above incorporates transition related activities and reflects anticipated lead times for implementation and transition milestones. The anticipated milestone dates for design, development, testing, implementation, and cutover to full operational readiness are as follows:

- **Design:** 60 days from contract
- **Development (Including Install & Configuration):** 300 days from contract
- **Testing:** 330 days from contract
- **Implementation (First PSAP):** 360 days from contract
- **Full Operational Readiness (First PSAP):** 360 days from contract

Please note that:

- Additional testing occurs for each PSAP and OSP and
- Each PSAP and OSP will have their own date for implementation and full operational readiness.

System Testing Approach during Transition

Allerium follows a rigorous testing approach on each aspect of the system before any services are utilized for production 9-1-1 traffic. This includes pre-production testing of the ESInet, NGCS applications, integration with PSAPs, and integration with OSPs. The following are key aspects of the testing approach and methodology.

ESInet and NGCS Core Acceptance Test Plan (ATP)

Allerium will create a NGCS Core Acceptance Test Plan (ATP) document that provides the customer with an overview of the test cases that Allerium will execute for each interface and/or system component on the NG9-1-1 system. This test plan is developed to prove that the NG9-1-1 solution that Allerium is delivering is operationally ready for the next stage of testing being conducted. The NGCS Core ATP is designed to test the following interfaces and system components, including:

- Voice trunks from OSPs.
- ISUP signaling associated with NG9-1-1 calls for aggregation.
- Other LEC's selective routing network into Allerium's network.
- Allerium's NG9-1-1 routing and location applications.
- Monitoring and alarming components in the NG9-1-1 platform.
- **ESInet Connections:**
 - Multi-Protocol Label Switching (MPLS) to NGCS
 - MPLS to CHE
 - PSAP equipment – pre-PSAP cut-over to Allerium's NG9-1-1 system.

Each interface and system is tested, and the results are recorded and shared with the customer. Continuation of the deployment plan is dependent on successful completion of all test cases.

PSAP Migration Acceptance Test Plan (ATP)

Following successful testing of the NGCS Core and applicable ESInet connections, the next phase of testing is pre-migration acceptance testing with each PSAP and Call Handling Host system. Allerium creates an ATP document for each PSAP to validate successful integration with the call handling system and delivery of applicable services. PSAP ATP test cases are designed to test the following functionality and features:

- ESInet redundancy and failover
- Allerium hardware redundancy and failover
- PSAP hardware redundancy and failover
- Voice and location delivery for wireline, wireless, VoIP and Text to 9-1-1
- Policy Routing
- Transfers
- Integration with downstream services such as CAD, recording, and analytics

PSAP ATP results are reviewed with applicable stakeholders prior to scheduling the PSAP migration.

OSP Migration Acceptance Test Plan

The final testing phase focuses on thoroughly testing each OSP connection into the NG9-1-1 system prior to traffic migration. These testing steps and test cases are designed to ensure proper connectivity, redundancy, failover, signaling, and media quality. Allerium also supports additional test cases that may be requested by OSPs. The following is an overview of OSP Migration ATP:

- Call-through testing
- Validate destination
- Validate two-way audio
- Validate caller location information delivery
- Failover
- Test each additional path for failover to next path, up to and including the route of last resort.
- Test active call on each path to ensure call remains up if route of call path fails.
- SIP Error code testing.
- Test for expected call behavior for each SIP Error code as agreed during compliancy review per market policy routing rules.

PSAP/site Cutover Approach, Including Phased Migration and Parallel Operation with Current Systems

Allerium's recommends the following approach for PSAP/site cutover as part of the service transition plan:

1. Establish connectivity between the NGCS and Legacy Selective Routers (LSR) serving NE PSAPs, as described below. LSR interconnections will be designed to support 911 traffic ingress from the LSRs to the NGCS as well as outbound transfers from the NGCS to the LSRs.
2. Work with CHE providers to configure ingress routes and location queries paths from Allerium ESInet while retaining existing configurations for the legacy provider. This capability and the applicable configurations are validated through PSAP migration planning calls with the PSAP and CHE providers. Establishing dual connections allows Allerium to perform pre-migration acceptance testing without interruption to existing services. This approach also allows for a simplified rollback should issues be encountered.

Testing of the LSR interconnections and traffic delivery to the PSAP/CHE is tested and validated prior to cutover.

Allerium establishes processes with the LSR provider to request and schedule support as well as perform traffic reroutes during the approved PSAP migration/cutover window. Steps for traffic reroutes are defined in the PSAP Migration Method of Procedures (MOP) and performed in coordination with PSAP, LSR provider, and Allerium.

At the appropriate step in the PSAP Migration MOP, the LSR provider will reroute 9-1-1 ingress traffic away from the legacy routes and repoint them to the Allerium NGCS. This change is performed on a per-PSAP or per-ESN basis.

Testing is performed immediately following the LSR reroute to ensure successful delivery to the PSAP and CHE systems.

Contingency & Rollback Plan for Implementation / Integration Failures

Allerium strives to eliminate implementation rollbacks via rigorous pre-migration testing as detailed above. However, should issues be found during or post implementation, all Allerium Migration Method of Procedure (MOP) documents include pre-defined rollback procedures. These procedures are designed to safely revert services to the legacy solution, including validation testing following the rollback steps.

Additional contingency plans include circuit redundancy and failover, hardware/software redundancy and failover, data center redundancy and failover, and PSAP Policy Routing Rules.

Once services are live, all maintenance and upgrade activities on the production system include pre-defined rollback procedures that are reviewed via the Allerium Change Control Board and documented in the approved Method of Procedure document(s).

Risks, Dependencies & Interdependencies Affecting Cutover

The most critical dependencies related to Allerium's recommended PSAP cutover approach are as follows:

1. Legacy Selective Router providers are willing to enter into a Interconnection agreement to support interconnection and cutover activities described above.
2. Call Handling systems are able to support dual ingress and location connections to allow thorough testing of traffic delivery through the Allerium ESInet without interruption to existing services.

Similarly, the most critical risks related to Allerium's recommended PSAP cutover approach are as follows:

1. Legacy Selective Router providers are unwilling or unable to enter into an Interconnection agreement to support interconnection and cutover activities described above.
2. Call Handling systems are unwilling or unable to support dual ingress and location connections.

Alternate PSAP/site cutover options should these risks manifest:

1. Establish an Interconnection agreement with the incumbent NG9-1-1 services provider, to allow connectivity from incumbent ESInet to Allerium's ESInet and perform 9-1-1 traffic reroutes on a per-PSAP or per-ESN basis.
2. Install and configure additional equipment to "intercept" legacy/incumbent 9-1-1 ingress traffic before it is presented to the call handling equipment. This traffic would be routed through the NGCS for routing intelligence and location determination and then delivered over the Allerium ESInet to the PSAP / CHE.
3. Perform NG911 traffic migrations OSP-by-OSP. In this model, Allerium would establish ESInet connectivity to the PSAP/CHE and then work with each OSP to schedule their traffic migration away from the legacy/incumbent system and repoint to the Allerium NGCS. In this model, the PSAP would receive traffic from both the incumbent provider and Allerium until all OSPs have migrated traffic to Allerium.

Legacy Selective Router Interconnection

To support the transition to Allerium's NG9-1-1 solution, it is expected that we will need to interconnect with Legacy Selective Routers (LSRs) that provide service to Nebraska PSAPs and surrounding areas. Allerium's NG9-1-1 Aggregation Service includes the equipment and services to receive calls from the LSRs in SS7/TDM protocols and convert that traffic to SIP before delivering to the NGCS data centers.

Inter-tandem SS7/TDM trunks will be established from each Selective Router to Allerium SS7/TDM Points of Interconnect (POIs). These connections allow 9-1-1 calls from OSPs that are not yet directly connected to the NG9-1-1 Aggregation Service to be routed through the Allerium NG9-1-1 solution.

Inter-tandem trunks to the LSRs are also needed to support call transfers from PSAPs connected to the ESInet to legacy PSAPs still connected to an LSR.

OSP Interface Transition & Service Migration to the NG9-1-1 System

Allerium's NG9-1-1 Aggregation Service provides the equipment and services to receive calls from Originating Service Providers and deliver those calls to the NGCS. The NG9-1-1 Aggregation Service establishes Point-of-Interconnect (POI) locations mutually agreed upon by the customer. Allerium will work with the customer to develop a Network Disclosure package which is distributed to OSPs within the market. The network disclosure package includes applicable documentation such as LOAs, POI locations, and timelines for OSPs to connect to the NG system.

Originating Service Provider Transition

OSP will be asked to establish connectivity to the POI locations identified by the customer. OSPs will receive circuit ordering details as well as interface configuration specs. Prior to any OSP traffic migration, the OSP ATP testing outlined above is carried out by Allerium and each OSP.

Legacy Selective Router Interconnection

To support the transition to Allerium's NG9-1-1 solution, it is expected that we will need to interoperate with Legacy Selective Routers (LSRs) that provide service to Nebraska PSAPs and surrounding areas. Therefore, the NG9-1-1 Aggregation Service also includes the equipment and services to receive calls from the LSRs in SS7/TDM protocols and convert that traffic to SIP before delivering to the NGCS data centers.

Inter-tandem SS7/TDM trunks will be established from each Selective Router to Allerium SS7/TDM Points of Interconnect (POIs). These connections allow 9-1-1 calls from OSPs that are not yet directly connected to the NG9-1-1 Aggregation Service to be routed through the Allerium NG9-1-1 solution. Inter-tandem trunks to the LSRs are also needed to support call transfers from PSAPs connected to the ESInet to legacy PSAPs still connected to an LSR.

Coordinating a Transition from the Current Provider

Allerium will engage the incumbent provider for transition support and planning. Allerium will also work in good faith with future providers to transition services away from the Allerium solution. In both cases, Allerium will endeavor to support the transition(s) with no degradation in services. Any risks, dependencies, schedule or scope changes will be communicated to the Contractor via the implementation plan and project schedule.

Additional examples of integration with third party systems may include:

- Establishing process to share data and system logs with reporting or analytics providers
- Interconnecting with neighboring states' ESInet vendors to enable ESInet-to-ESInet transfers
- Interoperability Testing (IOT) with Call Handling providers to test new designs, interface changes and new features prior to production deployment

4.5. Testing and Acceptance [Project Requirements and Scope of Work, Section C.3]

4.5.1. Testing (Comprehensive Test Plan)

5. Testing and Acceptance

a. Testing (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.

The comprehensive test plan will address, at minimum:

- *Test environment, facilities, and equipment.*
- *Test configurations and thresholds.*
- *Simulators and test-call processes.*
- *Final documentation of all tests and results.*

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.*

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.

Response:

Allerium maintains a comprehensive ATP featuring over 250 tests performed on all components and interfaces of the NG9-1-1 solution, including the network. The ATP focuses on testing normal operational conditions as well as failure conditions with testing processes addressing:

- Ingress service provider to NGCS,

- NGCS to ESInet egress,
- ESInet/NGCS to PSAP, including PSAP network edge failure cases, and
- Call transfers to/from neighboring jurisdictions

Allerium utilizes a detailed test and acceptance program and plan for both the NGCS ATP and PSAP ATPs. The Allerium test plan includes specific tests for all functions for testing review, approval, and acceptance. Each test record requires signoff from both Allerium and State representatives as well as a signature that shows agreement on the recorded result.

If there is an issue experienced during testing, the details are included as part of the test plan, and the recommended and agreed to disposition of the test is documented for future follow-up and remediation. All test records and the final acceptance test report are scanned and made available through the Allerium web portal.

4.5.2. Test Plan Methodology

b. 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.

Response:

Allerium performs extensive testing after installing the proposed solution and before passing production traffic to ensure that the solution functions as designed and implemented. Allerium leverages its comprehensive ATP to govern the testing process.

Two-Phased Approach to Acceptance Testing

Acceptance testing typically occurs in two phases: first the Next Generation (NG) Core, then the PSAPs. One aspect of Allerium's ATP focuses on fully testing each element within the NGCS and the underlying ESInet and verifying that normal operational conditions as well as fault conditions process as expected through the solution.

Another aspect of Allerium's ATP ensures that all network edge devices such as firewalls, routers, switches, and media gateways at the PSAP demarcation point interoperate with the NGCS and ESInet as expected pre-PSAP migration. Upon validation of the network edge configurations, Allerium also performs call flow scenario testing within the PSAP ATP. Allerium's PSAP acceptance testing occurs upon satisfactory completion of the NGCS/ESInet acceptance testing, but before the PSAP migrates onto the Allerium network for production traffic.

Allerium's operations engineering teams drive the ATP process with support from our program management, project management, and customer service management teams. Engineers with specialized knowledge in functional areas such as network, systems administrators, telecom, and Allerium applications work in tandem to execute each test case within the ATP document. Should Allerium experience any unexpected results, the engineering teams review the results, determine the root cause, and apply mitigation steps. Allerium documents the updated configurations and then executes the test case(s) again to ensure the proper expected result.

Logging and Documenting

Allerium runs a series of tests captured within its ATP to verify the NGCS/ESInet system components are working. Allerium follows the steps outlined for each test and then logs and documents the expected and actual results within the ATP document during the process.

Allerium documents test results using the following codes:

- **TP:** Test Passed
- **TF:** Test Failed
- **RTP:** Retest Passed
- **RTF:** Retest Failed
- **NA:** Feature not applicable to customer's final configuration

Allerium also certifies that all tests have passed prior to cutover.

Reporting on Tests

Allerium reviews the results of the testing with our customers as part of the final acceptance, obtains approval, and then proceeds to migrate traffic.

4.5.3. System Acceptance Testing

c. 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

Response:

Logging and Documenting

Allerium runs a series of tests captured within its ATP to verify the NGCS/ESInet system components are working. Allerium follows the steps outlined for each test and then logs and documents the expected and actual results within the ATP document during the process.

Allerium documents test results using the following codes:

- **TP:** Test Passed
- **TF:** Test Failed

- **RTP:** Retest Passed
- **RTF:** Retest Failed
- **NA:** Feature not applicable to customer's final configuration

Allerium also certifies that all tests have passed prior to cutover.

Reporting on Tests

Allerium reviews the results of the testing with our customers as part of the final acceptance, obtains approval, and then proceeds to migrate traffic.

4.5.4. Independent Validation and Verification (IV&V)

d. 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.

Remainder of page intentionally blank

Response:

Allerium supports the State's desire to conduct independent validation and verification. Allerium will work with the State and State appointed contractors to collaborate and produce a test scope, priorities, support, and costs. Allerium remains fully committed to compliance with STA-010.3f and future NENA i3 revisions but notes that solutions NENA envisions are not viable in operational markets today.

To expose areas that are not viable, Allerium recommends that the State consider the impact of i3 compliance throughout the solution to include OSP, NGCS, and PSAP elements. As such, the State can identify compliance gaps within their OSP & CHE footprints that may preclude certain features and functionality being enabled to support i3 call flows. The concepts may be demonstrable with use of simulators for the PSAP but if not applied to actual PSAP equipment, the call flows do not function as expected.

For example, STA-010.3f requires the use of queue and dequeue events via SIP SUBSCRIBE/NOTIFY to process a call to a PSAP. The ESRP must place the call into the PSAP queue and the PSAP must dequeue the call from the queue. Given lack of adoption for such features in the market, NG Core Service providers have implemented operational solutions which enable ESRPs to dequeue calls directly to a PSAP. As such, calls delivered to a queue within the ESRP generally are immediately dequeued and pushed toward the PSAP, allowing the NG 911 core to deliver calls when PSAPs are unable to request dequeue directly. Allerium also maintains active call statistics to every PSAP on the network and allows the configuration of maximum concurrent call counts to prevent PSAPs from becoming saturated.

Compliance with STA-010.3f is a journey for the entire ESInet and all connected elements. To determine the pathway vested stakeholders must prioritize and coordinate to ensure success. Until all parties are prepared to adopt and leverage fully i3 compliant mechanisms, Allerium

recommends leveraging existing operational solves, many of which have been in place since circa 2012.

5. Response to Technical Requirements [Proposal Instructions, Section A.5]

5. RESPONSE TO TECHNICAL REQUIREMENTS

Bidder should read the Technical Requirements Section of the RFP and provide a response as described in that section. Appendix B contains a Technical Matrix to assist with compliance.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

Response:

Allerium's Technical Requirements responses are included below.

5.1. ESInet Requirements [Project Requirements and Scope of Work, Section E.1]

1. ESInet Requirements

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.

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.

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.

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.

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.

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.

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.
- 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.

Response:

Network Operations Management

NOC/SOC Services

Allerium provides system monitoring, maintenance, incident management, and reporting services from our NG9-1-1 operations organization. This organization includes a Network & Security Operations Center (NSOC) team with 24x7x365 public safety dedicated resources strategically dispersed across all U.S. time zones and working out of a centralized communications hub.

The NSOC team is responsible for incident ticket management, field technician dispatching, partner escalation, and depot spares in Allerium's data centers. NSOC engineers engage from the start of the project deployment to assist application engineers with deploying the service. The NSOC team also manages planned maintenance events as well as root cause analysis (RCA) delivery and remains available for assistance throughout all phases of the project lifecycle.

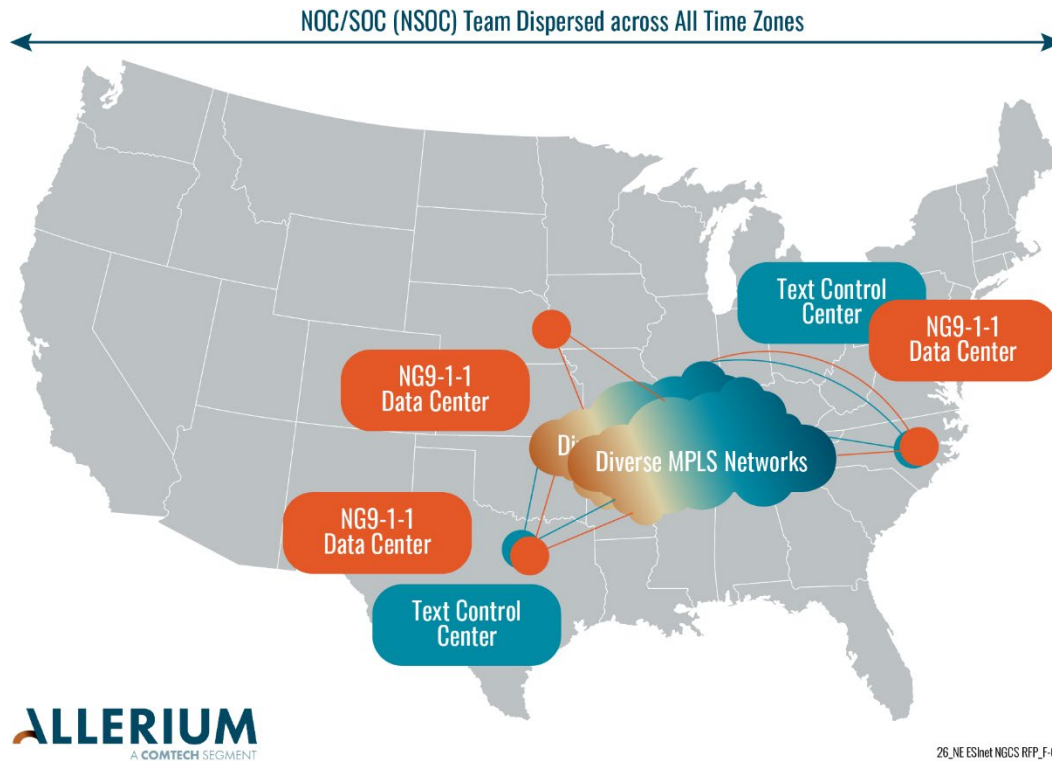


Figure 15. National System Design View

Single Point of Contact

Allerium's NSOC is available 24x7x365 for any service-related issues, serves as the single point of contact (SPOC) for all customer inquiries—including reporting, escalating, and receiving status updates on incidents as well as other communications—and provides rapid access to a live technician. Tiers 1-2 and supervisory personnel plus SMEs staff the NSOC.

Allerium's NSOC supports both statewide and regional Allerium ESInet/NGCS deployments. ISO 9001/TL 9000 certified, our NSOC is unique because it is an in-house resource solely focused on 9-1-1 and staffed 24x7x365 by Allerium employees specifically trained on 9-1-1 services and applications. Many other organizations within the NG9-1-1 space use multipurpose personnel and facilities to “include” 9-1-1 or contract with generic, third-party help desk solutions providers.

Methods, Procedures, and Strategies Defining the Operation

Allerium’s NSOC uses defined processes for incident and problem resolution and change management activities. Our team’s close work with 9-1-1 carriers, PSAPs, and other stakeholders relies on well-defined and documented workflow and roles and responsibilities to ensure quick and appropriate identification, classification, and resolution of incidents and problems regardless of the origin.

Our NSOC currently supports regional and state-level systems, providing incident and problem resolution support incorporating third-party provider systems ranging from CHE providers to ESInet and NGCS providers offering non-native solutions, including but not limited to:

- Real-time monitoring of third-party systems when available (if true integration is not available, a NOC-to-NOC process is put together which ensures we are notified of any impairments or maintenance and in turn make you aware),
- Ticketing and escalations with third-party systems, and
- Performance data collection.

The Allerium NSOC has well-defined methods, processes, procedures, and work instructions for all facets of support and maintenance, based upon ITIL principles and industry best practices. We maintain all NSOC procedural documentation in a digital library with online access for all staff members plus hard copies available for quick reference. All documentation updates go through a review-and-approval process, and the latest approved documents are available online.

Allerium ensures that all NSOC staff are trained on our NGCS and ESInet architecture and operational standards. The NSOC provides timely responses and replies as they coordinate team responses to maintenance, service, and customer service actions. The NSOC team is involved from the onset of testing and is familiar with the system as it has been deployed, understands the SLAs, and is trained in the NMS to understand alarm notifications, alarm generation, and their severity, assignment, and urgency in relation to maintaining the quality of service, response, and resolution times plus the appropriate escalation procedures based upon SLA requirements.

Real-Time Monitoring and Trouble Management

Allerium uses centralized management and monitoring systems that enable situational awareness across the NSOC team. Allerium follows a trouble ticket process whenever a system element does not function as expected.

The NSOC team is equipped with the tools required to monitor and manage all components of the State's NG9-1-1 system. This team works closely with engineering, defining a Tier 1-Tier 4 support structure to assign technical resources and a clear triage and escalation path to ensure Allerium meets or exceeds the SLAs required for operating the system.

Table 51. Levels of Assistance

Point of Contact	Expected Level of Assistance
Tier 1	Capture and triage
Tier 2	Mitigation/resolution
Tier 3	Advanced system analysis and troubleshooting/resolution
Tier 4	Release and patch changes

The NSOC provides NG9-1-1 services to multiple states and local government entities, upholds the high standards necessary for emergency services, and follows detailed provisioning and operations procedures to maintain network integrity at or above 99.999 percent.

Physical / Logical Security Measures & Strategies for Achieving 99.999% Uptime

Allerium maintains and applies policy requirements for technical and operational access controls to ensure physical and logical access is limited and authorized to the proper environment, equipment, networks, systems and information. All entities require pre-approval and identifying credentials to gain access to Allerium physical space and logical systems access. In addition, physical access controls include perimeter security controls, guards, surveillance cameras, and

intrusion detection. Logical access controls are role-based and include multi-factor authentication, designated passwords, and PINs. Unauthorized individuals are prevented from accessing the network via the following policy, technical, and operational controls:

- Strong passwords
- Multi-factor authentication
- Secure physical infrastructure
- Monitoring physical and logical access
- Secure network (e.g., firewalls)
- Updating systems and patch management software
- Implemented least privileged access.
- Encrypted data and systems

Allerium deploys redundant BCF capabilities at each network edge including the ESInet / NGCS, originating networks, and PSAPs. Allerium also deploys redundant BCF capabilities around the core 9-1-1 services for related ancillary services. Such ancillary services typically reside within a demilitarized zone (DMZ) of the ESInet to allow external access. All DMZs under Allerium's service leverage redundant BCFs.

Concerning Disaster Recovery / Business Continuity

We at Allerium understand and deeply appreciate the trust our customers place in us to support them and their businesses and public safety operations. Our mission has long involved advancing 9-1-1 services to meet the needs of our nation. Business continuity has always been a key focus of ours in supporting emergency response for our country's citizens. We remain resolute in ensuring continued delivery of best-in-class service to our customers while at the same time taking appropriate action to protect our team members who help deliver such critical services, the customer organizations that we support, and the public generally.

Allerium has long prepared for unexpected circumstances. For decades now, our teams have developed and tested comprehensive operational business continuity plans covering various aspects of our services from project implementation to customer support. Our preparedness includes:

- Locating our NSOC team and data center facilities in multiple locations across the United States to enhance our resiliency by ensuring geographical diversity.
- Maintaining redundant versions of our applications and solutions both logically and geographically, adding further diversity to the critical communication systems we support.
- Virtually monitoring, managing, and maintaining our networks and services by technical staff across the country.
- Developing sound staffing continuity and contingency plans to ensure continuation of services for our customers.
- Actively supporting social distancing objectives by implementing a work from home schedule, when necessary, for those personnel able to work remotely. Our NSOC team remains fully staffed 24x7x365 and continues to respond to customer needs.

- Maintaining well-established partnerships with state governments across the country and being designated as a critical infrastructure partner for prioritizing our staff and services.
- Where applicable, suspending all non-essential business travel under pandemic circumstances to protect Allerium, customer personnel, and the public. Allerium adheres to the recommendations of local and federal health officials.

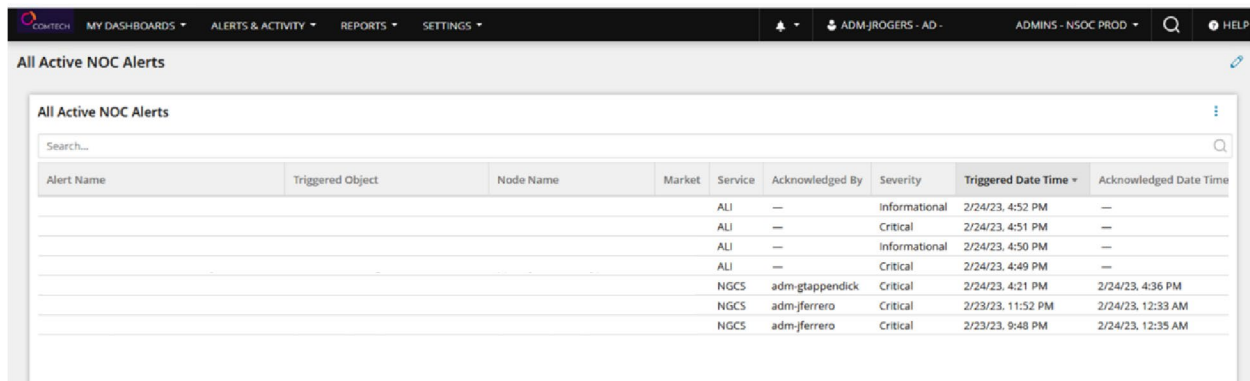
Our leadership is constantly reviewing and updating our approach to evolving events to ensure business continuity and service to our customers and reflecting those changes in the COOP. Beginning in March 2020, we activated our COOP because of COVID-19 to include secure remote access for a primarily remote work force. Allerium implemented a secure, work from home structure for essential workforce. This structure enables employees like our NSOC technicians to work remotely, when necessary, using virtual private network (VPN) and virtual desktop access as well as operations within Allerium facilities.

Allerium's NG9-1-1 operations continue to operate seamlessly and meet SLAs from a remote and onsite support perspective. This approach is important because, regardless of pandemics or weather-related issues like hurricanes, there is no loss of coverage, support, or responsiveness.

We continue to adapt and are proud of the response of our team and the clients we serve.

Continuous Performance Monitoring Mechanisms & Real-Time Alarm Generation and Notification Strategies

Allerium employs a monitoring platform to collect and monitor data from systems and applications used in the operation of ESInet and NGCS service functions. This platform provides real-time awareness of system health and operational status of the service. In conjunction with the monitoring platform, Allerium employs both dashboard and reporting tools for use by both internal and external users to measure operational performance.



The screenshot shows a web application interface for monitoring NOC alerts. The top navigation bar includes links for MY DASHBOARDS, ALERTS & ACTIVITY, REPORTS, and SETTINGS. The user is logged in as ADM-JROGERS-AD. The main section is titled 'All Active NOC Alerts' and contains a table with the following data:

Alert Name	Triggered Object	Node Name	Market	Service	Acknowledged By	Severity	Triggered Date Time	Acknowledged Date Time
				ALI	—	Informational	2/24/23, 4:52 PM	—
				ALI	—	Critical	2/24/23, 4:51 PM	—
				ALI	—	Informational	2/24/23, 4:50 PM	—
				ALI	—	Critical	2/24/23, 4:49 PM	—
				NGCS	adm-gtappendick	Critical	2/24/23, 4:21 PM	2/24/23, 4:36 PM
				NGCS	adm-ferrero	Critical	2/23/23, 11:52 PM	2/24/23, 12:33 AM
				NGCS	adm-ferrero	Critical	2/23/23, 9:48 PM	2/24/23, 12:35 AM

Figure 16. All Active NOC/SOC Alerts Dashboard

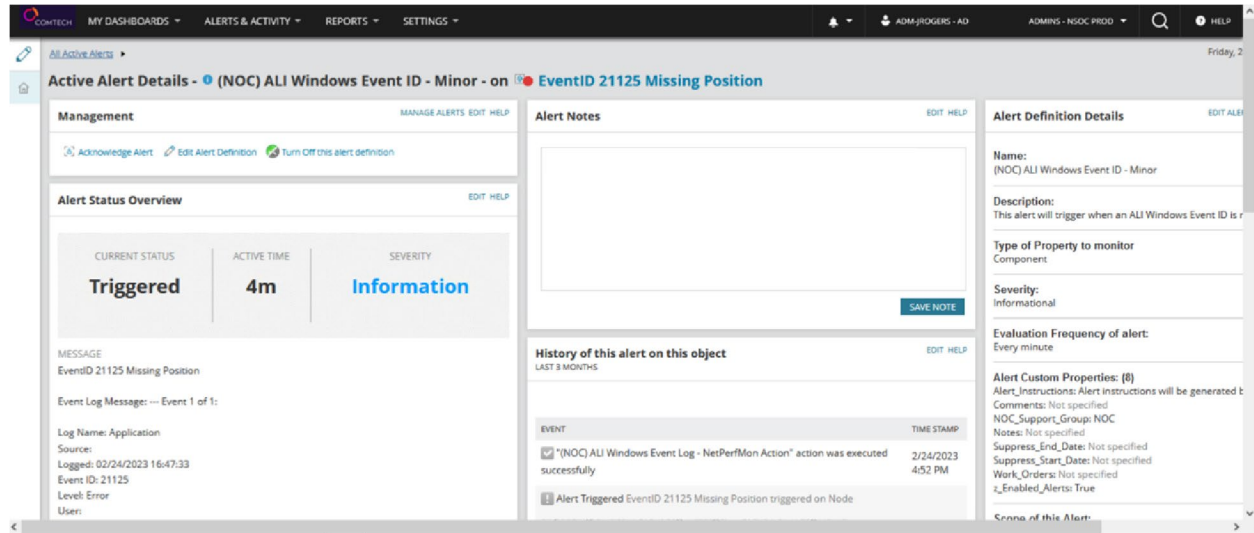


Figure 17. Node Summary of an Active Alert

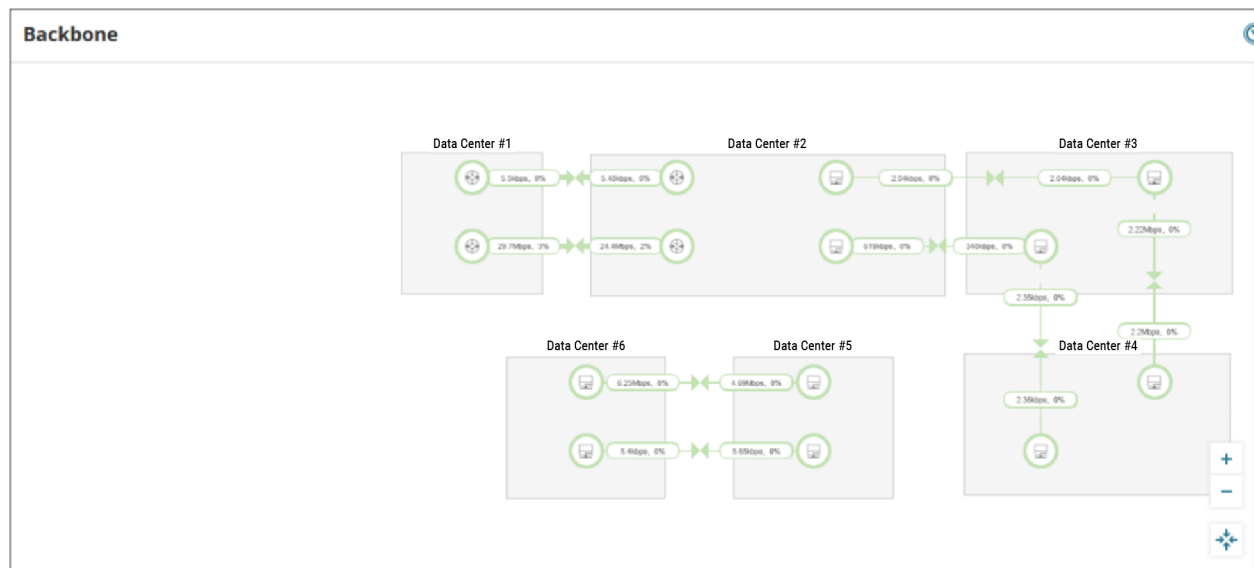


Figure 18. Major Backbone Network Connectivity Circuit Map

Routine, Update, and Emergency Maintenance Plus Comprehensive Disaster Recovery Plan

Allerium maintains a disciplined, automation-enabled Change Management framework purpose-built for the operational sensitivity and uptime requirements of NG9-1-1 environments. Our approach integrates structured governance, rigorous testing, formal approval workflows, vendor coordination, and proactive communication to ensure that all system modifications are executed with precision, transparency, and minimal service risk.

Governance and Control Framework

All production changes are governed through Allerium's enterprise IT Service Management (ITSM) platform (Remedy), which enforces standardized workflows, documentation requirements, approval routing, and audit traceability.

Each change request (CRQ) requires a fully documented Implementation and Backout Plan (IBOP), detailing:

- Scope and business justification
- Technical impact assessment across interconnected systems
- Risk classification and mitigation steps
- Validation and testing procedures
- Step-by-step implementation instructions
- Defined backout methodology

No non-emergency production change is executed without advance notice, documented approval, and customer-aligned communication.

Allerium's change governance extends beyond internal systems. We actively coordinate with third-party vendors, carriers, hosted platform providers, and infrastructure partners when their maintenance activities may impact the NG9-1-1 ecosystem. Vendor-led changes are reviewed through the same structured risk evaluation process, scheduled within approved maintenance windows, and monitored by our NOC/SOC to ensure unified situational awareness and accountability across all stakeholders.

Testing, Validation & Risk Mitigation

Prior to production deployment, all changes undergo structured validation in Allerium's dedicated lab environments. Test results are formally documented and attached to the IBOP record within the ITSM system to ensure technical completeness and operational readiness.

For complex or higher-risk modifications,

- Cross-functional Change Advisory Board (CAB) review is required.
- Director-level oversight is enforced for Level 1 and Level 2 changes.
- Client-facing Change Control Boards (CCB) may be convened when required by State governance.
- Vendor stakeholders are included in coordination discussions when applicable.

To further strengthen risk prevention, CAB meetings are held twice weekly to provide timely review of increasing change volume and complexity. This enhanced cadence reduces backlog risk, improves scrutiny, and minimizes change-related service disruptions.

Structured Approval & Oversight

Approval authority scales according to risk and impact:

- Routine operational updates may be completed within ITSM workflow.
- Moderate to high-impact changes require CAB review.
- Vendor-initiated maintenance impacting shared infrastructure is incorporated into the CAB review process when appropriate.
- Emergency changes follow an expedited Emergency IBOP process with shortened approval timelines and post-implementation review.

The Change Manager chairs and facilitates all CAB sessions, ensuring:

- Complete documentation and approvals prior to review
- Structured evaluation of technical quality and operational readiness
- Cross-functional accountability
- Vendor coordination when applicable
- Formal decision recording and follow-up tracking

This governance model ensures transparency, accountability, and alignment across Engineering, Operations, NOC/SOC, vendors, and program leadership.

Communication & Stakeholder Transparency

Allerium utilizes an automated notification platform supporting user-defined escalation tiers and multi-channel delivery (email, SMS, and voice). Notification preferences are established during implementation and may be modified at the State's request.

Stakeholders receive:

- Advance notice for scheduled changes
- Pre-work emergency notifications when applicable
- Vendor maintenance coordination notifications when third-party systems are involved
- Post-implementation confirmation
- Escalation updates if abnormal conditions are detected
- This structured communication model ensures that States, PSAPs, designated third parties, and vendor partners maintain continuous situational awareness.

Release Management & Operational Protection

Upon final approval, each change is scheduled with notifications sent to all stakeholders and it is moved to our release / maintenance calendar. No overlapping production changes are scheduled within the same window. Maintenance windows are aligned to lowest risk time period depending on the work being done. Vendor maintenance windows are coordinated to avoid cumulative or cascading risk. The NOC/SOC actively monitors release execution in real time. Customer-reported events are correlated against active change activity.

This layered monitoring model enables immediate detection of abnormal behavior and rapid rollback if necessary.

Disaster Recovery Plan and Business Continuity

Allerium maintains a NIST 800-53 compliant contingency planning policy and program encompassing business continuity, disaster recovery, and continuity of operations components. Allerium systems are technically designed with fault tolerance, replication, and redundancy to aid in faster recovery and reduced data loss. The Contingency Planning Program consists of the following:

- **Business Impact Analysis:** Includes business functions with dependency mapping to technology, process, and resource requirements to support the business's day-to-day operations.
- **Business Continuity Plan (BCP):** Details the functional, technical, and resource plans for recovering from a business-impacting event and plans for resuming normal business operations.
- **Disaster Recovery Plan (DRP):** Features short and long-term plans to restore the technical and operational resources required to support essential business functions.
- **Operational Capacity Plan:** Identifies the minimum process, telecommunications, and support services necessary for systems and services during a potential event.
- Annual review, training, and testing of contingency roles, responsibilities, plans, and applicable components.

Allerium ensures its clients receive notifications in a timely manner and establishes a tailored escalation procedure for service-impacting incidents, including critical service outages for Allerium and its subcontractors. We invoke our BCP and DRP in the event of a catastrophic failure of all or a significant portion of the 9-1-1 services, allowing for substantial time to repair or mitigate any adverse impact on public safety.

Allerium's sample, non-confidential COOP which features a BCP and DRP as well as a table of contents from our comprehensive, confidential COOP is included in Appendix 6: Sample COOP for the State's review.

Allerium's NG9-1-1 operations continue to operate seamlessly and meet SLAs from a remote and onsite support perspective. This approach is important because, regardless of pandemics or weather-related issues like hurricanes, there is no loss of coverage, support, or responsiveness.

We continue to adapt and are proud of the response of our team and the clients we serve.

RPO/RTO Measurement

Allerium deploys our NGCS in active/active pairs (with three such pairs in use for the State, totaling six active applications running in parallel). This active/active architecture ensures we comply with 99.999% uptime requirements and other metrics outlined as service level agreements (SLAs). As such, we do not measure our service per RPO and RTO metrics as our objectives, using an active/active architecture, are for near-instantaneous recovery points and times. This approach is governed by the SLAs and the architectural design and does not use RPO and RTO as those metrics are designed to allow for acceptable losses of service and data, which we do not.

Procedures for Service Restoration Post Incident

Service restoration procedures follow one of two scenarios:

1. Service impairment in the core network/service and
2. Service impairment at the edge/PSAP (addressed below as part of PSAP Contingency Planning).

Regarding core services, Allerium incrementally backs up all computer elements in the network on a nightly basis and schedules full backups once per week. We will follow this process for all systems provided as a part of the proposed solution. We manage all network gear configurations from a central configuration management tool, thereby enabling seamless restoration of any lost configuration. Full local and geo-redundant architecture allows for backup restoration without any negative service impact.

Allerium can manually trigger on-demand backups of all computer elements at any time outside the normal rotation. Our network engineering staff backs up network configurations into centralized management software and maintains those configurations.

Allerium's systems administrators manage daily backup schemas for data and system platforms. Should a restoration of any item become a priority, the Allerium NSOC acts as the POC to generate the support request for Allerium's engineering staff.

PSAP Contingency Planning and Service Restoration

During project planning and data collection, Allerium works with PSAPs to collect details entailing how PSAPs would like to manage call delivery if a PSAP is unable to operate normally. Allerium then provisions business logic into the PRF of the Allerium NGCS. If a PSAP desires to engage the PRF policies surrounding an outage or evacuation, a PSAP may call the Allerium NSOC team or access the PRF web UI to enact abandonment rules. The Allerium PRF also allows for detection of many network or CHE error conditions. Rules may be built to divert calls to alternate locations in such outage conditions.

Allerium's PSAP contingency plan template clearly outlines the steps taken to maintain or restore service in the event of an incident or interruption. The plan is based on the information gathered during the site survey, including the PSAP's mutual aid agreements, backup sites if any, and options for survivability. The plan takes these details into account for each site and is tailored to that site to ensure the best restoration possible.

Allerium will arrange to review the plan annually. Our program team will ensure each PSAP is scheduled for review of the plan as well as other annual maintenance tasks in a collaborative fashion.

Proactive Outage Prevention and Response Strategies

Allerium is proactive in both service design and outage prevention strategies. Our active/active architecture is designed to proactively prevent outages due to the load balancing we employ for all transactions. In addition, we regularly test the load balancing and active/active architecture through scheduled maintenance. During scheduled maintenance, one of the active systems will become unavailable as the maintenance starts. This mimics a run-time scenario where unplanned events would likewise make a system/service unavailable. By monitoring the load balancing and system response to the planned maintenance, we proactively ensure that our outage prevention mechanism are properly functioning.

Core routing architecture with diverse paths and load balancing

Allerium's proposed solution is a NENA i3-compliant platform committed to the "five nines" standard (99.999 percent reliability) for providing the delivery and receipt of 9-1-1 calls. The solution minimizes single points of failure and is composed of redundant central system components that provide load sharing and load balancing with failover capability. Manual intervention is not required since the solution is designed as a redundant system that employs automatic "failover" although we note that term is not applicable to active/active systems (that is, "failover" simply results in the surviving systems receiving more traffic - there is no "failover" in that regard). We configure our routing protocols with appropriate timers to mitigate instability anomalies such as faulty devices or unstable connectivity.

Allerium designs and operates its NG9-1-1 deployments in a highly diverse and resilient manner that ensures there are no single points of failure in the core network. Allerium uses device- and network-level redundancy, the pooling of resources, plus load sharing and policy routing to eliminate any single points of failure. Primary network- and systems-level devices and applications are designed and deployed in highly available pairs, ensuring that each device or system is fully capable of supporting 100 percent of call-routing volume, should the other device or system fail.

Figure 19 below depicts Allerium's data center footprint which includes geo-diverse sites located across the country. Each data center contains a redundant application stack of NGCS FEs, all operated in an active/active, load-balanced, secure solution achieving not only geo-diversity but local redundancy as well.

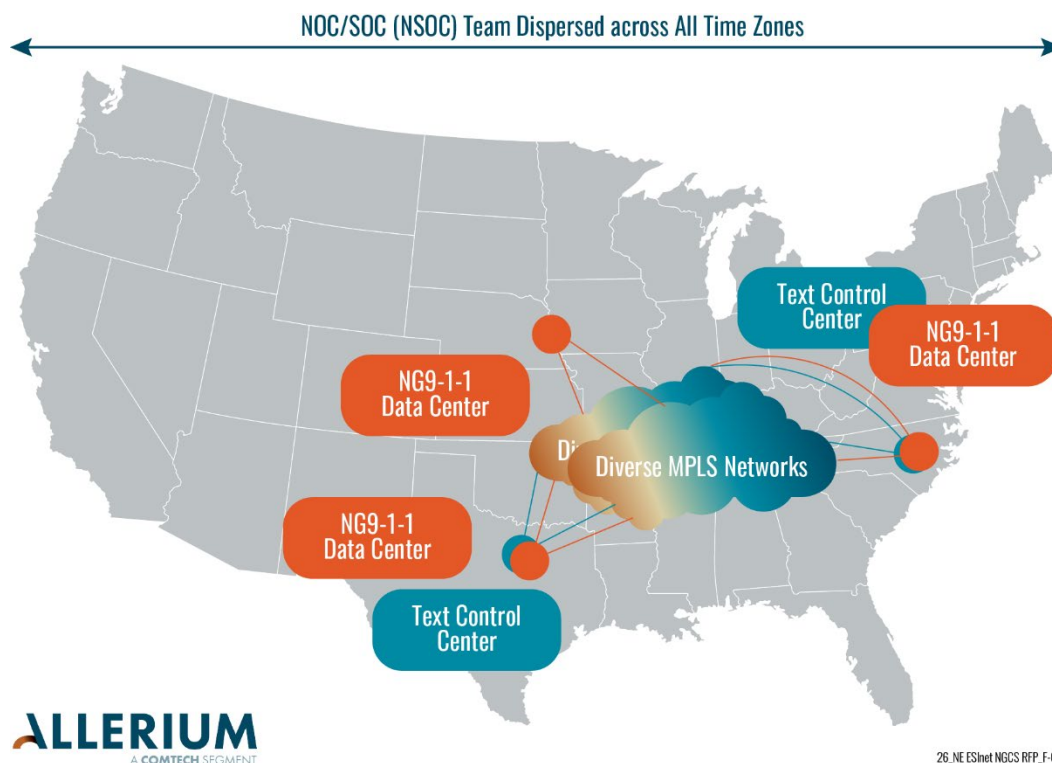


Figure 19. National System Design View

Figure 20 is a simplistic view of the designed redundancy methodology across the data center sites. We deploy each FE with both local and geographic redundancy as illustrated by the

redundant ESRP and PRF deployment in Figure 20. We deploy all other elements in similar fashion. This redundancy results in a total of four elements being available for each function.

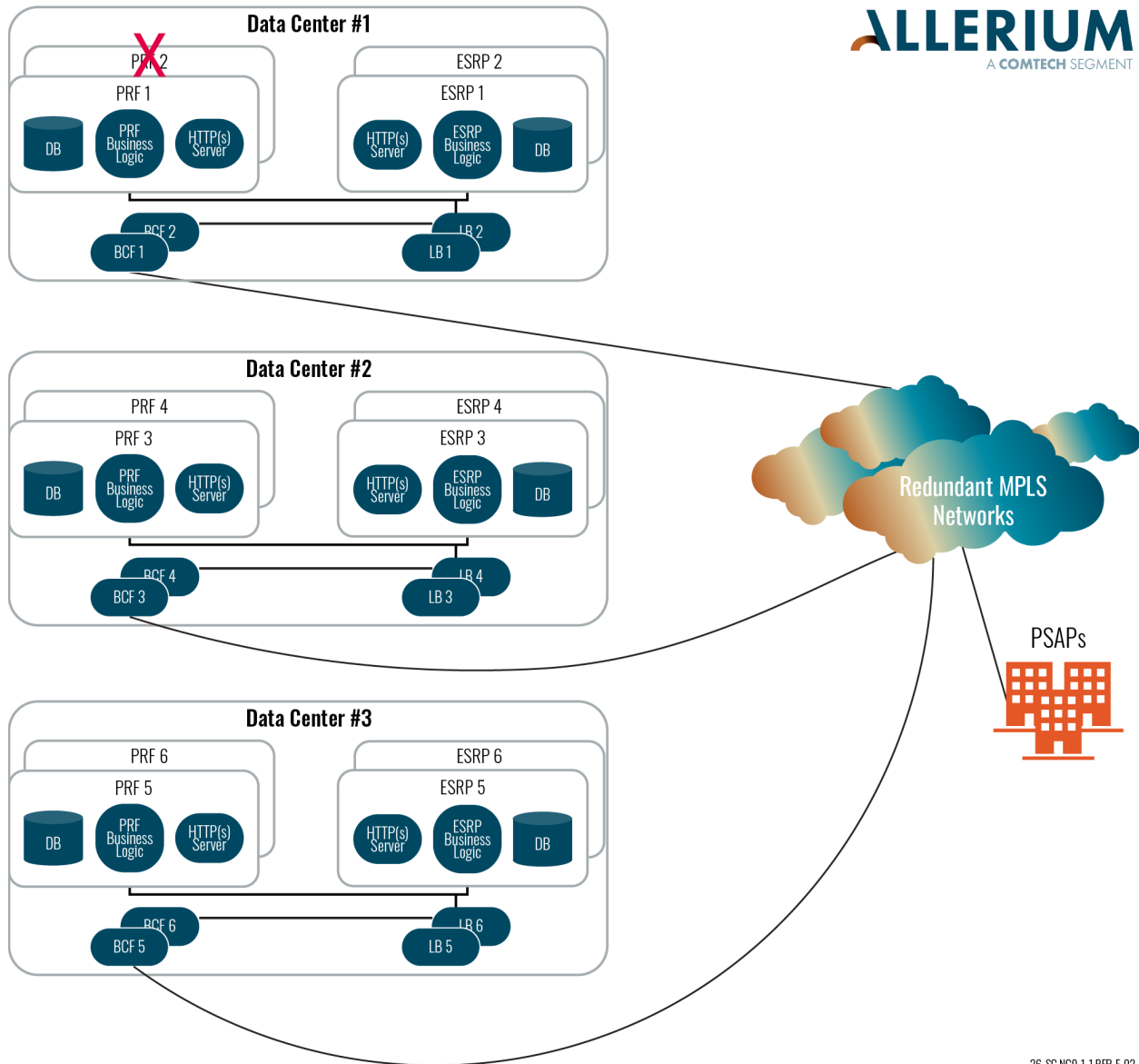


Figure 20. Failure of a Single Element or Connection

One of the common areas that needs to be reviewed for single points of failure is the ESInet, particularly the last-mile circuit connectivity. The Allerium NGCS and ESInet service design uses several different configurations of network connectivity, depending on what is available at each site. For instance, at well-connected PSAP call handling sites (which is true for all Nebraska host CHE locations), the network configuration includes the deployment of two independent Multi-Protocol Label Switching (MPLS) WANs to create the ESInet as depicted in Figure 21 below. Allerium configures all Open Systems Interconnection (OSI) layer 3 routing devices and implements the Bidirectional Forwarding Detection (BFD) protocol on each link and tunnel. BFD in combination with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) routing

protocol designs allows for configurable detection to initiate network convergence to maintain high availability in the network. The BFD protocol exchanges hello packets between the two routing devices on a link on a configurable interval in each direction. Thus, the BFD will trigger a link failure detection if the configured number of consecutive hello packets are missed which would trigger a network convergence onto a surviving path.

Figure 21 is **ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION**.

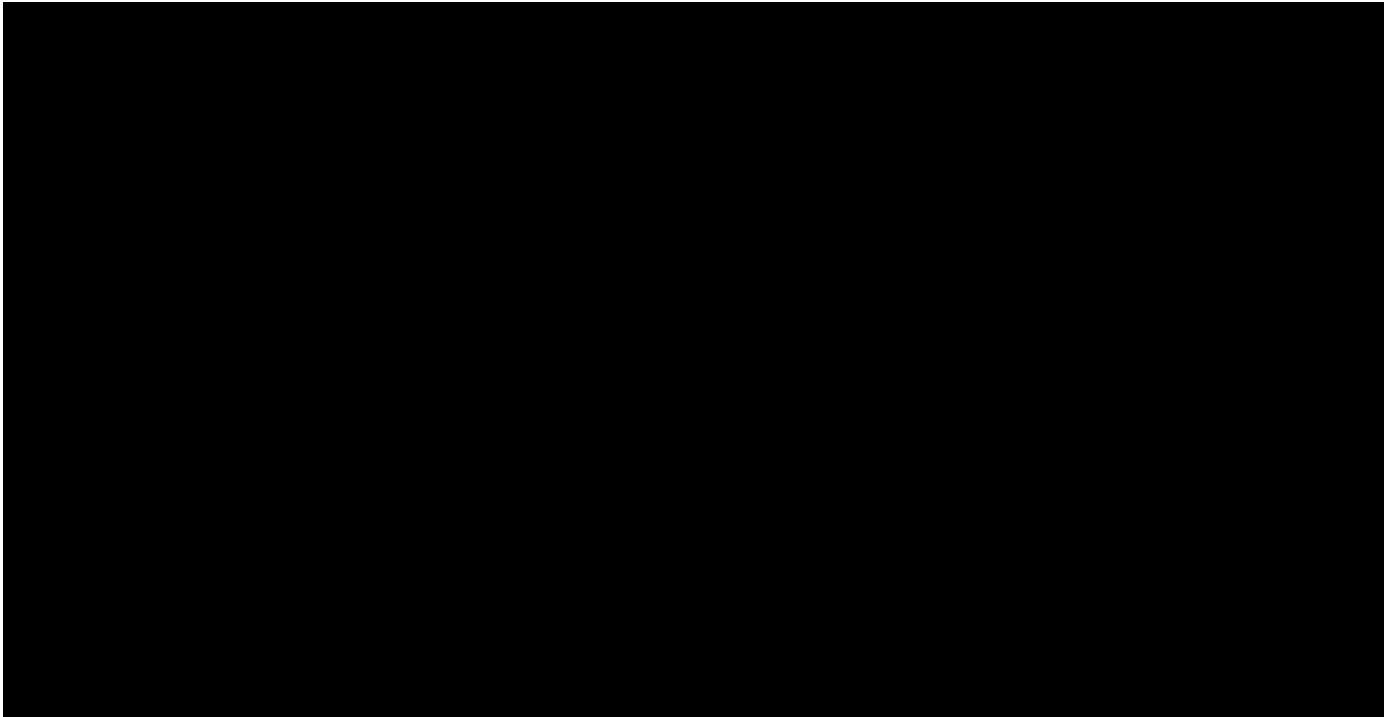


Figure 21. Diversity and Redundancy by Design (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

Allerium voice traffic will automatically reroute around functional elements that are having an adverse impact on audio traversing the element if the impact is related to a loss of connectivity or a failure of the element or its interface components. Additionally, traffic will be automatically rerouted if the adverse impact is due to network congestion or an impaired traffic path. By way of example, consider the case for network traffic convergence where Allerium has designed the system for no single point of failure and fast convergence times. Allerium does this by leveraging dynamic routing and configuring Quality of Service (QoS) to ensure BFD packets are treated as mission critical and queue priority is just below the real-time queue, sending ahead of most other traffic types on the ESInet. The QoS settings provide BFD high priority to detect link failure in the tight time window required.

The detection of a link failure by BFD is configured to trigger the routing protocol (BGP/OSPF) to recalculate the routing table. Allerium configures both the ESInet and NGCS networks to have four routes and uses route summarization to minimize the number of routes which are in the route table. Therefore, when the routing protocol has to reconverge, the convergence is very fast.

For example, Table 52 contains the PSAP locally connected interface routes (Voice, Workstation, Administrative, and Blue MPLS interfaces) for PSAP-1 Router 1 (RTR-001, the primary PSAP router for local devices). Router 1 receives over the encrypted IP Security (IPSec) tunnel, the summarized

POP-1 route from POP-1 RTR-001 and the summarized POP-2 route from POP-2 RTR-001. The routes over the IPsec tunnels are in a different Virtual Route Table than the MPLS interface, enabling a one-hop route to the POPs, skipping the potential multi-node convergence which may exist in ESInet carrier networks. Finally, the route table contains the two summarized POP-1 and POP-2 routes provided by PSAP-1 RTR-002 from the Red ESInet's IPsec tunnels. Weights are applied to each of the POP routes to ensure symmetric IP routing and predictive pathing while still enabling the failure of three POP routes as the higher weights (lower priority routes) take over.

Table 52. Demonstrative PSAP-1 RTR-001 Route Table

Route	Weight	Hop	Notes
Voice	0	Local	
Workstation	0	Local	
Administrative	0	Local	
POP-1 RTR-001	100	Blue MPLS Router	Only for IPsec tunnel use
POP-2 RTR-001	200	Blue MPLS Router	Only for IPsec tunnel use
POP-1 Supernet	100	POP-1 RTR-001	
POP-1 Supernet	300	PSAP-1 RTR-002	
POP-2 Supernet	200	POP-2 RTR-001	
POP-2 Supernet	400	PSAP-1 RTR-002	

There are numerous failure scenarios for the ESInet, including local circuit failure, intermediate circuit failure with loss of tunnel routes, and POP circuit failure. The routing protocol will remove the failed link's routes, leaving the remaining routes available for forwarding packets. If the route(s) removed do not include the best weighted route, there is no impact. If the route(s) removed include(s) the best weighted route, the router sends packets down the next best remaining weighted route. Worst case for PSAP-1 would be the loss of the blue circuit. In this case, RTR-001 will forward packets to RTR-002 while sending RTR-002 the route update, thus having RTR-002 remove the routes on the blue ESInet provided by RTR-001. The route update is very small and local, allowing for less than 20ms processing, though the update of RTR-002 table is not required for traffic to continue to forward packets.

Finally, the same process happens in the POP's RTR-001 and RTR-002, with the impact being a larger route table containing all PSAPs. Allerium deploys routers to the POPs with significantly more processing and memory as well as 10 Gbps ethernet links which enable faster movement of the routing update packet(s).

Interfaces with hosted solutions or third-party providers

Interfacing with hosted solutions and third-party providers takes two forms:

1. Physical/logical interfacing, including interoperability, and
2. Operational interfacing to ensure a high-quality service delivery and issue resolution as applicable.

Regarding the logical interfacing and interoperability, Allerium notes that the primary third-party providers in Nebraska include the MIS reporting system using 911 Logix, hosted call handling systems (both cloud and in-state), and ADR providers, including others. Allerium works hand-in-hand with 911 Logix in multiple other statewide deployments and is extremely confident that we meet all needs for data sharing processes to support the State's MIS system. In addition, Allerium has performed IOT with all major CHE manufacturers, including those deployed in the State:

- Allerium (Solacom),
- Intrado, and
- Motorola.

Allerium always arranges IOT and has the infrastructure and program in place to certify any new CHE manufacturers in addition to re-certifying existing manufacturers when releasing new NGCS routing software.

Regarding operational interfacing with third parties, Allerium's NSOC uses defined processes for incident and problem resolution and change management activities. Our team's close work with 9-1-1 carriers, PSAPs, and other stakeholders relies on well-defined and documented workflow and roles and responsibilities to ensure quick and appropriate identification, classification, and resolution of incidents and problems regardless of the origin.

Our NSOC currently supports regional and state-level systems, providing incident and problem resolution support incorporating third-party provider systems ranging from CHE providers to ESInet and NGCS providers offering non-native solutions, including but not limited to:

- Real-time monitoring of third-party systems when available (if true integration is not available, a NOC-to-NOC process is put together which ensures we are notified of any impairments or maintenance and in turn make you aware),
- Ticketing and escalations with third-party systems, and
- Performance data collection.

The Allerium NSOC has well-defined methods, processes, procedures, and work instructions for all facets of support and maintenance, based upon ITIL principles and industry best practices. We maintain all NSOC procedural documentation in a digital library with online access for all staff members plus hard copies available for quick reference. All documentation updates go through a review-and-approval process, and the latest approved documents are available online.

Fault zone design methodology identifying critical components and failure points

Allerium's fault zone design methodology for NGCS/ESInet components maintains the principle that faults are inevitable and must be contained. The objective is to ensure that any single failure—whether physical, logical, or operational—does not propagate beyond a defined boundary or disrupt end-to-end call processing.

In principle, we design "zones" around our NGCS applications as well as network segments. Each zone is anchored by a fully independent NGCS stack of applications and redundant network connectivity in the ESInet. Each zone includes a complete set of core services, including the Emergency Services Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Location Validation Function (LVF), Border Control Function (BCF), and supporting data services. Each NGCS "zone" is comprised of two locally redundant service stacks, with each capable of handling

100% of the State's traffic. Likewise, each zone has redundant and diverse network paths that are also sized for 100% of possible call volume.

The methodology begins with identifying relevant failure scenarios, including fiber cuts, data center outages, software defects, misconfigurations, and cyber events. By maintaining geographic redundancy (three separate data centers), network redundancy (diverse fiber providers), and operational redundancy (multiple NOC/SOC locations and logical path redundancy), we ensure that any failure is contained within the zone it occurs.

With our active-active architecture traffic is distributed across zones during normal operations, allowing each zone to function under load. In the event of a failure, traffic is automatically redirected without manual intervention.

In summary, our fault zone methodology ensures NGCS and ESInet service resilience by combining independent zones, active-active operation, true path diversity, and controlled logical call routing, resulting in a service that continues to function despite localized failures.

Bandwidth management protocols prioritizing emergency traffic

Allerium prioritizes emergency traffic through bandwidth design, scalability, and routing protocols. Allerium designs the initial network to ensure bandwidth is available to meet the service expectations without blocking or limiting the service level. Our bandwidth management methodology consists of monitoring bandwidth use and alarming/reporting on usage exceeding defined thresholds.

Bandwidth Design and Scalability

Allerium's resilient and redundant IP network core is capable of capacity growth commensurate with both planned and actual traffic and usage for the life of the State's contract. Our proposed design includes two diverse fiber paths to each ESInet endpoint but our service also has the capability to include broadband, LEO satellite, and wireless connectivity managed under a SD-WAN service, all of which are scalable without disruption.

The network can scale to accommodate up to 1 Gbps on the standard hardware ports for terrestrial connectivity, thereby ensuring future capacity growth and expansion. The backbone not only accommodates 9-1-1 call volume growth but also has the capacity to support future applications (e.g., call-handling systems, CAD, logging systems, geographic information system [GIS] data, streaming media, real-time text [RTT], IP traffic, traffic management systems, communications systems, and incident management systems).

The upgrade process will not interrupt, degrade, or in any way negatively impact network connectivity or established functionality for any system user. Allerium will perform any hardware change needed to accommodate bandwidth increases as a planned maintenance event and communicate those changes in advance to the State and PSAP personnel.

Routing Protocols

Allerium's solution includes a QoS structure using differentiated services code point (DSCP) markings based on the NENA i3 version 3 standard as outlined in Table 53. This table specifies ESInet-specific traffic. Allerium marks other traffic (e.g., dynamic host configuration protocol [DHCP], internet control message protocol [ICMP], border gateway protocol [BGP], etc.) according to industry standards and best practices.

Table 53. QoS Markings

DSCP	Use	Per-Hop Behavior (PBH)
0000 00	Routine Traffic except as specified	Default (Best Effort)
0000 11	9-1-1 Call (SIP) Signaling (including noninteractive calls) and emergency call related HTTP/S operations, DNS traffic	AF12
0001 11	9-1-1 Text Media (RTT and MSRP)	AF12
0010 11	9-1-1 Audio Media (9-1-1 calls and admin calls)	EF
0011 11	9-1-1 Video Media	AF11

Any bandwidth sharing arrangements with implications for priority traffic

Allerium does not share bandwidth with non-emergency traffic unless ancillary service network segregation is designed for, and approved by, the State. Within the context of priority traffic management, we provide QoS markings for priority traffic as outlined in the answer immediately above.

For background information, we provide at least 10 Mbps (depending on the size of the PSAP) as a starting bandwidth. Given the requirements and Allerium's design, the state network can scale from its starting capacity (bandwidth) upwards without blocking or limiting the overall network service level. There is no need for a "forklift" of existing copper-based facilities and equipment to replace with fiber and associated equipment. For instance, routers installed at PSAPs support 1 Gbps ports for expansion.

Allerium designed the network in such a way as to add more PSAPs, services, or interconnectivity to other networks for network growth. In these instances, Allerium does not anticipate any hardware or network capacity expansion costs outside of those costs to physically connect a new end point (e.g., PSAP) to the ESInet or to increase bandwidth.

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

Allerium proudly provides an end-to-end service and we strive to address every issue within the NGCS/ESInet environment directly on the behalf of the State and PSAPs (no "finger pointing" when it comes to resolving issues). We work to collaboratively resolve all issues with the 9-1-1 service, including those outside of our span of control. Some issues occur outside of control as 9-1-1 services span OSPs, NG9-1-1 providers, and call handling providers, as well as various third parties the State or PSAPs have elected to use. Our span of control is well documented in our interface control documents (ICDs) which are provided as documentation in support of this response. A general sense of understanding can be described as follows, which outlines our span of control in our:

- **Ingress/Aggregation Service:** Allerium's span of control starts with the aggregation service, which takes the form of points of interconnection (POIs) that act as the "gateway" for OSP traffic to enter the 9-1-1 ecosystem. Our span of control includes the POIs themselves and all circuits connecting the POI locations to the rest of the NG9-1-1

infrastructure. OSPs are responsible, per the FCC, to provide ingress circuits to the POI locations.

- **NGCS Service:** Allerium's span of control in the NGCS service areas is extensive and includes all call routing, call control, and network management between/through the OSP aggregation service all the way to the ESInet edge. Third party providers we transit data for, or provide data to, are outside of this span of control. For instance, collecting and sending data to 911 Logix is within our span of control, but the 911 Logix service itself, having been procured outside of this RFP, is outside of our control.
- **ESInet Service and the PSAP Edge:** Allerium's span of control includes the ESInet and the service delivery that uses that network, including the OSP aggregation circuits, core NGCS ESInet components (SBCs and network routing components) and the ESInet between the NGCS and PSAP LAN edge. Our span of control as it relates to the PSAPs is through the Allerium-provided edge equipment up to the PSAP LAN edge that connects to the PSAP hosts. Any remote PSAP that uses that host is on the PSAP network and is thus outside of Allerium's control.

No Single Point of Failure

Allerium designs and operates its NG9-1-1 deployments in a highly diverse and resilient manner that ensures there are no single points of failure in the core network. Our solution for the State provides connectivity to:

- **Hosted PSAPs:** Per the RFP, all PSAP sites are considered to be in a host/remote configuration today, using a separately procured regional network solution(s) to connect the hosts to the remotes. Our solution provides dual and diverse fiber connectivity to each of the CHE host sites in the state, including the cloud-deployed CHE sites.
- **Direct Connectivity to Remote PSAPs:** There are assumed to be no directly-connected remote PSAPs in the state (meaning, PSAPs that would move from their current regional networks directly onto a state-supplied ESInet). However, our solution allows for regional network replacement with our ESInet, if such a development were of interest to the State. In which case, Allerium would provide a minimum of two connections to each of these sites.
- **Standalone PSAPs:** There are assumed to be no standalone PSAPs in the state. However, our solution allows for such a deployment wherein we would provide a minimum of two connections to each of these sites.
- **Allerium-Provided Facilities:** Allerium installs call aggregation points of ingress (POIs) in two locations for the State and provides a total of four connections to these two sites. Similarly, these POI sites are connected to the NGCS core data center facilities in Council Bluffs, IA, Dallas, TX, and Raleigh, NC, which will use these circuits, as well as a more complex arrangement of circuits to interconnect to additional Allerium systems (such as Text to 9-1-1 and our internal monitoring networks, as examples). All circuits within the solution are designed for no single points of failure.

Our ESInet diversity strategy is based on selecting the best-available network resources for each site. Since we do not own or sell fiber networks, we have no interest in forcing the State to use "our" network facilities. Instead, we evaluate all network options for each site and choose the best paths available for our ESInet. Since each site may have a different set of network options available, our

ESInet is designed to take advantage of different technologies. Regardless of technology, our design ensures there are at least two redundant and diverse network paths to each endpoint.

Our ESInet for the State uses diverse fiber-based MPLS WANs for each endpoint. MPLS networks are preferred due to the low-latency and high-availability designs of those networks, which are ideal for voice traffic quality. Additional redundancy is available through the use of wireless transport (including satellite) and we look forward to discussing this with the State.

While the focus in this section has been related to last-mile connectivity, it is important to realize that all other aspects of our service employ the same design philosophy that enhances our solution and prevents single points of failure.

Detection and Activation of Standby Systems if Not Active-Active

Allerium's service is designed for active/active call routing across three data centers, using a combination of load balancing and both local and geographic redundancy.

ESInet Interconnection Points with OSPs and PSAPs for Full IP-based NG9-1-1 Functionality

Allerium supports an end-to-end fully IP-based NG9-1-1 routing service. Our ESInet is designed to deliver emergency traffic from the OSP to the PSAP using IP delivery methods while simultaneously supporting each edge with legacy gateways, if needed. We support the FCC's guidance as provided in the FCC R&O regarding OSP ingress and will require all OSPs to connect via IP. If that requirement can not be met by the OSP, we support a variety of other methods to ensure that our service continues without interruption. Likewise, we support IP functionality all the way to the PSAP edge. If a particular PSAP/host cannot support a NENA i3 interconnection, we provide legacy gateway functionality in order to keep the project moving forward. For certainty, we completely support and intend to deploy on fully IP-based functionality, but we also can support other connectivity options if needed by third parties.

5.1.1. Architecture and Topology

5.1.1.1. ESInet Diagrams

1.1. Architecture and Topology

1.1.1. 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.*

Response:

ESInet Diagrams Overview

Allerium generates architectural drawings, designs, rack layout, wiring diagrams and supporting documentation for every deployment. Allerium provides an operational as-built document in an electronic format which encompasses all aspects of the solution deployment. These documents are kept current and provided in a centralized knowledge base that the State can access at any time. As noted in the requirement, such diagrams are produced as part of the deployment activity and as such, we have provided sample information in Appendix 5: Sample Design Documentation. In addition, we've provided general information to aid in review of our proposal in the responses immediately below.

Comprehensive diagrams illustrating network maps (logical and physical topologies).

As-built documentation will be provided to the State prior to system final acceptance. Allerium's transitional and end state documentation packages will be detailed documents specific to each PSAP and Allerium's ESInet/NGCS solution. These documents will:

- Provide network maps showing both logical and physical topologies,
- Provide details for each facility, application, service, and appliance,
- State whether the application is virtualized, a physical appliance, or a server-based or cluster-based component, and
- Supply the system-level designations and names of the physical and virtual mappings.

Allerium will provide a task completion form at the conclusion of each milestone for mutual signoff. Any non-service-affecting punch list items will be documented on the task completion form. Upon signed approval by both parties, Allerium will proceed to the next project phase. The milestone and its related payment will be subject to the State's review and confirmation that all punch list items have been completed, closed, and documented on the task completion form.

The Allerium team will engineer, furnish, install, secure, test, and make operational a turnkey ESInet/NGCS solution for the State's implementation and transition. The migration to NG9-1-1 will occur in a series of phases with intermediate milestones and deliverables.

Physical and logical path diversity for redundancy.

Allerium's network maps will show physical and logical path diversity and will note any shortcomings in these areas as well (for instance, if a PSAP site does not have physically diverse entrance facilities).

One-time and transitional network elements.

Allerium's service does not include any one-time network elements but does include transitional network elements. These transitional elements include:

- **Location Database (LDB):** By nature, the LDB is a transitional element that bridges the gap between the legacy ALI database and the OSP-provided LIS. Our LDB allows for legacy process (ALI SOI files) while enabling NENA i3 location delivery.
- **Legacy Network Gateway (LNG) and Legacy Selective Router Gateway (LSRG):** These elements are transitional until such time that all OSPs support IP networking and all legacy selective routers are retired. Allerium provides these functions on an as-needed basis and has assumed that each will be necessary for the initial deployment period.

- **Legacy PSAP Gateway (LPG):** The LPG is used when a call handling system can not interface directly with a NENA i3 network. A LPG is sometimes necessary for CHE that can handle IP network connections but doesn't yet convey location in the proper form to be NENA i3 compliant.

Allerium has been designing and deploying ESInets for nearly 15 years and excels at meeting OSPs and CHE hosts "where they are" to ensure our deployments stay on track.

Network ingress and egress points with connections to OSPs, PSAPs, and external interfaces.

Network ingress and egress connectivity is governed through the use of our interface control documents (ICDs). These documents have been in use for years and provide invaluable connection detail that ensures each OSP, PSAP, and third party understands exactly how to interface with our ESInet. Sample ICDs are provided as part of this response.

Transport types (e.g., MPLS or Ethernet) with port speeds.

Our design documentation will include both the above-mentioned ICDs as well as as-built documentation. Our as-builts are compiled once we complete the necessary survey and design work for each endpoint. Once completed, the as-built documentation will provide a record of the transport type and port speeds for each network end point.

Allerium has designed the State network to use dual MPLS connections on diverse fiber circuits. This is a great configuration to ensure that voice, which requires low latency and a high-performance network, achieves the best quality possible. MPLS has been the standard for voice communications for many years and we have confirmed diverse MPLS connectivity exists for each PSAP host location.

Port speeds on our edge equipment will not be an issue as we support 1 Gbps ports on the edge. Coupled with a fiber network, the State will have as much scalability as needed to support not only current PSAP operations, but also as much bandwidth as necessary to support future capabilities and/or ancillary network needs.

Capacities and estimated bandwidth at ingress, core, and egress points.

Our final design documents will record the capacities and configured bandwidth at each ingress, core, and egress point. As a general guide, we provide capacity on all network segments that is designed for non-blocking traffic. Each network segment is evaluated for the maximum number of simultaneous calls possible and then increased to accommodate overhead and to ensure capacity. By way of example, we estimate core bandwidth needs by assuming every position at every PSAP can simultaneously have 1.25 calls (with the extra 0.25 representing conference calls) at a codec rate of 128 Kbps (the G.711 codec uses 64 Kbps per call, which we double for increased capacity and overhead). Therefore, across the entire State deployment of 224 positions, the core network bandwidth is estimated at a minimum of:

$$128 \text{ Kbps} * 224 \text{ positions} * 1.25 = \sim 36 \text{ Mbps}$$

However, given explicit guidance in this RFP for bandwidth of 1 Mbps per PSAP + 1 Mbps per position (in the case of a single circuit situation), the above calculation is adjusted to:

$$(1 \text{ Mbps per PSAP} * 70 \text{ PSAPs}) + (1 \text{ Mbps per position} * 224 \text{ positions}) = 294 \text{ Mbps}$$

Given this consideration, core circuits are sized for a minimum of 300 Mbps per circuit (with redundancy in the circuits this metric doubles, which is in accordance with the RFP's design goals).

For clarity, while this bandwidth sizing information is provided as a design example at 300 Mbps, Allerium maintains our core network infrastructure on 1+ Gbps bandwidth circuits.

For voice traffic and associated data, PSAP host locations will receive a minimum of 10 Mbps and ingress locations will vary depending on the number of interconnected OSPs at each site. All calculations and capacities will be recorded as part of our documentation.

Interconnection locations (nodes, data centers, POIs, LRGs); and any additional technologies and interfaces.

Allerium will record all designs for POI locations, data centers, and associated nodes in both a preliminary design document (typically delivered shortly after contract start) and finalized as-built documents. For reference, we have provided the high-level architecture design below which shows the locations for POIs, data centers, and PSAP hosts. Legacy selective router interconnections will be performed at the POI locations or the data center locations, depending on the specific legacy SR and the available on-net locations for that provider.

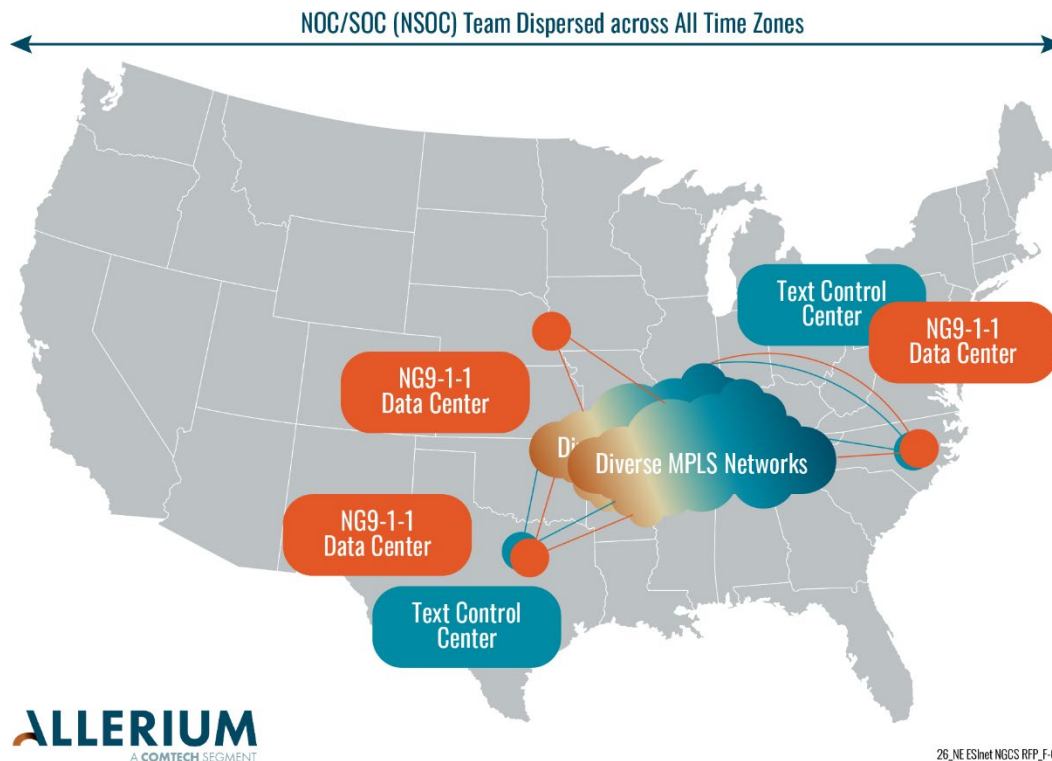


Figure 22. National System Design View

5.1.1.2. ESInet Interconnection

1.1.2. 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.*

Response:

Allerium understands and complies.

ESInet Interconnection Overview

Allerium will interconnect to other state and regional ESInets when those entities are ready to do so. We govern such interconnections through our ICD, which has been provided for review. In general, ESInet interconnections are performed in the following manner:

1. Initial interconnection request is made, and the ICD shared with the adjacent ESInet provider.
2. Any necessary interoperability testing is completed in the Allerium IOT (interoperability test) lab to ensure compliance with the ICD and prepare for production deployment.
3. Network node interfaces (NNIs) are determined with the other provider, with each ESInet typically providing one-half of the circuits to remain equitable.
4. Circuits are deployed to the NNIs and routing protocols are set to enable network-to-network communications.
5. Testing of the interconnection will be performed and upon successful verification the ESInet-to-ESInet connection will be complete.

Seamless interconnections with neighboring states/regions upon deployment.

Allerium is prepared to initiate interconnections with neighboring states once the deployment of the State is complete. If ESInet-to-ESInet connections are appropriate to manage transfers prior to the full State deployment, then Allerium will work in good faith to complete the arrangements in a mutually beneficial timeframe.

Connection capability for new ESInets within designated timeframe.

While it is impossible to predict the exact circumstances of future deployments, Allerium is ready to support the State in connecting new ESInets as needed.

Minimum two interconnection points for redundancy.

Allerium agrees with this best-practice approach for provisioning two interconnection points for redundancy.

Bandwidth provisioning for 200% of peak call volume.

Peak call volume calculations vary according to the business of borders between adjacent ESInets. Border conditions and associated call volume will be evaluated as part of the ESInet interconnection design phase and appropriately sized circuits will be provisioned to accommodate 200% of the expected peak call volume.

Equitable interconnecting methods/locations for cost management.

Allerium follows a best-practice approach of keeping all ESInet-to-ESInet connections equitable by providing one-half of the necessary circuits to complete the interconnection.

DSCP remapping if neighboring ESInets differ.

DSCP mapping will be reviewed as part of the design phase for ESInet interconnection.

Recommendation for BGP between networks.

Allerium uses BGP to connect between networks. Please see our design documentation for more detail.

Minimum qualifications for additional integrated networks; and collaborative security protection by providers.

Allerium's ICD contains information to qualify the minimum expected behavior for interconnected networks. The ICD will be tested against in the IOT lab as needed and further tested prior to being used for production traffic. All network edges are deemed to be a security threat and will require collaborative security protection from both ESInet providers to mitigate any security concerns.

5.1.2. External and PSAP Connectivity

5.1.2.1. Originating Service Provider (OSP) Connection

1.2. External and PSAP Connectivity

1.2.1. 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.*

Response:

OSP Connection Overview

Allerium is a registered competitive local exchange carrier (CLEC) in over 40 states and has established relationships with many OSPs in the area due to our work in other statewide NG9-1-1 deployments.

Allerium is well versed in carrier transitions and OSP integrations and will enact these changes on behalf of the State to ensure that Nebraska's constituents receive the best NG9-1-1 solution possible. Allerium has a carrier and industry relations (CaIR) team dedicated to OSP and carrier relationships and performance. This team has hundreds of real-world deployment experiences (e.g., LOAs, carrier ingress network design and deployment, cutover testing, circuit connectivity to demarcation points, ingress solution maintenance) and a proven methodical approach to ensuring a coordinated and orderly transition. The CaIR team will support Allerium's project manager with all efforts required for interconnection agreements to ensure there are no contractual or regulatory obstacles associated with facilitating the migration(s). The status of these agreements will be included as a regular part of the project status reporting. The experience and regular business practice of establishing and managing interconnection agreements is critical for ensuring OSP support and compliance.

Allerium will install call aggregation points of ingress (POIs) in two locations for the State aggregation service and will provide a total of four connections to these two sites. Similarly, these POI sites are connected to the NGCS core data center facilities in Council Bluffs, Dallas, and Raleigh, which will use these circuits, as well as a more complex arrangement of circuits to interconnect to additional Allerium systems (such as Text to 9-1-1 and our internal monitoring networks, as examples). Our OSP aggregation service is designed to support both IP interconnection and legacy interconnections (CAMA, SS7, etc.). Our implementation goal is to deploy all OSPs with IP circuits, per the FCC requirements for OSP interconnections, with each

OSP being required to connect to two POI locations. Legacy connections will be discouraged but supported as needed.

Facilitation of diverse and redundant connectivity for OSP traffic flow into the ESInet.

The POI locations facilitate diverse and redundant connectivity for OSP traffic flow into the ESInet. OSPs have the option to connect to the local POI sites, or directly to our data centers. Given that Allerium has provided this service in multiple states, some large OSPs prefer to connect at the data centers rather than the local POIs. Either is expected and allowed. Smaller, regional OSPs may choose to connect to the POI locations. In any case, we require the OSPs to connect to at least two of the sites to promote as much redundancy as possible in the end-to-end call flow.

Provisioning of sufficient bandwidth for OSP traffic (CAMA, SS7, IP, etc.) upon acceptance.

Bandwidth sizing is completed for each OSP that interconnects to the POI. We take the interconnection opportunity to "right size" each connection to ensure that the appropriate bandwidth is allocated. If the OSP is connecting via legacy means, the traffic is converted from legacy to IP using legacy network gateways (LNGs) prior to being sent on to the core. In this manner, we maintain an all-IP solution within our span of control.

Smooth migration to ESInet with aggregation of legacy traffic.

Call aggregation is a fundamental step to a successful deployment. While some NG9-1-1 providers ignore legacy traffic realities, to their detriment and eventually leading to failed or delayed implementations, we have been accepting, converting, and routing legacy traffic for nearly 15 years. Allerium's track record in completing deployments on-time is unmatched and the call aggregation step is one we take seriously starting day 1 of the deployment.

Redundant and diverse design for disruptions, interfacing with network gateways based on OSP capabilities.

Allerium prefers, and will press, the OSPs to connect via IP in accordance with the FCC report and order regarding carrier interconnection. In some cases, OSPs may still connect via legacy gateways. As is the case with the rest of our solution, the legacy gateways are carrier-grade devices that are deployed in redundant pairs to ensure the highest level of redundancy possible. In the instances where OSPs are providing multiple circuits to the gateway, we will install each incoming circuit on a different gateway to ensure full redundancy for the incoming traffic. In this manner, OSPs may have multiple circuits, with redundancy, to each POI with multiple POI interconnections. In addition, we will work with each OSP to provide a last routing option (LRO) in the extremely unlikely event that the entire NG9-1-1 service is unavailable, which will result in the OSP sending calls to a default PSAP to be answered. This is just one of many fallback/alternate routing scenarios we employ to ensure all calls are answered.

Identification of any risks to their system due to lack of diversity or redundancy from caller to call-taker.

Allerium will not deploy with risk to redundancy inside our span of control. Likewise, any known risk from the OSP to our POI locations will be:

1. Mitigated directly with the carrier and
2. Communicated with the State for awareness and to help ensure the proper pressure can be placed on the OSP to maintain redundancy.

Identification of risks from limited diversity and options to mitigate exposure for OSPs or PSAPs.

Along with identifying the risks the OSP network may have, within the visibility we are afforded to their networks, we are accustomed to providing options to OSPs to promote diversity and redundancy. Such options may include additional POI interconnect locations, support for legacy interconnections, and alternate connection types. We will work with the State, the OSPs, and the PSAPs to ensure all options are considered to resolve limited diversity concerns.

Continuous monitoring/increase of bandwidth at aggregation points.

Points of interconnection are managed the same as the rest of the NGCS and ESInet deployment, with full monitoring of performance by our NOC and network engineering team. Our bandwidth utilization strategy is to maintain less than 40% average utilization. This allows for 200% bandwidth peaks up to 80% utilization while still leaving 20% headroom for safety. Bandwidth usage is monitored with trend analysis and a scaling activity will commence when these levels are exceeded.

5.1.2.2. PSAP Connection

1.2.2. 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.*

Response:

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).

Allerium designs the ESInet to the PSAP host locations with full fiber diversity. Each circuit is provisioned in accordance with this requirement with 1 Mbps per PSAP/position on each circuit or 2 Mbps per PSAP + 2 Mbps per position with both circuits per normal operation.

Table 54. Bandwidth Details

Region	Number of PSAPs	Number of Positions	Required Bandwidth per Circuit (Mbps)	Provided Bandwidth per Circuit (Mbps)
East Central	8	25	33	40
Metro	3	26	29	30
Mid East 911	4	10	14	20
North Central	6	13	19	20
North East	8	26	34	40
South Central Panhandle	22	62	84	100
South East	17	62	79	100

Commitment to ongoing bandwidth monitoring and increases with 10% annual growth factor.

Allerium monitors bandwidth utilization on an ongoing basis. Our bandwidth utilization strategy is to maintain less than 40% average utilization. This allows for 200% bandwidth peaks up to 80% utilization while still leaving 20% headroom for safety. Bandwidth usage is monitored with trend analysis and a scaling activity will commence when these levels are exceeded. We commit to bandwidth capacity increases of 10% annually above baseline, per this requirement.

Facilitation of interconnections with PSAP systems (CAD, logging recorders), criminal justice networks, and secure public safety technologies.

Allerium works with all third-party systems and networks, at the State's discretion, to facilitate interconnections. If the State so desires, we will segregate a portion of the network into what we refer to as an ancillary segment. We have employed this strategy in other states to ensure that there is dedicated bandwidth for both emergency calls/data as well as other application data. This concept is above and beyond the requirement for "facilitation" and allows the State to better utilize, and thus better capitalize, on the network investment being made while not comprising emergency calls.

Ensuring uninterrupted SIP traffic for 911 calls.

As noted above, Allerium provides a variety of methods, including QoS, traffic shaping/policing, and ancillary network segregation to ensure that SIP traffic is uninterrupted for 9-1-1 calls. Our ESInets are designed to meet the fundamental need of connecting call makers to telecommunicators while also leveraging the network investment for additional purposes.

5.1.3. Legacy Interoperability

5.1.3.1. Legacy Network Gateway (LNG)

1.3. Legacy Interoperability

1.3.1. 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:**
 - o The LNG must maintain interface compatibility with existing Selective Routers, allowing for minimal disruption and cost implications.
- **Geographical Redundancy:**
 - o Legacy OSPs must have access to connections at two geographically diverse LNGs to enhance resilience.
- **Legacy Support:**
 - o 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:
 - o OSPs will be able to manage/make updates to their records directly in the database without having to submit SOI

- o OSPs will be able to run performance/statistical reports on their No Record Found (NRF)/Discrepancy and SOI processing
- o 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
- o OSP's have the ability to manually update their own records
- o OSP's have the ability to lock and unlock their own records
- o All manual updates be tracked in history
- Customer access to data
- Telco access to data
- Bulk modifications
- PSALI functionality
- Database reports
- NRF process
- o 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.

Response:

LNG Overview

Allerium provides legacy gateway functionality in alignment with the lengthy requirements above. Legacy gateways have been part of each of our many statewide deployments starting 15 years ago and are still part of the deployments today. The use of legacy gateways will eventually cease, and we plan to move all OSPs to IP ingress as part of that requirement. As noted, however, the legacy gateways are still needed until both OSPs and legacy selective routers are moved to IP (in the case of OSPs) or retired (in the case of selective routers).

Allerium's proposed solution includes our Legacy Network Gateway (LNG) and our Legacy Selective Router Gateway (LSRG) 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. Allerium's LNG and LSRG are two separate applications which conform with STA-010.3f with noted prior exceptions.

Allerium's LNG conforms to STA-010.3f for all calls originating from legacy networks arriving, processing, fetching location, and providing an i3 compliant SIP INVITE to Allerium's ESRP.

Allerium deploys our LNG in a quad-diverse model which includes both local and geographic redundancy. Each POI providing service for the State includes two functional LNG systems (PIF, LIF, NIF) to ensure that a single service impairment will not impact the entire service. Furthermore, Allerium provides a minimum of two geographically diverse POIs to ensure we have a minimum of four viable LNG/LSRG systems available under normal operating conditions.

LNG conformance to NENA-STA-010.3 for legacy OSPs until i3 migration.

Allerium expects to continue to leverage our LNG for all legacy OSPs until such time that the OSP migrates to i3 origination. As OSPs migrate to i3 origination, Allerium's ESRP will receive the call directly and bypass our LNG as per STA-010.3f. Allerium also notes that Phase 2 of NG 911 Acceleration as per 47 CFR § 9.29(b)(1)-(4) effectively migrates OSPs to an i3 origination method, thereby empowering transition.

Interface compatibility with existing Selective Routers.

Allerium's LNG interfaces with existing selective routers in our production deployments today. Allerium maintains strict interface controls to ensure compatibility with legacy origination providers, including selective routers, throughout our solution, including but not limited to our LSRG.

Geographically diverse connections for legacy OSPs.

Allerium deploys our LNG in a highly redundant configuration which requires both local and geographic redundancy across three different data centers, resulting in a 6-way redundant model. As OSPs leverage Allerium's service, we work with the OSP to ensure that connections to our LNG, and network in general, provide geographically diverse endpoints for resiliency.

This approach provides the State with a robust and fault-tolerant legacy ingress design, ensuring that OSPs retain reliable access to the NG9-1-1 system throughout their transition to native i3 origination.

Management of legacy PSALI records with migration processes.

Allerium works with third-party PS-ALI/MLTS providers to provision data into the LDB. This approach allows all records to exist within the same database and with the same operational controls. This approach has worked well across all of our statewide deployments.

TTY to RTT conversion.

Allerium's solution includes transcoding capabilities that support TTY to RTT conversion within the LNG environment. In production deployments, our experience shows that PSAPs more commonly rely on TTY workflows than native RTT, which often results in RTT-to-TTY transcoding being used more frequently than the reverse. Regardless of direction, Allerium's transcoding mechanisms ensure that text communications originating from legacy networks are delivered to the PSAP in a format that aligns with their operational capabilities.

E2 connections to MLCs/GMLCs/VPCs.

Allerium's service includes E2 connectivity to provider MLCs/GMLCs/VPCs to ensure location update requests are processed as expected. Our experience in this space spans over two decades as we have long provided MPC/VPC service, as well as carrier location services with the GMLC, for many of the top wireless and VoIP providers in the country. Our network connectivity to location databases and carrier networks is extensive.

Positioning outside ESInet before BCF.

In Allerium's design, the carrier facing interfaces of the LNG reside outside of the ESInet prior to the BCF. Our LNG is comprised of three major elements:

- **Protocol Interwork Function (PIF):** Provides connectivity to the legacy carrier leveraging TDM call delivery mechanisms such as SS7.
- **Location Interwork Function (LIF):** Provides interconnectivity to location platforms via STA-027.3 ALI query / response and via HELD-DI to an LDB.
- **Network Interwork Function (NIF):** Prepares SIP messages coming in for the next hop to the ESRP in expected format.

The PIF component of Allerium's LNG resides outside the ESInet and before the BCF, facing the carrier network. As a call arrives from the carrier, the LNG PIF processes the outgoing SIP call through the BCF to the NIF. Allerium leverages the BCF between the PIF and the NIF to ensure security and consistency in deployment model. Essentially the call passes through a BCF as the call converts to SIP and enters the ESInet.

In operation, the PIF receives incoming calls from the carrier network, processes the signaling, and forwards the SIP call through the BCF to the NIF. The placement of the BCF between the PIF and NIF ensures a secure and consistent deployment model and maintains proper boundary separation as calls migrate from legacy signaling into SIP and enter the ESInet.

This design reflects Allerium's focus on reliable interworking across legacy and NG9-1-1 environments, ensuring calls are transitioned securely, consistently, and in alignment with NGCS operational expectations

ElementState/ServiceState support.

Allerium's LNG platform is engineered to ensure that only healthy, available elements participate in call handling—and this capability is already fully embedded in our production deployments today. Allerium continuously monitors LNG endpoints using proven operational mechanisms that validate interface availability, media functionality, and routing behavior in real time.

Our solution uses SIP OPTIONS to confirm that each LNG element is responsive and immediately removes any element from rotation if it fails expected signaling behavior. In addition, Allerium performs automated heartbeat test calls to verify that calls route and complete as intended. These test calls validate end-to-end functionality across the LNG element group, allowing us to maintain an accurate picture of each element's operational state and overall service availability.

Through this approach, Allerium effectively delivers the practical intent of ElementState and ServiceState—ensuring that routing decisions always reflect the true availability of LNG resources and that the system adapts dynamically to changing conditions.

As part of our planned advancements, Allerium will expand these existing mechanisms to incorporate the full standards-defined ElementState and ServiceState models within our established 12-month roadmap. This work builds naturally on the monitoring and validation processes we already perform today, enabling a smooth alignment to the formal specification without affecting service reliability or performance.

5.1.3.2. Legacy Selective Router Gateway (LSRG)

1.3.2. 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.
- ALI 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)

Response:

LSRG Overview

Allerium's legacy selective router gateway (LSRG) complies with the stated requirements. We note that the requirements state that the LSRG is to be used only as a transitional element to assist in moving the OSPs to the POIs using IP ingress. However, the State should be aware of an additional complication that Allerium often solves for, which is for legacy transfers to PSAPs that are "off-net" of the ESInet (for instance, PSAPs across the state border that are still on legacy 9-1-1 systems but receive transfers from Nebraska's PSAPs). We have designed our solution to account for both a temporary gateway solution to aid in the deployment of PSAPs as well as a longer-term solution for

transfers, at the State's discretion. We look forward to working with the State to implement the LSRG in the manner that best meets the State's needs.

Notwithstanding the above, the LSRG is a fully-featured functional element that has been in use in every deployment for the last 15 years. The functionality is very similar to the above referenced LNG, and as such we have summarized the LSRG functionality below for ease of readability.

Interface for legacy Selective Routers via ISUP SS7 trunks.

Allerium's LSRG meets the requirements for interfacing with LSRs via ISUP. An in-depth description, including descriptions, call flows, and ladder diagrams, is provided in our interface control documentation (ICD).

Conversion to SIP/RTP.

The PIF function in the POI performs the conversion from legacy signaling and data to SIP/RTP in the same fashion as described above for the LNG.

ALI query and LoST-based routing.

As a gateway element, the LSRG supports both legacy and LoST-based routing. When configured to tabular routing, the LNG NIF/LIF uses the pANI or ANI received in the INVITE From header to determine the primary route for the call, based upon LNG provisioned pANI or ANI data, and the trunk group from the contact header to determine fallback/default routing. A route determination may require the LNG LIF to query an ALI or MPC/VPC/GMLC, or the information may simply be pre-provisioned (tabular routing – pANI/ANI to PSAP URI) in the LNG database.

Bi-directional communications for voice/data (star codes).

Allerium supports star and pound dual tone multi-frequency (DTMF) codes.

Allerium notes that support for star and pound codes is not within the context of NENA's i3 specification per NENA-STA-010.3. An i3 PSAP must signal with a SIP REFER which includes a Refer-To containing a SIP URI. As such, for a native i3 PSAP, Allerium expects a SIP REFER message containing a SIP URI vs. a TEL URI with a shortcut code (star or pound) defined.

However, Allerium does support star and pound DTMF codes for transitional SIP signaling from a legacy PSAP. In this case the PSAP may transfer via a SIP INFO message which contains a TEL URI and the necessary star/pound code the PSAP wishes to dial. To support star and pound code translations, Allerium obtains details regarding the expected codes and their appropriate destinations from all PSAPs during the data collection phase. We then configure the translations for each PSAP into the NGCS system accordingly.

Similar to a direct dial of 10-digit line, a PSAP may request an entity be added to the 9-1-1 voice session via a star or pound code that indicates a conference or transfer request. The LPG NG9-1-1 specific interwork function (NIF) processes the SIP INFO request and translates to the appropriate SIP URI. The SIP URI is used to set the Refer-To header value in a resulting REFER message from the LNG NIF to the ESRP to complete the transfer request. For translations that match on-network PSAPs, the ESRP invites the requested party to the call directly over the ESInet egress network to the destination PSAP. For parties not on the network, the ESRP processes the call out using the LSRG as the PSTN gateway.

Timeline/plan for LSRG removal as temporary solution for OSP traffic.

As mentioned in the summary, the timeline for LSRG removal depends on how the State wishes to address off-net transfers. Outside of that consideration, however, Allerium supports the FCC R&O regarding carrier ingress; those requirements give some OSPs up to one year for Phase 1 compliance (which would require IP ingress) and two years for full NENA i3 compliance. As such, our timeline would target one year from the date of the State's notification to carriers to proceed with Phase 1 (which we can help draft if the State so desires).

Deployed LSRG (where applicable) in conformance with NENA LSRG Standard (STA-034.1)

Allerium's LSRG is in conformance with the relevant standards and provides a tried-and-true approach to supporting legacy environments, as proven across over a dozen state and regional NG9-1-1 projects.

5.1.3.3. Legacy PSAP Gateway (LPG)

1.3.3. 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.*

Response:

LPG Overview

Allerium has deployed hundreds of LPGs across our deployments. While the use of LPGs has decreased as call handling vendors have embraced NENA i3 standards, it is still common to deploy LPGs as part of a deployment. We maintain an interoperability testing lab (IOT) to ensure that all of the CHE makes/models and versions are supported prior to production deployment. Having completed so many LPG deployments, we have already certified all standard CHE makes/models that exist in Nebraska. If a LPG is required for interfacing to the PSAP, the State can rest assured that the CHE will be certified with the LPG prior to any go-lives.

The LPG must be able to maintain the PSAP's existing ALI format.

Existing ALI formats are preserved with the use of the LPG.

The LPG must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3.

Allerium's LPG solution uses SIP OPTIONS to replicate the behavior that ElementState and ServiceState supply. We commit to updating the mechanism to fully align with the current standards, but we also note that the functionality those standards require is supported already in the LPG.

LPG connections shall allow for PSAPs to directly connect systems (cable IP) to the ESInet

The LPG is installed locally at the PSAP and serves as the gateway between the ESInet and local LAN. The connection is direct, per this requirement.

LPG queries ALI databases and maps NG911 location data to legacy formats.

The primary function of the LPG is to act as a gateway for voice and location purposes. As such, the LPG manages the connection and conversion between legacy systems at the CHE and the ESInet-connected location databases. The ALI data in the LDB is no exception, and the LPG queries that database to receive location and then maps that location to the required legacy format. This creates the desired scenario where the LPG translates "legacy" at the PSAP edge to NENA i3 within the ESInet/NGCS.

Converts TTY to RTT for text-to-911 in legacy PSAPs.

The LPG supports the conversion of TTY to/from RTT to enable text-to-911 in legacy PSAPs. As one of only two text control center (TCC) providers in the United States, we are well-versed in providing text-to-911 services and do so for thousands of PSAPs across the country.

Supports call transfers to/from legacy PSAPs, mapping i3 transfers to legacy systems.

Transfers are supported to/from legacy PSAPs. Similar to a direct dial of 10-digit line, a PSAP may request an entity be added to the 9-1-1 voice session via a star or pound code that indicates a conference or transfer request. The LPG NG9-1-1 specific interwork function (NIF) processes the SIP INFO request and translates to the appropriate SIP URI. The SIP URI is used to set the Refer-To header value in a resulting REFER message from the LNG NIF to the ESRP to complete the transfer request. For translations that match on-network PSAPs, the ESRP invites the requested party to the call directly over the ESInet egress network to the destination PSAP. For parties not on the network, the ESRP processes the call out using the LSRG as the PSTN gateway.

Logs call events, protocol conversions, and errors; supports discrepancy reporting.

All Allerium functional elements produce logs that record transactions and call events within the system. Logs are created for each transaction and are appropriately called transaction detail records (TDRs). A series of TDRs, representing the various functions the LPG performs, will be aggregated by the system into call detail records, or TDRs. In this fashion, the LPG records call events, transactions, and errors.

Implements TLS and authentication for secure connectivity.

Allerium uses secure tunnels, with digital certificates, on the ESInet to secure all traffic between the core functional elements and the PSAP edge, including to a LPG.

Monitors LPG performance; supports maintenance with minimal disruption.

The LPG service is continually monitored for both the hardware-based protocol converter (performing the PIF function) and the software-based location and NG9-1-1 interworking functions (the LIF and NIF functions). The LPG hardware is deployed in pairs to ensure that any maintenance on that hardware is minimally invasive and does not cause any disruption to PSAP operations.

LPG deployed with geo-redundancy to ensure high availability.

Allerium's LPGs are deployed with local hardware redundancy at the PSAP and geo-redundancy for the software components. In fact, there are six separate instances of the LPG software across three different data centers - operating at all times in an active/active configuration - to support the State.

Reports errors in call delivery, location, or protocol conversion.

All call delivery errors, for even a single call, are logged and investigated by the Allerium NOC, which operates 24x7x365.

5.1.4. Network Behavior and Performance

5.1.4.1. ESInet IP Routing

1.4. Network Behavior and Performance

1.4.1. 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.*

Response:

ESInet IP Routing Overview

Allerium's vision for the Nebraska deployment is to quickly and reliably implement the ESInet and NGCS to fulfill the near-term vision of the State while simultaneously placing the foundations that will enable future 9-1-1 functionality. The near-term and long-term visions are complementary, and both are achieved in Allerium's vision for the State of Nebraska.

Conformance with NENA standards for handling traffic under varying conditions.

Allerium builds and operates the ESInet in alignment with NENA and other industry standards. Our network is built to be non-blocking with low latency and high-quality voice transit. Our network configures QoS to shape traffic and we enforce DSCP to mark priority traffic. In addition, we offer the ability to segregate dedicated bandwidth for adjacent uses while preserving the integrity and capacity of the call handling network.

Documentation of ongoing bandwidth assessments, risk assessments, diversity and redundancy testing in a configuration management database.

Allerium manages the ESInet deployment with full monitoring of performance by our NOC and network engineering team. Our bandwidth utilization strategy is to maintain less than 40% average utilization. This allows for 200% bandwidth peaks up to 80% utilization while still leaving 20% headroom for safety. Bandwidth usage is monitored with trend analysis and threshold alarming in the NOC to alert for any activity that exceeds the threshold. Our network engineering team investigates such alerts and will manage bandwidth capacity accordingly.

Bandwidth assessments begin with the design of the ESInet where diversity and redundancy are arranged in the network transport. Allerium's proposal provides two fiber circuits to each PSAP host, which are built on separate carrier networks for diversity. We have the ability to add to that diversity with wireless circuit options, such as low earth orbit (LEO) satellite, at the State's discretion. Once deployed we will continually monitor the circuits and the carriers providing the

circuits for any change that would reduce diversity, which we have seen (and mitigated) in other deployments.

All design documents will be held in a State-accessible database and will be kept updated throughout the contract period as the project progresses.

Proactive measures to trace IP routing in diverse and redundant paths.

Allerium is circuit-agnostic, meaning we use the best available circuits regardless of underlying carrier (unlike existing telecom providers that show a strong proclivity to only use their own network infrastructure). Allerium's service incorporates a composite set of connectivity services that meets the performance requirements called out in the State's RFP for IP transport. This design delivers exceptional flexibility by leveraging diverse carriers and network facilities. ESInet core IP routing provides a highly available and redundant solution accompanied by proven SLA management and compliance. Allerium will register circuits for 9-1-1 priority through telecommunications service priority (TSP) markings to further enhance the ESInet's survivability.

Testing of IP routing failover mechanisms prior to any system change acceptance.

Allerium employs a robust change management procedure to ensure that all changes to the network or service are tested prior to acceptance. Once the change is approved, Allerium maintains a comprehensive suite of ATPs featuring over 250 tests performed on all components and interfaces of the NG9-1-1 solution, including the network. The ATP focuses on testing normal operational conditions as well as failure conditions with testing processes addressing:

- Ingress service provider to NGCS,
- NGCS to ESInet egress,
- ESInet/NGCS to PSAP, including PSAP network edge failure cases, and
- Call transfers to/from neighboring jurisdictions.

Allerium has included a sample ESInet/NGCS ATP, among others, in Appendix 3: Sample ATPs. While the full ATP won't be executed for each change, the relevant test cases will be repeated for any change that affects the network.

5.1.4.2. ESInet Bandwidth

1.4.2. 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.*

Response:

ESInet Bandwidth Overview

Allerium notes that the RFP requires an arbitrary bandwidth calculation to be used of 2 Mbps per PSAP plus 2 Mbps per position, in normal operation. We have provided our proposal using this calculation, as required by the RFP. However, we would like to note that the State is likely oversizing (and thus overpaying) for bandwidth it will not use. For clarity, the remainder of this overview provides a "right-sized" approach to bandwidth sizing that the State may wish to consider, but in no way results in our response offering anything less than that required by the RFP.

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.

While Allerium has provided a design and pricing related to the required bandwidth sizing mentioned above (the 2 Mbps + 2 Mbps calculation), we have provided this analysis for the State's consideration:

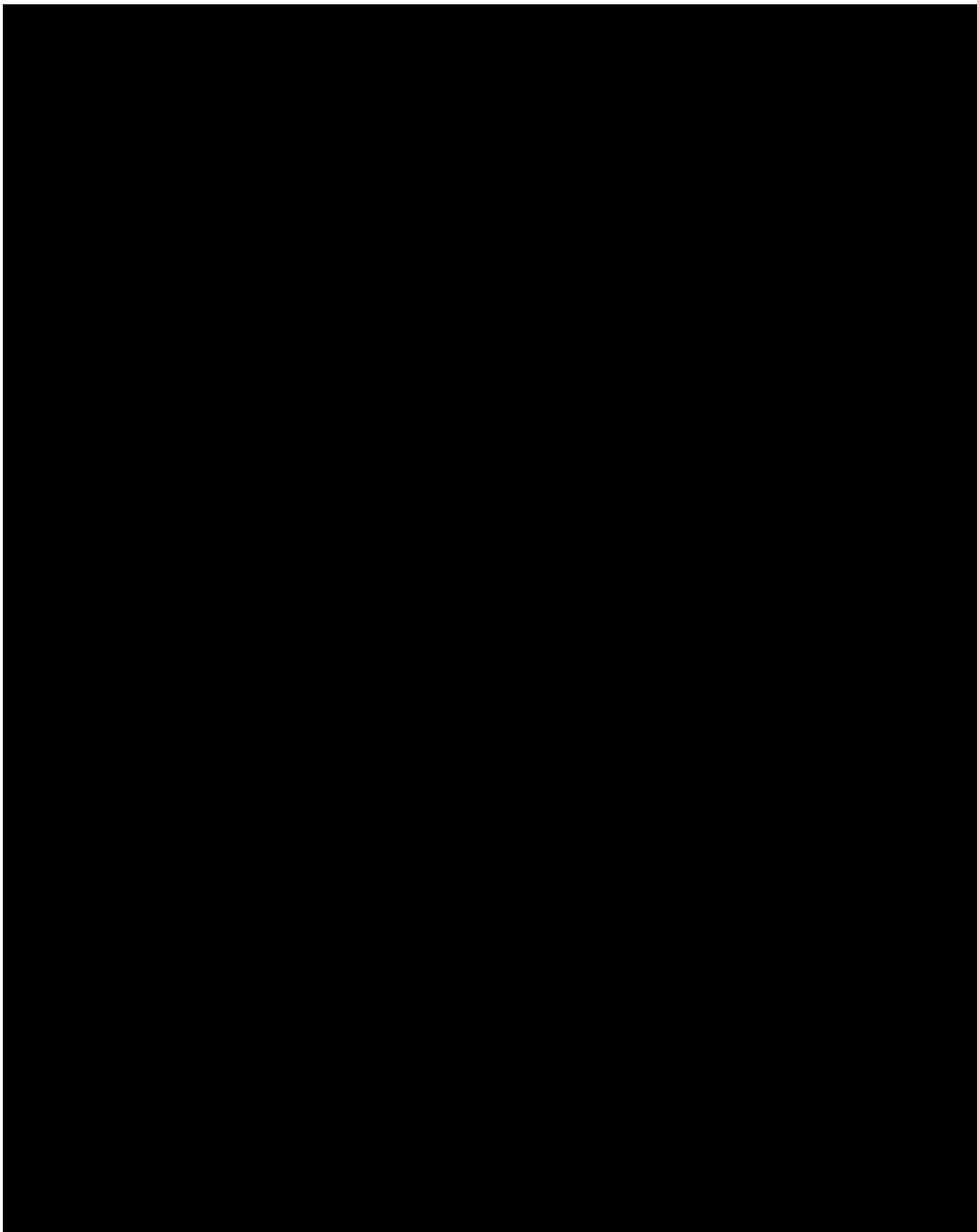
For PSAPs not receiving video today, the Allerium ESInet would typically be provisioned with a minimum of 128 Kbps per actual position at the PSAP plus 25 percent bandwidth to ensure support for multi-party calls. This bandwidth sizing is based on the G.711 codec that is used for high voice quality, which is then doubled to allow for signaling and operations/maintenance tasks. In practical terms, provisioning bandwidth with this minimum ensures that every seat at every PSAP in the State can be on a call simultaneously, with 25 percent "extra" to be used for conference calls.

For PSAPs receiving video, the H.264 codec is recommended. We follow the formula proposed in the latest NENA-INF document using that codec:

2 Mbps per PSAP + 2 Mbps per call-taker position equipped for video = Recommended bandwidth for each PSAP

Allerium designs the ESInet for optimal call delivery and cost efficiency. As such, the minimum calculation provided using the G.711 codec is sufficient for voice and text communications and is almost always the starting point for bandwidth needs analysis. Please note, however, that the network is highly scalable. As other services like video are added to the ESInet, our network will easily scale to accommodate these services. This approach, again, provides the most cost-effective approach to ensure that the State is not paying for excessive bandwidth it will not use for years to come.

For further clarity, Table 55 was developed based on our experience and demonstrates that Allerium's service can meet end-to-end bandwidth requirements for NG9-1-1 functional elements, including Text to 9-1-1, database access, call handling, and logging subsystems.



An annual growth factor of 10% must be incorporated into capacity planning.

Allerium has incorporated the ability to scale the network bandwidth by 10% annually.

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.

Allerium is truly network agnostic and is willing to use other networks when available. We implement similar arrangements in other statewide deployments as part of the ESInet design. Use of other networks requires that the network be designed for priority service of the emergency calls. Likewise, Allerium's ESInet supports the use of the ESInet for interoperability between other applications. In the case of cloud-based CAD, for instance, or any other ancillary service, the ESInet can serve as the transport for properly authenticated systems to communicate with one another. The ESInet is scalable to support additional applications and designed such that these applications can either be treated as 9-1-1 traffic or as non-9-1-1 traffic. If treated as 9-1-1 traffic, the ancillary traffic is treated with the same priority on the same network path as the 9-1-1 calls. If treated as non-9-1-1 traffic, Allerium implements a separate logical path on the ESInet to ensure the ancillary services cannot impact the bandwidth available to 9-1-1 calls.

Allerium recommends the second approach (segregated traffic) as the preferred route if the ancillary traffic is expected to include services that are not directly related to the 9-1-1 call flow.

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.

The Allerium ESInet is built on diverse fiber circuits to each PSAP host. Fiber offers extremely high bandwidth capability, especially as it relates to the limited call and data volume that NG9-1-1 uses. Additionally, given the requirement for 2 Mbps per PSAP + 2 Mbps per position, the provided bandwidth is very unlikely to need to be scaled. However, if any bandwidth increases are necessary, the fiber circuits provide extensive scaling ability to accommodate growth. A detailed plan to outline such scaling is, truthfully, unnecessary. Scaling on fiber circuits is done within a short time period (usually no longer than it takes to process the order for increased bandwidth) and is natively supported by the routers in the ESInet, up to 1 Gbps at minimum for supported port speeds.

5.1.4.3. Quality of Service (QoS)

1.4.3. 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.*

Response:

Employment of DiffServ throughout with packet marking per NENA-STA-010.3.

Allerium's QoS model is built on a Differentiated Services Architecture (DiffServ RFC 2475) that adheres to NENA-STA-010.3 to control per-hop behavior (PHB) at each network node to provide end-to-end QoS. Allerium's design utilizes Expedited Forwarding PHBs, Assured Forwarding PHBs, and Default PHBs. Class-selector PHBs are configured as required to achieve backwards compatibility when interfacing with older systems.

Commitment to packet loss below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during operations.

Allerium designs our ESInet for optimal performance and meets the operational requirements listed under normal operating conditions.

Standby measurement basis for performance metrics with State-initiated measurements.

Allerium maintains a network management system (NMS) that automatically captures network performance data. The State is welcome to review this data at any time.

Regular reporting on network performance including averages and worst-case scenarios.

Allerium maintains a network management system (NMS) that automatically captures network performance data. The State is welcome to review this data at any time. In addition, Allerium will work with the State to determine which network performance metrics it would like to see, including averages and worst-case performance, as part of a regular reporting activity.

5.1.4.4. Traffic Flow Requirements

1.4.4. 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.

Response:

Traffic Flow Overview

Traffic flow descriptions are complex. Allerium provides a high-level description in this response and supplements our response with technical design documents as appendices.

End-to-end traffic flow description compliant with standards.

Allerium aligns our ESInet and NGCS elements to NENA i3 and many other relevant standards. The below diagram illustrates the high-level architecture of the Allerium NENA i3-compliant ESInet (coupled with the NGCS service elements). This diagram is taken from our interface control documentation, which focuses on SIP (and other signaling such as SS7) interfaces into the Allerium NGCS platform, which are labeled 1 through 7 below.

The Allerium NGCS platform is a modular collection of NENA i3-compliant components. All components shown may not be required to complete call delivery to a PSAP. For example, an ECRF is not required if call routing is based upon the ESN that is retrieved from the ALI DBMS. For clarity, ESN-based routing is used during the transitional period to NENA i3 NG911 because location-based routing requires an accurate GIS Civic Location Data eXchange Format (CLDXF) compliant data layer in the ECRF.

An end-to-end traffic flow depiction is provided below. This diagram illustrates the complex nature of the 9-1-1 environment but can be simplified by understanding the flow of calls as follows:

- Calls originate on the left of the diagram, under the header of "Origination Networks." Origination networks include the various types of carrier networks that generate 9-1-1 traffic, including wireless, VoIP, and wireline networks that collectively account for most 9-1-1 traffic. The various nodes in the carrier networks are shown, with the underlying circuit technology and signaling identified in the "Key" at the bottom of the diagram.
- Calls move from the origination network into the NGCS section of the diagram (centrally located in dark blue). The connection methods are shown via color-coded connections, with TDM, IP, and location data connections shown separately. For instance, if the call originates from legacy central offices for wireline traffic (labeled "CO - TDM") then the circuit in use is a red-coded "TDM Call" and enters the NGCS through the legacy selective router via path "5" in the diagram, which connects to the "PIF" portion of the LSRG, as previously described. Each call path has a similar depiction to route to the NGCS segment.
- The right side of the diagram shows the interconnections with the PSAP network. Calls flow from the NGCS to the PSAPs, which the various types of PSAP interconnections illustrated (e.g., the "i3 PSAP" supports full NENA i3 call flows while the "IP PSAP" accepts IP connections but does not yet support i3 for location delivery). Also noteworthy is the use of the "LPG" functional element, which is called out in this RFP explicitly and fully supported in the Allerium service.

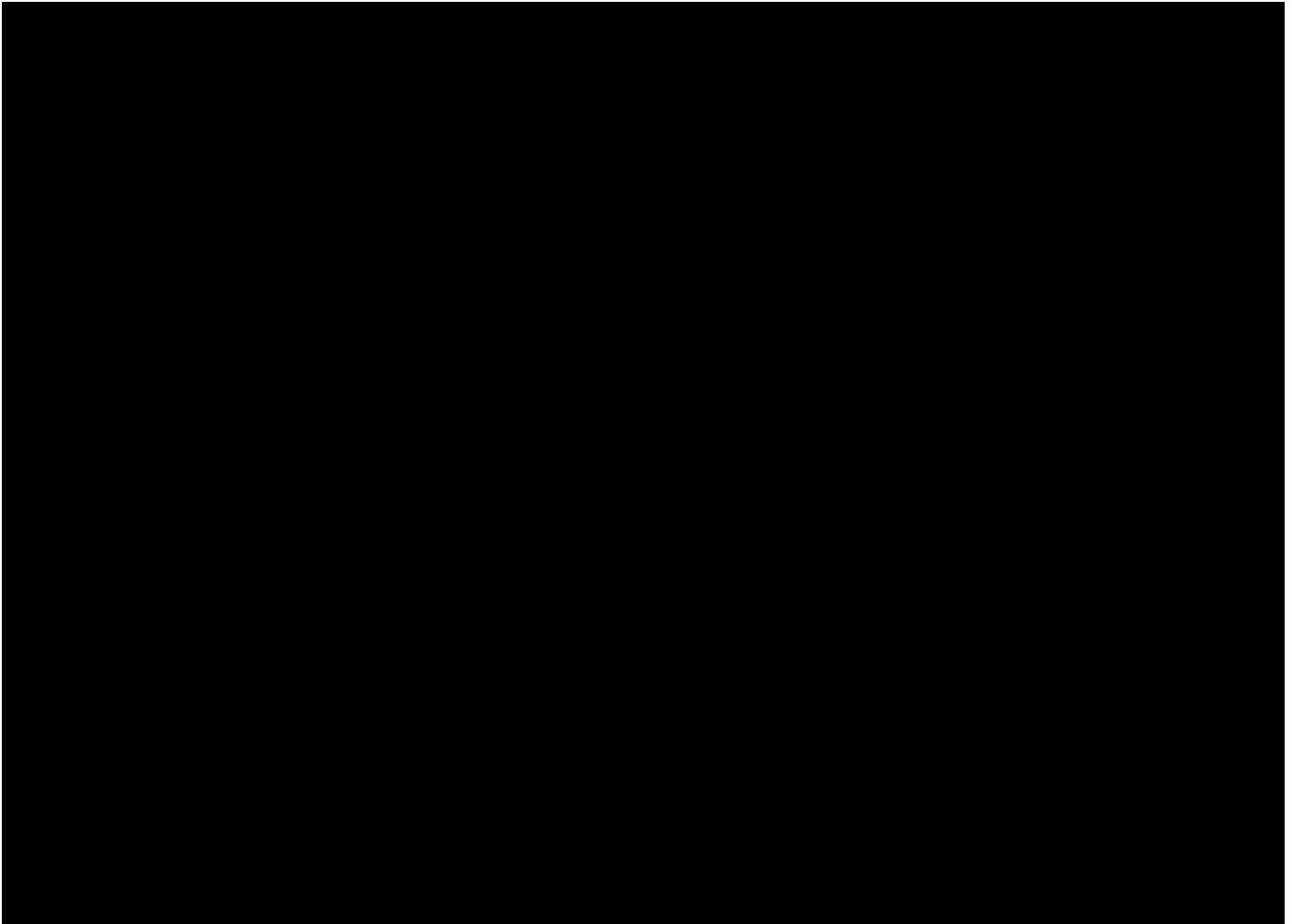


Figure 23. NENA i3 Interfaces (ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION)

Identification of operations on traffic in ESInet and NGCS.

Allerium's design documentation includes additional details regarding operations on traffic in the ESInet.

Diagrams for visualization if necessary; traffic flow under normal and abnormal conditions.

Allerium's design documentation includes additional details regarding traffic flow within the ESInet. As stated, traffic flow is complex and varied and impractical to show in its entirety within this section.

By way of example, this ladder diagram is taken from the referenced documentation and shows traffic flow for i3-compliant VoIP or wireless calls under normal operating 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.

Allerium's Appendix 4: Sample ICDs are included with the proposal for the State's review and features traffic flow details for multiple scenarios, including but not limited to:

- Successful Functional Scenarios for SIP Origination Networks
- i2-Compliant VoIP or Wireless Audio Call Origination
- i3-Compliant VoIP or Wireless Audio Call Origination
- i3-Compliant SIP MSRP Text911 Call Origination
- i3-Compliant RTT Call Origination

- SS7 ISUP Call Origination Successful Functional Scenarios
- SS7 ISUP Wireline or Wireless Call Origination
- SS7 ISUP Wireline or Wireless Call Origination to an Aggregation Point Selective Router Emergency
- SS7 ISUP Selective Router Call Origination
- TTY Call Routing and Delivery
- Successful Functional Scenarios for Audio Call Transfers
- Entering Audio Call Transfer from a Selective Router Connected PSAP
- Leaving Audio Call Transfer to a Selective Router Connected PSAP
- Leaving Audio Call Transfer to a 10 or 11-Digit PSTN Number
- Entering Audio Call Transfer from an External ESInet
- Audio Call Transfer to an External ESInet
- SIP MSRP Text911 Session Transfer
- Unexpected Scenarios
- Optional: Catastrophic Failure Audio Call Route

5.1.4.5. Traffic Shaping

1.4.5. 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.*

Response:

Traffic Shaping Overview

Allerium's QoS strategy includes the ability to perform traffic shaping and traffic policing as standard practice. Allerium's end-to-end QoS strategy leverages modular QoS to properly identify and classify traffic types, apply or reapply Differentiated Services Code Points (DSCP) markings, and prioritize traffic flows by applying policing and shaping policies as well as determining low-latency or class-based weighted fair queuing for each traffic classification.

Description of where traffic shaping is employed, the techniques used, and their intended benefits.

Allerium's end-to-end QoS strategy leverages modular QoS to properly identify and classify traffic types, apply or reapply Differentiated Services Code Points (DSCP) markings, and prioritize traffic

flows by applying policing and shaping policies as well as determining low-latency or class-based weighted fair queuing for each traffic classification.

When entering the network, traffic is analyzed as close to the source as possible, and traffic types are classified and marked or re-marked with the appropriate DSCP values. Traffic identification is performed by DSCP, access control lists (ACLs), Network-Based Application Recognition (NBAR), or a combination of these parameters.

DSCP markings are preserved, and adequate bandwidth is preserved as traffic traverses the LAN. At the network's edge, egress traffic destined for the ESInet is re-marked as needed and assigned guaranteed bandwidth, or a percentage of total bandwidth, as required by each traffic class. Media traffic utilizing RTP is put in a priority queue and marked with an Expedited Forwarding (EF) DSCP tag. The bandwidth for RTP is guaranteed, and low-latency queuing is applied. Signaling, which matches the SIP protocol, is also placed in its own class of service and allocated a percentage of bandwidth to ensure SIP packets are prioritized during periods of network congestion. Classes are also defined for mission-critical traffic, which includes mapping and location services, control and routing protocol traffic, and other applications that are vital to call path and related NG9-1-1 functions. A default class is defined for all traffic that is to be treated as 'Best Effort' (BE).

Creation of a formal traffic shaping policy document with transparency, regular updates, and availability to State personnel.

While Allerium has never been asked for a traffic-shaping policy document, we are happy to work with the State to derive such a document to describe and record the policy. We will provide regular updates to the policy, as needed, and make the policy available to the State from our central repository of information.

5.1.4.6. ESInet Network Time

1.4.6. 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.*

Response:

ESInet Network Time Overview

Allerium's proposed solution includes a network time protocol (NTP) and time source that meets this requirement. The NTP server functions as the single time source for all proposed components. Allerium's solution provides a network time server that all elements use to maintain a consistent network time. The network time server is located in our data centers on the same LAN as our Stratum 1 clock sources, which is best practice for accurate timing. The current configuration uses NTP servers attached to the Stratum 1 sources, but we have the option to use the Stratum 1 sources directly for even more accurate network timing, if needed.

Provision of NTP servers serving all ESInet elements (NGCS FEs, PSAPs, agencies) within 1 millisecond of absolute time with 4 nines (99.99%) availability.

As described, we employ the best practice of putting NTP servers on the same LAN as the Stratum 1 clocks, ensuring that all timing is available in the most accurate fashion possible. Using this configuration, our NTP is designed to support 1 ms or less accuracy of absolute time with the required 4 nines availability.

Preference for hardware clock but ensuring no more than 20 millisecond variances even on failure.

The NTP servers are on the same LAN as the hardware clock, meaning 20 ms time variance is supported by design.

Descriptions of NTP service provision, confirmation of 1 millisecond accuracy with 4 nines availability, and meeting 20 millisecond variance threshold.

Descriptions of the timing service are provided above. Confirmation of the accuracy can be undertaken at any time at the State's request. Outside of such a request, automatic synchronization is performed at all times as a standard feature of the service.

5.1.5. Resilience and Service Levels

5.1.5.1. ESInet Availability

1.5. Resilience and Service Levels

1.5.1. 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.*

Response:

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.

Allerium’s NSOC uses defined processes for incident and problem resolution and change management activities. Our team’s close work with 9-1-1 carriers, PSAPs, and other stakeholders relies on well-defined and documented workflow and roles and responsibilities to ensure quick and appropriate identification, classification, and resolution of incidents and problems regardless of the origin.

Our NSOC currently supports regional and state-level systems, providing incident and problem resolution support incorporating third-party provider systems ranging from CHE providers to ESInet and NGCS providers offering non-native solutions, including but not limited to:

- Real-time monitoring of third-party systems when available (if true integration is not available, a NOC-to-NOC process is put together which ensures we are notified of any impairments or maintenance and in turn make you aware),
- Ticketing and escalations with third-party systems, and
- Performance data collection.

The Allerium NSOC has well-defined methods, processes, procedures, and work instructions for all facets of support and maintenance, based upon ITIL principles and industry best practices. We maintain all NSOC procedural documentation in a digital library with online access for all staff members plus hard copies available for quick reference. All documentation updates go through a review-and-approval process, and the latest approved documents are available online.

Allerium ensures that all NSOC staff are trained on our NGCS and ESInet architecture and operational standards. The NSOC provides timely responses and replies as they coordinate team responses to maintenance, service, and customer service actions. The NSOC team is involved from the onset of testing and is familiar with the system as it has been deployed, understands the SLAs, and is trained in the NMS to understand alarm notifications, alarm generation, and their severity, assignment, and urgency in relation to maintaining the quality of service, response, and resolution times plus the appropriate escalation procedures based upon SLA requirements.

Allerium uses centralized management and monitoring systems that enable situational awareness across the NSOC team. Allerium follows a trouble ticket process whenever a system element does not function as expected.

The NSOC team is equipped with the tools required to monitor and manage all components of the State's NG9-1-1 system. This team works closely with engineering, defining a Tier 1-Tier 4 support structure to assign technical resources and a clear triage and escalation path to ensure Allerium meets or exceeds the SLAs required for operating the system.

Table 56. Levels of Assistance

Point of Contact	Expected Level of Assistance
Tier 1	Capture and triage

Point of Contact	Expected Level of Assistance
Tier 2	Mitigation/resolution
Tier 3	Advanced system analysis and troubleshooting/resolution
Tier 4	Release and patch changes

The NSOC provides NG9-1-1 services to multiple states and local government entities, upholds the high standards necessary for emergency services, and follows detailed provisioning and operations procedures to maintain network integrity at or above 99.999 percent.

Uptime calculations assessing physical device MTBF for critical equipment in serial/parallel configurations.

Allerium provides the following uptime calculations. To understand the calculations and how they apply, please note that the following represents a single analysis for a single PSAP edge. This is important to realize as this calculation represents a situation in which only a single router is analyzed. However, in truth, every PSAP has dual routers deployed for redundancy which enhances availability much beyond this single calculation. For clarity, this calculation is provided as an easy-to-understand example of how we calculate MTBF and uptime calculations.

Using the availability formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$

For 99.999% availability (A = 0.99999) and MTTR = 2 hours:

$$\begin{aligned} 0.99999(MTBF + 2) &= MTBF \\ 0.99999 \cdot MTBF + 1.99998 &= MTBF \\ MTBF - 0.99999 \cdot MTBF &= 1.99998 \\ 0.00001 \cdot MTBF &= 1.99998 \\ MTBF &= \frac{1.99998}{0.00001} \approx 199,998 \text{ hours} \end{aligned}$$

Therefore, the mean time between failures (MTBF), of a single router supporting this PSAP, would be approximately 22.8 years, assuming that a router replacement took 2 hours to complete. For reference, the MTBF of the routers we use in our PSAP deployments is 27.4 years, meaning even a single router (no redundancy) technically meets the uptime requirements for a 5-9s service.

However, Allerium never deploys a single router (or any other piece of equipment), and instead uses redundant high availability (HA) routers at the edge. Repeating the above calculation, with a MTTR of 1 second (an appropriate approximation for HA "failover" time), the resulting calculation yields a MTBF of 28 hours. Meaning, a router could fail at the PSAP every 28 hours and still maintain 5-9s availability.

Furthermore, when path redundancy is taken into account, availability is significantly improved even beyond the calculations above. In this example, we have used a MTBF of 150,000 hours for a redundant media gateway (the LNG PIF) using an MTTR of 2 hours and dual-path redundancy. First, single-path redundancy is calculated:

$$A \approx \frac{150,000}{150,002} \approx 0.9999867$$

Yielding single-path diversity of ~99.99867%.

To calculate dual-path diversity, we use: $A_{\text{system}} = 1 - (1 - A)^2$.

Failure probability per path is thus calculated:

$$\begin{aligned} A_{\text{system}} &= 1 - (0.0000133)^2 \\ A_{\text{system}} &= 1 - 1.77 \times 10^{-10} \\ A_{\text{system}} &\approx 0.999999999823 \end{aligned}$$

or nearly 11 nines of availability. Note that this level of availability is, in practice, unreasonable to expect as actual availability will be impacted by infrastructure, software, and human risks. Some risk can be mitigated with the use of diverse/independent systems (e.g., diverse router providers), but in truth the risk caused by human factors in such complex systems outweighs the benefits (as discussed elsewhere in response to the preference to have diverse manufacturers).

A key insight into these calculations is to understand that in highly available systems such as Allerium's service, MTBF calculations collapse into non-sensical values. Through the use of active/active systems, session replication, fast network convergence (under 1 second) and both local and geo-redundant systems, our service is designed to support 99.999% throughout the service.

A comprehensive sparing plan for all sites with replacement strategies.

Key spare components are provided, at a minimum, at the data center locations and at PSAP host sites. Allerium provides a separate, unpowered, cabinet that houses our spares immediately adjacent to the production equipment, meaning spares are available only feet away from the production systems. Spares can also be housed at agreed-to locations throughout the state, rather than at the host PSAPs, which provides "spare depots" that are centrally located to the PSAPs. This approach has been used when PSAPs do not have adequate space or desire to house spares locally, and both approaches have proven to be effective.

Established technician response times for outages.

Every outage or impairment is managed by the Allerium NSOC. For critical issues, technicians are paged out immediately upon triage of the event and will commence work towards resolution. Triage begins immediately in the NSOC (where up to 80% of issues are resolved without further involvement) and a remote technician response is provided within 15 minutes of the notification for critical incidents. On-site personnel, when required, are paged out for support of hardware-based incidents. Response times for on-site response vary by PSAP location but are targeted for < 2 hours.

Calculated MTTR based on spares and response times.

As noted above, the MTTR for a high-availability system (for instance, the HA routers at a PSAP) is almost instantaneous due to the nature of the redundant system. Given a 1 second approximation for the HA "handoff" between routers, the MTTR is just that, approximately 1 second. Even using a calculation for a single router (by way of example only as Allerium does not deploy single-router

solutions), the MTTR of 2 hours would yield a MTBF of 22.8 years, which is supported by the routers in use.

A consolidated overview of overall availability combining MTBF and MTTR data.

Overall availability remains at 99.999%, by design, for all aspects of the service. For reasons described above, the MTBF and MTTR data for active/active systems is not a relevant measure. For further certainty, most impairments are not the result of a failure by a single piece of equipment, but are instead the result of human error, lack of circuit diversity, large-scale network impairments, or configuration issues. Allerium has successfully mitigated the issues with equipment failure (which would rely on the referenced MTBF and MTTR calculations) by designing the system for high availability on redundant equipment elements.

5.1.5.2. ESInet Reliability

1.5.2. 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.*

Response:

Strategic diversity across geographic regions, technology, and vendors.

Allerium is supportive of, and in compliance with, FCC R&O 13-158, which includes taking reasonable measures in key areas, including:

- **Circuit Diversity:** Allerium's ESInet is based on the concept of redundant *and* diverse circuit paths. We have provided circuits that use different underlying carriers for each fiber circuit and will ensure that each circuit maintains last-mile diversity to each PSAP host. Additional diversity is achieved by deploying LEO satellite circuits (or other wireless paths), at the State's discretion.
- **Network Management and Monitoring:** We operate a 24x7x365 NSOC that supports, exclusively, our 9-1-1 services. The Allerium NSOC is purpose-built to support 9-1-1, and 9-1-1 only, and has been doing so for nearly three decades.
- **Power Redundancy:** Allerium proposes using three data centers to provide NG9-1-1 services to the State, with each of the three data centers (Council Bluffs, Dallas, and Raleigh) residing on a different power infrastructure grid. In addition, each data center is designed to Tier 3 equivalent infrastructure, which includes A + B side power, generator backup, and UPS.

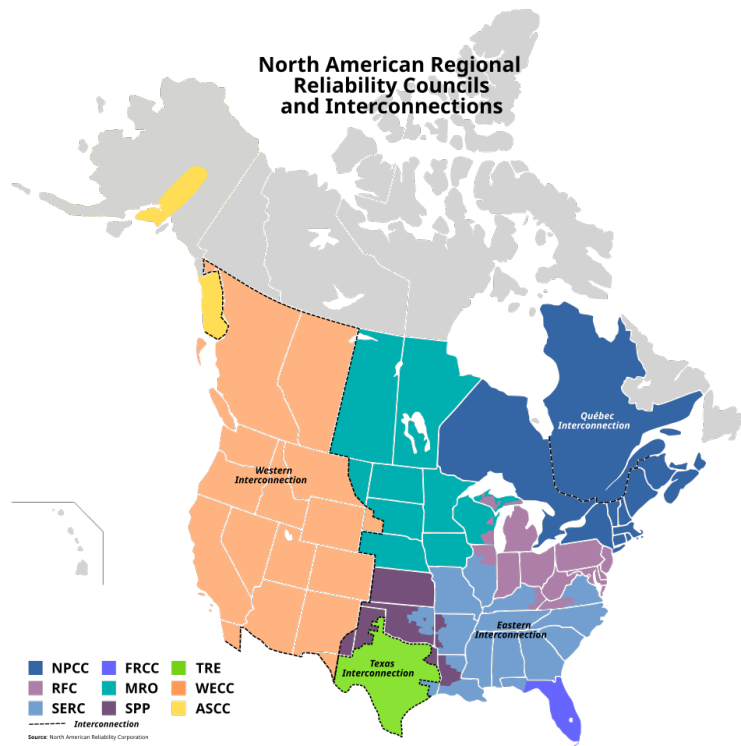


Figure 25. Electrical Grid Interconnects

Taken as a whole, Allerium's NG9-1-1 environment is extremely robust and further strengthened by our commitment to upholding the FCC's R&O for enhancing availability.

Use of at least two routers from different manufacturers per node for redundancy (or rationale if unfeasible).

While we recognize that the use of two different router manufacturers per node is technically feasible, we do not recommend pursuing this path. Allerium has the expertise to operate routers from different manufacturers (we operate both Juniper and Cisco routers in different deployments), we provide the following rationale as a recommendation to maintain a single-manufacturer solution:

- **Complexity:** As outlined elsewhere in this proposal, most impairments are not due to equipment failure. The most common causes of issues are network/circuit availability, power issues, and human error. None of these issues are addressed by operating different router manufacturers, and in fact at least one - human error - is exacerbated through the use of two manufacturers. Additional complexity in the network (i.e., two different sets of routers) leads to additional complexity and a higher risk of human error.
- **Troubleshooting:** While a separate set of routers may seem like a genuine solution, the additional time troubleshooting issues, as they would appear differently from each manufacturer, is likely to extend the time to resolution. When seconds count, any additional complexity that stands in the way of an immediate resolution should be avoided.
- **Cost:** Deploying a second set of routers invariably will lead to cost increases. Since routers are not designed to work in a highly available pairing with other manufacturers, creating

diversity in the router solution means deploying two different sets of routers at the PSAP, thus doubling the cost.

We recognize that scenarios exist where single-vendor solutions are at risk and we work to mitigate those risks in every deployment. However, the dual-router approach is very likely to extend those risks into other areas, to such a degree that Allerium recommends a single-router solution. We look forward to discussing the option further with the State.

Elimination of single points of failure (e.g., "backhoe incident").

Single points of failure are avoided in the Allerium service solution. Allerium designs the NGCS for high redundancy and diversity. We use an active/active architecture deployed across geographically redundant sites to ensure there is no single point of failure in the NGCS solution. In addition, we deploy local redundancy at each site as well, thus embracing both local and geographical redundancy. The result of this architecture is a NGCS system that has a total of six operating services for each of the NGCS elements, using an ESInet built on diverse fiber circuits to each endpoint. Since the architecture is active/active, a loss of any single element or even a single data center (housing both local elements) will not impair the service due to the surviving data center.

Particular to circuit availability (e.g., "backhoe incident"), Allerium's solution addresses this single point of failure scenario in three ways:

- **Circuit Diversity:** We provision each circuit path on a separate carrier network, using separate carrier POPs on separate fiber "rings" to ensure no single point of failure. The most common scenario for "backhoe" incidents is in the last mile to the PSAP, where the PSAP location may not have diverse entrances and both fiber paths use the same trench/overhead/entrance facility. We assess those situations as part of our site survey process and share the results with the State/PSAP. Remediation efforts, or site limitation acceptance, will be completed before the site is put into production.
- **Fast Convergence:** Using the built-in capabilities of a well-designed ESInet, we employ sub-second BFD timers to ensure that separate MPLS circuit paths will converge in the instance that one path becomes unavailable.
- **Automatic Alternate Routing:** In the event that a backhoe incident actually occurred and/or both circuit paths were otherwise compromised, we have built-in, automatic, alternative routing policies provisioned for each PSAP. Alternate routing can take the form of a PSTN fallback, a tertiary network fallback, or an alternate PSAP fallback. In no instance will calls go undelivered with our design.

For further certainty, Allerium does not sell "network" as part of our business and as such we are carrier-agnostic in our selection of ESInet circuits. In other words, we have no incentive to sell the State "our" network circuits as there is no benefit to doing so. We only select the best circuits available for the purpose of creating a highly available network and we will never provision a PSAP to use circuits that do not align with that purpose.

Conformance to FCC Report and Order FCC 13-158 for enhancing 911 reliability.

As referenced in the response above (regarding our strategic diversity in relation to FCC 13-158), we confirm our commitment to the remainder of the FCC R&O. As part of our commitment, we adhere to mandatory reliability standards and focus our service towards preventing outages in every way feasible, improving our response times and notifications to customers when impairments do occur.

Notably, we have found that the most important aspects of improving reliability are:

1. Designing the correct service from the beginning but also
2. Being prepared to be transparent and forthcoming with notifications and follow-ups.

We are proud and honored to be part of each NG9-1-1 deployment we have and believe in transparency—in both the design and operation—of each of those states where we operate.

5.1.6. Operations and Management

5.1.6.1. ESInet Monitoring and Management

1.6. Operations and Management

1.6.1. 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.*

Response:

Allerium provides a dedicated 24x7x365 Network Operations Center (NOC) responsible for continuous monitoring and management of the ESInet and all associated NG911 components.

Continuous Monitoring and Detection

Allerium's NOC provides real-time monitoring of all ESInet components, including network links, NGCS elements, and interconnections utilizing integrated observability platforms along with supporting monitoring and alerting systems.

Operational dashboards provide centralized visibility into:

- Network health and performance

- Link status and utilization
- Active alarms and incidents
- Service-impacting conditions across all markets

This enables immediate detection and response to any functional disruption within the system.

Congestion Monitoring and Mitigation

All ESInet network links are continuously monitored for capacity utilization and congestion thresholds. Allerium establishes defined performance thresholds that trigger proactive mitigation actions when exceeded.

Mitigation strategies include:

- Traffic rerouting and load balancing across redundant paths
- Coordination with transport providers for capacity adjustments
- Proactive escalation to engineering and vendor teams

This approach ensures that congestion is addressed before it impacts service delivery.

Failure Detection and Alerting

Allerium's monitoring systems are configured to generate automated alerts within one (1) minute of any link or component failure.

Alerts are:

- Automatically ingested into the NOC workflow
- Correlated with existing events where applicable
- Converted into actionable incidents within the ITSM system

NOC personnel immediately assess and initiate response procedures upon alert receipt.

Thresholds and Proactive Mitigation

Allerium defines and maintains explicit operational thresholds for key performance indicators, including:

- Link utilization and congestion levels
- Latency and packet loss
- System health and availability metrics

When thresholds are exceeded, predefined mitigation actions are initiated without delay. These thresholds and response actions are documented and consistently applied across the network.

Proactive Communication with the State

Allerium maintains structured and proactive communication with the State during any event requiring mitigation.

This includes:

- Immediate notification of service-impacting conditions

- Communication of mitigation plans and expected timelines
- Ongoing status updates and progress reporting through established channels

All communication workflows are defined within Allerium's NOC-to-NOC operational documentation, which establishes clear expectations for coordination, escalation, and information sharing between Allerium, the State, and partner organizations.

Operational Differentiation

What differentiates Allerium's NOC is its integrated operational model, combining:

- Real-time monitoring and observability
- Structured incident and escalation management
- Defined NOC-to-NOC communication frameworks
- Tight coordination between NOC, Engineering, and Field Services

This model ensures rapid detection, immediate response, and coordinated resolution of issues, while maintaining clear and consistent communication with all stakeholders.

Through this comprehensive monitoring and management approach, Allerium ensures high availability, rapid fault detection, proactive mitigation, and sustained performance of the ESInet in support of NG911 operations.

Interfacing with Other Service Providers

Allerium maintains documented operational processes that enable effective coordination between our NOC and the vendors that we work with to support the State.

Allerium develops and distributes NOC-to-NOC operational documentation that defines the communication and coordination framework between organizations. These documents include key operational details such as incident creation procedures, portal access and login information, service level agreement (SLA) expectations, escalation tables, and communication protocols for both incident and change management activities.

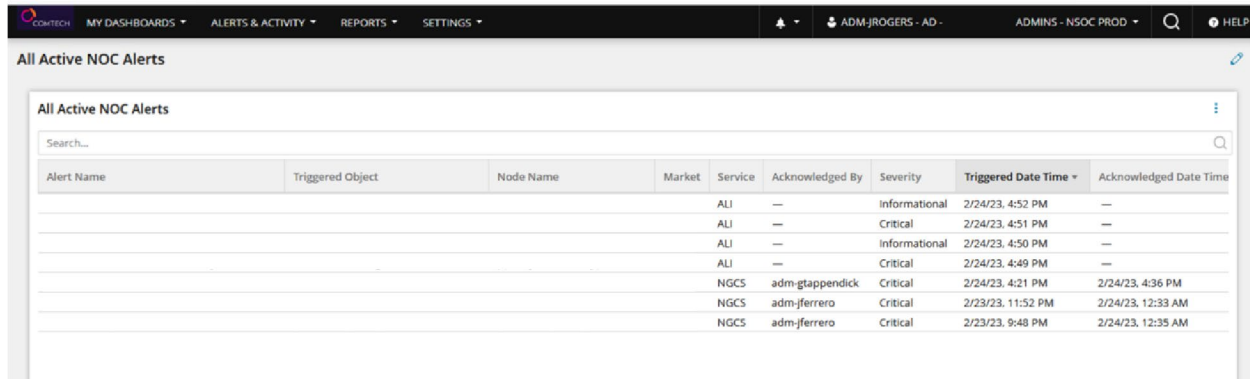
The Allerium NOC operates as the central coordination point for operational communications, ensuring that agencies and service providers receive timely notification of incidents, service impacts, restoration progress, and resolution updates. Communication channels supported by the NOC include email, text notification, web-based service portals (if applicable), and voice communications, enabling agencies to interact with the NOC through the method most appropriate for the situation.

To ensure continuous alignment and operational transparency, Allerium also establishes regular operational coordination meetings with service providers and stakeholders. These meetings are used to review open incidents and service requests, coordinate planned maintenance, and change activities, and identify opportunities for process improvement.

Through these documented procedures and structured communication channels, Allerium ensures efficient tracking, notification, and coordination of operational events, supporting timely resolution of incidents and maintaining clear and reliable communications.

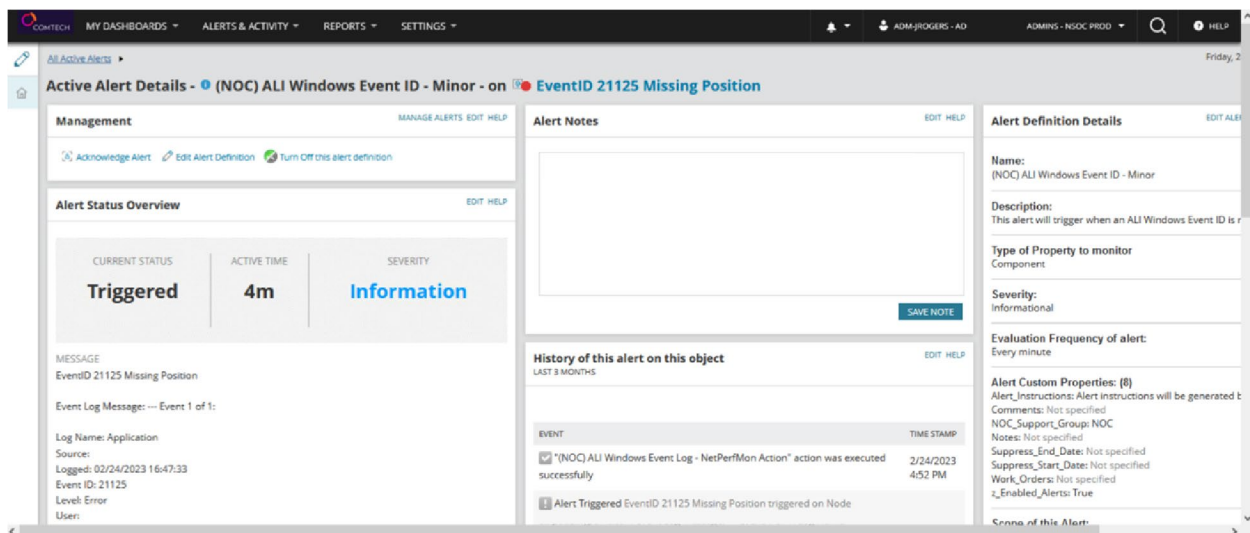
Monitoring Platform

Allerium employs a monitoring platform to collect and monitor data from systems and applications used in the operation of ESInet and NGCS service functions. This platform provides real-time awareness of system health and operational status of the service. In conjunction with the monitoring platform, Allerium employs both dashboard and reporting tools for use by both internal and external users to measure operational performance.



Alert Name	Triggered Object	Node Name	Market	Service	Acknowledged By	Severity	Triggered Date Time	Acknowledged Date Time
ALI	—	—	—	—	—	Informational	2/24/23, 4:52 PM	—
ALI	—	—	—	—	—	Critical	2/24/23, 4:51 PM	—
ALI	—	—	—	—	—	Informational	2/24/23, 4:50 PM	—
ALI	—	—	—	—	—	Critical	2/24/23, 4:49 PM	—
NGCS	adm-gtappendick	—	—	—	—	Critical	2/24/23, 4:21 PM	2/24/23, 4:36 PM
NGCS	adm-ferrero	—	—	—	—	Critical	2/23/23, 11:52 PM	2/24/23, 12:33 AM
NGCS	adm-ferrero	—	—	—	—	Critical	2/23/23, 9:48 PM	2/24/23, 12:35 AM

Figure 26. All Active NOC/SOC Alerts Dashboard



Active Alert Details - (NOC) ALI Windows Event ID - Minor - on EventID 21125 Missing Position

Management MANAGE ALERTS EDIT HELP

[Acknowledge Alert](#) [Edit Alert Definition](#) [Turn Off this alert definition](#)

Alert Status Overview EDIT HELP

CURRENT STATUS: **Triggered** ACTIVE TIME: **4m** SEVERITY: **Information**

MESSAGE
EventID 21125 Missing Position
Event Log Message: --- Event 1 of 1:
Log Name: Application
Source: 02/24/2023 16:47:33
Event ID: 21125
Level: Error
User:

Alert Notes EDIT HELP

Alert Definition Details EDIT ALERT

Name: (NOC) ALI Windows Event ID - Minor
Description: This alert will trigger when an ALI Windows Event ID is r
Type of Property to monitor: Component
Severity: Informational
Evaluation Frequency of alert: Every minute
Alert Custom Properties: (8)
Alert_Instructions: Alert instructions will be generated t
Comments: Not specified
NOC_Support_Group: NOC
Notes: Not specified
Suppress_End_Date: Not specified
Suppress_Start_Date: Not specified
Work_Orders: Not specified
z_Enabled_Alerts: True
Scope of this Alert:

History of this alert on this object EDIT HELP
LAST 3 MONTHS

EVENT	TIME STAMP
✓ "[NOC] ALI Windows Event Log - NetPerfMon Action" action was executed successfully	2/24/2023 4:52 PM
Alert Triggered EventID 21125 Missing Position triggered on Node	

Figure 27. Node Summary of an Active Alert

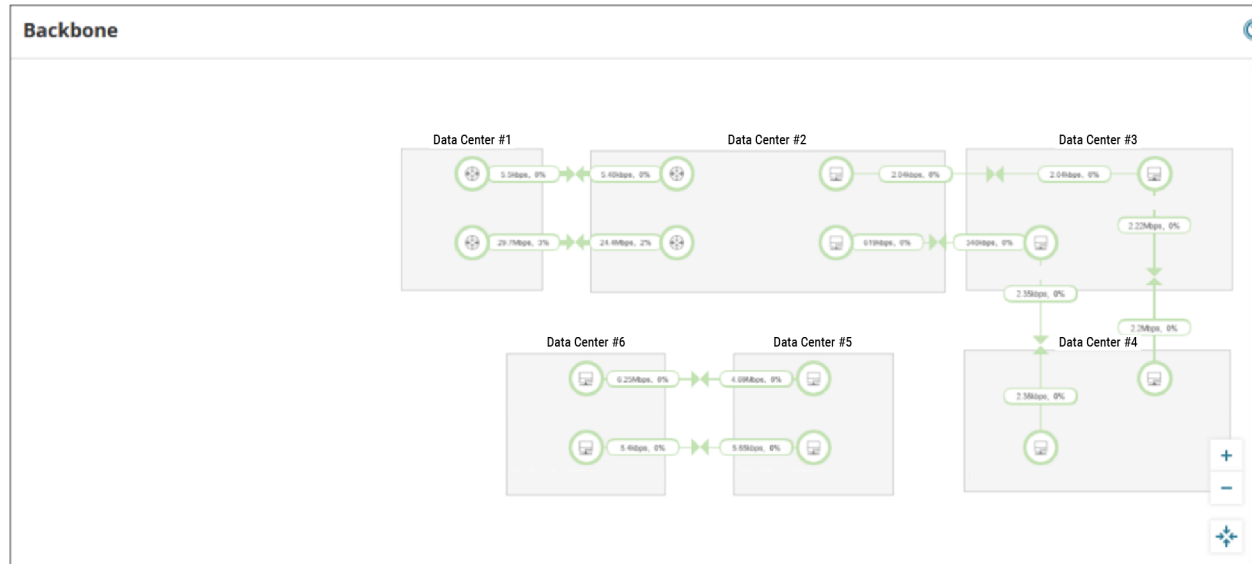


Figure 28. Major Backbone Network Connectivity Circuit Map

5.1.6.2. ESInet Maintenance Window

1.6.2. 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.

Response:

ESInet Maintenance Window Overview

Allerium's ESInet maintenance strategy is designed to support a no scheduled downtime operating model, consistent with the availability expectations of mission-critical public safety systems. Maintenance activities are carefully engineered, planned, and executed to ensure continuous

service availability through the use of redundant architectures, traffic failover mechanisms, and controlled change management procedures.

All maintenance is governed through Allerium's formal Change Management framework, ensuring that all activities are risk-assessed, documented, reviewed, and executed in a manner that preserves network stability and service continuity. Maintenance activities are only performed under approved processes that align with §E-9.5.1 and §E-9.5.2.

No scheduled downtime; completion of any maintenance impacting availability under specified terms (§E-9.5.1 and §E-9.5.2).

Allerium does not perform maintenance that results in scheduled downtime under normal operating conditions.

All maintenance activities that have the potential to impact service availability are executed strictly under the requirements defined in §E-9.5.1 (Change Management Requirements) and §E-9.5.2 (Scheduled Maintenance Process). These processes ensure that all changes are formally reviewed, approved, and executed within controlled maintenance windows with appropriate safeguards in place.

Where maintenance introduces potential risk to availability, Allerium ensures that mitigating controls—such as redundancy, traffic rerouting, and staged implementation—are implemented to maintain or exceed the 99.999% service level throughout the activity.

Prohibition of maintenance causing outages outside those terms.

Allerium strictly prohibits any maintenance activity that could result in a service outage unless it is conducted in full compliance with established Change Management and Scheduled Maintenance processes as defined in §E-9.5.1 and §E-9.5.2.

No maintenance activity with potential outage impact is performed outside of these controlled processes. This governance model ensures that all high-risk activities are subject to formal review, risk assessment, approval, and oversight prior to execution.

This disciplined approach minimizes the risk of unintended service disruption and ensures alignment with public safety operational requirements.

Requirement for a Maintenance Operation Plan (MOP) at least 14 days prior, including provisional configurations to maintain 99.999% service level.

Allerium requires a comprehensive Maintenance Operation Plan (MOP) for all applicable maintenance activities, developed and submitted no less than 14 days prior to the scheduled work.

Each MOP includes, at a minimum:

- Detailed scope of work and implementation steps
- Risk assessment and impact analysis
- Pre- and post-maintenance validation procedures
- Rollback and contingency plans
- Communication and notification plans
- Defined roles and responsibilities

- Provisional operating configurations to ensure continued service performance and adherence to the 99.999% availability requirement during maintenance execution

All MOPs are reviewed and approved through Allerium's Change Advisory Board (CAB) process prior to execution.

Descriptions of handling no-downtime requirements, planning/conducting maintenance without impacting availability, and the MOP process for guiding activities.

Maintenance activities are planned and executed using:

- Redundant ESInet architecture supporting failover and traffic rerouting
- Phased and non-impactful implementation strategies
- Real-time monitoring and validation throughout maintenance execution
- Controlled execution under approved MOPs and Change Management processes

The MOP serves as the authoritative guide for all maintenance activities, ensuring that each step is executed in a consistent, validated, and low-risk manner. During execution, the NOC maintains continuous oversight, monitoring system performance and readiness to initiate rollback procedures if required.

Through this approach, Allerium ensures that maintenance activities are conducted safely, predictably, and without impact to PSAP operations or service availability.

5.1.7. Implementation Details

5.1.7.1. Port Mapping

1.7. Implementation Details

1.7.1. 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.*

Remainder of page intentionally blank

Response:

Comprehensive documentation of port block/mapping/forwarding policies accessible to the State and PSAPs.

Allerium uses an IP address management (IPAM) solution to efficiently allocate and manage our IP addresses. Using IPAM improves our network efficiency and administration while simultaneously providing enhanced security and compliance. We will work with the State and PSAPs to provide both the policies and related documentation as part of our secure knowledge base that is shared with approved stakeholders.

An example of port assignments is provided in our ICD for ESInet-to-PSAP SIP ICD.

Provisions allowing stakeholders to request traffic on specific ports from external sources to predetermined network points.

Allerium supports the requested use case to allow stakeholders to request traffic on specific ports from external sources. We recognize that NG9-1-1 systems are highly interconnected and we will work with the PSAPs (and State) to address this need in a secure and controlled manner. The specific provisions to allow stakeholders to request such activity will be documented once a mutually-agreed-to process is completed.

5.2. Next Generation Core Services (NGCS) Requirements [Project Requirements and Scope of Work, Section E.2]

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.*
 - o *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.*
 - o *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.*
 - o *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.*
 - o *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.

Response:

NGCS Overview

Allerium designs its systems for high availability using a 6-way-redundant approach for active/active call processing across three geographically diverse data centers. We employ a load balancing methodology with each system being both locally and geographically redundant, resulting in each data center continually processing calls in an active/active manner. If any one element or physical connection is unavailable, the remaining elements or connections will handle the increased 9-1-1 traffic load rather than the system failing over. This methodology is extensible to the entire system so that any one element of the six available elements can handle the entire state's call volume.

Allerium is one of the largest NGCS providers in the country and has a proven record of deploying NG9-1-1 services quickly and practically. Our systems are designed to be modular and flexible, allowing us to deploy each customer in the manner that works best for them. We support legacy call flows when necessary, interacting with legacy OSPs, selective routers, and call handling models, but embrace the future of NENA i3 where these functions are no longer required. This flexibility brings value to our customers in shorter deployments with less difficulty. Our last statewide deployment deployed their first PSAP in only 8 months, and we've completed full statewide deployments in less than 18 months.

Allerium provides proven, standards-based, highly reliable NGCS services that meet our customers where they are in terms of their readiness for NG9-1-1. We look forward to working with the State and the PSAPs to build upon the work that Nebraska has already begun.

NGCS deployment in multiple redundant data centers (preference for at least 3, with one in-state and one >100 miles away).

Allerium's proposal includes three NGCS data centers, each operating with redundant NGCS application stacks, for a total of six active-active-active sets of NGCS elements. While not in-state, our existing data center in Council Bluffs is extremely close to the state border and offers an extremely low-latency and cost-effective option. Coupling our Council Bluffs location with our other NGCS data centers in Dallas, Texas, and Raleigh, North Carolina, provides excellent redundancy and geographic diversity.

Preference for separate instances (different VMs) if sharing data centers.

Allerium is proposing shared data centers as the best-value approach to the deployment. While the data centers are shared, the State will be segregated from other tenants as their own market. Provisioning the State's data in this manner ensures that all routing control, data segregation, and access control is specific to the state.

Redundant deployment of all components without single points of failure; resistance to external threats and internal disruptions from other ESInets/NGCS.

Our deployment model uses a six-way redundant design in NGCS elements, diverse fiber-based MPLS network paths to the PSAPs, and redundant POIs for carrier ingress. There are no single points of failure in the NGCS or core ESInet deployments. Our deployments are very resistant to external threats as well as internal disruptions, achieved through the use of layered cybersecurity controls, physical access controls, and security zone architecture. We go above and beyond NG-SEC security standards by implementing NIST 800-53 Moderate cybersecurity controls. We also are ISO 9001 compliant for information security and meet TL9000 security controls in our NSOC (the only non-carrier NSOC to achieve this). The logical separation in our data center deployments, coupled with secure networks, least-privileged access control, and a robust cybersecurity posture ensures that the State's deployment is not subject to influence from internal or external events.

Description/demonstration of unimpeded operation during disruptions.

Allerium implements multiple recovery mechanisms to ensure unimpeded operations during disruptions. Our NSOC is the frontline incident management organization, resolving 85% of issues within the NSOC with no further escalation. Prior to NSOC involvement, however, the service automatically recovers from many events with no interaction necessary. Recovery methods include but are not limited to:

- **Fast Convergence:** Our ESInet is made up of redundant and diverse fiber networks that automatically recover with sub-second convergence times when a ESInet circuit becomes compromised or unavailable.
- **Enhanced Policy Routing:** We have gone above and beyond the NENA i3 standard to offer enhanced PRF functionality. Not only can we alternate route by the standard methods in the standard (e.g., time of day), we offer web-based access for PSAP Make Busy functions as well as Nuisance Caller treatment.
- **Active-Active Design:** Allerium's active-active-active design for NGCS ensures that all three data centers are receiving traffic at all times through load-balancing. Each of the six application stacks are capable of processing 100% of the State's traffic in isolation,

meaning five of the six NGCS deployments could fail/become unavailable and the State would not lose a single call.

Policy retrieval from NENA-STA-010.3-compliant policy server with host name provisioning.

As described immediately above, our PRF uses policy routing rules to implement the function of a policy store. Our design exceeds the NENA i3 standard.

Preference for active-active redundant elements/databases serving traffic at all times.

Allerium's services are always deployed in active/active mode for NGCS elements. With three data centers in operation, the State's deployment will have six-way redundancy, with each serving traffic at all times. There is no "failover" in our active/active service.

Statements on non-active elements with failover mechanisms guaranteeing 99.999% availability.

Allerium's service is built for active/active call processing.

Descriptions of failure detection/recovery for active-active elements (worst-case timing, SLO maintenance).

The most relevant failure detections are 1) in the network, and 2) the routers at the PSAPs. In the first case, failed network circuit paths will recover automatically within 900 milliseconds (configurable to more/less) or the circuit will converge to the surviving network circuit within that time. Similarly, router clusters deployed with high-availability backplane connectivity have sub-second recovery, worst-case.

State maintenance/failover for databases/call-state data.

We use a trigger-based replication engine to replicate the call data from the local database to all remote databases. Data is replicated within milliseconds. Furthermore, Allerium applications utilize hunt group logic and query to all databases to retrieve call data rather than relying on data replication. This query mechanism allows applications to query all configured databases (not relying only on a local database) so any surviving database can be queried. This local-or-remote database strategy allows any database copy to be "down" while not impacting call data.

Replication strategy for call-time updated databases with max sync time.

Call time databases are updated in milliseconds, using the trigger-based mechanism described immediately above.

Dynamic ECRF service boundary updates with replication/sync description.

Allerium's ECRF supports dynamic, zero-downtime updates for all GIS layers, including the service boundary polygons, ensuring routing decisions always reflect the most current GIS data submitted by the GIS authority. The update workflow is designed to be resilient, fault-tolerant, and efficient, with replication across all NGCS data centers occurring within a strict timeframe.

After the GIS is to the Spatial Interface (SI) by the GIS authority, the data goes through an automated QA/QC validation process. Any identified discrepancies are sent back to the authorized jurisdiction for review. If the data passes all QA/QC checks it is automatically approved for provisioning to the ECRF and LVF. Provisioning is performed as part of a controlled operation to ensure all applicable NGCS components receive a consistent dataset version. The updates sent to

the ECRF and LVF can be scheduled at a frequency defined by the customer, though most choose a 24-hour update cycle. If desired, Allerium supports hourly or near real time updates as well.

During the replication process, all ECRF nodes remain fully operational. Once replication is complete, the updated dataset is activated without interrupting services. Allerium's process is focused on ensuring there is zero downtime within the system to avoid query failures, degraded routing, or service interruptions.

5.2.1. Edge Security and Ingress

5.2.1.1. Border Control Function (BCF)

2.1. Edge Security and Ingress

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.*

Response:

BCF Overview

Allerium's proposed solution includes a border control function (BCF). The BCF provides security and call control for IP-based traffic. The BCF is comprised of firewalls for data flows and SBCs for SIP call processing. Allerium employs a defense-in-depth strategy with multiple network layers protected by firewalls and SBCs within the service.

The border control function (BCF) is made up of two elements: a firewall and an SBC.

Employing redundant network appliances, Allerium secures entry into the ESInet as required on both the ingress and egress sides of the network. The proposed solution includes two firewall devices at each data center to provide Allerium with remote support and connectivity to the ESInet.

In an ESInet, the SBC controls SIP signaling and associated media to ensure that the call and call characteristics being presented to the ESInet are predictable and acceptable. All calls are expected to pass through the SBC, especially those that originate from an unmanaged source.

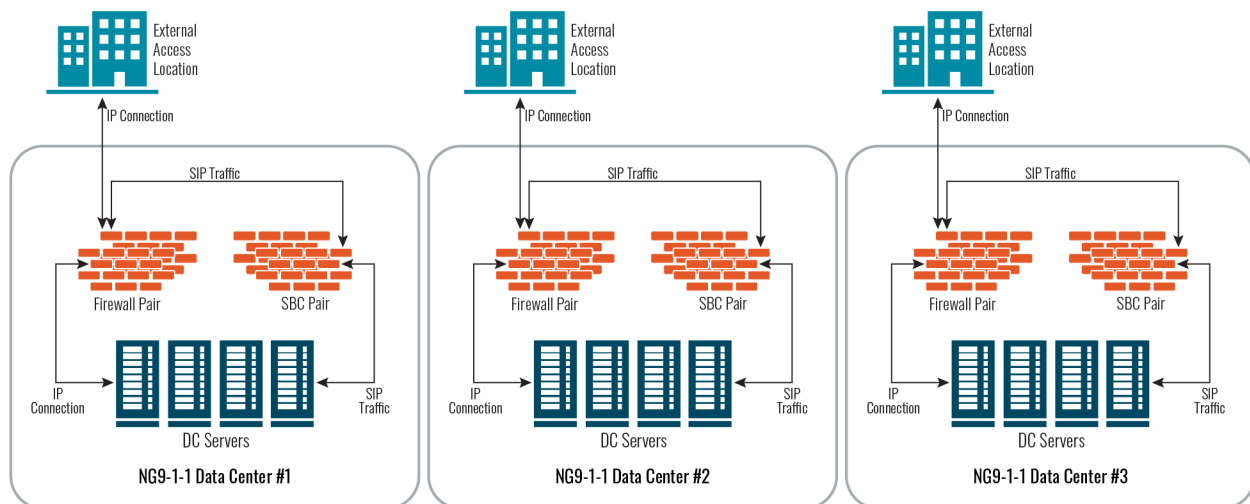


Figure 29. Border Control Function

Allerium is a provider of both ESInet and IP-based call-routing products. Allerium solutions are 100 percent Allerium engineered, built on open standards, and developed to meet NENA's published i3 standards. Allerium's call-routing and call-handling technologies can seamlessly integrate with other i3-compliant solutions through a direct SIP connection.

The proposed solution is interoperable with other NG9-1-1 systems on the market and is compatible with BCF/SBC vendors who meet the i3 requirements.

The SBC supports the following features that align with generally accepted security practices:

- Either acting as a firewall or working cooperatively with an existing firewall depending on the deployment model.
- Serving as a transcoder for codec conversion.
- Helping resolve any topology issues that stem from either network address translation (NAT) deployment or bandwidth misalignments (for example, by preventing low-speed links from being oversubscribed with voice traffic).

Regarding SIP repair, the SBC attempts to fix those elements required to process the call on the ESInet. However, a lack of support for certain SIP elements is not used to deny a call (i.e., all calls will be accepted). The SBC is expected to process reasonably malformed SIP INVITE messages, presuming the malformed data is not critical to processing the call. SIP proxies, including SBCs, ignore headers they do not understand.

The following treatments listed in Table 57 define the handling of malformed messages.

Table 57. Call Treatment of Malformed Messages

Message	Call Treatment
400 (Bad Request)	A 9-1-1 call is so malformed that the BCF cannot parse the message.
401	Should never occur for a 9-1-1 call, but proxy authorization is required for all calls originated by entities within an ESInet.
402	Should never occur for a 9-1-1 call or an internal call.
403 (Forbidden)	Normally, 403 (Forbidden) should not occur. However, if the BCF passes a malformed INVITE that downstream devices cannot handle, they may have no choice but to return 403.

The SBC has little or no impact on general call delivery and bandwidth performance characteristics given its nature as a high-performance, hardware-based component.

Allerium uses a multi-tiered approach to ESInet/NGCS design with respect to security borders. We place all sites in a security zone protected by redundant BCF elements. For instance, we firewall the PSAPs from the rest of the network to prevent intrusion from that vector. Likewise, we place outward-facing access points (such as the COMTECH INSIGHTS portal) in a separate security zone. Allerium protects the core network and NGCS components themselves from both upstream (from the ingress service provider) and downstream (the PSAPs) threats using redundant BCFs.

Conformance to NENA-STA-010.3 preferably from commercial SBC, Firewall, and NG911 capabilities.

STA-010.3f defines a robust feature set for BCFs along with the demand for use of COTS devices. As such, public safety has adopted use of commercially available BCF devices such as SBCs and firewalls. Commercial providers of BCF devices have no intent to implement some aspects of STA-010.3f. Allerium notes that the Standard leaves space for adding these services: "Commercial Off The Shelf SBCs and Firewalls may be extended to have NGCS-specific capability, *or a separate functional component may provide that functionality.*" As such, we have provided some mechanisms within other functional elements and intend to further our roadmap to support remaining required functions.

DDoS/TDoS mitigation up to terabit levels.

Allerium is prepared to mitigate Telephony Denial of Service (TDoS), DDoS, and other security threats. The security arrangement is flexible. The final operational implementation will consider the State's policies. Below is a description of how we mitigate security threats.

DDoS and Multimedia and Text Distributed Denial of Service (MTDDoS) attacks are typically IP-based attacks, whereas TDDoS are more SIP-based attacks. Comtech maintains active protections against these types of threats.

For TDoS, Allerium maintains several layers and methods of protection depending on the needs and request of the PSAPs. The Session Border Controllers (SBC) both at our third-party aggregator and at the ingress to the Comtech NGCS allow for automated call throttling. If a threshold is met, there is a temporary stopping or re-routing of calls from identified nuisance calls. For more controlled protections beyond the SBC layer, the PSAP can identify nuisance calls and enter rules into the system to again temporarily either block or re-route those calls. In addition to automation and PSAP layer identification, Allerium sets rules within the system to generate alarming at certain call thresholds that are relayed back to the Allerium NOC/SOC and can be used to inform the PSAP of high nuisance call levels to provide information for re-routing or blocking decisions.

Allerium DDoS and MTDDoS protection for data elements is supported by next-generation firewalls and third-party DoS mitigation services. The third-party DoS mitigation service operates in line with our incoming network traffic. When a potential DoS attack is detected, the service automatically applies predefined rules to reroute the traffic through a scrubbing process, ensuring that only legitimate transactions are allowed to pass through.

5.2.1.2. STIR/SHAKEN Support

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.*

Response:

STIR/SHAKEN requirements span both the Telecom infrastructure as well as the NG Core applications. Allerium has not implemented STIR/SHAKEN at this time and plans to do so in our 12-month roadmap.

5.2.1.3. Security Mechanisms

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.

Response:

Security Mechanisms Overview

Allerium is actively working with the NIOC to establish a certificate practice statement and develop ICAs. NENA PCA/PKI systems are in the very early stages of development within the public safety industry. Therefore, close coordination with the standards bodies is occurring to define the processes of generating services.

As such, Allerium is identifying all the included NG9-1-1 FEs that are required support credentials from the PCA and incorporating the plan tasks outlined below to establish ourselves as an ICA. We will issue certificates to all NG9-1-1 elements as a function of our ICA and plan to issue agency certificates when authorized by the NENA Root PCA.

Allerium's credentialing plan outlines the preliminary implementation plan for establishing the NENA PCA/PKI framework in support of our clients. There are certain technical and programmatic aspects yet to be fully implemented/defined by the NIOC. As additional information becomes available, Allerium will expand and/or elaborate on technical and operational elements.

Allerium's plan includes:

- **ICA Model Evaluation Process:** Evaluating PKI models available for implementation.
- **Establishment of Tier 2 ICA:**

- Procuring infrastructure, including the development of the certificate practice statement
- Performing technical review of all FEs
- Developing certificate management operational procedures and processes
- Issuing element certificates
- Issuing agency certificates
- Issuing user and role certificates (once defined by NIOC)
- **Management Procedures and Processes:**
 - Verification process
 - Certificate management process
 - Certificates issuance process
 - Change control
 - Audit

Allerium's is actively working with its clients to define a strategy to support the NIOC's PCA and PKI framework.

Serving as the Regional PSAP Credentialing Authority

Allerium will serve as the ICA for the State as the statewide NG9-1-1 provider. Allerium will hold local registration authority necessary to provide local agency certificates in compliance with the PCA certificate policy. In this environment, Allerium will issue, manage, and revoke element, agency, and device certificates traceable to the PCA.

Allerium is working with its clients to define a strategy to support the NIOC's PCA and PKI infrastructure. We are working with the NIOC in designing our solution as an ICA, which eases operational deployment at the PSAPs.

Furthermore, Allerium will serve as the ICA with established trust to the NENA/NIOC PCA Root. Acting as an ICA empowers us to grant certificates to all parties and manage certificates on behalf of our clients. The result is a simplified deployment strategy in establishing trust in exchanging certificates.

Unique Domain Names and Certificate Interoperability

Allerium supports and ensures the uniqueness of domain names and interoperability of certificates as required.

Generating and Maintaining Both PSAP and NGCS FE Certificates

Once the NENA PCA/PKI has been fully established, Allerium will acquire ICA status. As such, Allerium will be granted the authority to provide the service to issue both element certificates for the NGCS FEs as well as agency certificates to PSAPs as necessary. Once certificates are issued, Allerium will maintain the chain of trust of all certificated elements and agencies to include annual re-validation.

5.2.2. Core Routing and Location

5.2.2.1. Emergency Services Routing Proxy (ESRP)

2.2. Core Routing and Location

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.*

Response:

ESRP Overview

Allerium's proposed solution includes an emergency services routing proxy (ESRP). The ESRP provides centralized routing control within the NGCS to determine the next hop for call delivery. The ESRP is provisioned with redundant active/active instances in each data center with the capacity to handle the State's call traffic. The ESRP works in conjunction with the ECRF in routing to the PSAP and includes the policy routing engine. Connected i3 compliant PSAPs receive calls directly from the ESRP without the need for an LPG.

The Allerium ESRP provides centralized routing control within the NGCS to determine the next hop for call delivery. The ESRP is provisioned with six active/active instances, each with the capacity to handle the entire state's call traffic.

Once the ESRP receives a 9-1-1 call and its associated location, the FE uses the caller's location to perform a Location to Service Translation (LoST) routing query to the ECRF. The ECRF returns a uniform resource identifier (URI) that identifies the primary PSAP. The ESRP then uses the URI and the PRF to send the 9-1-1 call to the proper primary PSAP. The PRF is also used to identify alternate routes to the primary PSAP if need be.

The Allerium ESRP is a replacement for legacy selective routing technology and can interface with other ESRPs and receive and parse presence information data format location object (PIDF-LO) data from a SIP message geo-location header, via either location by value (LbyV) or location by reference (LbyR) response using a hypertext transfer protocol (HTTP) enabled location delivery (HELD) dereference request—geospatial or civic—per the NENA i3 standard.

Location information is conveyed within the SIP INVITE geo-location header that is part of the required NENA i3 standard. This header is expected to be included with every INVITE that arrives at the ESRP. The Allerium ESRP can deliver calls to legacy-based and NG9-1-1-based PSAPs, with the only differences reflected in the type of hardware—routers, switches, and gateways—that needs to be installed at any PSAP location. If needed, gateway hardware is installed at the PSAP for converting SIP to legacy signaling.

Addressing Security Threats

As it relates to the ESRP, Allerium secures the ESRP both physically and architecturally to prevent threats from impacting the ESRP. Physically, we install the ESRP hardware in geographically diverse, secured data centers. Architecturally, our security requirements ensure incoming connections originate from a trusted source. Users accessing the ESRP's PRF module must provide valid credentials and complete MFA.

Allerium's ESRP can integrate with the NIOC PCA architecture (if and when the State chooses to pursue such direction) to ensure that other connected entities are trusted and secured points of entry and egress. For example, the ESRP can leverage the PCA certification and verification process to guarantee that incoming connections from sources such as the ingress network are secured, trusted, and verified.

In addition, Allerium adheres to the NIST framework which requires that the ESRP undergo continual evaluation for potential security gaps and improvements. Each release of the Allerium ESRP undergoes a security evaluation by Allerium's security engineers. Any potential threats are identified, evaluated for level of risk, and slated for mitigation.

If a localized security event occurs at a PSAP, the ESRP will route calls based on policy routing rules. In particular, the make busy functionality at a PSAP can be used to remove a PSAP from service at the discretion of the local PSAP staff. The ESRP will also use the policy routing rules to automatically route calls away from a PSAP that is not responsive, regardless of the state of the make busy function.

Additional Functionality

Geospatial Routing Day One

The Allerium ESRP prefers the use of location-based routing via the ECRF and the location provided. Allerium is prepared to support geospatial routing at the initial implementation of the solution providing the State GIS data is ready to support such an implementation.

Other Routing Mechanisms

Should location-based routing encounter an error condition (due to lack of data or a failed lookup), the Dialed Number Identification Service (DNIS)/From/P-asserted-identity, the source IP address or even the ANI can be used to trigger a specific policy. Among other things, the policy determines whether the calls should be routed:

- Via NENA i3 (location information server [LIS]/ECRF queries),
- Directly (pre-configured route),
- Via legacy SR (selective routing database [SRDB] dip),
- Via NENA i2 (emergency services query key [ESQK] based), or
- Per virtual trunk group.

Location Conveyance

The Allerium ESRP supports receiving a caller's LbyV in an incoming call SIP INVITE and LbyR. When receiving a LbyR, the ESRP dereferences the location using HELD. In both cases, based upon instructions in the PRF, the ESRP can override this location by performing a HELD query to a predetermined LIS/LDB.

Transfer to 7/10 Digit Numbers

Allerium both conferences and transfers 9-1-1 voice calls to seven and 10-digit numbers. Typically, this action is for transfers off net (that is, not destinations on the ESInet) rather than on net transfers. The Allerium ESRP receives a request from a PSAP to generate a conference/transfer and determines that an off-network entity must be added to the 9-1-1 voice session. Assuming the off network is reached via PSTN, the ESRP then generates an outbound leg to the seven or 10-digit number using the LSRG as the PSTN gateway.

Support for Star & Pound DTMF Codes

Allerium supports star and pound dual tone multi-frequency (DTMF) codes.

Allerium notes that support for star and pound codes is not within the context of NENA's i3 specification per NENA-STA-010.3. An i3 PSAP must signal with a SIP REFER which includes a Refer-To containing a SIP URI. As such, for a native i3 PSAP, Allerium expects a SIP REFER message containing a SIP URI vs. a TEL URI with a shortcut code (star or pound) defined.

However, Allerium does support star and pound DTMF codes for transitional SIP signaling from a legacy PSAP. In this case the PSAP may transfer via a SIP INFO message which contains a TEL URI and the necessary star/pound code the PSAP wishes to dial. To support star and pound code translations, Allerium obtains details regarding the expected codes and their appropriate destinations from all PSAPs during the data collection phase. We then configure the translations for each PSAP into the NGCS system accordingly.

Similar to a direct dial of 10-digit line, a PSAP may request an entity be added to the 9-1-1 voice session via a star or pound code that indicates a conference or transfer request. The LPG NG9-1-1 specific interwork function (NIF) processes the SIP INFO request and translates to the appropriate SIP URI. The SIP URI is used to set the Refer-To header value in a resulting REFER message from the LNG NIF to the ESRP to complete the transfer request. For translations that match on-network PSAPs, the ESRP invites the requested party to the call directly over the ESInet egress network to the destination PSAP. For parties not on the network, the ESRP processes the call out using the LSRG as the PSTN gateway.

5.2.2.1.1. Policy Store

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.*

Response:

Policy Store Overview

Allerium implements the policy store concept through PRRs found in our PRF. Allerium's solution routes calls based on policy routing rules which account for many operational needs. The integration of the NENA i3-specific functionality of the Policy Store with our PRF is in Allerium's 12-month roadmap.

The Allerium PRF is a required function of the ESRP and includes a secure, web-based interface. The ESRP/PRF provides logic to supply final policies before completing the call. In compliance with NENA standards and subject to approval, our NG9-1-1 system assigns alternate and overflow routing policies via the PRF with the capability to define and set each PSAP. As part of our data gathering exercises, Allerium works with the PSAPs to determine the various routing policies the PSAPs want supported for its implementation before loading the policies into the PRF.

The Allerium PRF suite includes the ability to:

- **View PRF Summary Information:** An interface that provides a read-only view into configured PSAP PRF rules.

- **Set Time of Day Rules:** Allowing the PSAP to divert text messages from the PSAP to a defined alternate for a given period of time. The rules may be configured to occur as a single event or in a recurring manner.
- **Set SIP Error Rules:** Allowing the PSAP to divert text messages from the PSAP to a defined alternate based on a SIP error message from the PSAP CHE.
- **Set a Ring No Answer Timer:** Allowing the PSAP to configure the amount of time to allow the text session to "ring" into the PSAP. If the timer expires before the PSAP answers the text session, then the call follows alternate routing treatment.

- **Set Call Throttling Thresholds:** Allow for each PSAP to provide a maximum number of concurrent calls based on incoming service type (wireline, wireless, VoIP). The configured service type may roll to a configured alternate service type, then another, if desired (e.g. wireless rolls to wireline, then VoIP). Once all volume is exhausted, PRF alternate routing engages. A specific set of alternate destinations can be used for Call Throttling PRF overflow.
- **Enacting a Forced Shutdown / Abandonment:** Allowing for the selection of alternate location based upon session media type. For text sessions the PRF provides a mechanism to divert text sessions to an alternate location. As not all PSAPs leverage integrated text solutions, the alternate location does not need to match the voice call alternate destination.

The screenshot displays the PRF Home Page. At the top, the COMTECH logo is on the left, and the text 'NG9-1-1 Provisioning' is on the right. Below the logo, a navigation bar includes 'Home' and 'PRF'. A welcome message 'Welcome, Admin46@UpSkill.com (Sign Out)' is visible. The main section is titled 'Policy Routing Function' and contains a series of tabs: 'Home', 'Alternate Routing Plans', 'SIPError Rulesets', 'Time of Day Rulesets', 'Alternates', 'Call Throttling', 'Override Anchor', and 'Shutdown'. The 'Home' tab is active. Below the tabs, there is a section titled 'Select one from the following available PSAPs'. This section contains a table with columns for 'PSAP Number', 'PSAP Name', and 'Current PSAP Status'. The first row shows '35' for the number, '30 Arbor County (My PSAP)' for the name, and 'Active' for the status. Below the table, there are pagination controls showing '(Records: 1 - 1 of 1, Page: 1/1)'.

Figure 30. PRF Home Page

Specifying and Implementing Custom Policies

The PRF can specify multiple alternate routes for a given routing policy. There is no practical limit to the number of alternate routes that can be specified. Allerium has systems deployed in which more than eight alternate routes have been defined for a given PSAP. Some of these alternate routes include re-routing calls via the PSTN.

Allerium allows end users to edit the PRF, presuming the appropriate training and controls are in place. Please note that Allerium has provided the requisite training for use of the Allerium PRF within this proposal. The Allerium roadmap includes continual enhancements to PRF provisioning

tools to adopt more features for end users. PRF change requests may also flow through the Allerium NSOC for modification by Allerium employees who are provisioning specialists.

Policy Change Interface

Allerium provides a secure web-based GUI that allows pre-approved PSAP personnel to:

- Review and change their alternate routing rules or
- Force their PSAP to an unavailable status (a “make busy” function).

Approved PSAP personnel can select from a list of pre-determined alternate route lists or make a phone call into the Allerium NSOC to force their PSAP to an unavailable status.

Figure 31 and Figure 32 illustrate the web-based GUI for policy routing rule review and change. Figure 31 allows a PSAP to perform a “make busy” selection for their PSAP.

NG9-1-1 Provisioning

Welcome, Admin46@UpSkill.com ([Sign Out](#))

StandaloneUAT

Home PRF

Policy Routing Function

Home Alternate Routing Plans SIPError Rulesets Time of Day Rulesets Alternates Call Throttling Override Anchor Shutdown

Select one from the following available PSAPs

Name	Current Status	Effective Forced Alternates (Audio) (ordered as listed)	Effective Forced Alternates (Text) (ordered as listed)
30 Arbor County (My PSAP)	Active	<Use current Forced Alt Routing List>	<Use current Forced Alt Routing List>

(Records: 1 - 1 of 1, Page: 1/1)

Refresh Shutdown

<Use current Forced Alt Routing List>

Try 30 Bay County first...

Try 30 Cedar County first...

Try 30 Dogwood County first...

Figure 31. PRF PSAP Shutdown Page

Figure 32 shows how time of day rules can be set for a PSAP and its identified alternate routes.

Policy Routing Function

Home Alternate Routing Plans SIPError Rulesets Time of Day Rulesets Alternates Call Throttling Override Anchor Shutdown

Select one from the following available PSAPs

PSAP Name	Record Status
30 Arbor County (My PSAP)	EXPORTED
46 Arbor County (My PSAP)	EXPORTED

(Records: 1 - 2 of 2, Page: 1/1)

Time of Day Ruleset for selected PSAP

Rule Set ID	Rule Set Name	Record Status	Time of Day Active/Unused (Runtime)
1	One Day - 1-5	EXPORTED	Active
2	Rule 2	EXPORTED	Unused

(Records: 1 - 2 of 2, Page: 1/1)

Time of Day Rules for selected Ruleset

Rule ID	Start Date	End Date	Start Time	End Time	Effective Days	Record Status
1	Sat 2022-08-20 08:00:00	Mon 2022-08-22 20:00:00	13:00:00	16:59:59	SU	EXPORTED
2	Mon 2022-08-22 13:00:00	Mon 2022-08-22 23:00:00	13:00:00	16:59:59	MO	EXPORTED

(Records: 1 - 2 of 2, Page: 1/1)

Activate Time of Day Ruleset for PSAP Queue(s)

Media Type	Session Route Type	Rule Set ID	Record Status
Audio	New, Transfer, Alternate	1	EXPORTED
Text	New, Transfer, Alternate	1	EXPORTED

(Records: 1 - 2 of 2, Page: 1/1)

Activate Cancel

Figure 32. PRF Time of Day Page

Timelines

End-user changes made using the PRF GUI and change requests made to the NSOC team go from entry to update in live production immediately upon export from the PRF to the call processing core.

Experience

Allerium operates a PRF across all its regional and statewide ESInet/NGCS deployments. Allerium implements custom routing policies for each PSAP. We work closely with our clients to provide enhanced functionality of the PRF to meet their specific needs.

Allerium's PRF GUI is currently made available to PSAPs across all our regional and statewide ESInet/NGCS deployments.

5.2.2.2. Location Information Server (LIS)

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.*

1 <https://datatracker.ietf.org/doc/html/draft-ecrit-lost-planned-changes-00>

- *DRM-controlled storage/retrieval; and minimum 30-min/max 24-hour URI expiration.*

Response:

Per Q&A item #23 post-bid conference, “The State’s intent is to ensure that the NGCS solution fully supports the standard NENA i3 LIS interfaces used to retrieve location from i3 compliant OSPs and other access networks and properly consumes and uses location data provided by those LIS components for call routing and display. The RFP does not require the Contractor to deploy or operate LIS components within each OSP’s access network. However, if the bidder’s own architecture includes LIS components or other sources they manage, those must conform to NENA i3 and integrate as required.”

Allerium’s architecture aligns directly with that expectation. The NGCS does not replace or operate LIS components on behalf of OSPs; instead, it consumes the location information they provide, processes Location URIs in accordance with NENA-STA-010.3, and uses the resulting PIDF-LO to support accurate routing and display. This allows the system to interoperate seamlessly with diverse carrier, VoIP, and application provider environments while maintaining a standards-based NG911 workflow.

When an emergency call includes a Location URI in the SIP INVITE, the Emergency Services Routing Proxy retrieves the associated location through the mechanisms established in the NENA i3 standard. For HELD-based references, the ESRP issues a secured locationRequest over HTTPS, using the parameters required for real-time emergency routing. These processes are handled dynamically based on the type of URI received, ensuring consistent behavior regardless of how the originating network delivers the reference.

All LIS communication is protected through TLS with mutual authentication. The ESRP presents credentials such as those traceable to the authorized Public Safety Credentialing Authority to validate identity and ensure that only trusted components can dereference a Location URI. Once the LIS returns the PIDF-LO, the ESRP validates the content, confirms the civic or geodetic elements, and uses them to perform location-based routing against the Emergency Call Routing Function. The solution preserves the original Location URI at every stage so downstream systems, including PSAP equipment, can perform their own dereferencing when the call is transferred or when additional location updates are required. This keeps location current and ensures that transfers between agencies remain fully supported.

The system honors the expiration values assigned by the LIS. This ensures that Location URIs remain valid for the duration of the call and any subsequent transfers, meeting the minimum thirty-minute and maximum twenty-four-hour requirements set forth in the standard. The NGCS maintains continuity even when calls traverse networks that differ in their location delivery methods, and all dereferencing activity is logged to support operational oversight and troubleshooting.

While the NGCS already fulfills all required LIS interaction functions as defined in the updated requirement interpretation, Allerium can also make its Location Data Platform available as an optional service for jurisdictions that choose to offer a State-managed LIS. Several states have approached Allerium with this specific request, often driven by the needs of smaller carriers that lack the resources or infrastructure to maintain a compliant LIS during the transition to i3. These agencies seek a unified, standards-aligned platform that can support both legacy E9-1-1 and NG9-1-1 environments without forcing carriers to overhaul their operational practices. The LDP was enhanced specifically in response to this growing need.

Originally developed as a modern successor to traditional ALI systems, the LDP has evolved into a fully capable location database and, where desired, a LIS that can support the State throughout a controlled and orderly migration to NG9-1-1. It supports both legacy ALI and wireless E2 queries as well as NG911 protocols such as HELD. Because it can function as both an LDB and a LIS, the platform offers service providers and agencies a single unified source of location information by value or by reference, performing HELD-based dereferencing with consistently fast response times. Civic address data is stored in CLDXF-compliant format, validated through the State's LVF, and made available to either legacy or NG911 interfaces depending on the requesting system.

The platform's design emphasizes operational continuity for carriers. It includes a Service Order Input function that mirrors existing workflows and incorporates an MSAG Conversion Service so legacy SOI records can be translated into CLDXF structures for validation. This allows providers to continue using familiar processes while producing NG9-1-1 ready data. For legacy PSAPs, the platform converts validated CLDXF records into MSAG-style formats so existing call-handling equipment can continue functioning without disruption.

In support of long-term management, the LDP includes a complete suite of tools for agency users. Through a web-based interface, authorized staff can manage service order workflows, review validation failures, correct address issues, generate reports, perform data extracts, and maintain a full historical record of changes. These actions are governed by rights-based authentication, authorization, and auditing that can be aligned with the data-rights management principles in NENA-STA-010.3. Policies related to dereferencing behavior, including URI validity windows, are configurable under the State's direction. Additional capabilities such as evaluating planned changes or shaping event-rate behavior for repeated dereferencing can be incorporated through collaborative design if the State elects to adopt this optional service.

By offering the LDP as an optional, post-award component, Allerium preserves the integrity of the NGCS architecture, which already meets the requirement to consume LIS information from OSP networks, while also providing a clear pathway for agencies that wish to support carriers with a centralized, standards-aligned LIS. This allows the State to adopt a flexible approach that strengthens interoperability without imposing new obligations on carriers unless those carriers choose to participate.

5.2.2.3. Location Database (LDB)

2.2.3. 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:*
 - o *Public Safety Answering Point (PSAP) Boundaries*
 - o *Emergency Service Boundaries (Law, Fire, EMS)*
 - o *Road Centerlines*
 - o *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.*

Response:

Allerium's Location Data Platform (LDP) includes a fully capable Location Database (LDB) that serves as the State's authoritative source of civic location information across both legacy and NG9-1-1 environments. The LDB is designed for the realities of the NG9-1-1 transition, supporting the longstanding workflows that agencies and service providers rely on, while providing the standards-aligned architecture required for i3 operations.

At its foundation, the LDB maintains all of the capabilities of the existing ALI environment while extending those capabilities to support the full range of NG9-1-1 protocols and data formats. It continues to support traditional ALI query mechanisms, wireless location retrieval from MPCs and GLMCs, and the new CLDXF-based structures and HELD interfaces required in an NG9-1-1 deployment. These capabilities allow the LDB to function with both the Location Validation Function (LVF) and the Emergency Call Routing Function (ECRF), supplying validated GIS-aligned civic address information to the ECRF and validating civic location information against the authoritative GIS data contained in the LVF.

A central part of the transition strategy is ensuring that service providers maintain their existing operational processes while the State migrates to NG9-1-1. To support that continuity, the LDB accepts SOI updates exactly as they are delivered today. Those records are processed through the

MSAG Conversion Service (MCS), which translates legacy MSAG-style input into CLDXF-compliant data suitable for LVF validation. This preserves the provider workflow while ensuring that the State's location data moves forward into a standards-compliant structure without disruption.

The LDB supports both NG-capable and legacy PSAPs simultaneously. NG9-1-1 PSAPs retrieve CLDXF-compliant location data using the HELD interface, while legacy PSAPs continue to use a traditional ALI interface, with the LDB automatically converting the CLDXF data back into MSAG-style formats as needed through the MCS. This ability to serve both environments at once makes the LDB an ideal anchor during the State's multi-year transition.

To support geospatial routing, the LDB interfaces directly with the ECRF using the standard Location-to-Service Translation (LoST) protocol. Through this connection, the LDB provides the authoritative GIS-aligned data needed to determine the appropriate PSAP or emergency service agency for a given caller's dispatchable location. The same authoritative data supports the LVF, enabling real-time validation of civic addresses submitted by service providers, agencies, or call-handling systems.

Operationally, the LDB is built to sustain continuous availability. Allerium's NGCS platform is both geographically redundant and redundant within each data center, ensuring that location validation and call routing functions remain available even during localized infrastructure or network failures. This architecture protects the integrity of real-time query processing and ensures that the LDB supports high-volume traffic generated during major incidents.

For service providers and agencies, the LDB offers a comprehensive set of tools for location record management. A web-based interface gives authorized users the ability to review data, generate extracts, schedule reports, resolve validation failures, track NRF conditions, and maintain complete change histories for every record. The system automatically detects incoming SOI records, validates them, flags discrepancies, and provides guided workflows for corrections. Additional data elements defined in industry standards can be added or edited as needed, all with appropriate access controls.

Civic address information within the LDB is stored in CLDXF-compliant PIDF-LO format, including all required addressing and street name elements. Records are periodically reevaluated through LVF processes to ensure accuracy, and legacy MSAG records can be generated for providers that still require them—derived directly from CLDXF GIS data to ensure cross-system alignment.

Through this design, Allerium's LDB offers the State a unified, authoritative, and standards-aligned location database that powers both legacy and NG9-1-1 operations. It integrates GIS-based data with the LVF and ECRF, supports LoST-based routing, maintains continuous availability through a redundant architecture, and enables agencies and service providers to manage the full lifecycle of location information with confidence and clarity.

5.2.2.4. Emergency Call Routing Function / Location Validation Function (ECRF/LVF)

2.2.4. 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:

2 <https://datatracker.ietf.org/doc/draft-ietf-ecrit-similar-location/19/>

3 <https://datatracker.ietf.org/doc/draft-ietf-ecrit-lost-planned-changes/>

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.

Response:

ECRF/LVF Overview

Allerium's Emergency Call Routing Function (ECRF) is built for one purpose: to make sure every 9-1-1 call reaches the right place, every time. Our design follows NENA-STA-010.3f-2021 and the IETF LoST (RFC 5222) protocol, ensuring interoperability across the NG9-1-1 ecosystem while providing flexibility and resilience that statewide deployments demand.

How the Solution Works

At its core, the ECRF is a cluster of redundant LoST servers operating in both local and geographically diverse environments. These servers work together to process queries and return the correct destination URI based on either a civic address or geodetic location. The underlying GIS data is stored in a highly available databases, continuously updated when needed, through compatible feeds provided by the Spatial Interface (SI) provider in the NENA NG9-1-1 GIS Data Model.

Allerium strives to ensure continual, accurate, and reliable service within the ECRF architecture. Our ECRF allows for seamless update of data without service disruption and is configured upon a defined interval in conjunction with the SI provider and OK911MA. Similarly, data updates may be performed in an on-demand fashion. Such on-demand updates provide flexibility for support teams to offer rapid updates to GIS data and also allow for easy rollback to prior the prior GIS data file if needed. Allerium's data update process does not impact service queries to the ECRF cluster and provides a seamless customer experience.

This approach guarantees that the routing logic always leverages the most current, validated geospatial data — a key requirement for accuracy and reliability.

Capabilities that Matter

The Allerium ECRF:

- Validates and routes calls using both civic address elements (street, floor, room, etc.) and geodetic coordinates (point, circle, polygon, ellipse).
- Provides true geospatial routing from day one, assuming GIS data readiness, so the State can avoid interim table-based routing methods.
- Enables location-based selective transfer, allowing PSAPs to identify the correct receiving agency for a transferred call quickly and accurately.
- Maintains logging and error handling to ensure that every query, event, and exception is captured for auditing and troubleshooting.
- Integrates seamlessly with the ESRP, which applies fallback logic if a server is unavailable.
- When combined with the Allerium ESRP, allows for conversion of 3-Dimensional shapes into 2-Dimensional equivalent (e.g. sphere converts to circle).

Reliability Matters

Allerium engineered the ECRF to achieve carrier-grade (99.999%) reliability. Load balancing, active-active server clusters, and physical separation between services and data storage eliminate single points of failure. This architecture is proven in multiple statewide deployments that handle millions of calls each year.

Standards and Interoperability

Allerium's ECRF adheres to NENA and IETF specifications including:

- NENA-STA-010.3f-2021 (i3 architecture)
- RFC 5222 (LoST)

- RFC 4119, RFC 5139, RFC 5491 (PIDF-LO civic and geodetic formats)
- RFC 5031 (Service URNs)
- RFC 4848, RFC 5582 (LoST architecture and extensions, informative)

True i3 Geospatial Routing Starting Day One

Allerium's solution uses geospatial data to determine the destination PSAP for each call. Upon receiving a 9-1-1 call, the system queries the carrier network (in the case of mobile devices) for the latest known location and then maps that location against the location data held in the ECRF to determine the proper PSAP for routing the call. Routing in this way supports wireless carriers when they are ready to deliver the location with the call (some do today) and eliminates the need for any future upgrades.

Most NG9-1-1 deployments do not perform geospatial routing at the time of initial implementation (instead relying on table-based routing), but we have provided true geospatial routing for years and are doing so in multiple full state deployments today with millions of residents and millions of calls routed. We have been geospatially routing calls since day one for multiple clients, including the State of Arizona, Commonwealth of Massachusetts, NCT9-1-1, Commonwealth of Pennsylvania, State of South Carolina, and our State of Ohio projects.

Allerium is prepared to support geospatial routing at the initial implementation of the solution providing the State's GIS data is ready and the State supports such an implementation.

5.2.2.5. Forest Guide

2.2.5. 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.*

Response:

Allerium's ECRF and LVF solutions are fully NENA-compliant LoST protocol servers, ensuring interoperability with the Forest Guide as described in NENA-STA-010.3f-2021. Our solutions support querying the Forest Guide via LoST as well as updating coverage regions through the LoST-sync interface, aligning with the technical requirements of the standard.

Allerium personnel hold a seat on the NG9-1-1 Interoperability Oversight Commission (NIOC). Such involvement allows Allerium to contribute real-world deployment experience to the Commission and align our solutions with realistic adoption and implementation plans for services like the Forest Guide.

On August 26, 2025, NIOC issued a statement reaffirming its role in governing NG9-1-1 interoperability services and noting that the Forest Guide is not yet available for deployment. No formal release date has been established. The official statement is posted on the NIOC website (<https://ng911ioc.org/2025/08/26/ng9-1-1-interoperability-oversight-commission-nioc-issues-statement-on-the-forest-guide/>).

Once the NIOC-commissioned Forest Guide is available, Allerium's ECRFs and LVFs will support full access as required. In the interim, our ECRF and LVF solutions maintain both civic and geodetic coverage information, ensuring authoritative and reliable query responses for the geographic areas under their responsibility.

Allerium will work with the State to scope the Forest Guide once released and determine the level of effort and implementation plan at that time.

5.2.2.6. Service/Agency Locator (SAL)

2.2.6. 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.*

Response:

Allerium captures and provides some of the Service/Agency Locator data as part of our data provisioning process. While that data could be used in a record store, the structure itself does not constitute a SALRS. However, we do provide Service/Agency Locator feature sets within our NG9-1-1 service offering. Allerium notes that there are specific requirements related to ECRF query within the Service/Agency Locator FE, as defined in NENA-STA-010.3f, which requires underlying GIS data layers for URNs related to Service/Agency Locator queries. As such, any jurisdictions desiring to leverage the Service/Agency Locator ECRF interface must coordinate proper layers within the GIS data with Allerium.

Allerium has not implemented a SAL and plans to do so in our 12-month roadmap.

5.2.3. Data and Enrichment

5.2.3.1. Additional Data Repository (ADR)

2.3. Data and Enrichment

2.3.1. 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.*

Response:

Allerium supports ADR data and interfaces to commercial, third-party additional data repositories (ADR) and identity searchable ADRs (IS-ADRs).

For this project, the LDB will be the primary source for location data. For wireless calls, the LDB can retrieve location from traditional sources over an E2 connection to a mobile positioning center (MPC). Upon receiving the initial response from the MPC, the LDB will have the callback number and can use that to query other third-party location sources for improved location such as RapidSOS.

As presence information data format – location object (PIDF-LO) can store more than one location, the LDB HELD response can return multiple locations back to the query client (such as the emergency services routing proxy [ESRP]). For example, it could return the shell record, the Phase I location, the Phase II location, and a location from the third-party ADR/LIS. The query client could then determine which location to use for call routing and pass all four locations onto the PSAP CHE.

5.2.4. Call Flow and Media Handling

5.2.4.1. Call Flow and Session Handling Requirements

2.4. Call Flow and Media Handling

2.4.1. 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.

Response:

Call Flow and Session Handling Overview

Allerium's NG9-1-1 Core Services have been engineered from the ground up to fully embody the NENA i3 call model, ensuring that every emergency communication entering the ESInet is processed with consistency, reliability, and adherence to applicable NENA and IETF standards. Our call-flow architecture is the result of years of operational experience and continuous refinement across statewide deployments, enabling predictable routing behavior, accurate location handling, and seamless end-to-end session management.

Standards-Aligned Call Flow and SIP Handling

Calls may enter the Allerium network via the LSRG, LNG, or ESRP. In each case, the application's BCF subsystem receives the SIP INVITE, applies all required NENA headers, and assigns unique NENA call identifiers to maintain traceability through the entire lifecycle of the call.

Allerium retrieves location using ALI, HELD-DI, or dereferencing to the originating service provider's LIS. The ESRP then queries the ECRF using this location to determine the appropriate PSAP destination. The resulting SIP INVITE delivered to the PSAP contains all relevant information such as P-Asserted-Identity, PIDF-LO, Geolocation, and other NENA-specified headers.

Throughout the session, Allerium preserves PIDF-LO location information and essential call metadata, ensuring that routing, retargeting, and transfers never compromise the accuracy or integrity of caller information.

Media Handling, RTT, and Fallback Capabilities

Allerium supports voice and Real-Time Text (RTT) in accordance with NENA i3 standards. Our RTT implementation includes seamless transcoding between T.140 streaming text and Baudot (TTY/TTD), ensuring interoperability with legacy TTY endpoints. When Baudot conversion is required, the media appropriately transitions to a voice channel, with Baudot tones transmitted over that channel, providing a reliable fallback mechanism without disrupting the continuity of the call.

Additionally, Allerium supports media fallback and transcoding behaviors required for mixed-technology environments, ensuring that emergency communications remain viable even when endpoints differ in capabilities.

Selective Additional Data Support

Allerium supports text-based additional data embedded within SIP and NENA-compliant headers, such as callback numbers and device-provided metadata conveyed by the originating network. This ensures that key contextual information remains available to PSAPs without requiring supplemental interfaces or specialized applications.

Transfer Capabilities and Interoperability

Allerium provides full support for warm transfers, blind transfers, and inter-PSAP transfers, preserving call identifiers, timestamps, PIDF-LO, and all relevant metadata throughout the process. Our NGCS is built for seamless interoperability across jurisdictions, networks, and vendors, and these capabilities have been extensively validated in real-world deployments.

A defining example of Allerium's leadership in interoperability is our work as an active participant in the National 911 Program's Interstate Playbook initiative—a collaborative national effort designed to standardize and operationalize NG9-1-1 interstate call transfers. Beginning in 2016 with Chapter One of the Playbook, Allerium worked directly with the State of Iowa, the State of Minnesota, Mission Critical Partners, and key industry stakeholders to test and document interoperable transfer practices.

Through this effort, Minnesota and Iowa completed a groundbreaking technical proof of concept, delivering one of the first successful interstate NG9-1-1 call transfers via IP networks. Allerium served as the NGCS provider for Iowa during these tests, collaborating closely with Minnesota's NG9-1-1 environment.

Building on this foundation, Allerium and the State of Minnesota achieved full production deployment of interstate transfer capability on September 23, 2022. Allerium subsequently tested and validated transfer functionality with every PSAP in Iowa, ensuring statewide readiness and performance. Allerium is honored to still be Iowa's NGCS provider today.

Beyond the Iowa/Minnesota initiative, Allerium has enabled successful inter-ESInet transfers in multiple regions, including:

- Arizona ↔ Utah
- Pennsylvania ↔ Maryland
- Washington ↔ Oregon and Idaho
- South Carolina to a neighboring vendor's ESInet

These deployments demonstrate Allerium’s ability to support reliable, standards-based transfer capabilities across diverse architectures and partner networks.

For off-network destinations, Allerium supports transfers to seven- and ten-digit numbers using the LSRG as the PSTN gateway, ensuring seamless reachability to legacy agencies and external responders.

We also support star and pound DTMF codes in transitional environments. When legacy PSAPs send transfer commands via SIP INFO with TEL URIs and DTMF sequences, Allerium’s interwork function translates these into NENA-compliant SIP URIs, enabling smooth transfer execution across mixed-generation systems.

To promote predictable interoperability, Allerium publishes a comprehensive Interface Control Document (ICD) with each software release, defining expected messaging behavior at every network-to-network boundary.

Queuing, Overflow Routing, and Abandonment Handling

Allerium has extensive experience delivering queuing and overflow behaviors aligned with NENA STA-010.3f. Because PSAP CHE implementations vary in their adoption of SUBSCRIBE/NOTIFY, Allerium integrates our Policy Routing Function (PRF) directly into the NG Core to ensure universal access to intelligent routing capabilities regardless of CHE maturity.

The PRF supports:

- Time-of-day routing rules
- SIP-error-driven alternate routing
- Ring-no-answer timers for text sessions
- Configurable call throttling thresholds with service-type rollovers
- Forced shutdown and abandonment behaviors with per-media alternate routing paths

This integrated approach ensures that PSAPs maintain operational continuity during high-volume periods, outages, or maintenance conditions.

End-to-End Standards Conformance

From origination through routing, delivery, transfer, and termination, Allerium’s NG9-1-1 Core Services conform to applicable NENA and IETF standards. Our system reliably preserves essential call information—including PIDF-LO, NENA call identifiers, SIP signaling headers, and routing history—ensuring consistent and predictable handling of all supported media types.

5.2.4.2. Media Quality of Service (QoS)

5.2.4.2.1. Audio

2.4.2. Media Quality of Service (QoS)

2.4.2.1. 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.

Response:

Allerium's proposed solution implements QoS markings in alignment with NENA standards.

Allerium's solution includes a QoS structure using differentiated services code point (DSCP) markings based on the NENA i3 version 3 standard as outlined in Table 58. This table specifies ESInet-specific traffic. Allerium marks other traffic (e.g., dynamic host configuration protocol [DHCP], internet control message protocol [ICMP], border gateway protocol [BGP], etc.) according to industry standards and best practices.

Table 58. QoS Markings

DSCP	Use	Per-Hop Behavior (PBH)
0000 00	Routine Traffic except as specified	Default (Best Effort)
0000 11	9-1-1 Call (SIP) Signaling (including noninteractive calls) and emergency call related HTTP/S operations, DNS traffic	AF12
0001 11	9-1-1 Text Media (RTT and MSRP)	AF12
0010 11	9-1-1 Audio Media (9-1-1 calls and admin calls)	EF
0011 11	9-1-1 Video Media	AF11

Allerium applies this QoS structure in our ESInet/NGCS deployments. This is a standard deployment strategy.

5.2.4.2.2. Video

2.4.2.2. 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.

Response:

The video services requirements span both the Telecom/ESInet infrastructure as well as the NG Core applications, and Allerium continues to monitor the market for viability. Allerium has not implemented video and plans to do so in our 12-month roadmap.

5.2.4.2.3. Text

2.4.2.3. 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.*

Response:

Allerium, a Comtech segment, is one of only two text control center (TCC) providers. We interoperate seamlessly with the other provider to ensure both incoming texts and transfers are made between the two systems. We also serve other providers their incoming texts from our TCC to enable their solutions. We include our Text to 9-1-1 services as part of our deployment, integrating the SIP/MSRP text packets directly on our ESInet. No other provider will be needed to support text to 9-1-1, to any PSAP, when the Allerium service is used.

Allerium's NGCS service provides for both web-based and MSRP-integrated Text to 9-1-1. As both a TCC and NGCS provider, our knowledge of various text transport methods ensures a seamless transition to integrated text via SIP/MSRP.

How MSRP Works

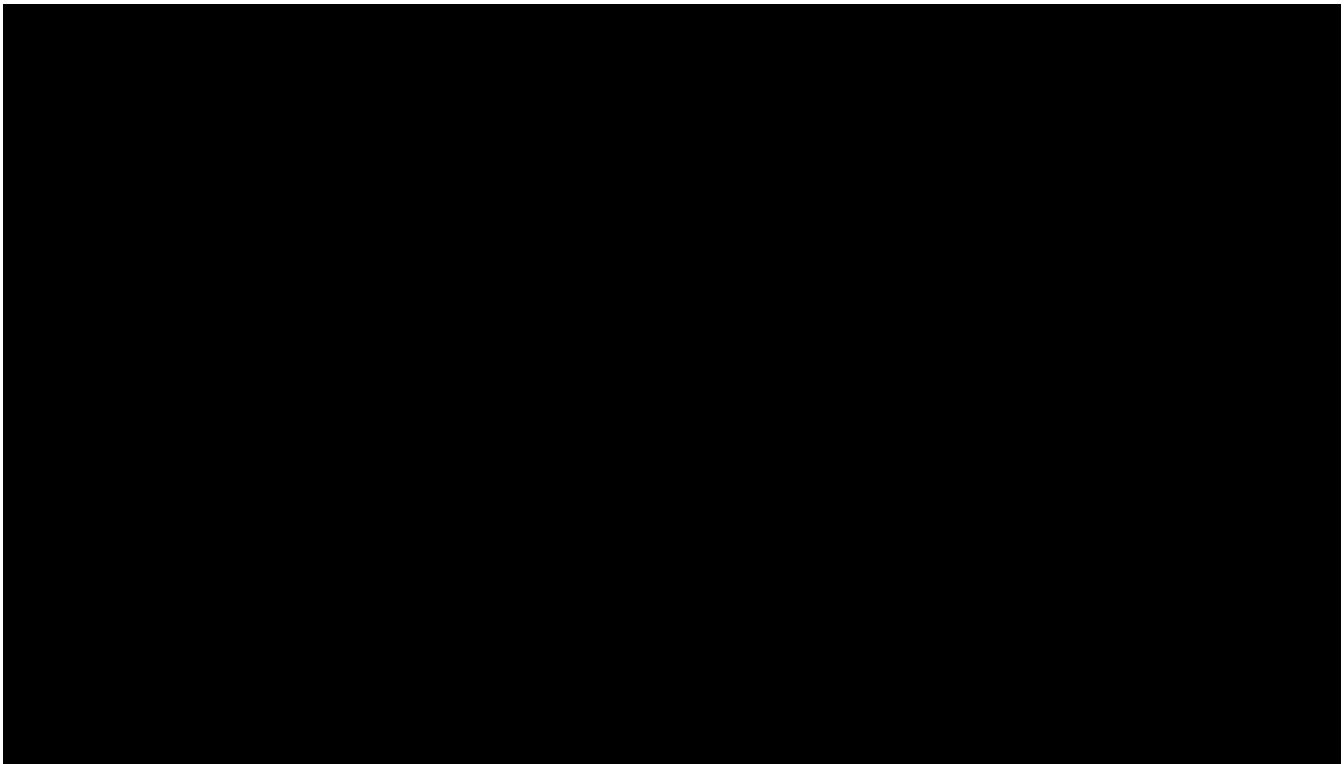
For MSRP-integrated Text to 9-1-1, the Allerium TCC receives the text payload and signals to the Allerium NGCS. The Allerium NGCS then routes the text payload via the ESRP and ECRF. The text payload is sent to the PSAP next hop SIP peer which may be an SBC.

Once SIP signaling is complete between the TCC and the PSAP's CHE, the Allerium ESRP establishes MSRP media between the TCC and the CHE using the NGCS/ESInet services as a transport and media anchor. PSAPs that are integrated with the Allerium NGCS for SIP/MSRP may transfer to other native SIP/MSRP PSAPs or to those using an over-the-top (OTT) solution. Similarly, a PSAP with an OTT solution has the capability to perform transfers to those integrated directly with the Allerium NGCS.

Transitioning Nebraska PSAPs to MSRP

Allerium also provides native MSRP support via the NGCS system. Given that MSRP is more widely deployed, the transition plan steps for Nebraska are limited to Allerium working with CHE manufacturers to certify their CHE against our NGCS system. Once certified, the PSAP can request integrated text via SIP/MSRP.

Table 59 displays the CHE SIP/MSRP certification status within column five (“Integrated SIP/MSRP”) and is **ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION**.



Correct Text Delivery

Allerium meets the requirement for correct text delivery. Allerium supports 4,400 PSAPs with text services nationwide.

Analyzing the solicitation’s PSAP information and our internal data, Allerium notes that all PSAPs in Nebraska are served by Allerium’s TCC service. Our text services resulted in the following text sessions delivered to Nebraska PSAPs:

- **2026 (YTD):** 663
- **2025:** 2,300
- **2024:** 2,458

Allerium has not implemented text from 9-1-1 services and plans to do so in our 12-month roadmap.

5.2.4.3. Interactive Multimedia Response Service (IMRS)

2.4.3. 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.

Response:

Allerium has not implemented IMRS and can do so within the 12-month roadmap timeframe once the State clarifies the intent and use case of having this functionality.

To date across our over 1,000 PSAP deployments, Allerium has neither implemented nor been asked to implement IMRS due to the fact that queuing in the core removes call control from and delivery to the PSAP.

5.2.4.4. Bridge

2.4.4. 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.*

Response:

Allerium supports bridging functionality as described in STA-010.3f per the “Route All Calls Via a Conference Aware UA” method defined in section 4.7.1.3 of the Standard. Allerium's ICD for PSAP CHE defines supported transfer / conference mechanisms from the PSAP. Additionally, during the PSAP acceptance testing phase, both transfer and conference are tested to ensure that PSAP signaling matches Allerium's expectations.

Bridging & Transfer Handling

Allerium is interoperable with other ESInets using SIP as well as supporting transfers to legacy networks. For NG9-1-1 transfers to other border NG9-1-1 solutions, Allerium will interconnect between networks and provide transfer functionality over native SIP signaling. Allerium's NGCS can:

- Receive transfers in and
- Send transfers to the next hop NG9-1-1 solution.
- Route/transfer to other i3-enabled ESInets, including standard data such as location information, provided the proper certificates are provisioned to allow secure interoperability.

For interconnection next hop NG9-1-1 solutions, Allerium publishes a network-to-network interface control document (ICD) with every software release. The ICD defines the expected messaging from and to border networks.

Allerium is committed to interoperability and has successfully established interstate call transfer service between various states. We demonstrated our commitment by actively engaging in the National 911 Program's Interstate Playbook efforts. Allerium and our client, the State of Iowa, participated in the Interstate Playbook effort hosted by Mission Critical Partners alongside Intrado and Minnesota which commenced in 2016 with Chapter One. During the Interstate Playbook development process, Minnesota and Iowa performed a proof of concept to deliver an emergency call transfer over the state boundaries via an IP network. Allerium worked collectively with Minnesota as the NGCS provider in Iowa. Allerium's interstate call transfer service between Iowa and Minnesota is available as of September 23, 2022. Allerium has fully tested all PSAPs within the State of Iowa and confirmed transfer capabilities.

Allerium can transfer 9-1-1 calls between neighboring states, regions, and counties in all our deployments regardless of whether legacy 9-1-1 or NG9-1-1 technology is in use. Allerium demonstrated this capability between disparate systems and vendors in multiple locations, including but not limited to the:

- **State of Arizona:** Transfers between client Arizona's ESInet and the State of Utah.
- **State of Iowa:** Transfers between client Iowa's ESInet and the State of Minnesota.
- **Commonwealth of Pennsylvania:** Transfers between client Pennsylvania's ESInet and the State of Maryland.
- **State of South Carolina:** Transfers from Allerium's ESInet to another vendor's network in the State of South Carolina as part of our statewide NG9-1-1 service.
- **State of Washington:** Transfers between Allerium's State of Washington NG9-1-1 solution and the neighboring states of Oregon and Idaho.

This expertise will prove beneficial to the State from an implementation perspective.

In the future, states may implement the NENA PCA and Forest Guide in which case there would be additional considerations associated with security certificates and GIS data sharing.

Bridging & Transfer to 7/10 Digit Numbers

Allerium both conferences and transfers 9-1-1 voice calls to seven and 10-digit numbers. Typically, this action is for transfers off net (that is, not destinations on the ESInet) rather than on net transfers. The Allerium ESRP receives a request from a PSAP to generate a conference/transfer and determines that an off-network entity must be added to the 9-1-1 voice session. Assuming the off network is reached via PSTN, the ESRP then generates an outbound leg to the seven or 10-digit number using the LSRG as the PSTN gateway.

Support for Star and Pound DTMF Codes

Allerium supports star and pound dual tone multi-frequency (DTMF) codes.

Allerium notes that support for star and pound codes is not within the context of NENA's i3 specification per NENA-STA-010.3. An i3 PSAP must signal with a SIP REFER which includes a Refer-To containing a SIP URI. As such, for a native i3 PSAP, Allerium expects a SIP REFER message containing a SIP URI vs. a TEL URI with a shortcut code (star or pound) defined.

However, Allerium does support star and pound DTMF codes for transitional SIP signaling from a legacy PSAP. In this case the PSAP may transfer via a SIP INFO message which contains a TEL URI and the necessary star/pound code the PSAP wishes to dial. To support star and pound code translations, Allerium obtains details regarding the expected codes and their appropriate destinations from all PSAPs during the data collection phase. We then configure the translations for each PSAP into the NGCS system accordingly.

Similar to a direct dial of 10-digit line, a PSAP may request an entity be added to the 9-1-1 voice session via a star or pound code that indicates a conference or transfer request. The LPG NG9-1-1 specific interwork function (NIF) processes the SIP INFO request and translates to the appropriate SIP URI. The SIP URI is used to set the Refer-To header value in a resulting REFER message from the LNG NIF to the ESRP to complete the transfer request. For translations that match on-network PSAPs, the ESRP invites the requested party to the call directly over the ESInet egress network to the destination PSAP. For parties not on the network, the ESRP processes the call out using the LSRG as the PSTN gateway.

5.2.5. Egress and External Interfaces

5.2.5.1. Outgoing Call Interface Function (OCIF)

2.5. Egress and External Interfaces

2.5.1. 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.

Remainder of page intentionally blank

Response:

Allerium supports outbound calls via the ESInet through in-call conference / transfer requests. In-call conference and transfer mechanisms are managed via a SIP REFER message to add a participant to an existing SIP session. The SIP REFER is consumed by Allerium's NGCS and the next hop destination is added either via the ESInet for a connected next hop PSAP or through the LSRG to the PSTN. Allerium also supports access to administrative outbound dial via the ESInet.

However, Allerium's experience has been that many PSAPs desire to manage outbound administrative trunks locally and therefore opt to route administrative call traffic such as abandoned callback or PSAP to PSAP communication locally.

5.3. GIS and Database Services Requirements [Project Requirements and Scope of Work, Section E.3]

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.

Response:

Operations and Administration

Allerium implements location-based routing using a fully NENA compliant GIS data architecture. The platform natively supports the NENA GIS Data Model (NENA STA 006.2) and ingests all required datasets.

Allerium's GIS repository is built on a high-performance spatial database engine, enabling millisecond level query performance for ECRF and LVF operations. The system validates all incoming GIS data against the NENA schema and enforces topology, attribute completeness, and boundary alignment to ensure authoritative routing. The ECRF and LVF operate on this authoritative GIS dataset, ensuring that routing decisions are fully aligned with NENA i3 functional standards.

Allerium's solution respects the operational division of responsibilities between PSAPs and the State and provides a controlled provisioning interface that accepts authoritative data submissions without altering any internal processes or contractual relationships. Our architecture preserves

existing PSAP workflows and does not require PSAPs to change GIS vendors or tools. Our GIS team works directly with all GIS stakeholders, be it State, PSAP, County, or designated vendor.

Location Conveyance

Throughout the entire call lifecycle, Allerium fully supports NG9-1-1 location conveyance standards, including PIDF-LO, per RFC 4119 and RFC 5139, NENA-specific extensions for geodetic and civic locations, and the delivery of location information that can be consumed by PSAP call-handling equipment, CAD, and any other mapping clients.

Validation and Determination

Allerium's LVF and LIS validates caller-provided locations against the authoritative GIS data. These systems support location sent via LocationbyReference and LocationbyValue. If a location cannot find a match during routing, Allerium has configurable fallback routing, ensuring uninterrupted service continuity and compliance with NENA i3 routing requirements.

Data Governance and Provisioning

Allerium provides a comprehensive and standards aligned GIS data governance framework designed to ensure accuracy, traceability, and operational reliability across the NG9 1 1 system. The system incorporates full version control and change tracking, maintaining time stamped snapshots of all GIS datasets and enabling rollback to prior states when necessary. Every modification is captured in a detailed audit log that records the timestamp and the specific data deltas applied.

To support ongoing data maintenance, Allerium automates both batch and incremental updates using NENA compliant provisioning formats, validating all incoming data against the NENA STA 006.2 schema before it is accepted into the authoritative repository. This governance model ensures that authoritative GIS data remains current, consistent, and fully auditable, supporting high confidence routing and validation operations.

5.3.1. Data Management and Interfaces

5.3.1.1. GIS and Database Management Functionality

3.1. Data Management and Interfaces

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.*

Response:

GIS and Database Management Functionality Overview

Allerium partners with GeoComm, who provides an online provisioning interface referred to as the GIS Data Hub which serves as the system for managing GIS data. Through the web interface, GIS data providers can submit their locally maintained datasets for validation, transformation into the NENA NG9-1-1 data model, and aggregation into a statewide dataset that supports Next Generation 9-1-1 Core Services, such as the Emergency Call Routing Function (ECRF), Location Validation Function (LVF), GIS-derived MSAG, and the MSAG Conversion Service (MCS). Additionally, data packages are made available to PSAPs for use in their CAD and other mapping systems.

The GIS Data Hub delivers quality control results for submitted GIS data in various formats—including Geodatabase feature classes and tabular .csv files—so GIS data maintainers can easily locate and address features flagged as errors or possible issues with clear guidance on how to correct them. This process enables data maintainers to efficiently make updates and quickly resubmit their data for inclusion in the statewide dataset. To ensure the accuracy of the dataset used for NG9-1-1 call routing and record validation, only datasets passing all critical error checks are aggregated. If any critical errors are found, the submitter receives immediate notification along with actionable information, allowing for prompt corrections and resubmission so that the latest data is always available for NG Core Services systems.

As part of the planning process, Allerium will work with the State to establish mutually acceptable maintenance procedures, which will be documented and shared with all stakeholders. GIS data quality control, aggregation and output of data packages that can be retrieved and utilized in local systems in addition to the NGCS systems, include road centerline, address points, PSAP emergency boundaries and any additional layers deemed necessary for end use systems. GIS data is accepted from all State approved data maintainers via GIS Data Hub. GeoComm's GIS Data Hub features an intuitive ETL (Extract, Transform, Load) process that smoothly maps local GIS data submitted in its native schema into the Nebraska NG9-1-1 schema. The setup also offers options for "input," "conditional," and "spatial lookup" values. This means that if an agency doesn't maintain certain fields required by the NG9-1-1 schema, those can usually be derived from other sources and added in by GeoComm's Managed Services team. These features make it simple for agencies to keep their data in their own local schema, without the need to add extra fields and attributes that are needed only for NG9-1-1 purposes. The statewide dataset will be managed and distributed through GeoComm's GIS Data Hub, utilizing individual PSAP and/or regional or State-maintained datasets submitted to it.

Use of PSAP GIS data for geospatial routing.

Both Allerium's ECRF and LVF use the authoritative GIS data provided to route calls based on their civic or geodetic locations. This is done by a point and polygon-type data lookup. If no geospatial routing option is found, Allerium has configurable fallback routing logic that ensures the calls are still delivered to the correct PSAP.

Web interface or automated method for provisioning and retrieving post-QA data for maps.

The GIS Data Hub is used to provision the authoritative GIS data and detailed discrepancy reports are available to the data provisioner to examine any record that is deemed to have a system-critical error. Post-processed data is available for download so that jurisdictions can use the data locally.

Reflection of PSAP updates in routes within 5 mins (online real-time).

The update time for the ECRF and LVF is configurable and can be adjusted to meet the needs of the customer.

Data structures organized in conformance to NENA Data Model Standards – NENA-STA-015.10 and NENA-STA-006.2.

All data, regardless of source format, is validated and stored in conformance with both NENA STA-015.10 and NENA-STA-006.2.

LVF for OSP civic address verification.

Allerium makes available an LVF for OSPs and their associated LIS's to connect to so that they can validate their customer's addresses against authoritative GIS.

Preferred ESRI SQL SDE exchange.

Allerium supports the State's request for an ESRI SQL Server SDE-based GIS data exchange. Our Spatial Interface (SI) can be configured to ingest GIS datasets exported directly from ESRI ArcSDE environments, ensuring seamless compatibility with existing statewide and local GIS workflows. The system accepts SDE-derived feature classes delivered as file geodatabases (FGDB), shapefiles, or other ESRI-standard export formats without requiring schema changes.

Replacement of MSAG with GIS for routing/validation.

One of Allerium's main goals is to move customers off of tabular MSAG as quickly as possible and transition to a better, GIS-based validation method. GIS is taken and converted into an MSAG-formatted file so that OSPs that have not fully migrated to NENA i3 are still able to validate their customer records. Those carriers that have migrated to NENA i3 location validation can utilize the LVF.

PSAP maintenance with contractor discrepancy reports.

PSAPs will continue to have control over their data; Allerium will be there to support them along the way. After PSAPs or the State have submitted their data to the GIS Data Hub, an automated discrepancy report is produced and available for the PSAPs to review and resolve. Any questions can be answered by Allerium's GIS team, which is there to ensure the PSAPs transition their GIS to Allerium successfully.

Use of existing source data.

All existing source data will be converted to conform to NENA data standards.

Responsibility for all GIS data maintenance.

PSAPs maintain the data; Allerium and GeoComm maintain the provisioning, validation, and routing infrastructure.

Inclusion of road centerline, address points, PSAP emergency boundaries, and additional layers.

Allerium accepts the required NENA data layers (road centerline, address points, emergency boundaries, provisioning boundary) and any additional data layers the customer feels necessary to operate a success 911 network.

Mutually acceptable maintenance procedures with State.

Allerium will collaborate with the State to define sustainable, repeatable, and auditable maintenance workflows.

5.3.1.2. Spatial Interface (SI) Functionality

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.*

Response:

Spatial Interface Functionality Overview

Allerium, in partnership with GeoComm, delivers a fully compliant Spatial Interface (SI) that provisions, validates, transforms, and distributes NG9-1-1 GIS data in accordance with all applicable NENA standards. The SI is engineered to support real time and near real time updates, ensuring that authoritative GIS data is continuously available to the ECRF, LVF, mapping services, and PSAP operational systems without disrupting existing workflows.

GeoComm's GIS Data Hub, which hosts the Spatial Interface (SI), will deliver comprehensive GIS data management, validation, and near real-time provisioning in alignment with all applicable NENA standards and operational requirements. PSAPs will supply the core GIS datasets used throughout the NG9-1-1 environment, and these datasets will be ingested, validated, and aggregated within the SI. All updates and corrections will be automatically propagated to the ECRF, LVF, mapping services, and other consuming systems through structured, automated workflows. In addition to the GIS Data Hub web application subscription, GeoComm will provide GIS managed services to support continuous data maintenance, discrepancy resolution, and quality assurance, with all procedures documented and shared to ensure full transparency and operational reliability. This approach ensures that NG9-1-1 systems always have access to the most current, accurate, and standards compliant GIS data for emergency call routing, validation, and mapping functions.

To comply with NENA STA010.3 Section 4.3.7 (Spatial Interface), the SI supports provisioning of GIS data to the ECRF, LVF, and mapping systems with real-time or near-real-time update capabilities. All data will undergo rigorous quality and integrity checks in accordance with relevant NENA standards, including NENA-STA015.102018,

Each PSAP's GIS provider will be responsible for supplying all GIS datasets required for location routing, validation, mapping, and ongoing maintenance. This includes road centerlines with address ranges, address points, PSAP boundaries, municipal boundaries, and police, fire, and EMS. Additional display layers will also be supported, and all data will conform to the NENA NG9-1-1 data model. GeoComm will work with the State to define mutually acceptable data maintenance

procedures that promote consistency, transparency, and a strong cooperative relationship across all participating agencies.

Allerium acknowledges OGC Document 10069r2, which defines a WFS- and ATOM-based layer replication interface, and has intentionally delayed full adoption due to the prevalence of nationwide batch processing workflows that require merging disparate datasets into a single, quality checked package for multi-endpoint distribution. Allerium will continue to work with our partners to track evolving data exchange needs and will determine by the end of Q4 2026 whether incorporation of this approach into the SI is appropriate for future roadmap development.

Finally, the SI will ensure that all GIS data used for geospatial routing is validated prior to provisioning into the ECRF and LVF. A web interface will support retrieval of post QA datasets for mapping applications, and all data structures will adhere to the NENA-STA-015.10 and NENA-STA-006.2 data model standards. The SI will also support LVF functionality for OSP civic address validation and can generate a GIS-derived MSAG based on locally submitted data, providing a modernized replacement for legacy MSAG processes. Through this structured, standards aligned approach, Allerium guarantees that all NG9-1-1 systems will receive timely, accurate, and fully compliant GIS data essential for emergency call routing, validation, and situational awareness.

SI implementation with data-quality and integrity checks per NENA standards while maintaining real-time updates.

The SI performs automated data quality and data integrity checks on all GIS datasets provisioned by PSAPs and the State. These checks validate schema compliance, topology, attribute completeness, geometry validity, and boundary alignment against NENA STA 015.10 2018, NENA STA 006.2 2022, NENA 02 014, and NENA STA 010.3 2021. Allerium and GeoComm's combined QA/QC engine ensures that only compliant, error free data is accepted for routing and validation, while still maintaining the required online, real time update capability.

Conversion to ECRF/LVF format via Web feature service.

Allerium supports the State's interest in standards-aligned GIS data exchange; however, while Web Feature Service (WFS) is mentioned in NENA documentation as a potential mechanism for GIS data delivery, NENA has not published a formal, interoperable specification for WFS-based ECRF or LVF data exchange. Because of this, Allerium does not recommend it for NG911 ECRF and LVF provisioning.

Instead, Allerium uses standards-aligned ingestion workflows based on file geodatabases (FGDB) or shapefiles, both of which are formats fully compatible with the NENA GIS Data Model and widely adopted across NG911 deployments. These formats allow Allerium's Spatial Interface (SI) to perform vigorous automated QA/QC checks, ensuring that only validated, topologically correct, NENA-compliant data is provisioned to the ECRF and LVF.

Incremental near real-time updates to ECRF/LVF, map viewer, and PSAP displays.

The SI provisions both full and incremental updates to the ECRF, LVF, map viewer services, and PSAP mapping displays. Incremental updates are processed in near real time, allowing PSAPs to see the impact of GIS changes within minutes. Allerium guarantees that any update affecting routing is reflected in the operational ECRF within five minutes, assuming no data errors are detected.

Validation prior to provisioning with online real-time updates.

All GIS updates undergo validation before being provisioned into the ECRF/LVF. The SI's validation pipeline includes schema checks, topology checks, address range consistency, and boundary continuity. Once validated, updates are automatically pushed to the operational environment using secure, real time provisioning workflows that do not require system downtime.

Alignment with PSAP processes.

The SI is designed to integrate seamlessly with existing PSAP GIS workflows. GeoComm's tools support the formats, schemas, and update cycles already used by PSAPs, while Allerium's provisioning engine ensures that updates flow into the NG9 1 1 core services without requiring PSAPs to change vendors, tools, or maintenance practices. This minimizes operational impact and preserves local control of GIS data.

Incorporation of PSAP prepared datasets.

The SI accepts all datasets prepared by PSAPs or their designated GIS vendors, including road centerlines, address points, PSAP boundaries, municipal boundaries, and emergency service polygons. These datasets are incorporated into the statewide authoritative GIS repository and provisioned to the ECRF/LVF after passing QA/QC checks.

Web tools for incidents, change tickets and policy-routing views.

Allerium provides a secure web interface that allows authorized users to:

- Submit and track GIS related incidents and change tickets
- View policy routing plans and routing logic
- Retrieve post QA datasets for mapping and CAD
- Monitor data quality metrics and provisioning status

These tools enhance transparency and support collaborative data maintenance across PSAPs and the State.

Secure reliable update and testing application without problems.

The SI includes a controlled staging environment where updates can be tested before being applied to the operational ECRF. Updates are deployed using secure, authenticated channels that ensure reliability and prevent operational disruptions. Allerium's deployment workflow includes automated rollback mechanisms to maintain service continuity.

Database audits for gaps/overlaps/conflicts referred to PSAP.

The SI performs automated database audits to detect common GIS issues such as:

- Road centerline gaps or overlaps
- Address range conflicts
- Boundary misalignments
- Invalid geometries
- Missing or inconsistent attributes

When discrepancies are identified, they are documented and returned to the responsible PSAP or GIS vendor for remediation. This ensures continuous improvement of the statewide GIS dataset.

5.3.2. Core Data Services

5.3.2.1. Mapping Data Service

3.2. Core Data Services

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.*

Response:

At this time, our solution does not include a fully deployed Mapping Data Service (MDS) as defined in NENA-STA-010.3. This position is deliberate and reflects the broader realities of the NG911 GIS environment. While the MDS construct is well-defined within the NGCS architecture, its successful execution depends on a stable, mature, and consistently stewarded nationwide GIS data supply chain—an ecosystem that is still actively evolving.

Authoritative GIS data continues to be maintained at the local and regional level, with each jurisdiction following its own update schedules, quality controls, and governance practices. As a result, the industry has not yet reached the level of operational maturity needed to support a unified, continuously synchronized national mapping layer. NENA standards such as NENA-STA-006.2 and NENA-STA-010.3 continue to develop in parallel with these local and state-level transitions, creating additional variables that need to stabilize before a nationwide MDS can reliably perform.

Our position is strengthened by continuous monitoring of the NG9-1-1 landscape. We actively track market progression through our direct customer base, strategic partner ecosystem, and ongoing participation in industry groups, including NENA, APCO, and other national and state-level working committees. These channels provide early insight into functional enhancements, data-management challenges, and evolving governance models. This engagement confirms that while progress is steady, the foundational elements required for a dependable national MDS—particularly around data governance and cross-jurisdictional sharing—are still maturing.

Within this context, we see a clear path for supporting map data for all entities inside a single ESInet. The governance boundaries, data flows, update cycles, and authoritative sources are well understood and manageable. However, the long-term feasibility of providing accurate and up-to-date map data for entities outside of an ESInet—across multiple interconnected ESInets—remains an area requiring thoughtful evaluation. We are actively engaged in planning and discussion around the data-collection requirements for out-of-area support, with careful attention to the risks associated with stale, inconsistent, or incomplete data entering the ecosystem. Our goal is to ensure that when this capability is introduced, it is both reliable and sustainably maintained, without introducing the risks associated with unmanaged or misaligned data sources.

Taken together, these factors support our decision to defer deployment of a full MDS until the broader technical and governance framework is sufficiently mature. This approach ensures that our future MDS will meet the accuracy, interoperability, and performance standards required for mission-critical NG911 operations across all participating ESInets.

5.3.2.2. MSAG Conversion Service (MCS)

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.*

Response:

Allerium provides a NENA-compliant MSAG Conversion Service (MCS) that bridges the gap between legacy MSAG/ALI data structures and Next Generation (PIDF-LO/CLDXF) formats. The MCS ensures interoperability during the transition to NG9-1-1 and supports seamless operation in mixed legacy and NG environments.

Purpose and Role

The MCS is designed to translate between PIDF-LO and MSAG address formats as required by NENA-STA-010.3f-2021:

- **PIDF-LO to MSAG:** Converts an incoming PIDF-LO record into an MSAG XML object conforming to NENA 02-010 v4.
- **MSAG to PIDF-LO:** Converts a legacy MSAG XML object into a PIDF-LO in CLDXF format, aligned with RFC 4119, RFC 5139, and RFC 5491.

This translation supports multiple use cases, including:

- Routing and transfers between NG9-1-1 and legacy PSAPs.
- Converting addresses before location queries are sent to the ECRF.

- Supporting legacy CHE deployments in mixed environments.
- Enabling LDB-to-LVF interoperability during transitional deployments.

Provisioning and Data Alignment

The MCS provisions data using the Spatial Interface (SI), aligning with the same mechanisms Allerium uses for the ECRF and LVF. All MSAG records are automatically derived from the GIS database within the ECRF (geoMSAG), ensuring consistency between legacy and NG formats.

This approach eliminates discrepancies between datasets by tying all conversions directly to the authoritative GIS source. By standardizing on geoMSAG as the single method of MSAG maintenance, Allerium simplifies operations, reduces the risk of mismatched records, and accelerates the transition to NG-native models.

Operational Scenarios

The MCS plays a critical role in transitional and hybrid deployments:

- **SOI Processing:** Converts legacy service order inputs into NG9-1-1 CLDXF-compliant records for storage in the LDB.
- **Dynamic Updates:** Converts address data received dynamically over an E2 interface into PIDF-LO format for use by the ECRF.
- **Legacy Interoperability:** Provides converted ALI/MSAG data for legacy CHEs that remain in operation.
- **Cross-Network Transfers:** Facilitates accurate location transfer between NG and legacy PSAPs.

Without the MCS, call location data would not align with the GIS-based ECRF and LVF, leading to significant routing risks. Allerium's solution ensures all call-associated data is normalized into NG9-1-1 formats, eliminating inconsistencies.

Features and Capabilities

The Allerium MCS delivers:

- Bidirectional conversion between MSAG XML and PIDF-LO/CLDXF.
- Full support for all MSAG fields per NENA-STA-015.10-2018.
- Automatic synchronization of MSAG records from authoritative GIS data in the ECRF (geoMSAG).
- Detailed reporting of unmatched records to highlight and resolve discrepancies between MSAG and GIS.
- Web-based tools for role-based access, record search, reporting, and full audit trails of all translations and updates.
- Complete audit history, recording every translation and edit for accountability and compliance.
- Integration with the LDB for MSAG queries, including daily download of full and delta MSAG files.

Reliability and Standards Alignment

The MCS operates within Allerium's carrier-grade NGCS architecture, ensuring high availability, redundancy, and security. It aligns with NENA and IETF standards, including:

- NENA-STA-010.3f-2021 (NG9-1-1 i3 architecture)
- NENA 02-010 v4 (MSAG XML schema)
- NENA-STA-015.10-2018 (MSAG fields and definitions)
- RFC 4119, RFC 5139, RFC 5491 (PIDF-LO formats)

5.3.2.3. Geocode Conversion Service (GCS)

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.*

Response:

Allerium's solution can provide a compliant Geocode Service and the necessary protocol details if required. However, in practice, we have seen that most CAD and mapping applications already provide this service, thus making it unnecessary in the NGCS. Please note that limited implementation details are provided within the standard.

5.3.3. PSAP-Facing Services

5.3.3.1. PSAP Mapping Service

3.3. PSAP-Facing Services

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.*

Response:

Allerium's service supports multiple methods for reporting location errors. The most widely-used of these error-correction procedures deals with discrepancies in location data during the provisioning of the LDB and, similarly, in the GIS data in the SI provisioning flow. Both of these are well-known processes that report the discrepancy back to the submitting authority. In the case of the LDB, the discrepancy is recorded during the data update process, flagged as a discrepancy, and automatically entered into the database management system (DBMS) for resolution between the OSP, the local jurisdiction, and Allerium. This is a common, well-understood process by all parties involved.

In the case of GIS (ECRF/LVF or SI) data discrepancies, the provisioning of GIS data is followed by several quality control procedures, including gap/overlap and address point discrepancies. If any QA check fails, the data is automatically flagged and returned for error resolution. Again, this process is well-understood by the parties. Similarly, if any geospatial errors occur in the ECRF, reports are generated for investigation as part of the day-to-day maintenance of the system.

Allerium recognizes that there are additional methods for error and discrepancy reporting in these areas and looks forward to working with the State to determine the State's and PSAP community's needs based on their workflows.

5.3.3.2. Map Discrepancy Reporting**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.

Response:

Allerium, in partnership with GeoComm, provides a comprehensive and standards aligned workflow for identifying, documenting, and referring all geospatial discrepancies to the State for remediation. As part of the Spatial Interface (SI) and GIS data management framework, all GIS datasets submitted by PSAPs or their designated vendors, undergo automated and manual quality checks based on NENA STA 006.2, NENA STA 015.10, NENA 02 014, and NENA STA 010.3. These checks evaluate topology, attribute completeness, schema compliance, address range consistency, boundary alignment, and geometry validity. When discrepancies are detected, such as gaps, overlaps, address range conflicts, invalid geometries, or misaligned emergency service boundaries, the system automatically generates structured discrepancy reports.

These reports are delivered directly to the State through the SI's secure web interface, ensuring that the State receives timely, actionable information for remediation. Each discrepancy record includes detailed metadata such as the affected feature, the nature of the issue, the originating PSAP, timestamps, and recommended corrective actions. This process ensures that the State

retains full oversight and control of the authoritative GIS dataset while enabling PSAPs and their GIS vendors to address issues efficiently.

The Allerium and GeoComm workflow is designed to align with existing State and PSAP maintenance processes. Discrepancy notifications are integrated into the same operational channels used for routine GIS updates, minimizing disruption and ensuring that remediation activities fit naturally into established workflows. This structured, transparent, and collaborative approach ensures that all geospatial discrepancies are consistently identified, escalated, and resolved, supporting the accuracy and reliability of NG9 1 1 routing and validation services statewide.

5.3.4. External Integrations

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.

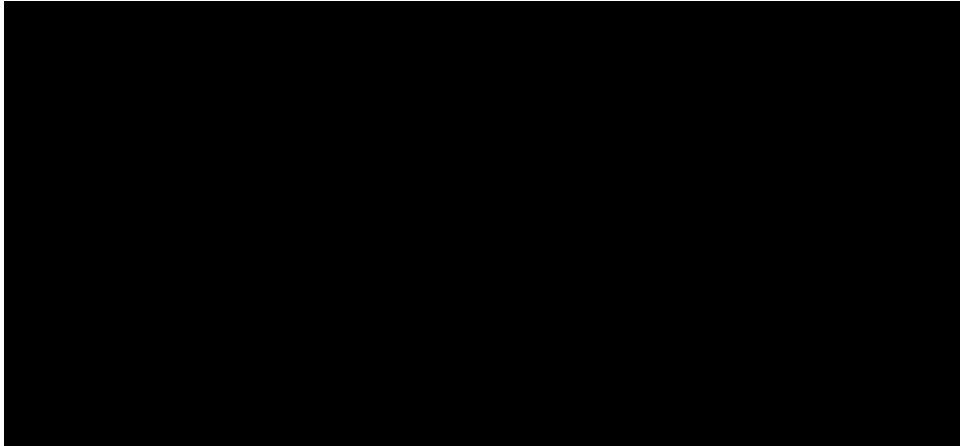
Remainder of page intentionally blank

Response:

Allerium, in partnership with GeoComm, provides an open, standards based integration framework designed to support seamless interoperability with all third party systems currently utilized by PSAPs across the State. The solution is built on NG9 1 1 i3 compliant interfaces, industry standard APIs, and flexible data exchange mechanisms that allow the system to integrate with existing CAD platforms, mapping applications, and GIS vendors without requiring changes to PSAP workflows or vendor contracts. This ensures that PSAPs can continue using their preferred systems while benefiting from the enhanced routing, validation, and data management capabilities provided by the Allerium and GeoComm platform.

The integration architecture supports both real time and event driven data exchange, enabling the system to communicate with external vendors for location validation, mapping updates, incident data sharing, and operational coordination. Allerium's NG9 1 1 Core Services expose secure, well documented SIP based interfaces, while GeoComm's GIS management tools support ESRI based data exchange. Together, these capabilities ensure that all PSAPs, regardless of their current vendor, can fully participate in the statewide NG9 1 1 environment without disruption.

The partnership's approach is intentionally vendor neutral and designed to preserve local autonomy. Allerium and GeoComm work directly with PSAPs and their existing technology providers to establish integration patterns that align with current operational practices. This includes supporting legacy interfaces where required, enabling hybrid environments during transition periods, and ensuring that all external systems receive accurate, validated, and standards compliant data. Through this flexible and collaborative integration model, the solution guarantees that every PSAP can maintain its current operational capabilities while seamlessly adopting NG9 1 1 functionality.



5.5. Reporting Services Requirements [Project Requirements and Scope of Work, Section E.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.

Response:

Allerium's reporting and analytics capabilities are built on a strong, six-year, production-proven partnership with PSN Americas and their 911 Logix analytics platform. This collaboration has shaped how NGCS reporting is delivered across our deployments and has created a uniquely aligned, seamless reporting experience for PSAPs and statewide stakeholders.

A deeply integrated partnership that exceeds expectations

Through years of joint work with PSN Americas, Allerium has established 911 Logix as our standard reporting and analytics environment across NGCS deployments. Together, we have tied together Call Handling, NGCS, and companion system data in a way that gives PSAPs a near true end-to-end operational view of each emergency call. This includes enriched network insights, correlated identifiers, and visual displays shaped directly by user group feedback.

This close cooperation has resulted in reporting that not only meets NENA and RFP requirements but also delivers enhanced clarity, accuracy, and operational value well beyond typical NG9-1-1 analytics.

Comprehensive end-to-end logging in RAW format

Allerium provides complete end-to-end RAW logging for every call and transaction event across the ESInet and NGCS. Each log record includes the elements required by the RFP—ISO 8601 timestamps with offsets, unique correlation IDs, call identifiers, high-level SIP summaries, PIDF-LO location snapshots (appropriately privacy-protected), routing decisions, ECRF/LVF lookups, PSAP handoff timing, and error details.

Logs are stored in an immutable, tamper-evident environment with protections against unauthorized access. This ensures the State receives a trustworthy and auditable record of NG9-1-1 operations.

Standards-aligned CDR/TDR generation for every call

Every emergency call entering Allerium’s NGCS generates a Transaction Detail Record (TDR), fully aligned with NENA CDR expectations. Each TDR contains calling line information, the location used for routing, receiving PSAP ID, key timestamps (start, answer, end), media negotiation details, disposition codes, and any transfers.

These records support export in XML or JSON formats if needed; however, most customers access the data directly through the PSC analytics platform using existing integrations.

Secure long-term retention, indexing, and exportability

All logs and TDRs are securely retained long-term, consistent with jurisdictional requirements such as seven-year minimum retention. Data remains fully indexed and searchable and can be exported in standard formats including CSV, JSON, and PDF. Access is exclusively role-based to ensure security, with audit trails available to track query activity.

Optimized data delivery to PSN Americas’ 911 Logix platform

Because 911 Logix is already Allerium’s standard analytics platform across NGCS deployments, all required reporting, call volumes, answer times, transfers, location validation outcomes, outage visibility, and ad-hoc analysis—is immediately available.

Outage-related reporting is further supported through the delivery of data via secure API integration.

Auditable trails for system, GIS, and policy changes

Allerium maintains auditable logs for system configuration adjustments, policy updates, and GIS changes. Each entry captures the responsible user, timestamp, and before/after change information, ensuring traceability across all NGCS operational elements.

Why this Matters for the State

The State is not adopting a new or untested reporting model, it is building on a proven, five-year partnership between Allerium and PSN Americas using 911 Logix, a platform already optimized for NGCS data and shaped through joint design, customer feedback, and real-world operational use.

This means the State benefits from:

- Rapid deployment with minimal integration effort,
- Reporting accuracy validated through years of live operations,
- Dashboards and visualizations heavily influenced by PSAP user groups, and

- Mature, deeply coordinated workflows across NGCS and analytics teams.

Allerium and PSN Americas don't just meet the State's reporting requirements, we have been delivering them successfully together for years.

5.5.1. Reporting and Data Collection Requirements

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.

Response:

Allerium's Next Generation Core provides transaction and detail logging beyond the metrics required in STA-010.3f. Throughout our operational footprint, our NG Core has integrated with several reporting providers including tight integration with PSN Americas / 911Logix.

Every functional element within Allerium's NG Core produces logging that, then, process into reporting platforms via existing data feeds. To ensure that all logging meets the expectation of reporting providers, Allerium distributes documentation for each release, including:

- Transaction detail definitions for every log event generated.
- Application error definitions.
- Application error action guides.
- Updated report definition functional specifications (as needed).
- A detailed Reporting Impact Analysis document

After distribution of the documentation with a given release, Allerium holds meetings with reporting provider stakeholders to review any unclear details. Stakeholders generally include staff from the reporting provider and Allerium staff, including but not limited to:

- **Technical Product Management:** Providing technical oversight and first line of answers.
- **Product Line Management:** Providing business guidance as necessary.
- **Technical Program Management:** Ensuring consistency throughout the reporting solution in conjunction with the reporting provider.
- **Systems Engineering:** Providing detailed technical reference information.
- **Development:** As needed for granular analysis of transaction usage.

Allerium understands that reporting and analytic visibility into the NG Core are paramount and provide a window into operation of our solutions. As such, Allerium has dedicated Technical Program Management staff, which leverages relationships with reporting service providers to ensure customer expectations are met.

5.5.2. Logging Service

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.

Response:

The Logging Service requirement centers on comprehensive visibility into NG911 activity, and Allerium's current approach reflects a mature operational model that supports detailed event tracking across the call flow. Our platform uses established logging interfaces that collect events from each functional element and deliver them into a centralized repository. This repository provides a unified view of log activity, allowing service providers to analyze event sequences, trace call handling behavior, and support operational diagnostics. Each log event is accompanied by detailed analysis documentation, which equips reporting service providers with the context needed to understand system behavior at each stage of the call.

The centralized repository accepts all log events generated by Allerium applications and can also receive logging feeds from PSAP systems when available. This model allows PSAPs to integrate their own event records with NG Core event data, creating a broader operational picture that supports incident review, troubleshooting, and performance monitoring. Events stored in the repository can be accessed through established query and retrieval mechanisms, and these capabilities are already in use across our NG Core Service footprint. In several deployments, Allerium maintains operational alignment with PSN Americas 911Logix solution, which supports customers with direct access to event history through their reporting platforms.

For media logging and recording, Allerium partners with Equature. The Equature media logging service provides a centralized location for media access, creating a cohesive environment where call audio and event records can be reviewed together. This integrated approach helps customers correlate call media with corresponding signaling and operational events, improving the accuracy and speed of post incident analysis.

Allerium recognizes that the industry is moving toward full support for NENA STA 010.3f logging requirements, including the event catalog, query and retrieval behaviors, and subscription based mechanisms such as ElementState and ServiceState notifications. As part of our ongoing standards alignment, we have a development initiative underway to deliver a fully compliant logging service within the next twelve months. This roadmap is informed by our staff who participate actively in NENA, APCO, and related standards bodies, which ensures our direction remains synchronized with the broader NG911 ecosystem.

5.5.3. i3 Logging and Reporting Requirements

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.

Response:

The requirement for i3 aligned logging and reporting places emphasis on capturing functional element activity, aggregating that information in a structured manner, and making it accessible for analysis. Allerium's current approach supports this objective through a centralized model that collects log events from each functional element within the call flow. Our logging interfaces deliver these events into a consolidated repository that allows service providers to observe event sequences, understand call handling behavior, and review system activity holistically. Each event includes documentation that assists reporting service providers in interpreting the underlying operational behavior.

The repository accepts all log events produced by Allerium applications and has the ability to receive PSAP logging feeds when they are available. This structure allows PSAPs to combine their own operational records with NG Core event data, giving them a detailed view of call processing across both the network and the PSAP environment. Event records stored in the repository can be queried and retrieved using established mechanisms that are already deployed within our NG Core customer base. In several implementations, Allerium works in coordination with PSN Americas and their 911Logix solution to provide customers with direct access to historical event information.

For media event logging, Allerium relies on its partnership with Equature. The Equature media logging and recording service offers a central access point for call media, providing an environment where audio and associated event records can be reviewed together. This combined perspective assists operational teams in reconstructing call scenarios and identifying the relationship between signaling, media, and call handling actions.

Allerium recognizes that the industry continues to advance toward the full scope of NENA STA 010.3f i3 logging requirements, including expanded event definitions, enhanced query behaviors, and subscription based functions associated with ElementState and ServiceState reporting. To support this direction, Allerium has an active development initiative aimed at delivering a fully compliant logging service within the next twelve months. Ongoing involvement in NENA, APCO, and related standards bodies ensures that this development effort remains aligned with the evolution of the i3 standard and the needs of the NG911 community.

5.5.4. Functional Element Reporting

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.

Response:

Enterprise-Wide NG9-1-1 Logging, Data Collection, and Reporting System

Allerium's NG Core has been designed from the ground up to ensure every functional element within the ESInet produces rich, actionable, standards-aligned reporting data. Across our nationwide deployments, we have consistently delivered enterprise-wide NG911 logging, data collection, and reporting that not only satisfies but exceeds the requirements defined in NENA STA-010.3f. This depth of visibility is foundational to how we support monitoring, troubleshooting, security analysis, and long-term performance management across complex NG911 ecosystems.

Every major component, ESRP, ECRF, LVF, LIS, BCF, LNG, and supporting services, generates structured operational status reports, critical event logs, alarms, and performance metrics. These outputs conform to standard protocols and are fully interoperable with centralized logging and monitoring platforms.

While the Allerium NG Core natively captures every metric requested in the RFP, our experience has shown that the most effective way to surface and operationalize these insights is through our established integration with PSN Americas' 911Logix reporting and analytics suite. This platform, already contracted within the state, provides a unified, browser-based reporting environment that transforms raw NG Core metrics into intuitive dashboards, historical analyses, and real-time monitoring views.

Documentation and Release Governance

With each software release, Allerium delivers comprehensive documentation packages that ensure consistency and transparency in all reporting feeds. These include:

- Transaction-level definitions for every generated log event
- Application error definitions and action guides
- Updated report definition and functional specifications
- A Reporting Impact Analysis outlining changes relevant to downstream systems

To ensure proper alignment and clarity, Allerium facilitates review sessions with reporting stakeholders, including PSN Americas, supported by Technical Product Management, Systems Engineering, Technical Program Management, and Development resources. This coordinated approach ensures that reporting partners always understand precisely how to interpret and operationalize new or updated data structures.

Enterprise Reporting Coverage

Allerium's integrated reporting environment supports detailed visibility into each of the metrics requested by the State.

ESInet to PSAP Call Delivery Transactions

The NG Core logs every call delivery event from ingress to final PSAP routing, including timestamps, routing decisions, transfer outcomes, policy application indicators, and error conditions. 911Logix presents these as end-to-end transaction reports that allow customers to trace individual calls or analyze performance trends across the ESInet.

SIP Conference Metrics

Conference session attempts, participants, SIP signaling outcomes, and session duration are recorded by the ESRP and BCF. Metrics such as bridge utilization, failure rates, and participant counts are surfaced in dashboard views to support operational monitoring and troubleshooting.

PSAP Routing Duration Report

All routing latencies, including ESRP decision times, ECRF/LVF query durations, and final call setup intervals, are logged and available through summarized or detailed reports. These provide insights into routing efficiency and can be used to validate compliance with performance SLAs.

Concurrent Calls

The NG Core continuously tracks concurrent call volumes across the ESInet, ESRP, and BCF elements. These metrics support capacity management and trend forecasting, and are visualized in near real-time through 911Logix dashboards.

BCF Session Reporting

The Border Control Function generates detailed SIP session logs, including call ingress, security events, protocol validations, media negotiation details, and session terminations. These logs provide essential insight into traffic patterns and interconnection performance.

ESRP Session Reporting

The Emergency Services Routing Proxy produces transaction-level routing session records that include policy routing outcomes, queue interactions, alternate routing attempts, and error states. These records are instrumental for understanding call flow behavior and policy impacts.

ESRP Queue State

ESRP queues are continuously monitored, with queue length, estimated wait time, overflow conditions, and dequeue events reported in real time. This enables PSAPs and system administrators to assess congestion points and validate operational readiness.

ECRF Session Reporting

Every ECRF location query is logged with the input, response time, returned routing information, schema validation results, and any error or exception generated. These metrics support auditing, GIS accuracy efforts, and routing validation analysis.

LVF Reporting

Validation requests received by the LVF, including validation outcomes, reason codes, and response duration, are logged and included in GIS governance reports, supporting address quality improvement programs.

LNG Session Reporting

The LNG produces session-level data on location retrieval attempts, confidence values, downstream LIS interactions, and timing metrics. Reports assist agencies in evaluating the reliability and speed of location acquisition workflows.

5.5.5. Monitoring, Outages, Failover, Trouble Tickets, and Escalation

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.

Response:

Allerium operates a mature, 24x7x365 Network Operations Center (NOC) designed to support mission-critical NG911 environments.

Continuous Monitoring and Alerting

Allerium provides continuous monitoring of the ESInet, NGCS, gateways, and all associated infrastructure components. Monitoring is performed using integrated network management and observability platforms that ensure:

- Real-time visibility into system health and performance
- Automated alert generation for any deviation from normal operation
- Immediate ticket creation for all actionable alarms

All faults, degradations, or anomalies generate alerts to the NOC, where trained personnel immediately assess and initiate response actions.

Outage Classification and Escalation

Allerium treats any element failure as an outage and any service-impacting failure as a high-priority, life-safety event.

Incidents are classified using a structured severity model (e.g., SIL 1–4), with defined response, escalation, and notification timelines aligned to SLA commitments. For high-severity outages:

- Escalation to the highest non-executive technical level occurs within defined SLA thresholds (e.g., within five (5) minutes for critical services)
- All necessary technical resources—including NOC, Engineering, Field Services, and vendor partners—are engaged immediately
- A single Incident Owner is assigned and empowered to direct all resources required for resolution
- The Incident Owner is promptly communicated to the State and stakeholders

Major Incident Management (MIM)

For significant outages, Allerium initiates a formal Major Incident Management (MIM) process, which includes:

- Immediate activation of an internal technical bridge for coordinated troubleshooting
- Establishment of a customer-facing communication bridge for the State and affected PSAPs
- Structured incident command, ensuring clear roles, responsibilities, and decision authority

- Continuous status updates, including impact, mitigation actions, and estimated time to restoration

This dual-bridge model ensures focused technical resolution while maintaining clear and consistent communication with stakeholders.

Notification and Communication

All outages visible to PSAPs are promptly communicated to both the affected PSAP(s) and the State. Allerium supports multiple notification methods, including:

- Automated notifications (e.g., text, email)
- Voice communications and incident bridges
- Web-based portals for ticket visibility

Notifications include initial alerting, ongoing status updates, and final restoration confirmation, all aligned with SLA-defined timelines.

Root Cause Analysis and Corrective Action

Any outage resulting in SLA impact triggers a formal Root Cause Analysis (RCA) process. Allerium provides:

- Detailed RCA reports outlining root cause(s), contributing factors, and corrective actions
- Committed timelines for remediation activities
- Ongoing progress reporting, including quarterly updates where applicable

Allerium collaborates with the State to review findings and will adjust corrective action plans as needed to ensure alignment and effectiveness.

Help Desk Operations and Ticket Management

Allerium provides a fully integrated 24x7x365 Help Desk, staffed by trained technical personnel capable of resolving common PSAP issues.

Key capabilities include:

- Ticket submission via phone and web-based portal
- Telephone calls answered by qualified technicians within defined SLA thresholds
- Immediate automated acknowledgment for web submissions, with rapid follow-up response
- First-contact resolution targets aligned with performance KPIs
- Full ownership of all reported issues until resolution

Every reported issue generates a ticket within Allerium's IT Service Management (ITSM) system, ensuring complete tracking and accountability.

eBonding and Supplier Coordination

Allerium supports eBonding (ticket integration) with suppliers and subcontractors to ensure seamless coordination across all parties involved in incident resolution.

This capability provides:

- Real-time visibility into supplier and subcontractor ticket activity
- Bi-directional ticket updates and status synchronization
- Centralized tracking within Allerium's ITSM platform

While suppliers or subcontractors may perform portions of the resolution work, Allerium retains full ownership of the incident and is responsible for coordination, follow-up, and communication with the State.

Sustained Outage Management and Workarounds

For sustained outages (greater than 15 minutes), Allerium prioritizes rapid service restoration through:

- Immediate investigation and isolation of the issue
- Implementation of temporary workarounds or failover strategies to restore partial or full service
- Continued efforts toward permanent resolution

Where a workaround can restore service faster than full repair, it is implemented without delay to minimize impact to PSAP operations.

Operational Philosophy

Allerium's NOC operates under a life-safety-first model: detect early, respond immediately, escalate without delay, and maintain ownership through resolution. This disciplined approach ensures high availability, rapid restoration, and transparent communication for all stakeholders.

5.5.6. Maintenance and Configuration Reports

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*

Response:

Governance and Control Framework

All production changes are governed through Allerium's enterprise IT Service Management (ITSM) platform (Remedy), which enforces standardized workflows, documentation requirements, approval routing, and audit traceability.

Each change request (CRQ) requires a fully documented Implementation and Backout Plan (IBOP), detailing:

- Scope and business justification
- Technical impact assessment across interconnected systems

- Risk classification and mitigation steps
- Validation and testing procedures
- Step-by-step implementation instructions
- Defined backout methodology

No non-emergency production change is executed without advance notice, documented approval, and customer-aligned communication.

Allerium's change governance extends beyond internal systems. We actively coordinate with third-party vendors, carriers, hosted platform providers, and infrastructure partners when their maintenance activities may impact the NG9-1-1 ecosystem. Vendor-led changes are reviewed through the same structured risk evaluation process, scheduled within approved maintenance windows, and monitored by our NOC/SOC to ensure unified situational awareness and accountability across all stakeholders.

Notifications

High-Level Incident Response & Notification

The Allerium notification platform can support user-definable levels of notification with delivery via:

- Email,
- Text, and
- Phone.

Allerium can provision authorized recipients of incident notifications in the system based on preference for notification type during the implementation phase of the project. Users can request to change established preferences through an NOC request. Figure 33 shows a high-level incident response and notification flow with notification delivery via email, text, and phone.

Allerium works with the State and/or its designated third-party to define the user-definable notification levels. This process is applicable to both the State and other stakeholders.

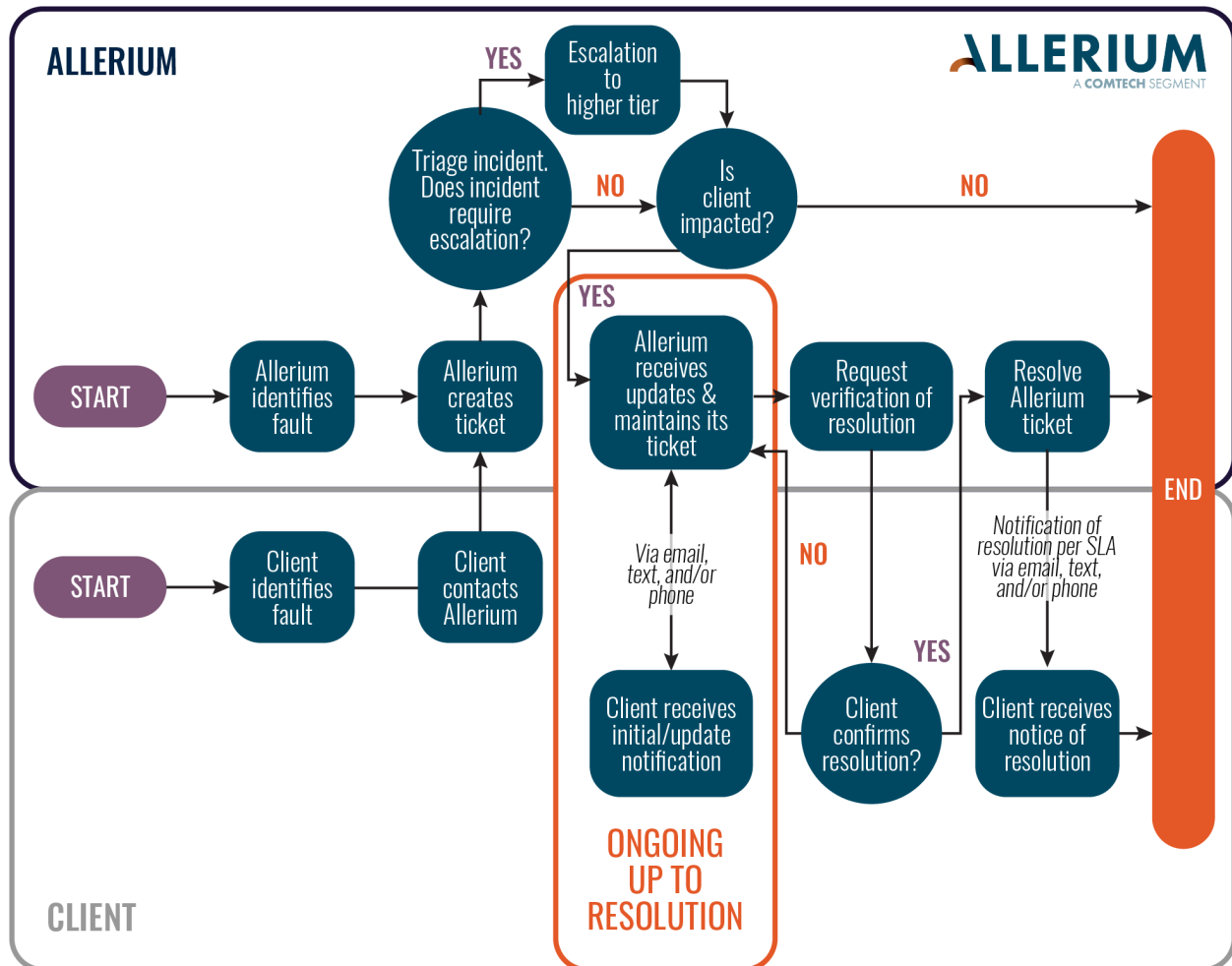


Figure 33. High-Level Incident Response and Notification Flow

Automated PSAP Connectivity Monitoring & Notification

Allerium has implemented enhanced automation for PSAP firewall node connectivity monitoring to further strengthen service assurance and SLA compliance across deployments.

This enhancement introduces automated ITSM ticket creation and real-time notifications when predefined loss-of-connectivity thresholds are detected via our monitoring platform. The automation ensures immediate awareness by both the NOC and customer stakeholders, reducing detection time and accelerating response.

Redundancy Loss Monitoring

When a PSAP experiences a loss of network redundancy for more than 10 minutes:

- An ITSM Incident (INC) is automatically created.
- An automated Service Notification Incident (NSI) is generated.
- Notifications are delivered to designated stakeholders.

This ensures that degraded resilience conditions are identified early, allowing corrective action before a full outage occurs directly supporting SLA protection and continuity objectives.

Complete Outage Monitoring

When a PSAP experiences a complete network outage for more than 3 minutes:

- An ITSM Incident (INC) is immediately created.
- An automated Impairment Notification is issued.
- Real-time notifications are sent to appropriate operational and customer contacts.

This rapid detection and notification model minimizes Mean Time to Awareness (MTTA), accelerates remediation, and ensures transparent communication during high-severity events.

Operational Handling & Governance

While the detection and notification process is automated, all resulting incidents are managed under Allerium's established NGCS PSAP firewall alarm procedures. This ensures:

- Consistent troubleshooting workflows
- Structured escalation paths
- Documented RCA and closure controls
- SLA tracking and reporting alignment

The automation enhances speed and visibility without altering the disciplined operational framework already in place.

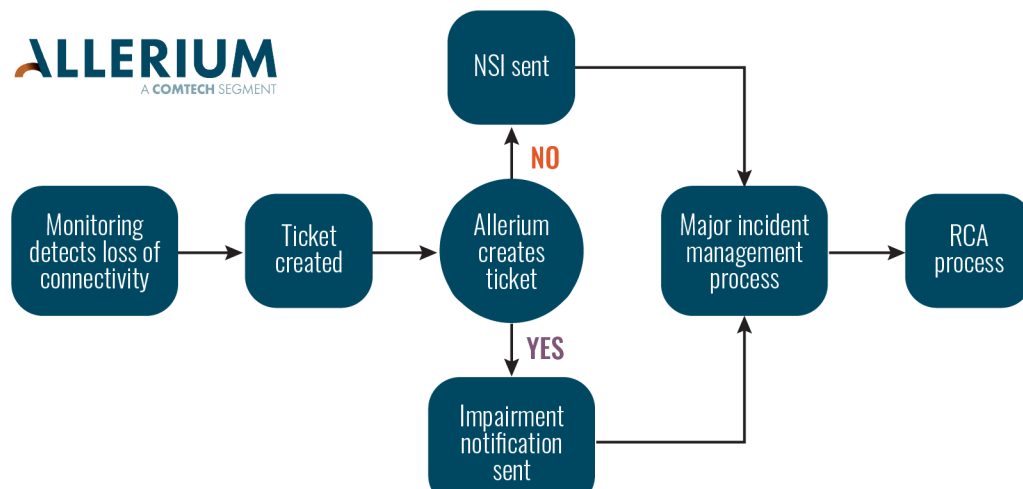


Figure 34. Automated PSAP Network Events Incident Detection & Notification Flow

5.5.7. Discrepancy Reporting

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).*

Response:

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed. When LVF becomes the validation method, Allerium will establish a similar support process for LVF data management.

The Allerium data integrity group directly supports end users of the Allerium Location Data Platform during the integration and onboarding phases and throughout the life of the contract. Between the user interaction with our location data product and our data integrity group, this service acts as the SPOC for OSPs and PSAPs to coordinate resolution and support overall data integrity. In addition to a dedicated team of experts supporting our Location Data Platform, Allerium has integrated numerous features of automation in the Location Data Platform workflows, ranging from automated discrepancy reporting and automated revalidations to automated notification of change request and task/act item reminders.

Allerium's Location Data Platform provides automated support for generating discrepancy reports (DRs) of ALI records that are not spatial master street address guide (MSAG) valid by assigning action and creating audit trails for resolution as depicted in Figure 35.

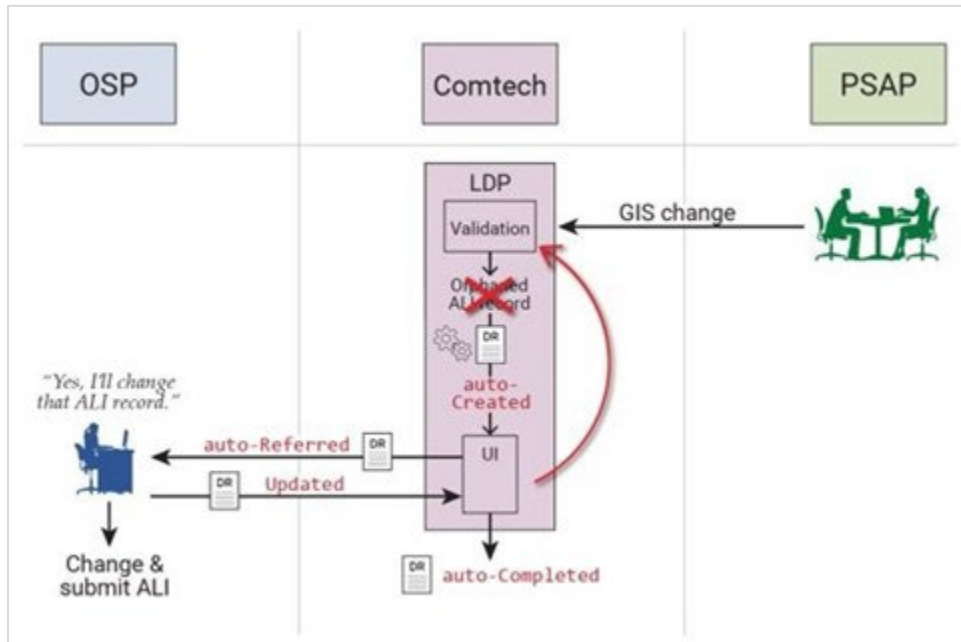


Figure 35. Auto Generated Discrepancy Report

In addition to providing process automation for discrepancy reporting, the Allerium Location Data Platform also retains the ability to manually create DRs as outlined in Figure 36 to support the ALI processes. Once generated, these DRs provide the same level of audit trail the automated processes provide.

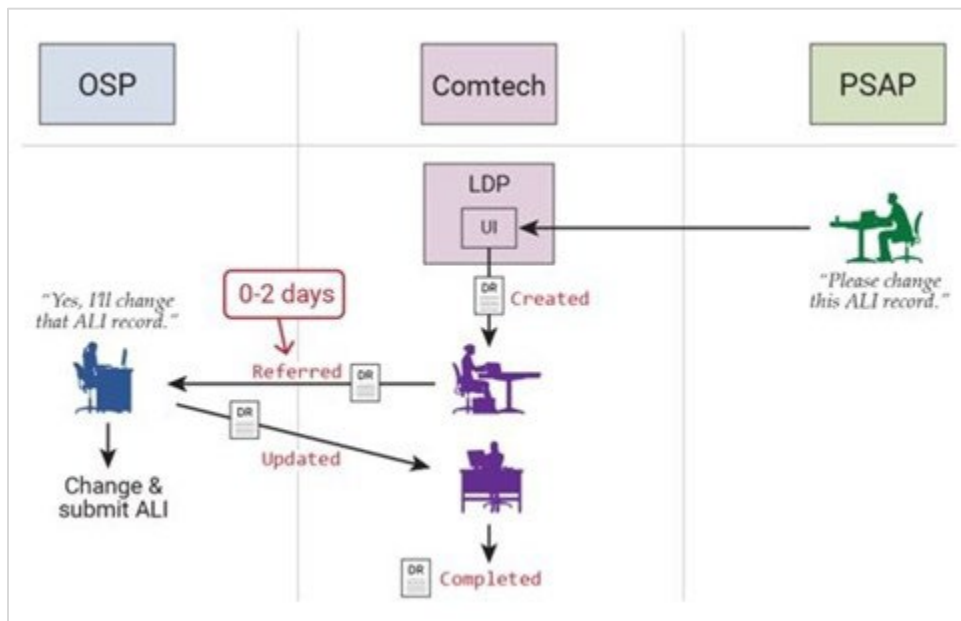


Figure 36. Manually Generated Discrepancy Report

Figure 37 and Figure 38 below outline the workflow process by which OSPs can request changes to the SPATIAL MSAG® as well as the approach and denial processes. Much like the DR process, the change request (CR) process provides a full audit trail for each step of the process.

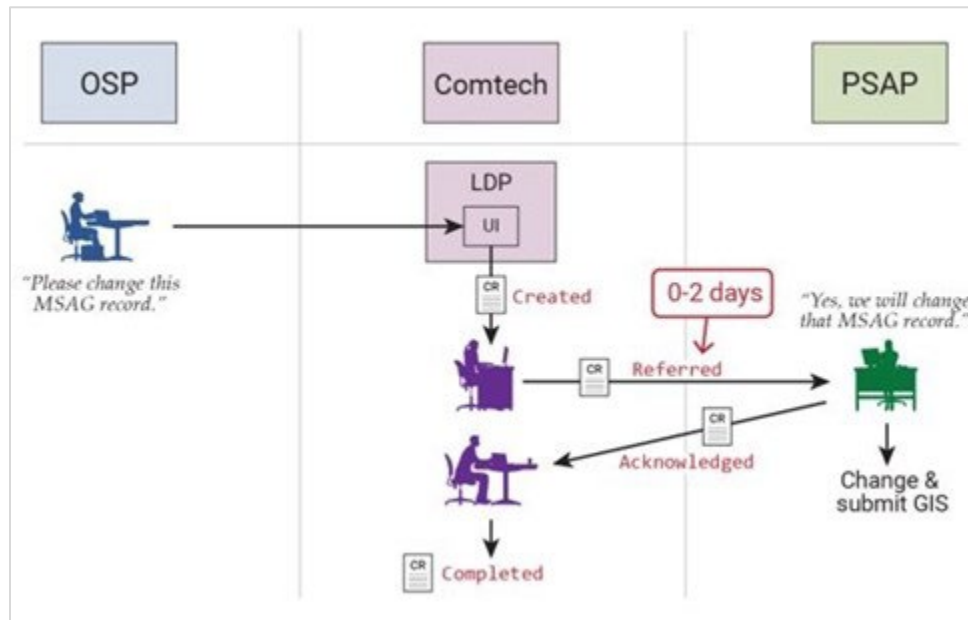


Figure 37. SpatialMSAG® Change Request

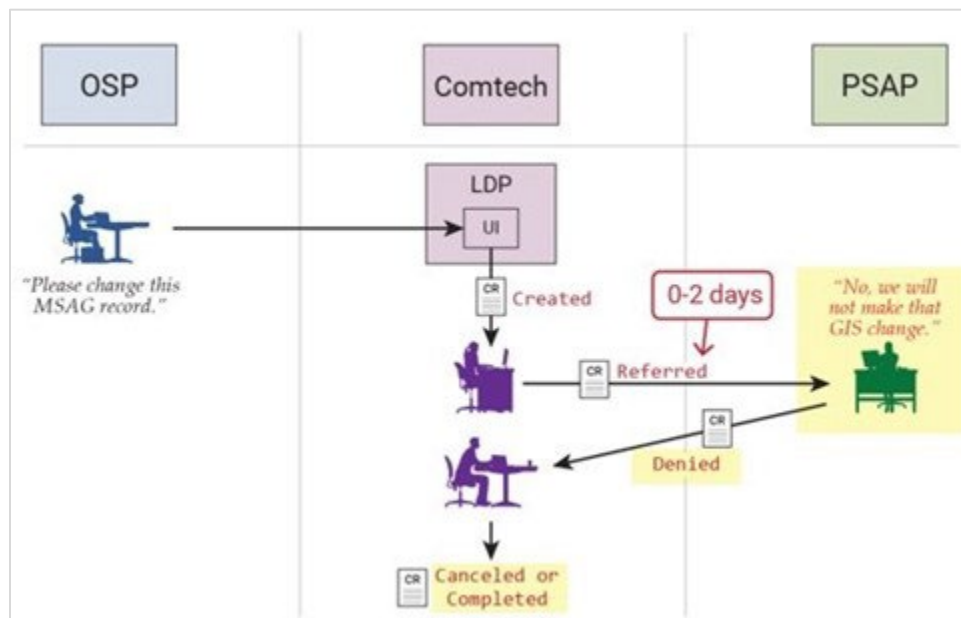


Figure 38. SpatialMSAG Change Request (Denied)

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.1. Policy and Core Routing

5.5.7.1.1. Policy Store Discrepancy Report

5.7.1. Policy and Core Routing

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

Response:

The Policy Store is designed to preserve the integrity of policy information by ensuring that any policy retrieved through a query reflects the exact content originally provided by the policy owner. In NG911 operations, this consistency is critical because routing decisions depend on stable and predictable policy behavior. A discrepancy report provides the mechanism for identifying situations in which a retrieved policy does not match the stored version or contains elements that differ from what the owner submitted.

Within Allerium's NGCS, the Policy Store operates in close coordination with the Policy Routing Function to maintain continuity across policy creation, retrieval, and verification. When a policy owner consults the system to review or edit an existing policy, the interface allows that owner to examine the current ruleset as well as previous versions. This provides a reliable method for confirming that a policy has remained intact over time and that query results align with what was originally entered.

If a consuming functional element encounters behavior that suggests a discrepancy, the responsibility for reporting it lies with that consuming element. In most cases, the ESRP is the component that identifies issues because it depends on the Policy Store for real-time routing decisions. When the ESRP retrieves a policy and identifies unexpected characteristics, such as structure or content that differs from the expected result, the system records the condition through detailed transaction logging. These logs capture the query, the returned policy, and the full context of the exchange, providing a clear trail for investigating the issue.

The monitoring framework associated with the Policy Store and the ESRP is built to surface unusual conditions that may indicate a policy retrieval problem. When such a condition occurs, the system generates an error event that can form the basis of a discrepancy report.

Through this combination of visibility, auditability, and consistent policy handling, the NGCS provides a structured pathway for identifying and reporting policy discrepancies whenever they arise.

5.5.7.1.2. Policy Discrepancy Report

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).

Response:

A Policy Discrepancy Report provides a structured method for identifying situations in which a routing policy behaves differently than the policy owner intended. In an NG911 environment, this reporting process is essential because policies influence real-time routing decisions, and any deviation from the expected behavior must be captured promptly. NENA-STA-010.3 sets the expectation that any entity using a policy may report a discrepancy to the policy owner, including situations where the ESRP identifies an unexpected condition.

Within Allerium's NGCS, the handling of policy discrepancies mirrors the overall approach used for Policy Store discrepancies. The focus remains on the consuming functional element, which is best positioned to identify behavior that falls outside expected norms. When a functional element retrieves a policy and encounters an issue, such as content that does not align with the expected structure or behavior, the responsibility for filing the discrepancy rests with that consuming component.

The ESRP is the primary consumer of routing policies in the NG Core and therefore serves as the most frequent originator of discrepancy reports. When the ESRP queries the Policy Store and receives a response that suggests a mismatch, the system captures the full context of the event through detailed transaction logging. This includes the incoming query, the policy returned, and any exceptions that occurred during processing. These logs provide a clear record that can be reviewed by the policy owner to determine whether the discrepancy represents an error in the policy content, a misconfiguration, or a broader operational issue.

To support this process, the ESRP and the Policy Routing Function maintain extensive monitoring to identify unexpected results. When an anomaly is detected, the system generates an error event within the transaction logs. This event becomes the basis for a Policy error report directed to the policy owner, which may be a PSAP, an ESRP operating under a different administrative domain, or another authorized entity. The process ensures that inconsistencies are identified through operational use and can be corrected before they affect additional routing decisions.

Through this monitoring and reporting structure, the NGCS supports the NENA intent for policy discrepancy identification by ensuring that consuming elements can detect unexpected outcomes and direct those findings to the appropriate policy owner for review.

5.5.7.1.3. Emergency Services Routing Proxy (ESRP) Discrepancy Report

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.

Response:

Allerium's ESRP and PRF log all transactions and raise error events through transaction detail logging. The transaction details have extensive monitoring for cases in which the solution does not behave as expected. Allerium's ESRP transaction details are continuously monitored in near real time and any variance from expected call delivery raises events to our NOC.

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.2. Location and GIS Sources

5.5.7.2.1. Location Information Server (LIS) Discrepancy Report

5.7.2. Location and GIS Sources

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.

Response:

Allerium's LDP provides integrated Discrepancy Reporting.

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed.

The Allerium data integrity group directly supports end users of the Allerium Location Data Platform during the integration and onboarding phases and throughout the life of the contract. Between the user interaction with our location data product and our data integrity group, this service acts as the SPOC for OSPs and PSAPs to coordinate resolution and support overall data integrity. In addition to a dedicated team of experts supporting our Location Data Platform, Allerium has integrated numerous features of automation in the Location Data Platform workflows, ranging from automated discrepancy reporting and automated revalidations to automated notification of change request and task/act item reminders.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.2.2. GIS Discrepancy Report

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).

Response:

The Allerium data integrity group directly supports end users of the Allerium Location Data Platform during the integration and onboarding phases and throughout the life of the contract. Between the user interaction with our location data product and our data integrity group, this service acts as the SPOC for OSPs and PSAPs to coordinate resolution and support overall data integrity. In addition to a dedicated team of experts supporting our Location Data Platform, Allerium has integrated numerous features of automation in the Location Data Platform workflows, ranging from automated discrepancy reporting and automated revalidations to automated notification of change request and task/act item reminders.

Allerium's Location Data Platform provides automated support for generating discrepancy reports (DRs) of ALI records that are not spatial master street address guide (MSAG) valid by assigning action and creating audit trails for resolution as depicted in Figure 39.

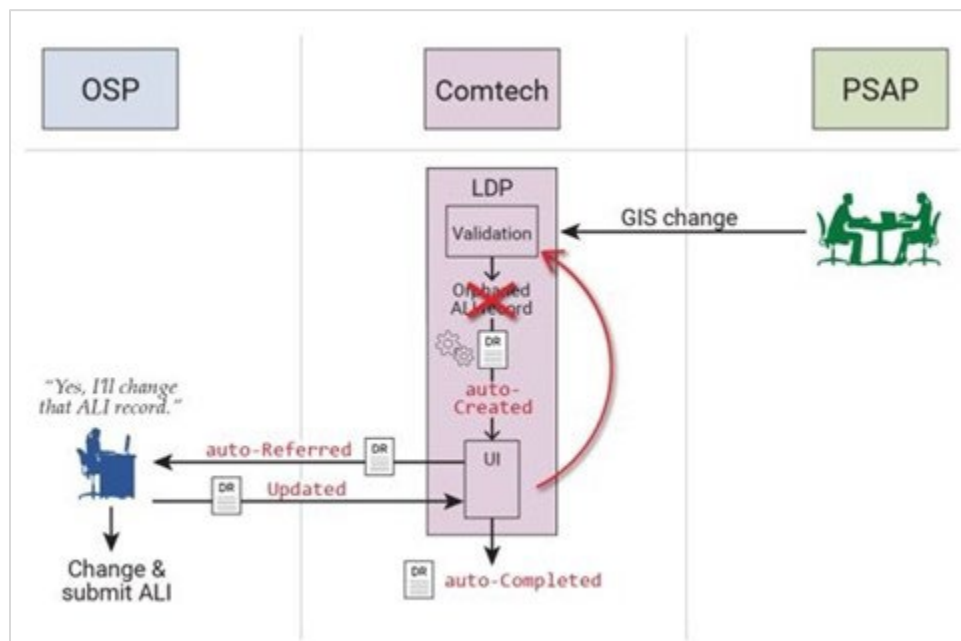


Figure 39. Auto Generated Discrepancy Report

In addition to providing process automation for discrepancy reporting, the Allerium Location Data Platform also retains the ability to manually create DRs as outlined in Figure 40 to support the ALI processes. Once generated, these DRs provide the same level of audit trail the automated processes provide.

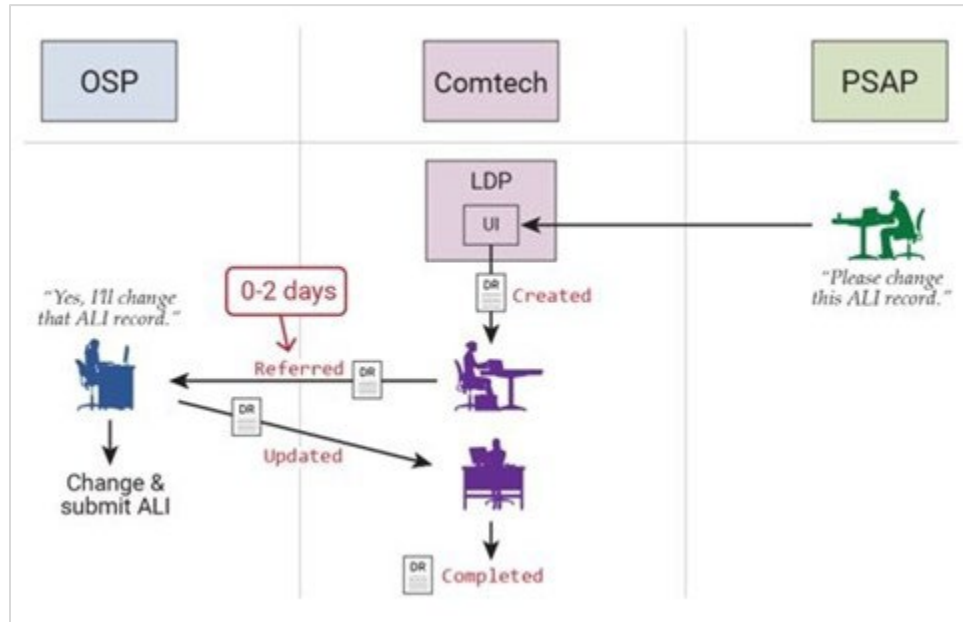


Figure 40. Manually Generated Discrepancy Report

Figure 41 and Figure 42 below outline the workflow process by which OSPs can request changes to the SPATIAL MSAG® as well as the approach and denial processes. Much like the DR process, the change request (CR) process provides a full audit trail for each step of the process.

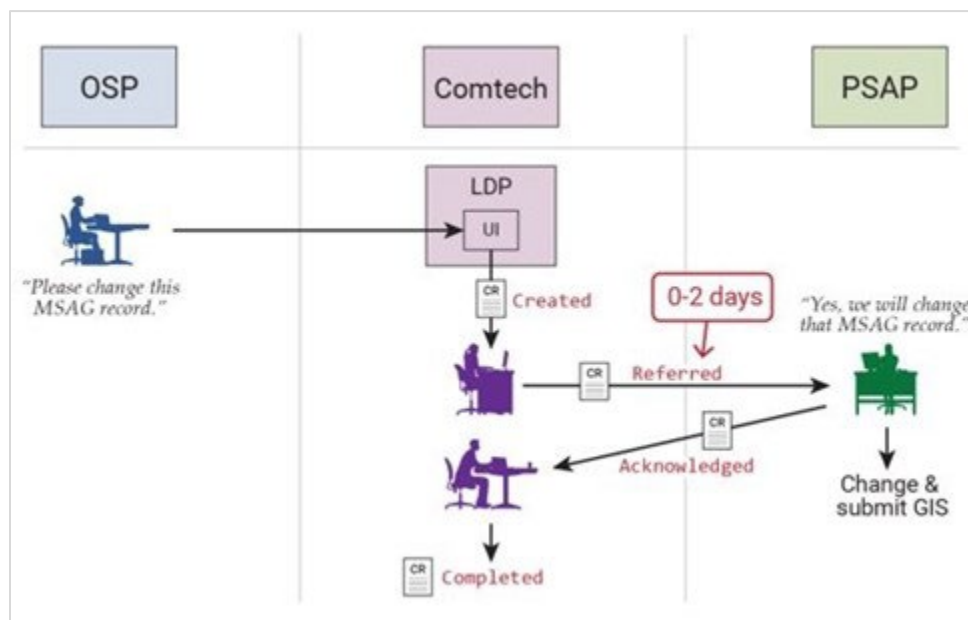


Figure 41. SpatialMSAG® Change Request

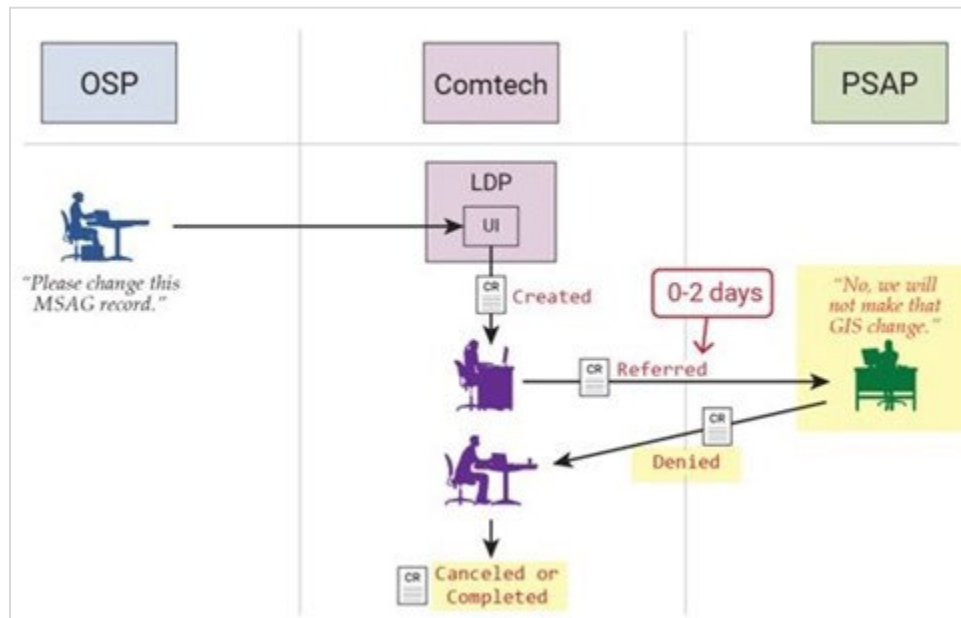


Figure 42. SpatialMSAG Change Request (Denied)

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.2.3. MSAG Conversion Service Discrepancy Report

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).

Response:

Allerium's MCS provides detailed transaction reports for all events occurring within the application. The events include but are not limited to requests received, responses sent, data validation errors, and general application errors. The events feed into Allerium solutions in near real time similar to the ESRP.

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.2.4. LoST Discrepancy Report

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.

Response:

Allerium's ECRF provides detailed transaction reports for all events occurring within the application. The events include but are not limited to requests received, responses sent, data validation errors, and general application errors. The events feed into Allerium solutions in near real time similar to the ESRP.

Allerium's ECRF works in conjunction with our ESRP in order to ensure that all facets of discrepancies are captured. For instance, if the ESRP receives an error when placing a LoST query, the ESRP generates additional transaction detail which in turn feeds into our NOC.

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.3. Signaling and Edge

5.5.7.3.1. SIP Discrepancy Report

5.7.3. Signaling and Edge

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).

Response:

Allerium's NGCS logs all transactions and raises error events through transaction detail logging, including any SIP messaging discrepancies. The transaction details have extensive monitoring for cases in which the solution does not behave as expected. Allerium's ESRP transaction details are continuously monitored in near real time and any variance from expected call delivery raises events to our NOC.

Discrepancy Reporting as per STA-010.3f requires the entire ESInet ecosystem to leverage the feature set to recognize the value of leveraging the subsystem. As such, Discrepancy Reporting functionality rests with the Allerium Location Data Platform such that PSAPs, OSPs, and Allerium all remain informed.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.3.2. Border Control Function (BCF) Discrepancy Report

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).

Response:

Allerium implements commercial grade SBCs within our BCF component which provide internal logging and alarming during discrepancy events. The events process through to the Allerium NOC for resolution.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.4. Network and Infrastructure

5.5.7.4.1. Network Discrepancy Report

5.7.4. Network and Infrastructure

5.7.4.1. Network Discrepancy Report

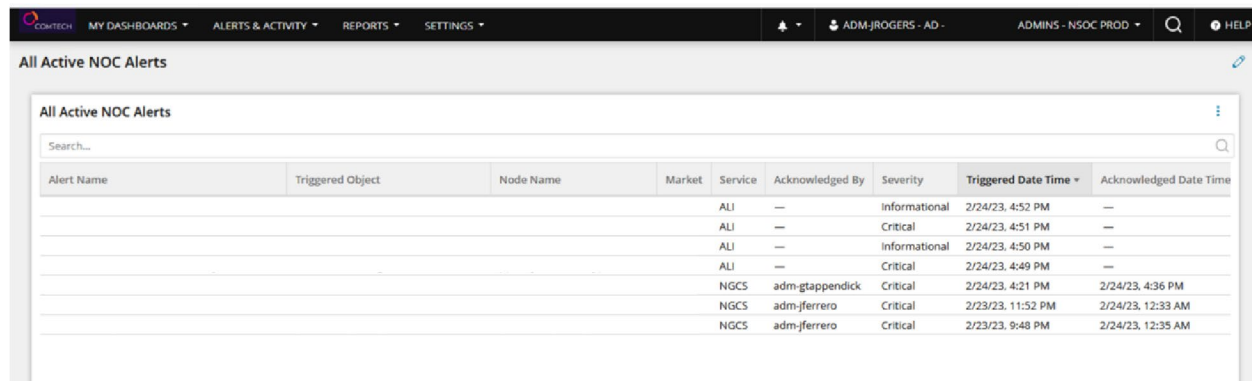
A Network Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. Any entity will be able to report a general networking discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 general networking DR.

Response:

Allerium employs a monitoring platform to collect and monitor data from systems and applications used in the operation of ESInet and NGCS service functions. This platform provides real-time awareness of system health and operational status of the service. In conjunction with the monitoring platform, Allerium employs both dashboard and reporting tools for use by both internal and external users to measure operational performance.



Alert Name	Triggered Object	Node Name	Market	Service	Acknowledged By	Severity	Triggered Date Time	Acknowledged Date Time
				ALI	---	Informational	2/24/23, 4:52 PM	---
				ALI	---	Critical	2/24/23, 4:51 PM	---
				ALI	---	Informational	2/24/23, 4:50 PM	---
				ALI	---	Critical	2/24/23, 4:49 PM	---
				NGCS	adm-gtappendick	Critical	2/24/23, 4:21 PM	2/24/23, 4:36 PM
				NGCS	adm-jferrero	Critical	2/23/23, 11:52 PM	2/24/23, 12:33 AM
				NGCS	adm-jferrero	Critical	2/23/23, 9:48 PM	2/24/23, 12:35 AM

Figure 43. All Active NOC/SOC Alerts Dashboard

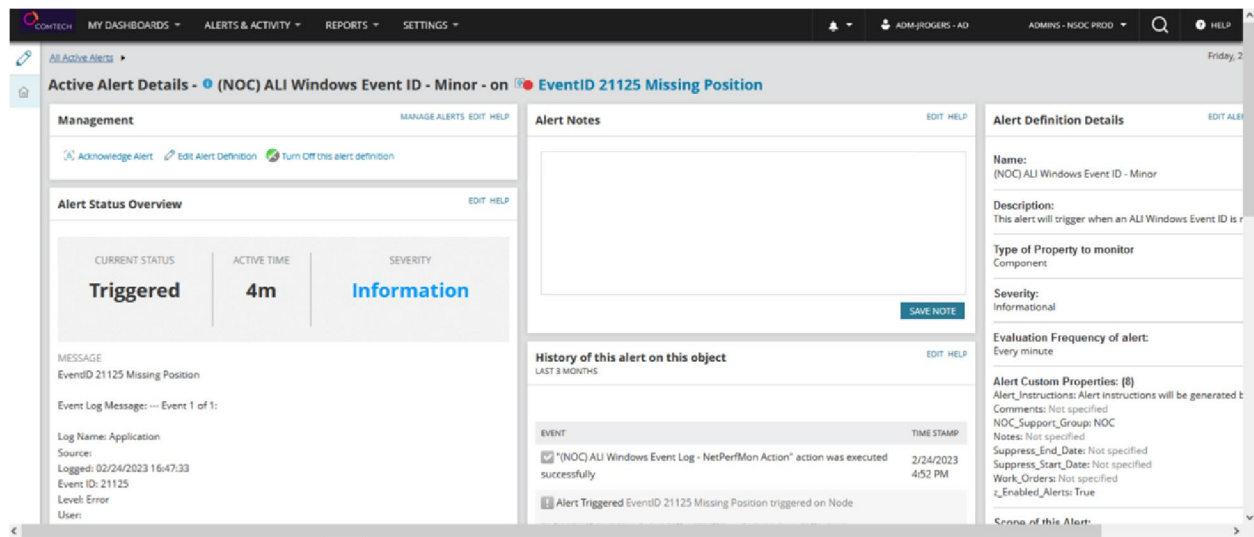


Figure 44. Node Summary of an Active Alert

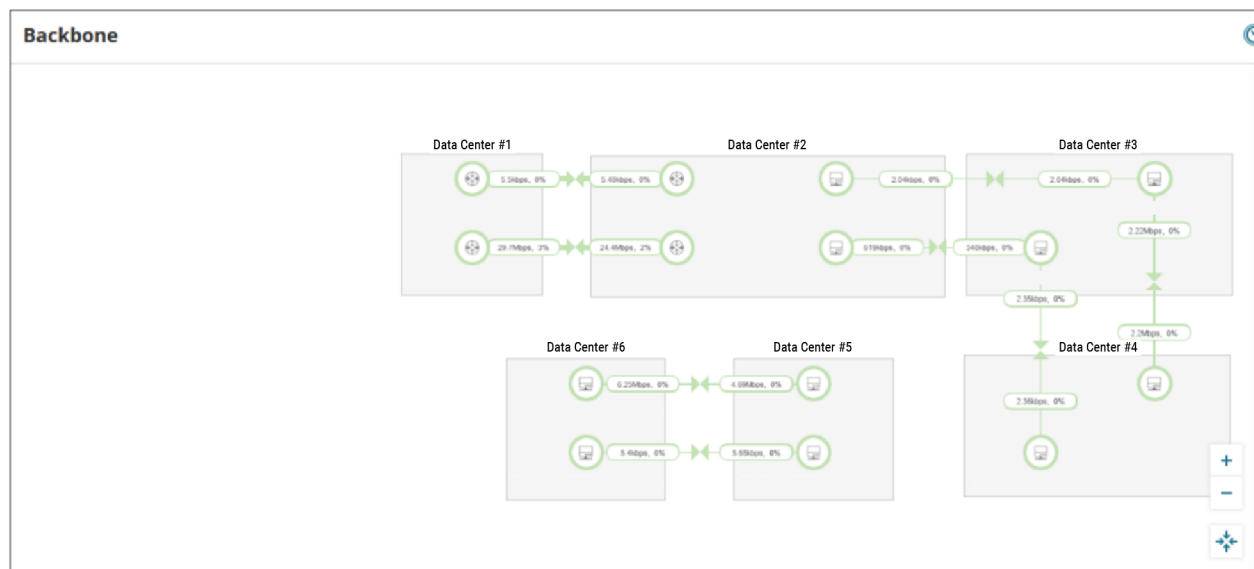


Figure 45. Major Backbone Network Connectivity Circuit Map

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.5. Security and Trust

5.5.7.5.1. Permissions/Security/Authentication Discrepancy Report

5.7.5. Security and Trust

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).

Response:

The Allerium capability enables an entity that identifies an apparent security, permissions, or authentication error to submit a discrepancy report through the discrepancy reporting interface associated with the entity or element believed to be responsible. The design is intended to support auditable, structured reporting of access-control, authentication, secure-transport, and signature-validation anomalies so that discrepancies can be triaged, investigated, and resolved through controlled workflows. Allerium works with customers to define expected reports for the proposed scope, a delivery approach, report contents, service commitments, assumptions, and acceptance criteria.

The discrepancy reporting may include the report categories/ event classes:

- 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 or modify a resource.
- Unable to delete a resource.
- Able to read a resource when it should have been denied.
- Able to write or 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, including TLS certificate invalidity or TLS negotiation failure.
- Unable to verify a digital signature of a resource, including signature verification failure, invalid certificate chain, or an untrusted certificate authority.

5.5.7.5.2. Log Signature/Certificate Discrepancy Report

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).

Response:

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.6. Data and Logging

5.5.7.6.1. Logging Service Discrepancy Report

5.7.6. Data and Logging

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.

Response:

Allerium’s NGCS leverages transaction detail level reporting and plans to implement a full i3 Logging Service within our 12-month roadmap.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.6.2. ADR/IS-ADR Discrepancy Report

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.

Response:

Current ADR implementations within Allerium's networks provide ADR information related to service provider, provider type, and service information via our LDP. Current management of discrepancies related to ADR reside within our LDP and we plan to expand functionality to encompass other ADR elements in the next 12 months.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.7. PSAP Operations and Treatments

5.5.7.7.1. PSAP Call Taker Discrepancy Report

5.7.7. PSAP Operations and Treatments

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).

Response:

The Allerium data integrity group directly supports end users of the Allerium Location Data Platform during the integration and onboarding phases and throughout the life of the contract. Between the user interaction with our location data product and our data integrity group, this service acts as the SPOC for OSPs and PSAPs to coordinate resolution and support overall data integrity. In addition to a dedicated team of experts supporting our Location Data Platform, Allerium has integrated numerous features of automation in the Location Data Platform workflows, ranging from automated discrepancy reporting and automated revalidations to automated notification of change request and task/act item reminders.

Allerium's Location Data Platform provides automated support for generating discrepancy reports (DRs) of ALI records that are not spatial master street address guide (MSAG) valid by assigning action and creating audit trails for resolution as depicted in Figure 46.

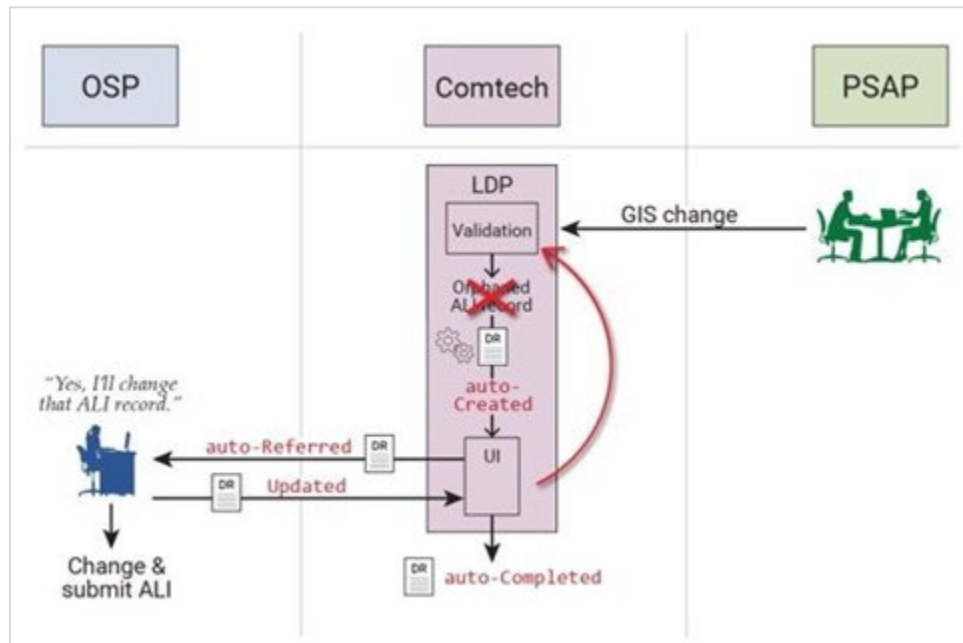


Figure 46. Auto Generated Discrepancy Report

In addition to providing process automation for discrepancy reporting, the Allerium Location Data Platform also retains the ability to manually create DRs as outlined in Figure 47 to support the ALI processes. Once generated, these DRs provide the same level of audit trail the automated processes provide.

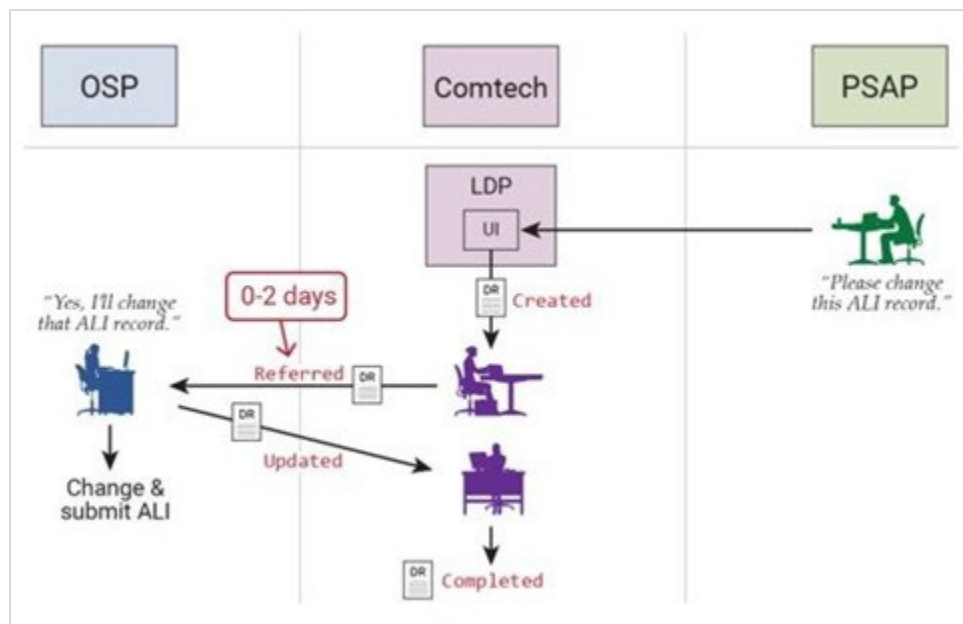


Figure 47. Manually Generated Discrepancy Report

Figure 48 and Figure 49 below outline the workflow process by which OSPs can request changes to the SPATIAL MSAG® as well as the approach and denial processes. Much like the DR process, the change request (CR) process provides a full audit trail for each step of the process.

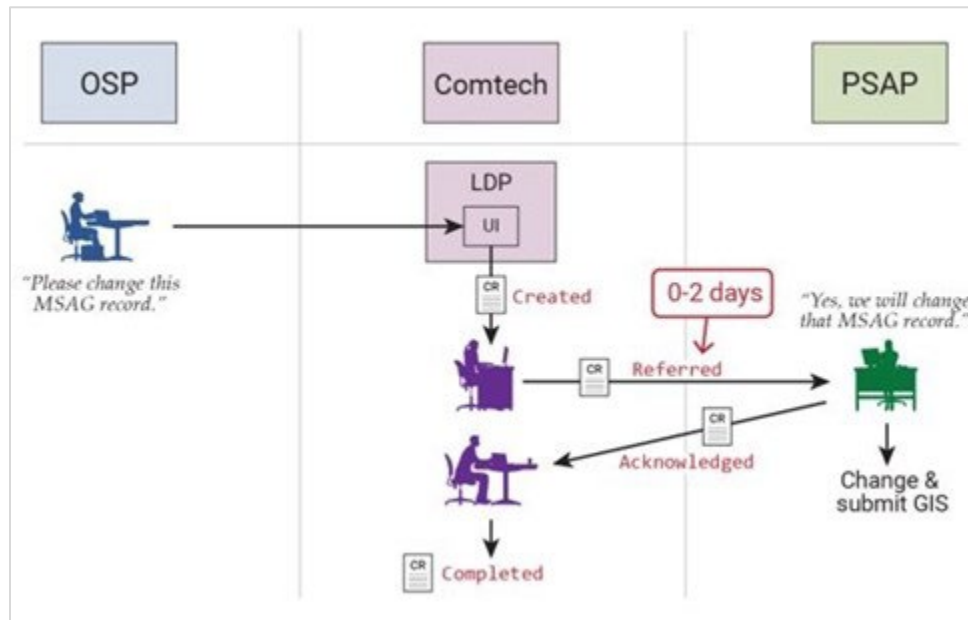


Figure 48. SpatialMSAG® Change Request

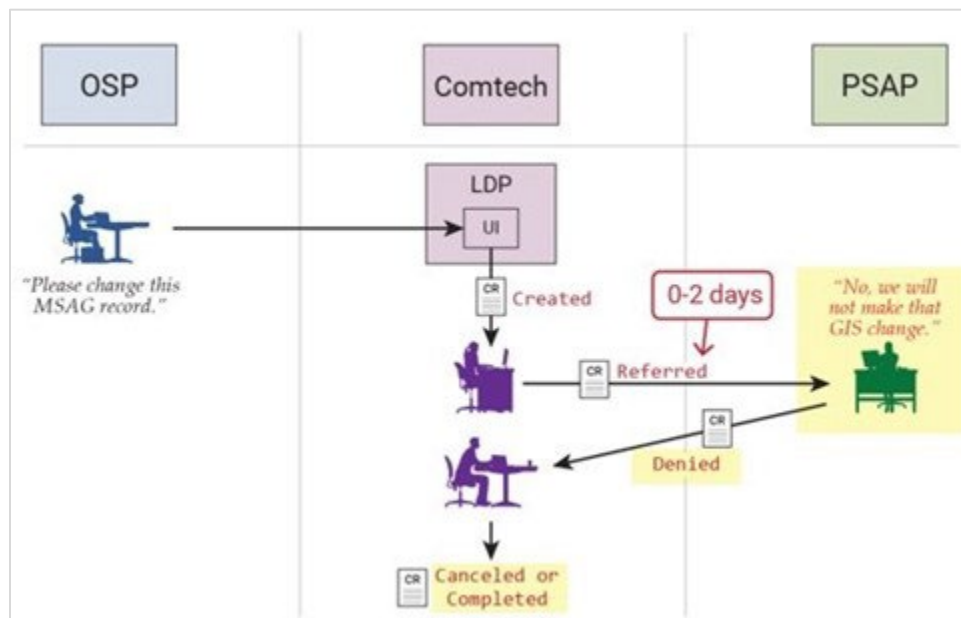


Figure 49. SpatialMSAG Change Request (Denied)

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.7.2. Call Transfer Failure Discrepancy Report

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.

Response:

Allerium's NGCS records all transfer attempts for success and failure conditions both. In the event that there are call transfer failures, alarms are generated to our NOC for review and resolution.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.7.3. Interactive Media Response (IMR) Discrepancy Report

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.

Response:

Allerium does not implement IMR devices with our NGCS solution. Use of IMR and associated discrepancy reporting are on our 12-month roadmap.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.8. External Providers

5.5.7.8.1. Originating Service Provider Discrepancy Report

5.7.8. External Providers

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.

Response:

The Allerium data integrity group directly supports end users of the Allerium Location Data Platform during the integration and onboarding phases and throughout the life of the contract. Between the user interaction with our location data product and our data integrity group, this service acts as the SPOC for OSPs and PSAPs to coordinate resolution and support overall data integrity. In addition to a dedicated team of experts supporting our Location Data Platform, Allerium has integrated numerous features of automation in the Location Data Platform workflows, ranging from automated discrepancy reporting and automated revalidations to automated notification of change request and task/act item reminders.

Allerium's Location Data Platform provides automated support for generating discrepancy reports (DRs) of ALI records that are not spatial master street address guide (MSAG) valid by assigning action and creating audit trails for resolution as depicted in Figure 50.

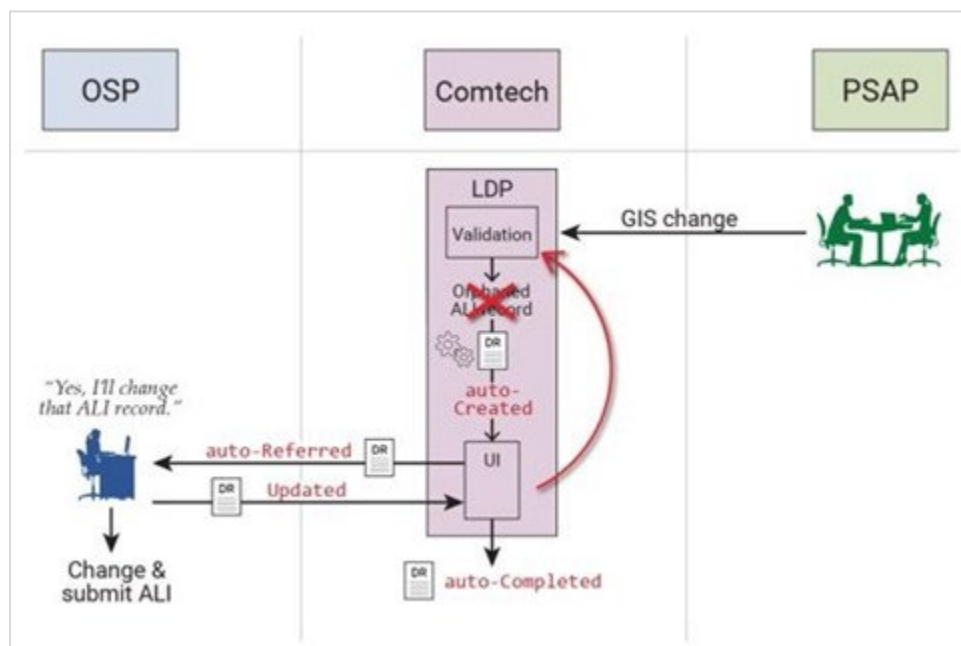


Figure 50. Auto Generated Discrepancy Report

In addition to providing process automation for discrepancy reporting, the Allerium Location Data Platform also retains the ability to manually create DRs as outlined in Figure 51 to support the ALI processes. Once generated, these DRs provide the same level of audit trail the automated processes provide.

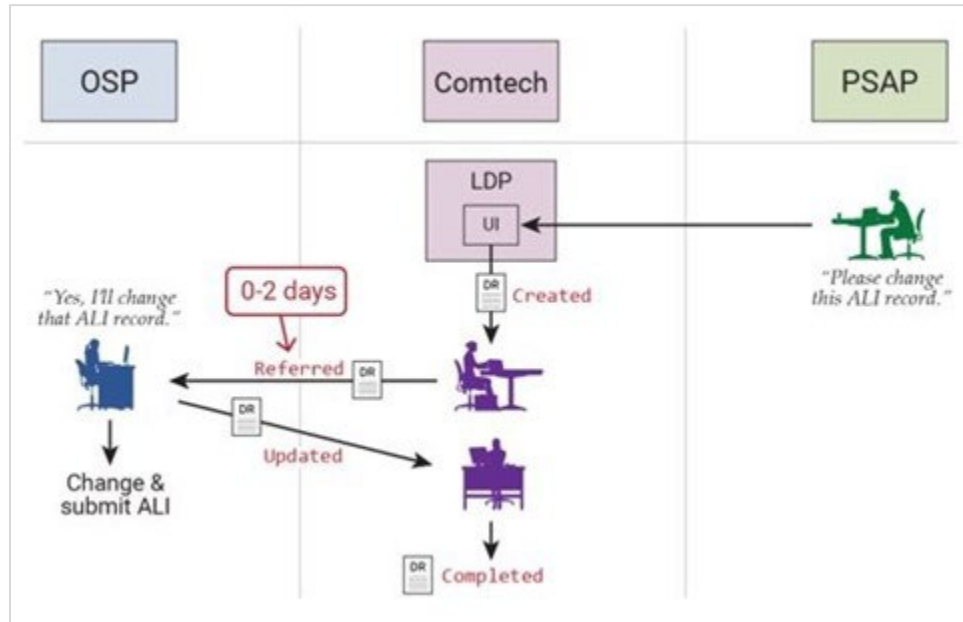


Figure 51. Manually Generated Discrepancy Report

Figure 52 and Figure 53 below outline the workflow process by which OSPs can request changes to the SPATIAL MSAG® as well as the approach and denial processes. Much like the DR process, the change request (CR) process provides a full audit trail for each step of the process.

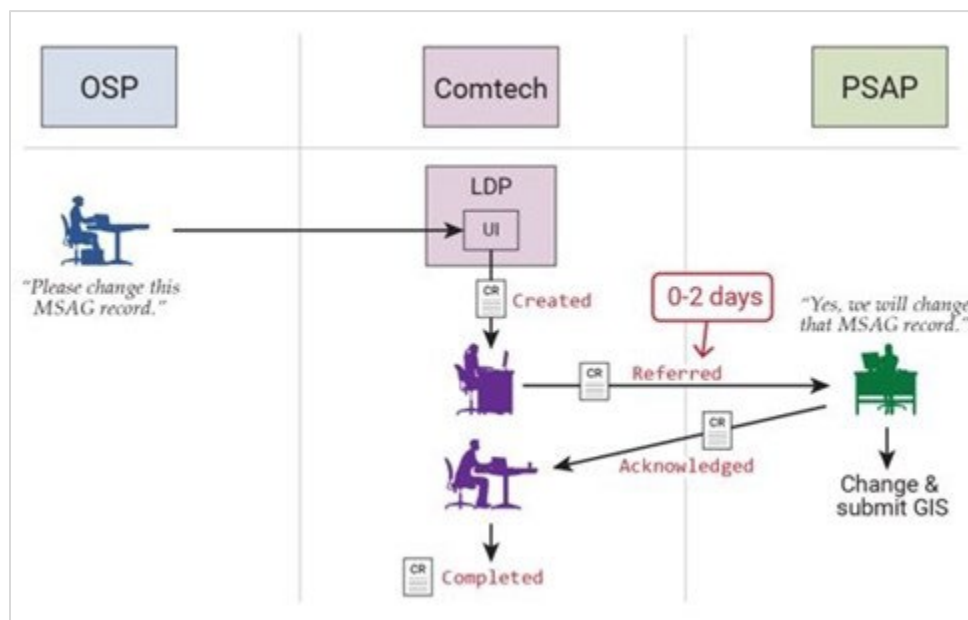


Figure 52. SpatialMSAG® Change Request

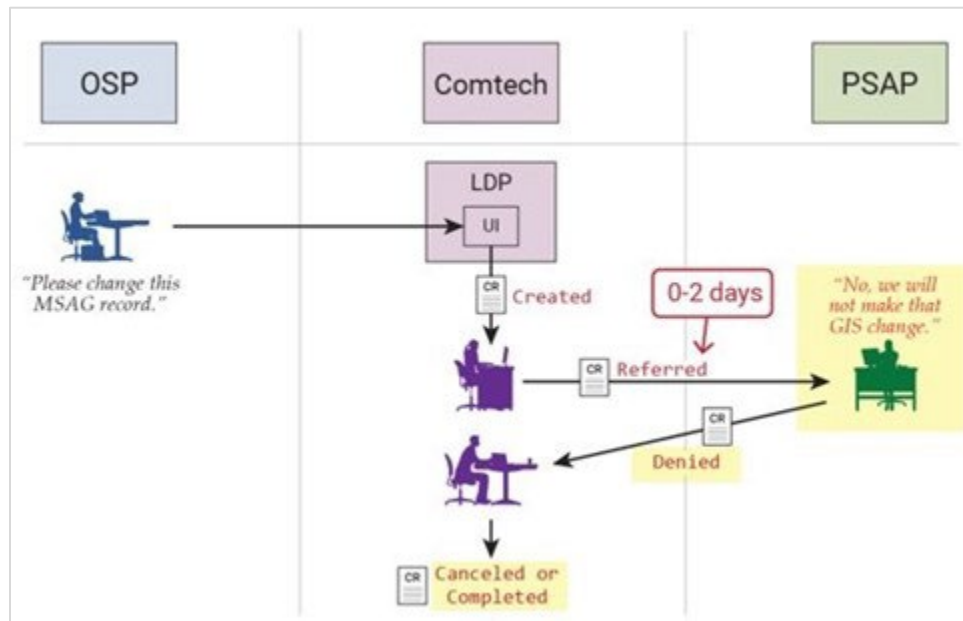


Figure 53. SpatialMSAG Change Request (Denied)

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.5.7.9. Test and Tools

5.5.7.9.1. Test Call Generator Discrepancy Report

5.7.9. Test and Tools

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).

Response:

Allerium's NGCS leverages internal test call subsystem which monitors the health of our solution. In the event that any discrepancy in the expected test call interval fails, the transaction details are logged and alarms are raised to our NOC in near real-time.

Allerium understands the desire to drive toward compliance with the full STA-010.3f end-state and plans to implement necessary subsystems within our NG Core in the next 12 months.

5.6. Installation Requirements [Project Requirements and Scope of Work, Section E.6]

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
 - o Ingress
 - o Core
 - o Egress
- Coordination with current 911 system service provider
 - o Ingress
 - o Core
 - o 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.

Response:

All aspects of the installation are incorporated into the Implementation plan, including coordination with applicable stakeholders for requirements, scheduling, and testing at a minimum. Installation activities and status as well as risks and dependencies are reported through established project schedule and implementation plan reviews.

5.6.1. Installation Services

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:*
 - o *Coordination with PSAPs*
 - o *System and service migration (i.e., logging, recording, CAD)*
 - o *UPS integration to support a minimum 3-hour backup validated with an MTTR / MTBF calculation*
 - o *Coordination with OSPs*
 - o *Coordination with current 911 system service provider*
- *Traffic migration*
- *Data migration*
- *Staging*
- *Acceptance testing*
- *Cutover planning*
- *Training*

Response:

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.

All installation and service migration activities are incorporated into, and tracked via, the Implementation plan. This includes identification and procurement or development of applicable components/services, coordination with stakeholders, testing of installed components/services and tracking of status and risks.

As detailed in previous sections, and in the sample Implementation plan, Allerium understands and has extensive experience executing on, requirements for installation and implementation of ESInet and Core services, Integration with 3rd party networks, PSAP integration and OSP Integration. The following sections provide more detail on the activities.

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.

Allerium's NG9-1-1 Aggregation Service provides the equipment and services to receive calls from Originating Service Providers and deliver those calls to the NGCS. The NG9-1-1 Aggregation Service establishes Point-of-Interconnect (POI) locations mutually agreed upon by the customer. The

following list provides critical activities that Allerium is responsible for related to installation and implementation of telecommunications companies 911 call delivery:

- Establish Data Center locations where POIs will be installed
- Ensure all applicable requirements related to power, cooling, and data center facility are met
- Procurement, Installation and Configuration of components utilized in for the POIs
- Establishment and tracking of network connectivity
- Testing of components, connectivity and 9-1-1 call delivery services

Allerium will work with the customer to develop a Network Disclosure package which is distributed to OSPs within the market. The network disclosure package includes applicable documentation such as LOAs, POI locations, and timelines for OSPs to connect to the NG system. OSPs will be asked to establish connectivity to the POI locations identified by the customer. OSPs will receive circuit ordering details as well as interface configuration specs. Prior to any OSP traffic migration, the OSP Acceptance Test Plan (ATP) outlined in previous section is performed by Allerium and each OSP.

The complete list of OSPs is identified through registration with state utilities commission (or appropriate agency), if available. Additional data sources includes review of existing ALI records and/or review of existing 911 connections into LSRs.

All activities related to communication and coordination with OSPs is tracked via the Implementation plan.

Plan to coordinate with all current 911 system service providers.

Allerium's NG9-1-1 Implementation plan includes outreach and coordination with current 911 system providers such as the incumbent NG911 provider, Legacy Selective Router and ALI providers, Call Handling Equipment providers and other service providers identified through data collection with the State and PSAPs.

Incumbent NG911 provider

To support the transition to Allerium's NG9-1-1 solution, it may be necessary to establish interconnection with the incumbent NG911 provider. Allerium's NG9-1-1 Aggregation Service includes the equipment and services to interconnect and pass traffic between the incumbent provider network and the Allerium NG911 system.

If this service is necessary, the interconnection is expected to be an IP-based network connection and will be designed to support both 911 ingress traffic as well as egress traffic for call transfers.

Installation and coordination of activities related to integration with the incumbent NG911 service provider are considered a part of the NG911 Aggregation Service and included with the activities outlined above.

Legacy Selective Router/ALI Providers

To support the transition to Allerium's NG9-1-1 solution, it is expected that Allerium will need to interconnect with Legacy Selective Routers (LSRs) that provide service to Nebraska PSAPs and surrounding areas. Allerium's NG9-1-1 Aggregation Service includes the equipment and services to

receive calls from the LSRs in SS7/TDM protocols and convert that traffic to SIP before delivering to the NGCS data centers.

Inter-tandem SS7/TDM trunks will be established from each Selective Router to Allerium SS7/TDM Points of Interconnect (POIs). These connections allow 9-1-1 calls from OSPs that are not yet directly connected to the NG9-1-1 Aggregation Service to be routed through the Allerium NG9-1-1 solution.

Inter-tandem trunks to the LSRs are also needed to support call transfers from PSAPs connected to the ESInet to legacy PSAPs still connected to an LSR.

Installation and coordination of activities related to integration with the incumbent NG911 service provider are considered a part of the NG911 Aggregation Service and included with the activities outlined above.

PSAP and Call Handling Equipment Providers

To support the transition to Allerium's NG9-1-1 solution, Allerium will interconnect with Call Handling Equipment (CHE) providers. The following provides critical activities related to installation and implementation of services with CHE providers and PSAPs

- Identify CHE facilities/locations Allerium will interconnect to
- Evaluation against mutually agreed-upon facility requirements such as UPS, cooling, and redundancy
- Track and ensure facility requirements are met prior to service migration
- Evaluation of CHE Hardware/Software readiness
- Track and ensure facility requirements are met prior to service migration
- Establish ESInet connectivity to appropriate locations
- Procurement, Installation and Configuration of components utilized for 911 traffic handoff from the Allerium ESInet to the CHE
- Configuration of CHE system to interface specifications provided by Allerium
- Testing of components, connectivity and 911 call delivery services

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

Allerium's NG9-1-1 Implementation plan includes installation and service migration tasks related to coordination with PSAPs/CHEs, OSPs and additional system providers such as CAD, Recording and logging services. The implementation plan is specifically designed to identify stakeholders, system/service providers, risks/dependencies and applicable tasks for successful integration. Additional details on each of these aspects are provided above.

Facility / Environmental requirements such as UPS, generator back, cooling and secure access are mutually agreed upon by Allerium and the state and documented in Allerium's Facility Requirements document.

The Facility Requirements document is shared with applicable stakeholders and evaluated via a site survey performed by Allerium. Conformance against Facility requirements are reported to the State and any non-conformances are tracked for update and completion.

Traffic migration

Traffic migration processes are detailed above in the implementation and transition sections of this RFP. Additionally, traffic migration processes are incorporated into the implementation plan and shared with stakeholders throughout pre-migration planning activities.

Data migration

Data migration activities are defined in the implementation plan. Key aspects of data migration include collection and provisioning of current ALI records, collection and provisioning of PSAP GIS data and collection and provisioning of PSAP, CHE and other system provider contacts.

Staging

Allerium will install the equipment into the POIs and perform acceptance testing. This work is done directly in the pre-production environment. There is no separate staging process apart from acceptance testing. Allerium's sample ATPs feature staging efforts and are included in Appendix 3: Sample ATPs.

Acceptance testing

Acceptance testing processes and approach for each aspect of installation and implementation are outlined above in the implementation and transition sections of this RFP. These details are documented in Acceptance Test Plan documents which are reviewed with the state and applicable stakeholders prior to commencement of testing activities.

Cutover planning

Cutover planning activities are incorporated into the implementation plan and project schedule. Allerium coordinates pre-migration cutover planning with PSAPs, CHEs, additional system providers and OSPs. Pre-migration cutover planning follows Allerium's 5 Phase implementation approach and is performed over multiple, recurring planning sessions with applicable stakeholders.

Training

Training activities are outlined in previous sections of this RFP response and are coordinated by Allerium based on the services/system used by each stakeholder and the timing of implementation of services. More specifically, Allerium provides training to the State, PSAPs, and OSPs on applicable tools, systems and services. Training is designed to occur at the optimal time within the implementation to ensure that the information is current and relevant to each use.

5.6.2. Wiring and Cabling

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*

Response:

Allerium's wiring and cabling work adheres to the requirements and standards listed above.

5.6.3. Grounding

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.

Remainder of page intentionally blank

Response:

Allerium's grounding work adheres to the requirements listed above.

5.7. Training [Project Requirements and Scope of Work, Section E.7]

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.

Response:

Allerium will work cooperatively with Nebraska's 911 Program Office and designated State and PSAP staff to ensure that all PSAP personnel — operators, supervisors, system administrators, and technical staff — are fully trained on Contractor-supplied software and equipment throughout the full term of the contract.

Allerium has a tradition of and reputation for state-specific NG9-1-1 training built across multiple statewide implementations. Each program is developed and delivered with the particular deployment, regional structure, and personnel needs of that state's 9-1-1 community in mind. Nebraska will benefit from that accumulated experience while receiving a training program tailored specifically to its seven regions and 68 PSAPs.

Training does not conclude at cutover. Allerium's commitment is ongoing — encompassing just-in-time delivery timed to each migration milestone, immediate support during the transition period, and structured refresher training as personnel change, system updates occur, or operational needs evolve. All sessions are recorded, edited, and indexed within Allerium's learning platform so that personnel can locate and access precisely what they need, when they need it, without waiting for a scheduled live session. On-demand sessions with a live instructor are available at the State's request throughout the contract term, to complement the recorded and indexed library as desired.

5.7.1. Audiences and Scope

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*

Response:

Allerium delivers role-based training designed around the specific operational responsibilities of each audience group — what each needs to understand, act on, and be accountable for within Nebraska's NG9-1-1 environment.

PSAP Operations personnel receive training covering network status monitoring and interpretation, help desk engagement processes, trouble ticketing procedures, and the full range of system features relevant to daily PSAP operations. Allerium has a consistent record of developing clear, authoritative training in step with new and evolving capabilities as they are introduced into the NG9-1-1 environment — ensuring that PSAP personnel are prepared and confident when those capabilities go live.

State-level operations personnel receive training on network status reporting, help desk processes, trouble ticketing workflows, and root-cause analysis and review procedures — equipping State

staff to monitor system performance, identify patterns, and engage effectively with Allerium's support and operations teams throughout the contract term.

In addition to both synchronous and a-sync online sessions, both audiences have access to Allerium's recorded, indexed training and documentation library throughout the contract, ensuring that personnel at every level can review, refresh, and onboard to current content at any time.

5.7.2. Training Elements

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*

Response:

Allerium's training program addresses all elements of the proposed ESInet and NGCS solution within its scope of delivery. Training is developed and maintained by a dedicated, experienced training team with deep familiarity with NG9-1-1 systems and PSAP operational environments across multiple statewide implementations.

System and Network Features

Training covers discrepancy reporting procedures, network status monitoring, trouble ticketing, and all operational features of Allerium's ESInet and NGCS solution relevant to PSAP and State-level personnel. As new capabilities are introduced or updated, training materials are revised accordingly and made available through Allerium's learning platform.

Equipment and Call Handling Functions

Features specific to call handling equipment — including login and logout procedures, password reset, call transfer, call conferencing, rebid/refresh of call information, and instant recorder/playback — are the training responsibility of the designated CHE vendor providing that equipment to Nebraska's PSAPs. Allerium will coordinate with the applicable CHE vendor to ensure that PSAP personnel receive complete, integrated training coverage across all system components prior to cutover.

Equipment Problem Reporting

PSAP personnel will be trained on Allerium's trouble ticketing and incident reporting process for issues related to ESInet and NGCS components. CHE-specific hardware problem reporting procedures will be addressed within the CHE vendor's training program.

Language Access

Allerium will work cooperatively with the State to address Nebraska's foreign language interpretation process requirements, consistent with applicable federal language access standards and Nebraska's operational needs as defined during the planning process.

Emerging and Evolving Capabilities

Allerium maintains a consistent record of developing and integrating training for new and evolving capabilities as they are introduced into the NG9-1-1 environment, ensuring PSAP personnel are prepared when those capabilities go live in Nebraska's deployment.

5.7.3. Technical Assistance

7.3. Technical Assistance

Upon request by the State, the Contractor shall provide technical assistance to PSAP personnel during training and testing.

Response:

Allerium provides technical assistance to PSAP personnel during training and testing upon request. Our training team operates as an integrated part of a support structure that connects directly with Allerium's NOC, engineering, client services, and project management staff — ensuring that technical questions arising during training reach the right people without delay and come back to PSAP personnel in clear operational terms.

Nebraska's 911 Program Office and PSAP staff will have established named points of contact throughout the deployment, consistent with the coordinated approach Allerium continuously develops and applies across its statewide implementations.

5.7.4. Schedule and Locations

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.

Response:

Allerium will complete training for all PSAP personnel — including State and administrative personnel assigned to the PSAP — no later than fourteen (14) calendar days prior to each PSAP's cutover date. Managing pre-cutover training across large, regionally structured deployments is familiar territory; Allerium has coordinated this successfully across multiple statewide implementations and brings that logistical experience directly to Nebraska's seven regions and 68 PSAPs.

Allerium's online training environment is available around the clock, and sessions are recorded, indexed, and accessible at any time, allowing personnel to complete, review, and be assessed and certified on their own schedule. On-site delivery at temporary training facilities within Nebraska, including weekend and evening sessions, is equally a standard part of how Allerium works — whatever combination best serves the State's deployment schedule and its personnel.

5.7.5. Training Materials

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.

Response:

Allerium will develop and deliver a complete Train-the-Trainer (TtT) curriculum submitted for State approval prior to delivery. Train-the-Trainer is not an ancillary offering: it is fundamental to how Allerium approaches every deployment. The goal is not to create dependence on Allerium's presence but to build genuine expertise within Nebraska's own 9-1-1 community, so that the State's personnel can train, assess, and certify their colleagues with confidence and authority as desired.

TtT materials include complete facilitation guides, assessment instruments, and platform access enabling certified trainers to enroll participants, track progress, and document completion — drawing on the same recorded, indexed, and around-the-clock online environment available to all Nebraska personnel throughout the contract.

All training materials — both those delivered directly by Allerium and those comprising the TtT curriculum — will be maintained in current, up-to-date form and available to the State for the full duration of the contract, updated as system changes or upgrades warrant.

5.7.6. Post-Deployment Training and Costs (Proposal Requirement)

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.*

Response:

Provide a proposed cost for post-deployment training for up to fourteen (14) students per class

Allerium provides post-deployment instructor-led training designed to ensure that Nebraska's 9-1-1 community retains operational proficiency throughout the full contract term — accommodating personnel transitions, system updates, and evolving operational requirements as they arise.

Post-deployment training sessions are delivered by the same seasoned training staff who conducted the initial program, with materials updated to reflect the current state of the system at the time of delivery. Each session includes instruction, interval assessment, and end-of-course certification documentation maintained within Allerium's learning platform.

The proposed cost for post-deployment training for up to fourteen (14) students per class is included in our Cost Proposal.

Provide a proposed cost for the post-deployment TtT course, including the maximum class size.

The TtT post-deployment course refreshes and recertifies designated State or PSAP trainers, incorporating any system changes since original certification. Maximum class size for TtT sessions is determined in coordination with the State based on the number of designated trainers requiring recertification at the time of delivery.

The proposed cost for the post-deployment TtT course is included in our Cost Proposal.

5.7.7. Comprehension, Testing, and Certification

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.

Response:

Allerium applies a structured assessment framework throughout initial and ongoing training — not only as a compliance exercise, but as a genuine measure of whether each participant has the knowledge and confidence to operate effectively in Nebraska's NG9-1-1 environment.

Interval Testing

Knowledge checks are administered at defined points within each training sequence, allowing the delivering instructor to identify comprehension gaps and address them before the participant moves forward. This approach reflects Allerium's micro-learning methodology — content is sequenced to match what each role needs at each stage of the deployment, and assessment confirms that the sequencing is working.

Instructional Methods

Sessions incorporate lectures, group discussion, audiovisual materials, role-playing exercises, and hands-on system interaction. Delivery format is calibrated to audience and content — technical staff and PSAP operators receive instruction appropriate to their roles and responsibilities.

Final Evaluation

Nebraska's requirement for a final per-student knowledge evaluation reflects a serious and commendable commitment to verified competency rather than attendance alone. Allerium shares that commitment. Each student receives a final evaluation upon course completion, incorporating written, oral, and hands-on components as appropriate to the course. Results are documented and maintained within Allerium's learning platform, available to the State upon request throughout the contract term.

End-of-Course Certification

Students who successfully complete required assessments receive end-of-course certification. Certification records are maintained within the platform, providing the State with a verifiable, ongoing record of trained and certified personnel across all seven regions and 68 PSAPs.

5.7.8. Training Plan and Samples (Proposal Requirement)

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.*

Remainder of page intentionally blank

Response:

Allerium's proposed training plan for Nebraska's NG9-1-1 deployment is included in Appendix 7: Sample Training Plan as a companion document to this response and details the full course catalog organized by audience, with course descriptions, learning objectives, delivery methods, and timing relative to each region's cutover schedule. Sample course materials illustrating the depth and format of content Nebraska's personnel will receive are included as exhibits within that document.

The plan addresses all topics and audiences identified in Section E-8.1 and E-8.2, organized across Allerium's two primary delivery tracks — Regional and State Authority sessions and PSAP sessions — sequenced to deliver the right content to the right audience at each stage of Nebraska's seven-region deployment.

All materials will be adapted to Nebraska's specific system configuration, regional structure, and operational terminology, and submitted for State approval prior to delivery. Materials are maintained in current form throughout the contract term, updated as system changes or upgrades warrant, and accessible at any time through Allerium's learning platform.

5.8. Operations and Service Management Requirements [Project Requirements and Scope of Work, Section E.8]

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.

Response:

Allerium fully understands and complies with this requirement and provides a comprehensive Operations and Service Management framework designed to support mission-critical NG911 environments.

Service Support and Integration

Allerium serves as the central operational authority for all NG911 service support, coordinating across internal teams, partners, and subcontractors to ensure seamless service delivery.

Allerium's NOC and Service Operations teams provide 24x7x365 oversight and management of all system components, ensuring:

- End-to-end service visibility across ESInet, NGCS, and integrated partner systems
- Centralized incident ownership and coordination
- Integrated communication and escalation across all involved parties

Through established processes and eBonding capabilities, Allerium ensures full lifecycle management of incidents, changes, and service requests across all stakeholders.

Service Levels and Escalation

Allerium commits to meeting or exceeding the defined service levels, including:

- 99.999% availability for core voice paths
- Mean Time to Repair (MTTR) of less than 2 hours for Priority 1 incidents
- Defined response and acknowledgment times, including rapid initial engagement (e.g., within 15 minutes or better)
- Allerium enforces these commitments through:
- Structured incident classification (SIL-based severity model)
- Defined escalation paths with rapid engagement of Tier 2, Engineering, Field Services, and vendor resources
- Formal Major Incident Management processes for high-impact events

- Continuous SLA tracking and reporting

All SLA breaches trigger formal Root Cause Analysis (RCA) processes, with documented corrective actions and accountability measures. Where applicable, SLA performance frameworks may include penalty provisions aligned with contractual requirements.

Operations Enablement

Allerium provides a comprehensive operations enablement program to ensure all stakeholders are fully prepared to support and interact with the NG911 system.

This includes:

- Role-based training programs, delivered both in-person and virtually
- Structured onboarding and certification pathways for PSAP operators, network administrators, and GIS personnel
- Detailed operational runbooks covering common and critical scenarios, including failover procedures, GIS updates, and incident response workflows
- Ongoing training updates aligned with system enhancements and operational changes

All documentation and training materials are aligned with NENA functional-element nomenclature to ensure clarity and consistency across stakeholders.

Change Management

Allerium maintains a mature, fully documented Change Management framework aligned with industry best practices and NG911 operational requirements.

Key elements include:

- Formal Change Advisory Board (CAB) governance
- Documented change-control procedures, including risk assessment and impact analysis
- Defined rollback and contingency planning for all applicable changes
- Scheduled maintenance activities conducted during approved windows and in accordance with no-downtime requirements
- Advance notification (minimum 30 days) for changes impacting routing, GIS, or call handling

This structured approach ensures that all changes are executed in a controlled, low-risk manner that preserves system stability and service continuity.

Standards Conformance and Interoperability

Allerium's NG9-1-1 solutions are designed and operated in accordance with NENA i3 and NGCS standards.

Allerium demonstrates compliance through:

- Formal self-attestation to applicable standards
- Participation in multi-vendor interoperability events, including NENA ICE

- Proven interoperability with third-party systems and components, including CHE from multiple vendors

Testing and validation processes incorporate NENA-defined call flows and functional requirements to ensure full interoperability across the NG911 ecosystem.

Testing Program

Allerium executes a comprehensive, phased testing program to ensure system reliability, performance, and security.

The testing program includes:

- Unit and component-level testing
- Integrated system testing across all functional elements
- Failover and resiliency simulations
- Performance and load testing, including validation at 200% of peak capacity
- Security validation aligned with NENA standards and best practices

All critical workflows must meet 100% success criteria prior to production deployment.

Product Documentation

Allerium provides complete and structured product documentation to support all operational stakeholders.

Deliverables include:

- Detailed user manuals tailored to PSAP operators, administrators, and technical staff
- API specifications provided in OpenAPI format where applicable
- Release notes documenting system updates, enhancements, and changes
- Comprehensive operational documentation aligned with NENA terminology

All documentation is maintained as a living knowledge base and updated regularly to reflect system and operational changes.

Summary

Through its integrated NOC operations, structured service management framework, and adherence to industry standards, Allerium delivers a reliable, scalable, and fully supported NG911 environment that meets the operational and life-safety expectations of the State.

5.8.1. Service Management Framework

5.8.1.1. Service Management Plan

8.1.	Service Management Framework
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

Response:

Service Management Plan Overview

Allerium's Service Management Plan is built on industry best practices aligned with the Information Technology Infrastructure Library (ITIL) framework. Allerium incorporates the full service lifecycle—Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement to ensure that NG911 services are designed, implemented, and operated with a focus on reliability, resilience, and performance.

This framework ensures that all services maintain required levels of availability, capacity, security, and operability, while enabling structured governance, measurable performance, and continuous improvement throughout the contract lifecycle.

Integrating Service Management Approach into Project Management Activities

Allerium integrates service management directly into project management activities to ensure a seamless transition from implementation to steady-state operations.

During project execution, service management components—including monitoring, incident management, change control, and escalation procedures—are defined, validated, and operationalized prior to go-live. Operational readiness activities include documentation development, training, process validation, and system integration with ITSM and monitoring platforms.

This approach ensures that upon transition, the NG911 system is fully supported by mature operational processes with no gap between deployment and ongoing service management.

Ability to Maintain Consistent Performance and the Service Levels of the Network

Allerium maintains consistent performance and adherence to service levels through continuous monitoring, proactive operational management, and structured governance processes.

Key practices include:

- 24x7x365 NOC monitoring and response
- Real-time performance and availability tracking
- SLA measurement and reporting
- Incident, problem, and change management aligned with ITIL
- Regular operational reviews and continuous improvement initiatives
- This ensures sustained network reliability and alignment with contractual service expectations.

Framework for Consistent Performance and the Service Levels of the Network

Determination of the Single Point of Contact

Allerium provides a centralized single point of contact (SPOC) through its 24x7x365 NOC/Help Desk.

All PSAPs, State personnel, and partners engage through this centralized entry point for incident reporting, service requests, and operational communications. The NOC maintains ownership of all tickets and coordinates resolution activities across all involved teams and providers.

Management of Subcontracted Support Components

Allerium maintains full operational ownership of all subcontracted components and services.

Through established processes and eBonding capabilities, Allerium ensures:

- Seamless integration with subcontractor ticketing systems
- Real-time visibility into subcontractor activities
- Coordinated escalation and resolution management
- Allerium remains accountable for end-to-end service delivery, regardless of subcontractor involvement.

Support Personnel Required and Identification of Key Personnel

Allerium provides a structured support organization consisting of Tier 1, Tier 2, Engineering, Field Services, and Service Operations personnel.

Key personnel roles are clearly defined and include operational leadership, incident management, and technical escalation resources. Staffing models ensure appropriate coverage, expertise, and responsiveness to meet NG911 operational requirements.

Third-Party Support Contracts

Allerium manages all third-party support contracts to ensure alignment with NG911 service requirements.

This includes coordination of vendor support, enforcement of performance expectations, and integration into Allerium's incident and escalation processes. Third-party providers are held to the same operational standards required under the contract.

Pre-Emptive Support

Allerium ensures consistent network performance and adherence to service levels through a proactive, pre-emptive support model designed to identify and address potential issues before they impact service.

This approach includes continuous 24x7x365 monitoring of the ESInet, NGCS, and all supporting infrastructure, with automated alerting and real-time performance visibility. Allerium leverages trend analysis, problem management practices, and historical data to identify recurring patterns, degradation indicators, and emerging risks.

Pre-emptive support activities include:

- Proactive identification and remediation of potential faults or performance degradation
- Problem management processes to address root causes before incidents occur
- Capacity and performance monitoring to prevent resource constraints
- Preventative maintenance and system health checks
- Coordination with vendors and partners to resolve known issues in advance of impact

Through these practices, Allerium minimizes incident occurrence, reduces service disruptions, and ensures sustained compliance with SLA performance targets, supporting the reliability and resilience required for NG911 operations.

Equipment Refreshes

Allerium maintains consistent performance and service levels through a proactive equipment lifecycle management and refresh program. Hardware is tracked against vendor support timelines, performance metrics, and end-of-life status to ensure timely refresh before service degradation occurs.

All refresh activities are planned in coordination with the State and executed under formal Change Management processes, including risk assessment, MOPs, and rollback procedures. This approach ensures infrastructure remains current and reliable while maintaining uninterrupted service and SLA compliance.

Preventative Maintenance

Allerium ensures consistent network performance and adherence to service levels through a structured preventative maintenance program.

Maintenance activities are proactively scheduled based on manufacturer recommendations and operational best practices to maintain system health and reliability. All activities are executed under formal Change Management processes, including MOPs, risk assessment, and rollback procedures, ensuring no impact to service availability.

This proactive approach reduces the likelihood of failures and supports sustained SLA performance for NG911 operations.

Bug Fixes

Allerium ensures consistent network performance and SLA adherence through a structured bug fix and defect management process.

All identified defects are tracked within the ITSM system, prioritized based on impact and severity, and coordinated with engineering teams and vendors for timely resolution. Fixes are tested and validated prior to deployment and implemented through formal Change Management processes to ensure system stability.

This disciplined approach minimizes risk and ensures reliable, uninterrupted NG911 operations.

Patching and Upgrades

Allerium ensures consistent network performance and SLA adherence through a controlled patching and upgrade management process.

All patches and system upgrades are evaluated for risk and impact, tested and validated prior to deployment, and executed under formal Change Management processes, including MOPs and rollback procedures. Activities are scheduled to avoid service disruption and maintain continuous availability.

This approach ensures systems remain secure, up-to-date, and fully capable of supporting NG911 service requirements.

Warranty

Allerium ensures consistent network performance and SLA adherence through active warranty management of all covered components.

Warranty status is tracked across all assets to ensure timely repair or replacement of defective equipment in accordance with manufacturer agreements. Coordination with vendors is managed through established support processes to expedite resolution and minimize service impact.

This approach ensures rapid remediation of hardware issues and supports continuous, reliable NG911 operations.

Out of Warranty Items

Allerium ensures consistent network performance and SLA adherence through proactive management of out-of-warranty assets.

Out-of-warranty components are tracked and assessed based on risk, performance, and criticality. Allerium provides recommendations for repair, replacement, or upgrade, coordinated with the State to maintain system reliability.

All actions are planned and executed under formal Change Management processes to prevent service impact and ensure continued support of NG911 operations.

Service Level Agreements

Allerium ensures consistent network performance through the establishment, monitoring, and enforcement of Service Level Agreements (SLAs) aligned with NG9-1-1 operational requirements.

SLA metrics—including availability, response times, and MTTR—are continuously tracked through the NOC and ITSM platforms. Performance is reported regularly and reviewed with the State to ensure transparency and alignment.

Any SLA deviations trigger formal review and corrective action processes, ensuring continuous improvement and sustained compliance with service expectations.

5.8.1.2. Service Level Agreement (SLA)

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.

Response:

Allerium’s sample Service Level Agreement (SLA) describes the support services and the respective responsibilities of Allerium and the State.

The purpose of this sample SLA is to (1) identify the levels of service delivered by Allerium to the State; (2) define information required to be provided by both Allerium and the State for the delivery of the desired levels of service; and (3) ensure delivery of certain information to Allerium and State personnel who need such information in support of the System.

Allerium’s service shall be provided per the descriptions in our sample SOW in Appendix 11: Sample SOW. SLAs are applicable to Allerium’s Service span of control. Issues outside Allerium’s span of control shall not be considered in scope in this document.

SLA Categories and Assistance

Allerium has mapped the State-expected SLA categories and assistance to its standard severity levels and levels of assistance as defined below.

Table 61. Levels of Assistance

Point of Contact	Expected Level of Assistance
Tier 1	Capture and triage
Tier 2	Mitigation/resolution
Tier 3	Advanced system analysis and troubleshooting/resolution
Tier 4	Release and patch changes

Allerium assesses the required level of technical expertise through the process of responding to a trouble ticket and engages the appropriate technical support personnel. Allerium has a multi-layered support organization that consists of the following personnel:

- **Tier 1:** Responsible for monitoring systems, remediating issues when possible, managing the trouble ticket process through to resolution, and communicating updates to customers.
- **Tier 2:** Provides the first tier of escalation for NOC/SOC technicians. Tech support technicians are capable of resolving a wide range of issues within an Allerium solution.
- **Application Engineers:** Tier 3 technical staff focused within a specific Allerium application platform. Application engineers focus on the operation of NGCS platforms.
- **Network Engineers:** Tier 3 technical staff focused on network technologies. Network engineers provide escalation path support and work closely with application engineers to resolve technical issues.
- **Development:** Tier 4 role to address required code changes.

Table 62. Mapped Severity Levels and Assistance

State-Expected SLA Category	Allerium Severity Level	Allerium Description of Problem	State-Expected Assistance and Timeframe	Allerium Assistance and Timeframe
Critical – Network Outage	SIL 1	An incident shall be categorized as a “Severity 1 Incident” if the incident is characterized by the following attributes: a. Renders a business-critical	• 1st Level Support – Immediate • Continuous problem resolution / workaround effort • 2nd Level Support – within 15 minutes	• Tier 1 Support provides immediate capture/triage • Continuous problem resolution / workaround effort

State-Expected SLA Category	Allerium Severity Level	Allerium Description of Problem	State-Expected Assistance and Timeframe	Allerium Assistance and Timeframe
		system, service, software, equipment, or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work. b. Affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.	3rd Level Support – within 30 minutes or upon Customer request	- Tier 2 Support assigns/dispatches applicable support teams within 15 minutes - Tier 3 Support provides advanced system analysis and troubleshooting within 30 minutes
Major – Service effecting	SIL 2	An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes; an incident that: a. Does not render a business-critical system, service, software, equipment, or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work. b. Affects either (i) a group or groups of people, or (ii) a single individual performing a	1st Level Support – Within 5 minutes 2nd Level Support – Within 30 minutes 3rd Level Support – Within 2 Hours or upon Customer request	- Tier 1 Support provides immediate capture/triage - Tier 2 Support assigns/dispatches applicable support teams within 30 minutes - Tier 3 Support provides advanced system analysis and troubleshooting within two hours

State-Expected SLA Category	Allerium Severity Level	Allerium Description of Problem	State-Expected Assistance and Timeframe	Allerium Assistance and Timeframe
		critical business function.		
Minor – Non-service effecting	SIL 3	An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes: a. An incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment, or network component or a key feature thereof and a reasonable workaround is not available but does not prohibit the execution of productive work.	1st Level Support – Within 30 minutes 2nd Level Support – Within 2 Hours 3rd Level Support – Within 1 business day or upon Customer request	- Tier 1 Support provides capture/triage within 30 minutes - Tier 2 Support assigns/dispatches applicable support teams within two hours - Tier 3 Support provides advanced system analysis and troubleshooting within one business day

Service Impairment Levels

Allerium defines four SILs as shown in Table 63. The SIL determines the responsibilities of the Allerium NOC/SOC when responding to a system impairment which is within the systems or the service parameters that are the obligation of Allerium to provide under this SLA.

Table 63. SIL Levels

Severity Level	Description of Problem	Response Time (Max)	Notification Time (Max)	Target Resolution Time (Max)
SIL 1	An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes: a. Renders a business-critical system, service, software, equipment, or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work.	15 minutes	30 minutes	Four hours

Severity Level	Description of Problem	Response Time (Max)	Notification Time (Max)	Target Resolution Time (Max)
	b. Affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.			
SIL 2	An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes; an incident that: a. Does not render a business-critical system, service, software, equipment, or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work. b. Affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.	30 minutes	30 minutes	Eight hours
SIL 3	An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes: a. An incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment, or network component or a key feature thereof and a reasonable workaround is not available but does not prohibit the execution of productive work.	Two hours	Eight hours	48 hours
SIL 4	An incident shall be categorized as a "Severity 4 Incident" if the incident is characterized by the following attributes: a. An incident may require an extended resolution time but does not prohibit the execution of productive work and a reasonable workaround is available.	12 hours	24 hours	96 hours

5.8.1.3. Compliance and Risk Management

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.

Response:

While enterprise risk governance may be shared across organizational and partner domains, Allerium implements a structured, operationally focused approach to risk identification, tracking, and mitigation through its established Problem Management, Change Management, and Service Operations frameworks.

Allerium's approach is centered on identifying and managing risks that directly impact NG9-1-1 service delivery, including call routing, location accuracy, availability, latency, and overall system resilience.

Risk Identification and Management Approach

Allerium leverages its Problem Management process as the primary mechanism for identifying and managing operational risks. Risks are typically identified through:

- Incident trends and recurring issues
- Root Cause Analysis (RCA) outcomes
- Monitoring and alerting systems
- Vendor and partner escalations

- Change and release activities

Each identified issue or risk condition is documented as a Problem record, with associated Problem Tasks used to track investigation, mitigation, and resolution activities.

These records include:

- Affected asset or system component (ESInet, NGCS, etc.)
- Description of the issue or vulnerability
- Impact assessment (e.g., service availability, latency, call delivery)
- Severity and prioritization
- Assigned ownership and remediation actions

Risk Treatment and Tracking

Allerium applies practical risk treatment strategies aligned with operational best practices, including:

- Reduction through corrective actions and system improvements
- Avoidance via controlled change management and preventative measures
- Mitigation through redundancy, failover, and workaround strategies

All remediation efforts are tracked through Problem and Change Management workflows to ensure accountability, visibility, and completion.

Third-Party Risk and Visibility

Allerium maintains visibility into third-party risks through:

- Integrated ticketing (eBonding) with vendors and subcontractors
- Escalation processes aligned with SLA commitments
- Active coordination during incidents and problem resolution

While direct control of third-party environments may be limited, Allerium ensures that risks impacting NG9-1-1 services are actively tracked, escalated, and mitigated through coordinated response efforts.

Review Cadence and Continuous Improvement

Problem records and associated risks are reviewed on a regular cadence, including:

- Daily operational reviews for active issues
- Ongoing tracking through Service Review Meetings and Problem Management workflows
- Post-incident RCA reviews to identify systemic risks and required improvements

High-impact issues are prioritized and tracked through to resolution, with progress monitored and reported to stakeholders as appropriate.

Non-Compliance and Corrective Action

Any identified gaps, non-compliance conditions, or operational risks are documented and addressed through Problem Management and Change Management processes.

Corrective actions are defined, tracked, and validated to ensure resolution. Where required, Allerium coordinates with the State and relevant stakeholders to review findings and align on remediation strategies.

Summary

Through its integrated Problem Management and Service Operations framework, Allerium provides a structured and effective approach to identifying, tracking, and mitigating risks that impact NG9-1-1 operations, ensuring continued service reliability and alignment with contractual and operational expectations. Activities related to risk identification and mitigation, as well as status of associated problem records and change management activities, are provided to the State via ongoing Service Review Meetings.

5.8.1.4. Monthly Project Review and Compliance

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).*
 - o *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.*

Response:

During project implementation project, Allerium will organize and lead Project Status Meetings with the State and requested representatives. Project Status Meetings will be set up at the desired cadence of the State and can be adjusted as needed throughout the project. Both parties have input on the agenda, but, at a minimum, Project Status Meetings will provide visibility on the following items:

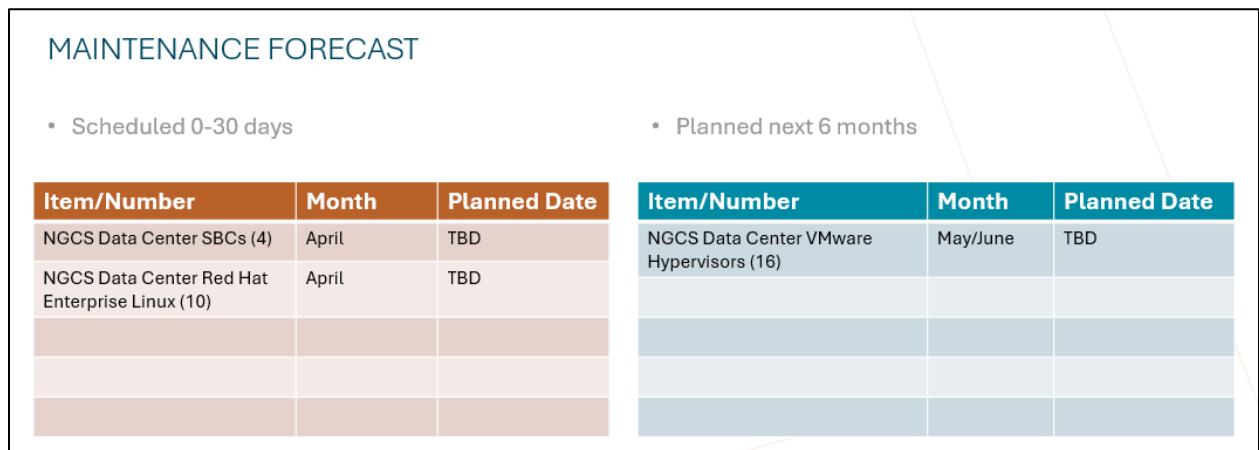
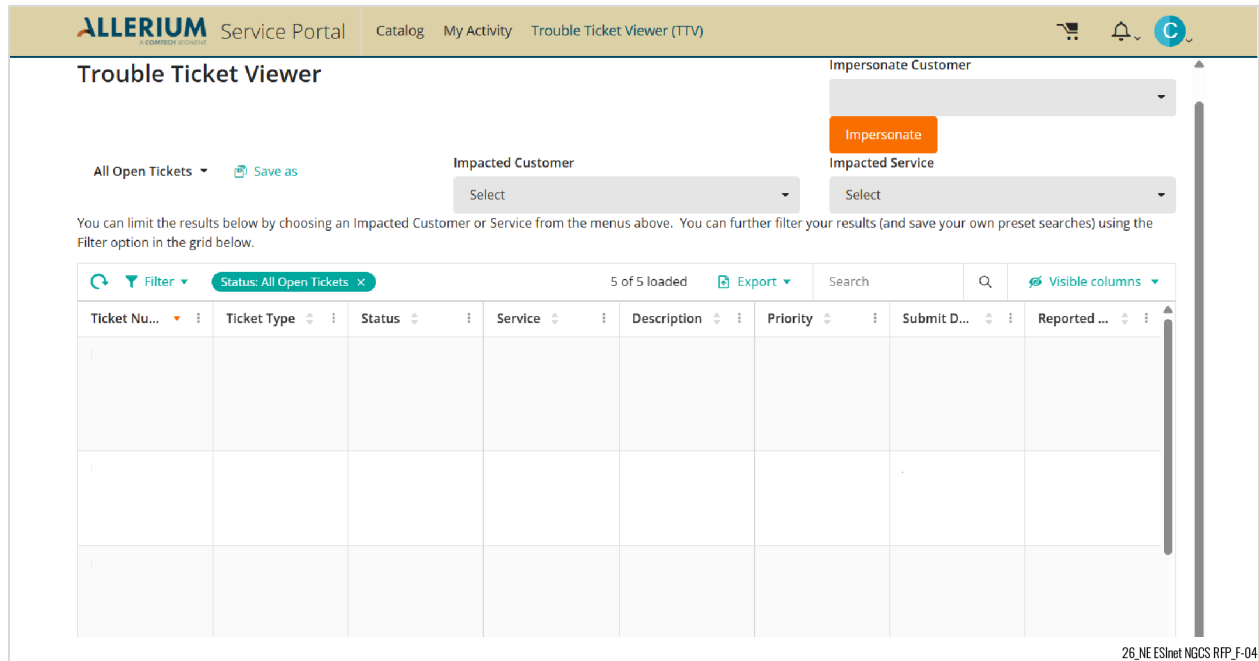
- Status/progress toward project milestones and critical path activities
- Identified risks and risk mitigation plans
- Changes to project schedule
- Review of documents such as network designs, testing plans, user guides, SOPs, etc.

In addition to project status meetings, Allerium recommends topic-specific meetings as needed. Examples of topic specific meetings include PSAP migration requirements and planning, OSP migration planning, GIS data readiness.

As we move from the implementation phase into the operation and maintenance phase, Allerium will organize and lead Service Review Meetings with the State and requested representatives. Service Review Meetings will be set up at the designed cadence of the State and will continue through the contract term. Both parties have input on the agenda, but at a minimum Service Review Meetings provide visibility and reporting on the following items:

- Organization processes and changes
- Progress against open issues/tickets
- Prioritization of open issues/tickets
- Planned maintenance activities
- Service performance/compliance levels
- Support performance/compliance levels
- RCA/RFO status and corrective actions
- System issues
- Security issues

The following images provide examples of how service-related activities are tracked and reported in Service Review Meetings.



SERVICE PERFORMANCE/COMPLIANCE LEVELS

Months:	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sept-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25
Total Seconds in month	2,678,400	2,592,000	2,678,400	2,592,000	2,678,400	2,678,400	2,592,000	2,678,400	2,592,000	2,678,400	2,678,400	2,419,200
Seconds ESInet Available	2,678,400	2,592,000	2,678,400	2,592,000	2,678,400	2,678,400	2,592,000	2,678,400	2,592,000	2,678,400	2,678,400	2,419,200
Seconds ESInet unavailable	0	0	0	0	0	0	0	0	0	0	0	0
% time ESInet was Available	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Figure 56. Service Performance/Compliance Levels

RCA/RFO STATUS AND CORRECTIVE ACTIONS

Description	Date	Detail	No.	Issue	Status
INC000000xxxxxx	XX/XX/XX	Preliminary RCA: Due XX/XX/XX (Delivered) Final RCA: Due XX/XX/XX (In Progress)	1	Sample Corrective Action 1	Complete
			2	Sample Corrective Action 2	In progress
			3	Sample Corrective Action 3	In progress

Figure 57. RCA/RFO Status and Corrective Actions

5.8.2. Continuity and Resilience

5.8.2.1. Availability

8.2. Continuity and Resilience

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

Response:

Availability Overview

Allerium's service is designed for continual operation at 99.999% availability. Each element in the call flow path is redundant and operating across three load-balanced data centers, each with two locally redundant application stacks. Combined with our fiber-based diverse ESInet, all IP path/call services/data transactions are maintained at 99.999% availability.

99.999% availability for IP path/call services/data transactions end-to-end (with caveat for non-redundant PSAPs).

Allerium maintains 99.999% availability for the IP path. By way of example the following represents an analysis for a single router at the PSAP edge. This is important to realize as this calculation represents a situation in which only a single router is analyzed. However, every PSAP has dual routers deployed for redundancy which enhances availability much beyond this single element calculation. For clarity, this calculation is provided as an easy-to-understand example of how we calculate MTBF and uptime calculations.

Using the availability formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$

For 99.999% availability ($A = 0.99999$) and $MTTR = 2$ hours:

$$\begin{aligned} 0.99999(MTBF + 2) &= MTBF \\ 0.99999 \cdot MTBF + 1.99998 &= MTBF \\ MTBF - 0.99999 \cdot MTBF &= 1.99998 \\ 0.00001 \cdot MTBF &= 1.99998 \\ MTBF &= \frac{1.99998}{0.00001} \approx 199,998 \text{ hours} \end{aligned}$$

Therefore, the mean time between failures (MTBF), of a single router supporting this PSAP, would be approximately 22.8 years, assuming that a router replacement took 2 hours to complete. For reference, the MTBF of the routers we use in our PSAP deployments is 27.4 years, meaning even a single router (no redundancy) technically meets the uptime requirements for a 5-9s service.

However, Allerium never deploys a single router (or any other piece of equipment), and instead uses redundant high availability (HA) routers at the edge. Repeating the above calculation, with a MTTR of 1 second (an appropriate approximation for HA "failover" time), the resulting calculation yields a MTBF of 28 hours. Meaning, a router could fail at the PSAP every 28 hours and still maintain 5-9s availability.

99.9% for non-call provisioning

Allerium supports the 99.9% non-call provisioning requirement for functions outside of the call path. Typically, these are provisioning or database services that rarely have issue but are allowed some leeway in availability given they are non-call processing.

5.8.2.2. Continuity of Operations Plan (COOP)

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.

Response:

Allerium maintains policy, plan and controls structure to enable the continuation of critical business processes, information systems, and essential missions while operating in other than normal conditions.

The BCP contains the following:

- Identify risks and threats to the business unit functions and essential missions.
- Coordinate with related plans that have been identified as dependencies by the BIA (internal or external).
- Identify the contingency scopes (examples):
 - Full mission outage.
 - Partial mission outages
 - Business function failure
- Establishes response strategies relative to risks, threats, and scopes.
- Establishment of contingency roles, responsibilities, and assigned individuals with contact information.
- Establishment of Plans for communicating with the following internal and external dependencies as needed and authorized by Allerium T&W Leadership:
 - Key decision makers.
 - Key personnel participating in recovery.
 - General personnel/ workforce team members.
 - Customers and Suppliers.
 - Regulatory authorities.
 - The Public (as needed).
- Establishment of recovery objectives and measurements, restoration priorities.
- Establishment of Recovery Time Objective (RTO) according to each system-specific Contingency Plan
- Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure.
- Establishment of procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.
- Establishment of eventual full system restoration without deterioration of the security measures originally planned and implemented:
 - Establishment of alternative processing and storage recovery sites.
 - Establishment of alternative networking circuits.
 - Establishment of funding methods for recovery.

Allerium has included Appendix 9: Sample BCP for the State's review.

5.8.2.3. Disaster Recovery (DR)

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.*

Response:

Allerium maintains policy, plan and procedures for managing a structured approach for recovery of critical business processes and functions, essential missions and information systems. The Disaster Recovery Plan contains the following:

- Short-term methods to return to immediate operations in the event of a failure of a process, facility, service, information system, or component.
- Detailed long-term plans for the return to normal operations in the event of a failure of a process, facility, service, information system or component.
- Activation procedures
- Roles & Responsibilities
- Designated Recovery Team members
- Recovery strategies & response
- Recovery management procedures
- Recovery resources
- Recovery communications
- Management of stakeholders
- Subcontractor, Supplier, Partner communications and coordination
- Recovery Strategies and response

Allerium's sample, non-confidential COOP which features a BCP and DRP as well as a table of contents from our comprehensive, confidential COOP is included in Appendix 6: Sample COOP.

5.8.3. Operations Centers and Support

5.8.3.1. Network Operations Center (NOC)

8.3. Operations Centers and Support

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.*

Response:

NOC Overview

Allerium provides system monitoring, maintenance, incident management, and reporting services from our NG9-1-1 operations organization. This organization includes a Network Operations Center (NOC)/Security Operations Center (SOC) team—also referred to as a Network & Security Operations Center [NSOC] team—with 24x7x365 public safety dedicated resources strategically dispersed across all U.S. time zones and working out of a centralized communications hub.

The NOC team is responsible for incident ticket management, field technician dispatching, partner escalation, and depot spares in Allerium's data centers. NOC engineers engage from the start of the project deployment to assist application engineers with deploying the service. The NOC team also manages planned maintenance events as well as root cause analysis (RCA) delivery and remains available for assistance throughout all phases of the project lifecycle.

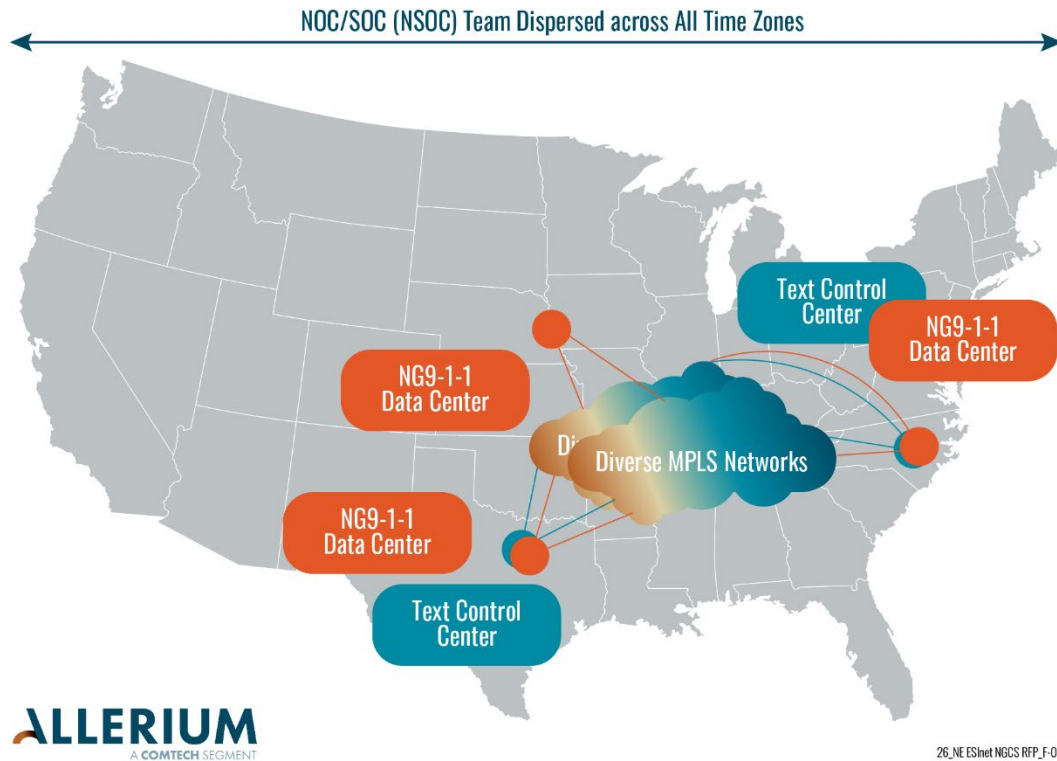


Figure 58. National System Design View

24x7x365 NOC with remote maintenance/restoration.

Allerium operates a dedicated 24x7x365 Network Operations Center (NOC) providing continuous monitoring, maintenance, and support for the NG911 system.

The NOC is equipped with the capability to perform remote maintenance and restoration activities, including system diagnostics, configuration changes, service restarts, and failover actions as required. These capabilities enable rapid response to alarms and incidents, minimizing service impact and supporting continuous system availability.

Single point for monitoring/maintenance/support.

Allerium's NSOC is available 24x7x365 for any service-related issues, serves as the single point of contact (SPOC) for all customer inquiries—including reporting, escalating, and receiving status updates on incidents as well as other communications—and provides rapid access to a live technician. Tiers 1-2 and supervisory personnel plus SMEs staff the NSOC.

Allerium's NSOC supports both statewide and regional Allerium ESInet/NGCS deployments. ISO 9001/TL 9000 certified, our NSOC is unique because it is an in-house resource solely focused on 9-1-1 and staffed 24x7x365 by Allerium employees specifically trained on 9-1-1 services and applications. Many other organizations within the NG9-1-1 space use multipurpose personnel and facilities to “include” 9-1-1 or contract with generic, third-party help desk solutions providers.

Interface with help desk/PSAPs.

Allerium's NOC/SOC serves as the central point of coordination for all operational and security-related communications, interfacing directly with the Help Desk, PSAPs, and designated State personnel.

All interactions—including incident reporting, status updates, escalation, and resolution communication—are managed through established workflows and communication channels such as phone, email, notification systems, and web-based portals. This ensures clear, timely, and consistent communication with all stakeholders.

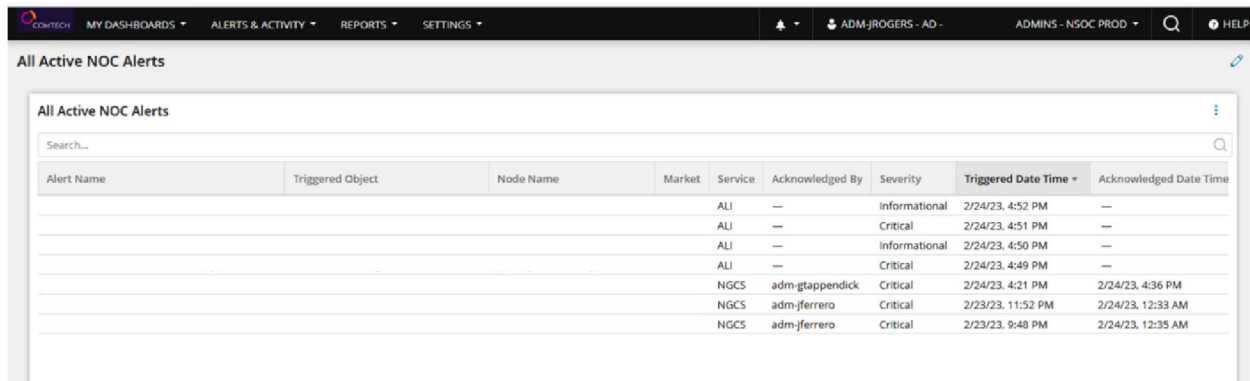
Staffed for troubleshooting/recovery.

The Allerium NOC is staffed with qualified technical personnel across Tier 1, Tier 2, and engineering support functions, ensuring the capability to effectively troubleshoot, diagnose, and recover from system issues.

Staff are trained in NG9-1-1 systems, ESInet operations, and incident management processes, enabling rapid identification of root causes and coordinated restoration efforts. Additional resources, including Field Services and vendor support, are engaged as needed to support resolution.

Monitoring of ESInet/connections/functional components.

Allerium employs a monitoring platform to collect and monitor data from systems and applications used in the operation of ESInet and NGCS service functions. This platform provides real-time awareness of system health and operational status of the service. In conjunction with the monitoring platform, Allerium employs both dashboard and reporting tools for use by both internal and external users to measure operational performance.



Alert Name	Triggered Object	Node Name	Market	Service	Acknowledged By	Severity	Triggered Date Time	Acknowledged Date Time
				ALI	—	Informational	2/24/23, 4:52 PM	—
				ALI	—	Critical	2/24/23, 4:51 PM	—
				ALI	—	Informational	2/24/23, 4:50 PM	—
				ALI	—	Critical	2/24/23, 4:49 PM	—
				NGCS	adm-gtappendick	Critical	2/24/23, 4:21 PM	2/24/23, 4:36 PM
				NGCS	adm-fferrero	Critical	2/23/23, 11:52 PM	2/24/23, 12:33 AM
				NGCS	adm-fferrero	Critical	2/23/23, 9:48 PM	2/24/23, 12:35 AM

Figure 59. All Active NOC/SOC Alerts Dashboard

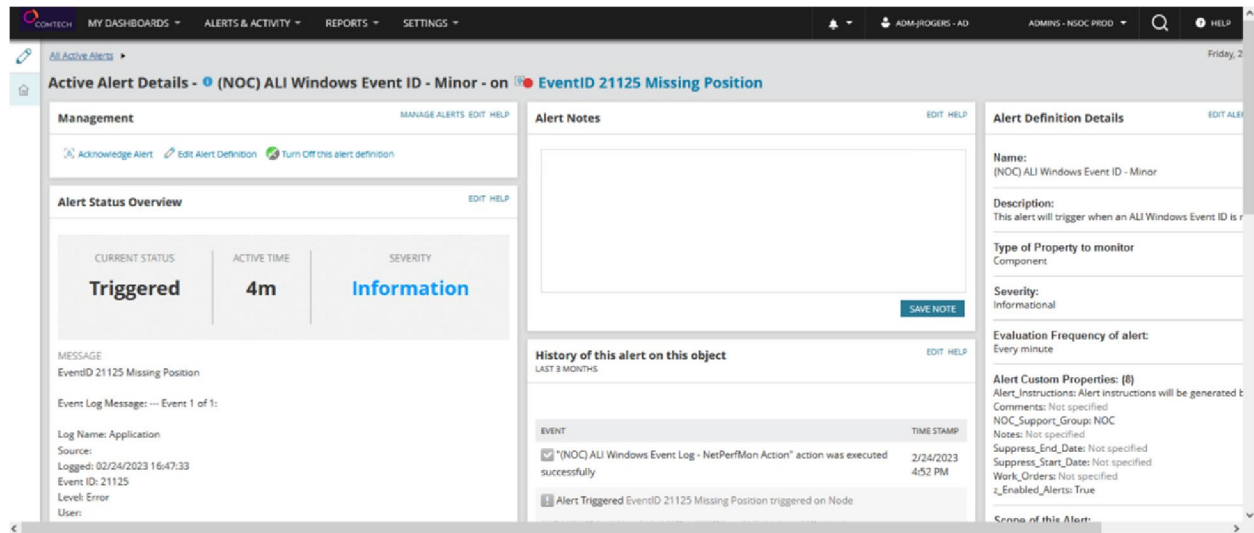


Figure 60. Node Summary of an Active Alert

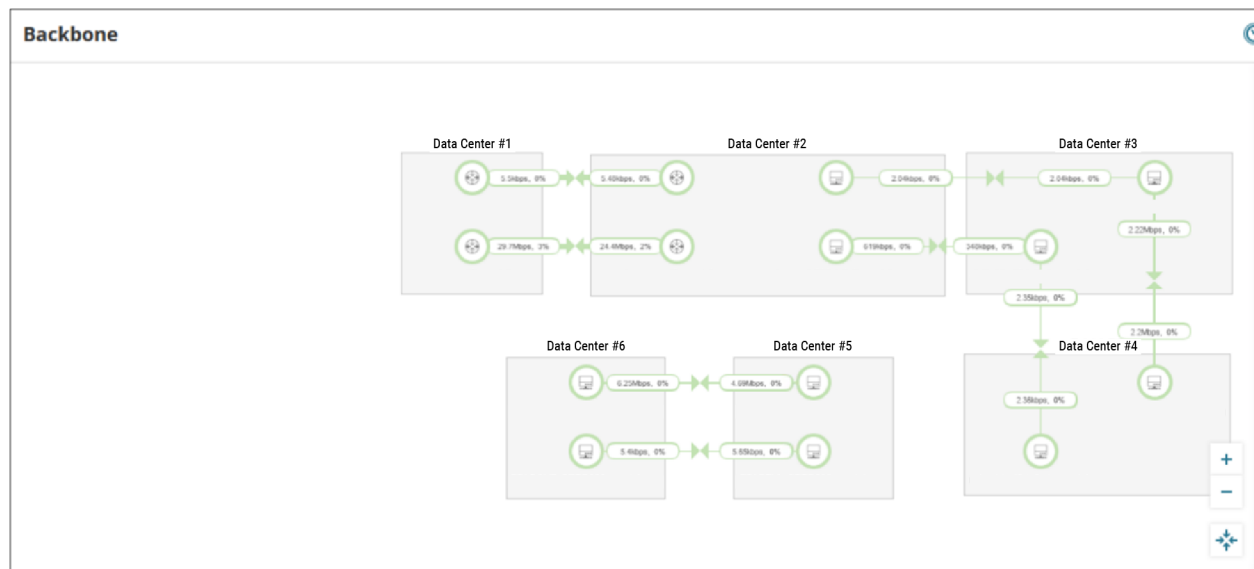


Figure 61. Major Backbone Network Connectivity Circuit Map

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.

Allerium utilizes an integrated Network Management System (NMS) to provide comprehensive monitoring and alerting across the NG911 environment.

The NMS capabilities include:

- Continuous monitoring of device performance and availability across all ESInet and NGCS components
- Monitoring of key network performance metrics, including throughput, latency, jitter, packet loss, and other critical parameters
- Detection of network intrusion attempts and security events, with automated alert generation
- Threshold-based alarm creation and notification, ensuring timely awareness of performance deviations or failures
- Monitoring of data center and point-of-presence environments, including environmental conditions impacting system health
- Monitoring of ancillary systems, including power utilization and backup power systems, to ensure operational continuity

These capabilities provide full visibility into network and infrastructure performance, enabling proactive management and rapid response to any operational issue.

5.8.3.2. Security Operations Center (SOC)

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:

- *24×7×365 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.*

Response:**SOC Overview**

Allerium's Security Operations Center (SOC) is fully integrated with the Network Operations Center (NOC) to provide a unified operational model for both network and security event management.

The NOC performs continuous monitoring of all systems and is trained to identify, triage, and initiate response to security-related events. A dedicated security team supports this model as an on-call and escalation resource, providing advanced analysis, guidance, and resolution support for security incidents.

This integrated approach ensures rapid detection and response while leveraging specialized security expertise when required.

24x7x365 SOC (possibly combined with NOC) with remote maintenance/restoration of security events.

Allerium provides 24x7x365 security operations coverage through its integrated NOC/SOC model.

Security events are continuously monitored, and the organization maintains the capability to perform remote maintenance and restoration actions, including containment, configuration updates, access controls, and remediation activities. This enables rapid response to security incidents while minimizing potential impact to NG9-1-1 operations.

Single point for monitoring/maintenance/support identifying security faults.

Allerium provides a single operational point of contact through its integrated NOC/SOC for all monitoring, maintenance, and support activities, including the identification and management of security faults.

All security events are centrally monitored, triaged, and managed through this unified operations model, ensuring consistent handling, coordinated response, and full visibility across all NG911 system components.

Interface with help desk/PSAPs.

Allerium's NOC/SOC serves as the central point of coordination for all operational and security-related communications, interfacing directly with the Help Desk, PSAPs, and designated State personnel.

All interactions—including incident reporting, status updates, escalation, and resolution communication—are managed through established workflows and communication channels such as phone, email, notification systems, and web-based portals. This ensures clear, timely, and consistent communication with all stakeholders.

Staffed for security troubleshooting/recovery.

Allerium's SOC capabilities are supported by a combination of trained NOC personnel and dedicated security specialists.

NOC staff are trained to identify and respond to common security events, while advanced security troubleshooting and recovery activities are supported by the security team. This includes investigation, containment, remediation, and coordination with vendors or partners as needed to resolve security incidents effectively.

Security monitoring of system/connections/components.

Allerium provides comprehensive security monitoring across the entire NG9-1-1 system, including all network connections and functional components involved in call routing.

A dedicated security team utilizes specialized monitoring and security tools to oversee:

- Security event detection and analysis
- Threat and vulnerability monitoring
- Log collection and correlation across systems
- Identification of anomalous or unauthorized activity

This capability ensures continuous visibility into the security posture of the NG911 environment and enables rapid identification and response to potential threats.

5.8.3.3. Help Desk

8.3.3. Help Desk

A help desk will be included with the NG911 system. The help desk(s) will operate on a 24×7×365 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:

- *24×7×365 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.*

Response:

Help Desk Overview

Allerium fulfills the Help Desk function through its dedicated 24x7x365 Network Operations Center (NOC), which serves as the central hub for all operational support and customer engagement.

The NOC is continuously staffed with trained technical personnel and responsible for receiving, managing, and resolving all NG9-1-1 system and service-related requests. This integrated model ensures seamless coordination between support intake, monitoring, and resolution activities without handoffs between separate organizations.

24×7×365 staffed help desk trained in support.

Allerium provides a fully staffed 24x7x365 NOC, which serves as the Help Desk and is staffed by trained and qualified technical personnel.

NOC staff are experienced in NG911 operations, incident management, and customer support, enabling them to effectively receive, triage, and resolve issues in alignment with service level expectations.

Single point for all system matters/components/providers.

Allerium's NOC serves as the single point of contact (SPOC) for all NG911 system matters, including all components and supporting service providers.

All incidents, requests, and communications are centralized through the NOC which maintains ownership and coordinates resolution across internal teams, partners, and subcontractors, ensuring consistent and efficient service delivery.

No automated attendant.

Allerium does not utilize automated attendants for Help Desk call handling.

All incoming calls are answered directly by a trained NOC technician, ensuring immediate human interaction, rapid issue intake, and efficient escalation when required.

Accessible via voice/text/email/etc.

Allerium's NOC (Help Desk) is accessible through multiple communication channels, including:

- Voice (primary method),
- Email, and
- Web-based portals and ticketing systems.

Text-based communication is not a standard intake method, ensuring that all reported issues are captured, documented, and managed through controlled and trackable communication channels aligned with operational and compliance requirements.

Direct/immediate communications with maintenance/support including network troubles/partners.

Allerium's NOC maintains direct and immediate communication pathways with all maintenance and support resources, including internal teams, network providers, and third-party partners.

These communication and coordination processes are formally defined within Allerium's NOC-to-NOC operational documentation, which establishes clear procedures for escalation, collaboration, and real-time coordination during incidents.

This ensures rapid engagement of all necessary resources to address network troubles and system issues without delay.

5.8.3.3.1. Trouble Handling and Ticketing Requirements

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.

Response:

Trouble Handling and Ticketing Overview

Trouble Reporting Process Overview

Allerium leverages its 24x7x365 NSOC team for incoming trouble reports as well as outgoing notifications to all stakeholders for optimal coordination. Allerium's defined trouble reporting process for coordination with all stakeholders is as follows:

- Once the NSOC team is aware of an incident, we notify all stakeholders of that trouble.
- Based on the severity of the trouble, Allerium provides updates and status via email.
- If the trouble requires technical resolution, a conference bridge with the appropriate stakeholders may be opened to resolve the incident.
- Once resolved, Allerium notifies all stakeholders and closes the ticket.

How to Report Problems to the NSOC

Stakeholders can report problems and incidents through multiple channels to Allerium's NSOC team, including phone and email.

Much like telecommunicators responding to a request for emergency service, the gathering of initial information about an incident is critical in reducing resolution time after dispatching. Therefore, our NSOC team prefers to have direct interaction with customers reporting incidents through phone reporting of incidents. We know that these interactions provide a better initial response to incident escalation and allow technicians to capture vital information about the incident being reported. We understand that not all incidents being reported are critical in nature; therefore, for lower priority incidents, the State, PSAPs, or other stakeholders may choose to submit information through email or direct access to the Allerium ticketing system. To facilitate this exchange of information, Allerium provides users with a client facing user interface (UI) where they can open tickets and review status of existing tickets for ease of access.

Trouble Handling/Tracking

Incident Management Overview

Allerium maintains an IMP that details internal policies and procedures for managing requests and incidents. This IMP describes the set of actions to be taken by the Allerium NSOC during a service incident. At all times during service impairment, the Allerium NSOC follows established procedures to resolve the impairment and captures all communications within the ticketing system. The NSOC team's responsibilities include:

- Creating and updating trouble tickets,
- Managing escalation, and
- Keeping all stakeholders informed of ongoing progress.

At any time, authorized personnel from the State can obtain a status on the incident by either calling the NSOC or accessing the customer management portal (known as COMTECH INSIGHTS®).

The IMP includes six stages to facilitate the fastest possible resolution. These stages often overlap since the NSOC leverages different resources to assist in prompt incident resolution. These six stages are as follows:

- **Detection & Identification:** Allerium NSOC analysts become aware of the incident and immediately open a trouble ticket with a unique tracking number. NSOC analysts investigate and assess the incident and determine the severity level.
- **Escalation & Notification:** NSOC analysts escalate the incident to the appropriate support tiers and/or to management, as warranted by the severity level. NSOC analysts notify internal and external stakeholders of the incident as required by the severity level and by the IMP policies for the affected service. IMP policies for each service are described in the IMP module for that service. Follow-up notification occurs regularly thereafter.
- **Troubleshooting & Analysis:** NSOC analysts document the steps being taken to resolve the incident, facilitate communication among relevant parties, and distribute updates.
- **Resolution:** The incident is resolved, and the system is restored to full integrity. NSOC analysts verify its resolution, send a final notification of the resolution to all stakeholders, and change the status of the trouble ticket to “resolved.”
- **RCA/RFO:** The technical owner and NSOC owner of the trouble ticket complete the RCA/RFO on the trouble ticket.
- **Closure:** If necessary, the NSOC lead reviews and sends the RCA/RFO to relevant parties. The NSOC closes the trouble ticket.

High-Level Incident Response & Notification

The Allerium notification platform can support user-definable levels of notification with delivery via:

- Email,
- Text, and
- Phone.

Allerium can provision authorized recipients of incident notifications in the system based on preference for notification type during the implementation phase of the project. Users can request to change established preferences through an NOC request. Figure 62 shows a high-level incident response and notification flow with notification delivery via email, text, and phone.

Allerium works with the State and/or its designated third-party to define the user-definable notification levels. This process is applicable to both the State and other stakeholders.

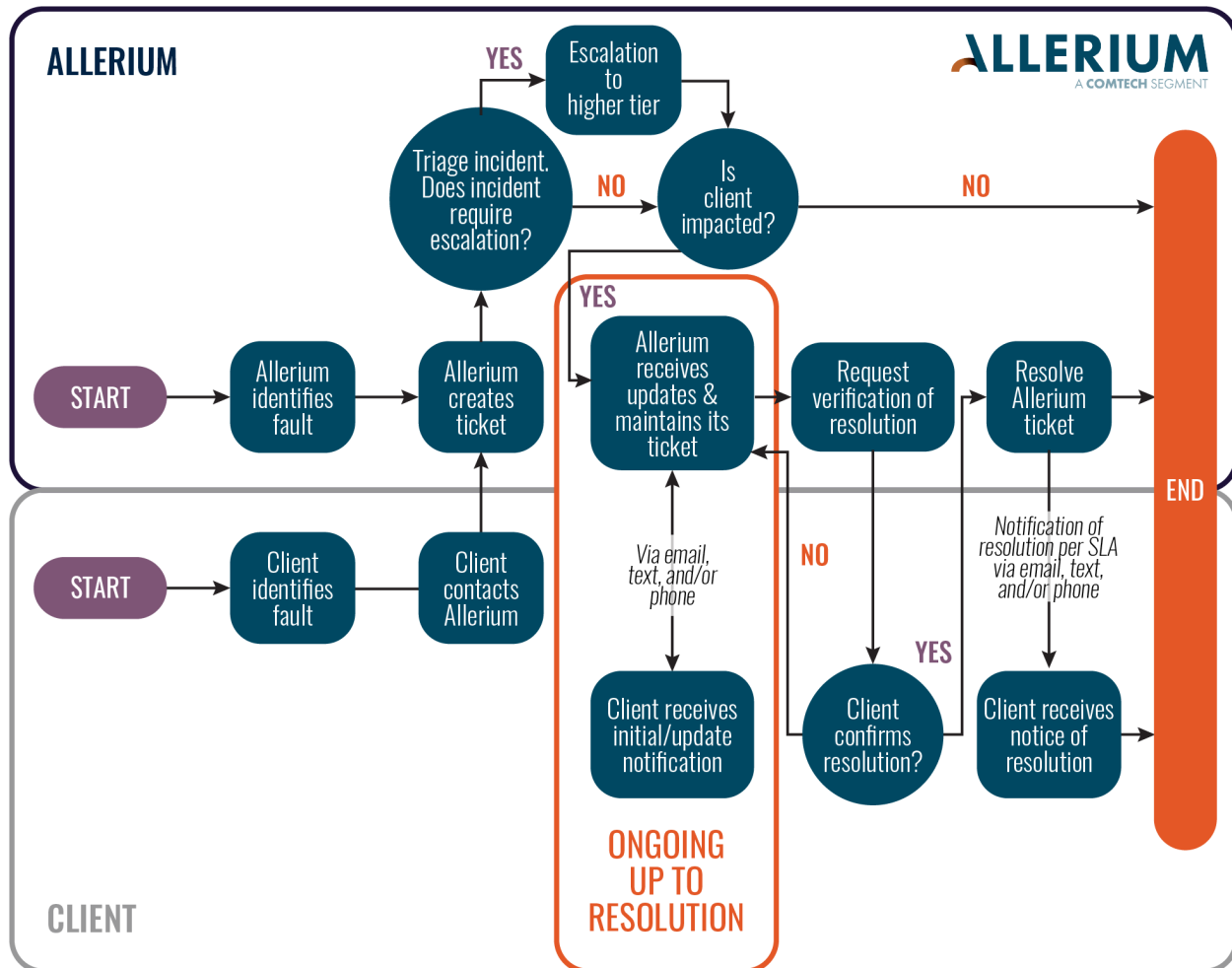


Figure 62. High-Level Incident Response and Notification Flow

Automated PSAP Connectivity Monitoring & Notification

Allerium has implemented enhanced automation for PSAP firewall node connectivity monitoring to further strengthen service assurance and SLA compliance across deployments.

This enhancement introduces automated ITSM ticket creation and real-time notifications when predefined loss-of-connectivity thresholds are detected via our monitoring platform. The automation ensures immediate awareness by both the NOC and customer stakeholders, reducing detection time and accelerating response.

Redundancy Loss Monitoring

When a PSAP experiences a loss of network redundancy for more than 10 minutes:

- An ITSM Incident (INC) is automatically created.
- An automated Service Notification Incident (NSI) is generated.
- Notifications are delivered to designated stakeholders.

This ensures that degraded resilience conditions are identified early, allowing corrective action before a full outage occurs directly supporting SLA protection and continuity objectives.

Complete Outage Monitoring

When a PSAP experiences a complete network outage for more than 3 minutes:

- An ITSM Incident (INC) is immediately created.
- An automated Impairment Notification is issued.
- Real-time notifications are sent to appropriate operational and customer contacts.

This rapid detection and notification model minimizes Mean Time to Awareness (MTTA), accelerates remediation, and ensures transparent communication during high-severity events.

Operational Handling & Governance

While the detection and notification process is automated, all resulting incidents are managed under Allerium's established NGCS PSAP firewall alarm procedures. This ensures:

- Consistent troubleshooting workflows
- Structured escalation paths
- Documented RCA and closure controls
- SLA tracking and reporting alignment

The automation enhances speed and visibility without altering the disciplined operational framework already in place.

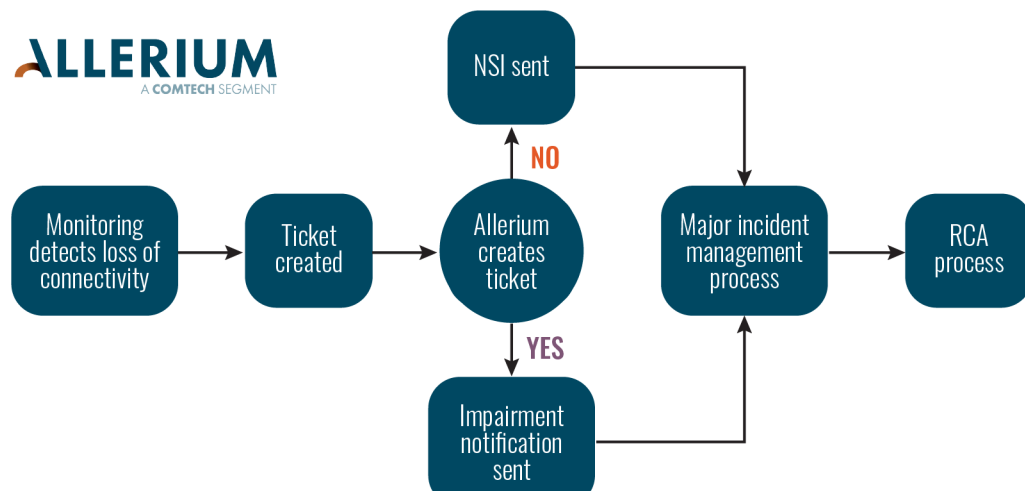


Figure 63. Automated PSAP Network Events Incident Detection & Notification Flow

Escalation guideline document/procedure.

Allerium’s immediate point of contact (POC) for any outage or service failure is the NOC team. Allerium has a clear escalation path that can be exercised by State stakeholders beyond the NOC team if issues are not being resolved in a timely manner. Table 64 below lists resources available should unique situations arise that warrant an escalation. Whenever a PSAP may feel the need to escalate an incident more quickly than via the standard process, contacting members of this escalation tree is the process.

Table 64. Incident Escalation Matrix

Level of Escalation	Contact Name/Title	Contact Information
First	NOC	Phone and email provided within our standard operating procedures documentation.
Second	Senior Manager, NOC Monitoring	Office, mobile, and email provided within our standard operating procedures documentation.
Third	Vice President, NOC & Field Services	Office, mobile, and email provided within our standard operating procedures documentation.
Fourth	Chief Operating Officer	Office, mobile, and email provided within our standard operating procedures documentation.

Allerium provides NSOC user guides that are posted to the externally accessible portal site. Allerium has included a sample NSOC SOP to give awareness to expectations, methods of communication, sample notifications, and the change management process. Allerium's sample NSOC SOP is included in Appendix 8: Sample NOC SOP for the State’s review.

5.8.3.3.2. Monitoring of Applications and Equipment

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.*

Response:

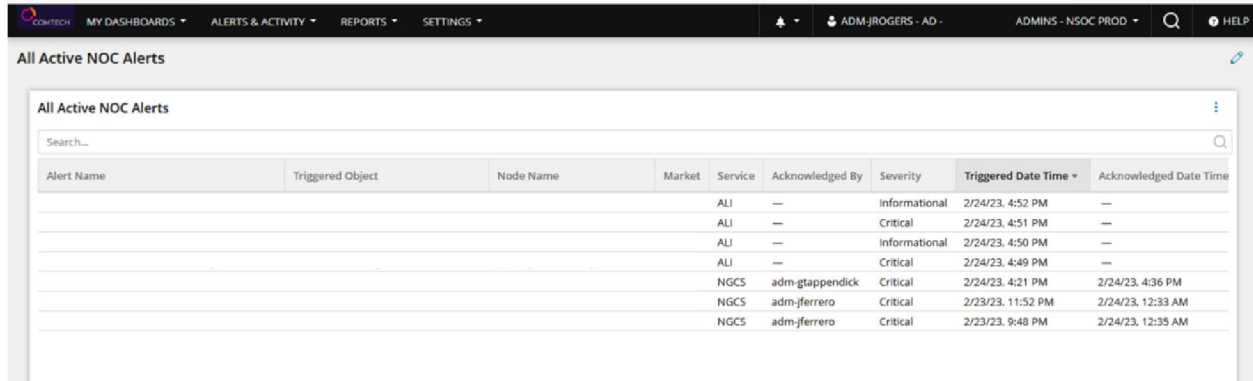
Monitoring of Applications and Equipment Overview

Allerium provides:

- Centralized monitoring performed through Allerium’s 24x7x365 NOC
- Integrated observability across ESInet, NGCS, applications, and infrastructure
- Use of monitoring platforms for real-time visibility
- Automated alerting and ITSM integration for rapid incident creation and response

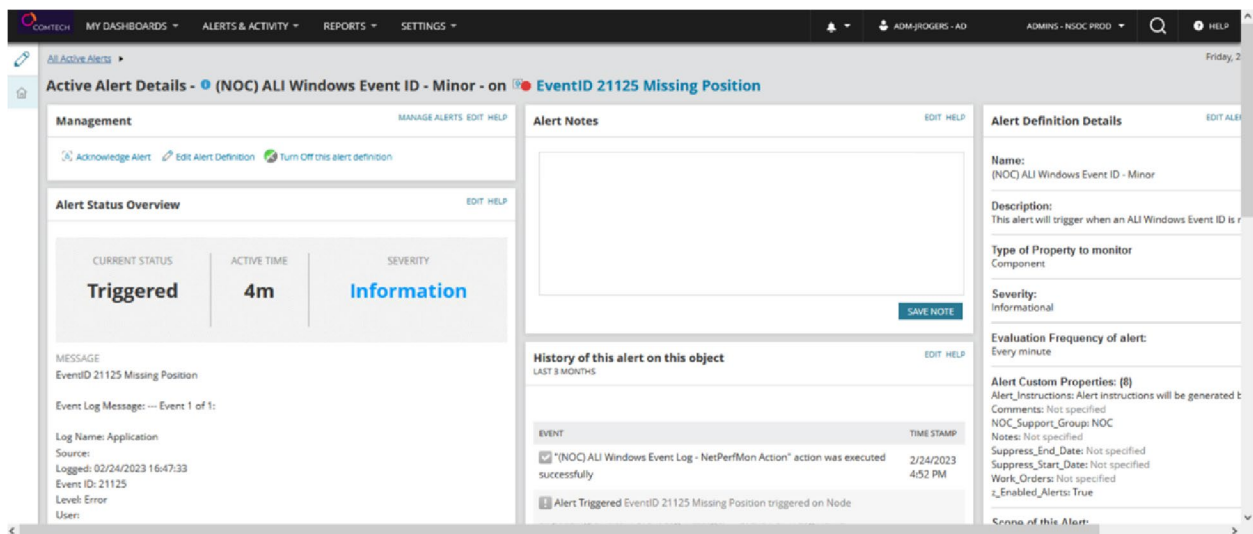
Proactive monitoring of components for operation/performance/faults.

Allerium employs a monitoring platform to collect and monitor data from systems and applications used in the operation of ESInet and NGCS service functions. This platform provides real-time awareness of system health and operational status of the service. In conjunction with the monitoring platform, Allerium employs both dashboard and reporting tools for use by both internal and external users to measure operational performance.



Alert Name	Triggered Object	Node Name	Market	Service	Acknowledged By	Severity	Triggered Date Time	Acknowledged Date Time
				ALI	—	Informational	2/24/23, 4:52 PM	—
				ALI	—	Critical	2/24/23, 4:51 PM	—
				ALI	—	Informational	2/24/23, 4:50 PM	—
				ALI	—	Critical	2/24/23, 4:49 PM	—
				NGCS	adm-gtappendick	Critical	2/24/23, 4:21 PM	2/24/23, 4:36 PM
				NGCS	adm-jferrero	Critical	2/23/23, 11:52 PM	2/24/23, 12:33 AM
				NGCS	adm-jferrero	Critical	2/23/23, 9:48 PM	2/24/23, 12:35 AM

Figure 64. All Active NOC/SOC Alerts Dashboard



Active Alert Details - (NOC) ALI Windows Event ID - Minor - on EventID 21125 Missing Position

Management MANAGE ALERTS EDIT HELP

[Acknowledge Alert](#) [Edit Alert Definition](#) [Turn Off this alert definition](#)

Alert Status Overview EDIT HELP

CURRENT STATUS	ACTIVE TIME	SEVERITY
Triggered	4m	Information

MESSAGE
EventID 21125 Missing Position

Event Log Message: --- Event 1 of 1:

Log Name: Application
Source:
Logged: 02/24/2023 16:47:33
Event ID: 21125
Level: Error
User:

Alert Notes EDIT HELP

Alert Definition Details EDIT ALERT

Name:
(NOC) ALI Windows Event ID - Minor

Description:
This alert will trigger when an ALI Windows Event ID is r

Type of Property to monitor
Component

Severity:
Informational

Evaluation Frequency of alert:
Every minute

Alert Custom Properties: (8)
Alert_Instructions: Alert instructions will be generated t
Comments: Not specified
NOC_Support_Group: NOC
Notes: Not specified
Suppress_End_Date: Not specified
Suppress_Start_Date: Not specified
Work_Orders: Not specified
z_Enabled_Alerts: True

History of this alert on this object EDIT HELP
LAST 3 MONTHS

EVENT	TIME STAMP
✓ "[NOC] ALI Windows Event Log - NetPerfMon Action" action was executed successfully	2/24/2023 4:52 PM
⚠ Alert Triggered EventID 21125 Missing Position triggered on Node	

Figure 65. Node Summary of an Active Alert

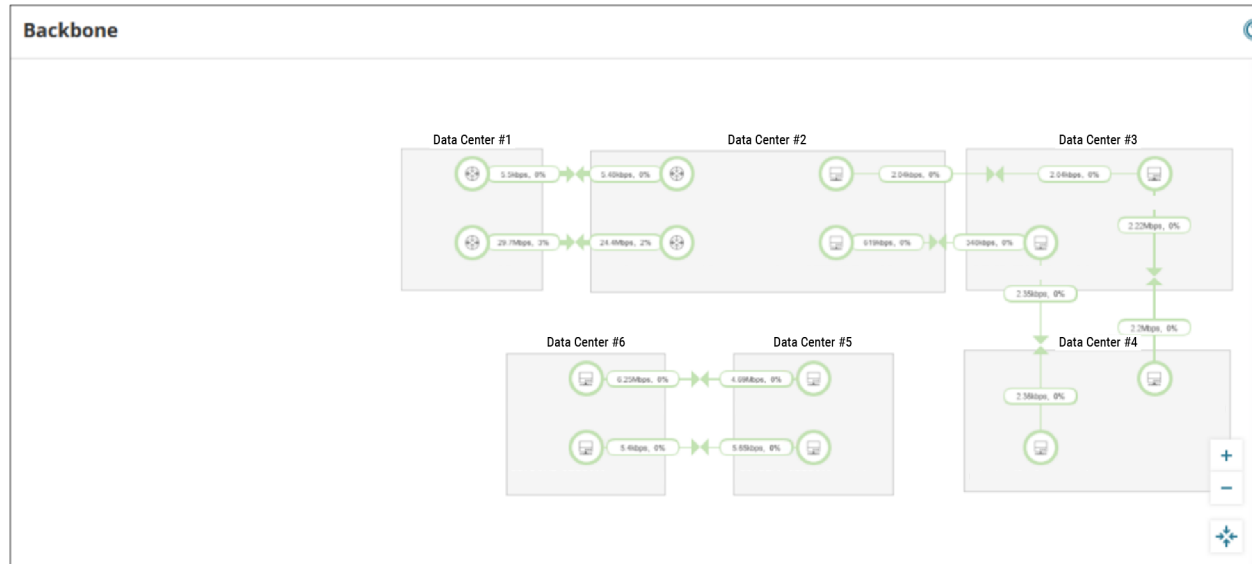


Figure 66. Major Backbone Network Connectivity Circuit Map

Allerium provides:

- Continuous monitoring of all NG911 components, including applications, network devices, and infrastructure
- Tracking of key performance metrics (availability, latency, utilization, error rates)
- Automated detection of faults, degradation, and abnormal conditions
- Proactive identification and mitigation of issues before service impact

Receipt/monitoring of alarms including environmental in NOC.

All system and environmental alarms are ingested into the NOC monitoring environment. Monitoring includes power systems, cooling, and facility conditions at data centers. NOC personnel have immediate visibility into automated alerting. Allerium correlates alarms to identify service impact and drive rapid response.

5.8.3.3.3. Root Cause Analysis

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.*

Response:

RCA for troubles (within 5 business days for critical/outages).

Allerium fully complies with this requirement and provides comprehensive Root Cause Analysis (RCA) for all critical events and major outages.

Allerium maintains a dedicated Problem Management function responsible for conducting detailed RCA investigations. For critical incidents and outages, RCAs are completed and delivered within five (5) business days, providing a thorough analysis of the issue, contributing factors, and corrective actions.

Immediate documentation shared online.

Allerium begins documenting RCA details immediately upon identification of a qualifying event.

RCA documentation is developed in real time and made available to the State through formal deliverables (e.g., PDF reports) and, where required, can be shared via secure shared repositories or collaboration platforms to provide visibility as information becomes available.

Format with dates/times/discoveries.

Allerium utilizes a structured and well-defined RCA format that includes:

- Detailed timelines with dates and timestamps
- Documented investigation steps and findings
- Identification of root cause(s) and contributing factors
- Impact assessment and resolution actions

Allerium takes pride in delivering high-quality, well-documented RCAs that provide clear, actionable insight into system events and support continuous improvement.

Final submission for State approval.

Upon completion, RCAs are formally submitted to the State for review and approval.

Allerium conducts internal review and quality assurance processes prior to submission to ensure accuracy and completeness. Additionally, Allerium will coordinate with the State to review findings, answer questions, and ensure alignment before final acceptance of the RCA.

5.8.3.4. Customer Support Services

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
 - o Performance measurement and monitoring
 - o Guaranteed delivery
 - o 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.

Response:

Customer Support Services Overview

Customer support services are delivered through Allerium's 24x7x365 NOC (serving as Help Desk and operations hub), providing an integrated support model covering monitoring, incident, problem, and change management with centralized coordination across internal teams, vendors, and partners.

All services are aligned to SLAs and measured through defined SLOs and KPIs with monthly Performance Reviews provided to our clients.

SLA management (performance/monitoring/delivery/reporting/review) on a monthly basis to the PSC.

Allerium provides:

- Continuous SLA monitoring via NOC and ITSM platforms
- Defined KPIs aligned to availability, response, and resolution targets
- Monthly reporting and performance review with our clients
- Tracking of SLA compliance, trends, and improvement actions
- Ongoing refinement of SLA performance based on operational data

Event/incident management.

Allerium provides:

- 24x7x365 monitoring with automated alerting and event correlation
- Structured incident classification and prioritization (SIL-based)
- Rapid escalation and Major Incident Management for critical events
- Centralized ownership through NOC with coordinated response

Diagnostics/reporting.

Allerium provides:

- Real-time diagnostics via monitoring tools and dashboards
- Detailed incident, performance, and trend reporting
- Root Cause Analysis (RCA) for major incidents
- Regular and ad hoc reporting

Problem resolution/trouble handling.

Allerium provides:

- Formal Problem Management process for root cause identification
- Problem records and tasks tracked within ITSM system
- Corrective actions implemented through Change Management
- Continuous improvement driven by RCA and trend analysis

Network fault monitoring.

Allerium provides:

- Continuous monitoring of ESInet, NGCS, and all network components
- Automated alerts for faults, degradation, and threshold breaches

- Event correlation to identify service impact
- Immediate NOC response and escalation

Request fulfillment.

Allerium provides:

- Centralized intake of service requests through the NOC (Help Desk)
- Standardized workflows for request tracking and fulfillment
- SLA-aligned response and completion timelines
- Full lifecycle tracking within ITSM platform

Access management.

Allerium provides:

- Role-based access control for systems and applications
- Secure provisioning and deprovisioning processes
- Coordination with security and operations teams
- Audit tracking of access changes

Remote diagnostics.

Allerium provides:

- Remote access for troubleshooting and system validation
- Log analysis, configuration review, and service checks
- Rapid issue isolation without requiring on-site presence
- Escalation to Field Services when necessary

Environmental requirements.

Allerium provides:

- Monitoring of data center and PoP environmental conditions
- Oversight of power, cooling, and infrastructure health
- Integration with monitoring systems for alerting
- Coordination with facilities/vendors for remediation

Capacity/change/configuration/transition management; training.

Allerium provides:

- Capacity monitoring and planning to prevent performance issues
- Formal Change Management with CAB, MOPs, and rollback procedures
- Configuration management to maintain system integrity
- Structured transition from implementation to operations

- Role-based training and operational runbooks for stakeholders

Commercial availability.

Allerium provides:

- Highly available architecture supporting 99.999% uptime objectives
- Redundant systems and failover capabilities
- 24x7x365 operational support ensuring continuous service delivery
- Proven support model for mission-critical environments

All tied to SLOs for SLA measurement.

Allerium maps all services to defined Service Level Objectives (SLOs) with SLOs aligned to SLA metrics (availability, response, MTTR). Allerium provides continuous measurement and reporting of performance with monthly reviews with our clients to ensure compliance and improvement.

5.8.4. Monitoring and Event Management

5.8.4.1. Alarm Categories

8.4. Monitoring and Event Management

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.*

Response:**Alarm Categories Overview**

Allerium provides:

- Centralized alarm management through NOC monitoring platforms
- Structured classification of alarms based on operational impact and severity
- Integration with ITSM for automated ticket generation and tracking
- Alignment of alarm handling with incident management and SLA requirements

Alarms by criticality (critical/major/etc.).

Allerium provides:

- Defined alarm categories aligned to severity levels (e.g., Critical, Major, Minor, Informational)

- Severity based on impact to service, PSAP operations, and system performance
- Direct mapping of alarm severity to incident priority (SIL levels)
- Immediate escalation and response for high-severity (Critical/Major) events

Dynamic notification thresholds for new categories; automatic NOC notification.

Allerium provides:

- Configurable thresholds for performance metrics (e.g., utilization, latency, errors)
- Ability to dynamically adjust thresholds as network conditions and requirements evolve
- Automatic alert generation and notification to the NOC upon threshold breach
- Integration with monitoring and alerting systems for real-time visibility and response

Varying notification/escalation per category.

Allerium provides:

- Defined notification and escalation workflows based on alarm severity
- Critical alarms trigger immediate NOC action, escalation, and stakeholder notification
- Lower-severity alarms follow structured triage and response processes
- Escalation paths include NOC, Engineering, Field Services, and vendor partners as needed

5.8.5. Change, Maintenance, and Release Management

5.8.5.1. Change Management Requirements

8.5. Change, Maintenance, and Release Management

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.*

Response:

Allerium maintains a disciplined, automation-enabled Change Management framework purpose-built for the operational sensitivity and uptime requirements of NG9-1-1 environments. Our approach integrates structured governance, rigorous testing, formal approval workflows, vendor coordination, and proactive communication to ensure that all system modifications are executed with precision, transparency, and minimal service risk.

Governance and Control Framework

All production changes are governed through Allerium's enterprise IT Service Management (ITSM) platform (Remedy), which enforces standardized workflows, documentation requirements, approval routing, and audit traceability.

Each change request (CRQ) requires a fully documented Implementation and Backout Plan (IBOP), detailing:

- Scope and business justification
- Technical impact assessment across interconnected systems
- Risk classification and mitigation steps
- Validation and testing procedures
- Step-by-step implementation instructions
- Defined backout methodology

No non-emergency production change is executed without advance notice, documented approval, and customer-aligned communication.

Allerium's change governance extends beyond internal systems. We actively coordinate with third-party vendors, carriers, hosted platform providers, and infrastructure partners when their maintenance activities may impact the NG9-1-1 ecosystem. Vendor-led changes are reviewed through the same structured risk evaluation process, scheduled within approved maintenance windows, and monitored by our NOC/SOC to ensure unified situational awareness and accountability across all stakeholders.

Testing, Validation & Risk Mitigation

Prior to production deployment, all changes undergo structured validation in Allerium's dedicated lab environments. Test results are formally documented and attached to the IBOP record within the ITSM system to ensure technical completeness and operational readiness.

For complex or higher-risk modifications,

- Cross-functional Change Advisory Board (CAB) review is required.
- Director-level oversight is enforced for Level 1 and Level 2 changes.
- Client-facing Change Control Boards (CCB) may be convened when required by State governance.
- Vendor stakeholders are included in coordination discussions when applicable.

To further strengthen risk prevention, CAB meetings are held twice weekly to provide timely review of increasing change volume and complexity. This enhanced cadence reduces backlog risk, improves scrutiny, and minimizes change-related service disruptions.

Structured Approval & Oversight

Approval authority scales according to risk and impact:

- Routine operational updates may be completed within ITSM workflow.
- Moderate to high-impact changes require CAB review.
- Vendor-initiated maintenance impacting shared infrastructure is incorporated into the CAB review process when appropriate.
- Emergency changes follow an expedited Emergency IBOP process with shortened approval timelines and post-implementation review.

The Change Manager chairs and facilitates all CAB sessions, ensuring:

- Complete documentation and approvals prior to review
- Structured evaluation of technical quality and operational readiness
- Cross-functional accountability
- Vendor coordination when applicable
- Formal decision recording and follow-up tracking

This governance model ensures transparency, accountability, and alignment across Engineering, Operations, NOC/SOC, vendors, and program leadership.

Communication & Stakeholder Transparency

Allerium utilizes an automated notification platform supporting user-defined escalation tiers and multi-channel delivery (email, SMS, and voice). Notification preferences are established during implementation and may be modified at the State's request.

Stakeholders receive:

- Advance notice for scheduled changes
- Pre-work emergency notifications when applicable
- Vendor maintenance coordination notifications when third-party systems are involved
- Post-implementation confirmation
- Escalation updates if abnormal conditions are detected
- This structured communication model ensures that States, PSAPs, designated third parties, and vendor partners maintain continuous situational awareness.

Release Management & Operational Protection

Upon final approval, each change is scheduled with notifications sent to all stakeholders and it is moved to our release / maintenance calendar. No overlapping production changes are scheduled within the same window. Maintenance windows are aligned to lowest risk time period depending on the work being done. Vendor maintenance windows are coordinated to avoid cumulative or cascading risk. The NOC/SOC actively monitors release execution in real time. Customer-reported events are correlated against active change activity.

This layered monitoring model enables immediate detection of abnormal behavior and rapid rollback if necessary.

5.8.5.1.1. Security Considerations in Change Management

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.*

Response:

Allerium maintains policies and controls to manage change, maintenance, and release management to information processing facilities and systems. These include equipment, software, and configurations with design and development changes maintained and operated by Allerium. Changes are controlled by using a formal process that creates records of the following:

- Identification and detailed description of the changes.
- Impact assessment of the changes.
- Formal approval of the changes.
- Verification that information security requirements have been met.
- A risk assessment if any change to an information asset may create security vulnerability.
- Communication of the changes to all necessary individuals.
- Whenever possible, changes to operational software are tested in a production-like environment to determine the impact of the change to the functionality of the operational software and security controls.
- The results testing is documented and analyzed to minimize risk to production environments.
- Back-out procedures for the change.
- Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.

- The formal change control process ensures that the system, operational, and application documentation is updated as part of any change, and that out-of-date documentation is archived or disposed of as required

5.8.5.2. Scheduled Maintenance Process

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.*

Response:

Scheduled Maintenance Process Overview

Allerium maintains a disciplined, automation-enabled Change Management framework purpose-built for the operational sensitivity and uptime requirements of NG9-1-1 environments. Our approach integrates structured governance, rigorous testing, formal approval workflows, vendor coordination, and proactive communication to ensure that all system modifications are executed with precision, transparency, and minimal service risk.

Governance and Control Framework

All production changes are governed through Allerium's enterprise IT Service Management (ITSM) platform (Remedy), which enforces standardized workflows, documentation requirements, approval routing, and audit traceability.

Each change request (CRQ) requires a fully documented Implementation and Backout Plan (IBOP), detailing:

- Scope and business justification
- Technical impact assessment across interconnected systems
- Risk classification and mitigation steps
- Validation and testing procedures
- Step-by-step implementation instructions
- Defined backout methodology

No non-emergency production change is executed without advance notice, documented approval, and customer-aligned communication.

Allerium's change governance extends beyond internal systems. We actively coordinate with third-party vendors, carriers, hosted platform providers, and infrastructure partners when their maintenance activities may impact the NG9-1-1 ecosystem. Vendor-led changes are reviewed through the same structured risk evaluation process, scheduled within approved maintenance windows, and monitored by our NOC/SOC to ensure unified situational awareness and accountability across all stakeholders.

Testing, Validation & Risk Mitigation

Prior to production deployment, all changes undergo structured validation in Allerium's dedicated lab environments. Test results are formally documented and attached to the IBOP record within the ITSM system to ensure technical completeness and operational readiness.

For complex or higher-risk modifications,

- Cross-functional Change Advisory Board (CAB) review is required.
- Director-level oversight is enforced for Level 1 and Level 2 changes.
- Client-facing Change Control Boards (CCB) may be convened when required by State governance.
- Vendor stakeholders are included in coordination discussions when applicable.

To further strengthen risk prevention, CAB meetings are held twice weekly to provide timely review of increasing change volume and complexity. This enhanced cadence reduces backlog risk, improves scrutiny, and minimizes change-related service disruptions.

Structured Approval & Oversight

Approval authority scales according to risk and impact:

- Routine operational updates may be completed within ITSM workflow.
- Moderate to high-impact changes require CAB review.
- Vendor-initiated maintenance impacting shared infrastructure is incorporated into the CAB review process when appropriate.
- Emergency changes follow an expedited Emergency IBOP process with shortened approval timelines and post-implementation review.

The Change Manager chairs and facilitates all CAB sessions, ensuring:

- Complete documentation and approvals prior to review
- Structured evaluation of technical quality and operational readiness
- Cross-functional accountability
- Vendor coordination when applicable
- Formal decision recording and follow-up tracking

This governance model ensures transparency, accountability, and alignment across Engineering, Operations, NOC/SOC, vendors, and program leadership.

Communication & Stakeholder Transparency

Allerium utilizes an automated notification platform supporting user-defined escalation tiers and multi-channel delivery (email, SMS, and voice). Notification preferences are established during implementation and may be modified at the State's request.

Stakeholders receive:

- Advance notice for scheduled changes
- Pre-work emergency notifications when applicable
- Vendor maintenance coordination notifications when third-party systems are involved
- Post-implementation confirmation
- Escalation updates if abnormal conditions are detected
- This structured communication model ensures that States, PSAPs, designated third parties, and vendor partners maintain continuous situational awareness.

Release Management & Operational Protection

Upon final approval, each change is scheduled with notifications sent to all stakeholders and it is moved to our release / maintenance calendar. No overlapping production changes are scheduled within the same window. Maintenance windows are aligned to lowest risk time period depending on the work being done. Vendor maintenance windows are coordinated to avoid cumulative or cascading risk. The NOC/SOC actively monitors release execution in real time. Customer-reported events are correlated against active change activity.

This layered monitoring model enables immediate detection of abnormal behavior and rapid rollback if necessary.

Developed/maintained process document for coordinating/scheduling preventative maintenance.

Allerium maintains a formal Scheduled Maintenance Process governed through Change Management and overseen by the Change Advisory Board (CAB), ensuring all activities are properly reviewed, approved, and coordinated. Each maintenance activity is supported by a detailed Maintenance Operation Plan (MOP), including defined procedures, risk assessment, and rollback strategies. Coordination with the State, PSAPs, and partner organizations is performed through established communication frameworks, with continuous updates and process improvements based on operational experience.

No degradation/disruption during activities.

All maintenance is designed and executed to maintain 99.999% service availability, utilizing phased and non-impactful implementation methods to avoid disruption. The NOC provides real-time monitoring throughout all maintenance activities, ensuring system performance is maintained. Immediate rollback procedures are in place to address any potential degradation, with strict adherence to approved MOPs and Change Management controls.

Allowance for individual component downtime with alternates/redundancy.

Allerium performs maintenance on individual components using redundant architecture and failover capabilities to maintain uninterrupted service. Traffic is dynamically rerouted to alternate paths or systems, with redundancy validated prior to execution and continuously monitored throughout the activity. Components are restored in a controlled manner following successful maintenance completion to ensure consistent system performance.

5.8.5.3. Software Development Process

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).

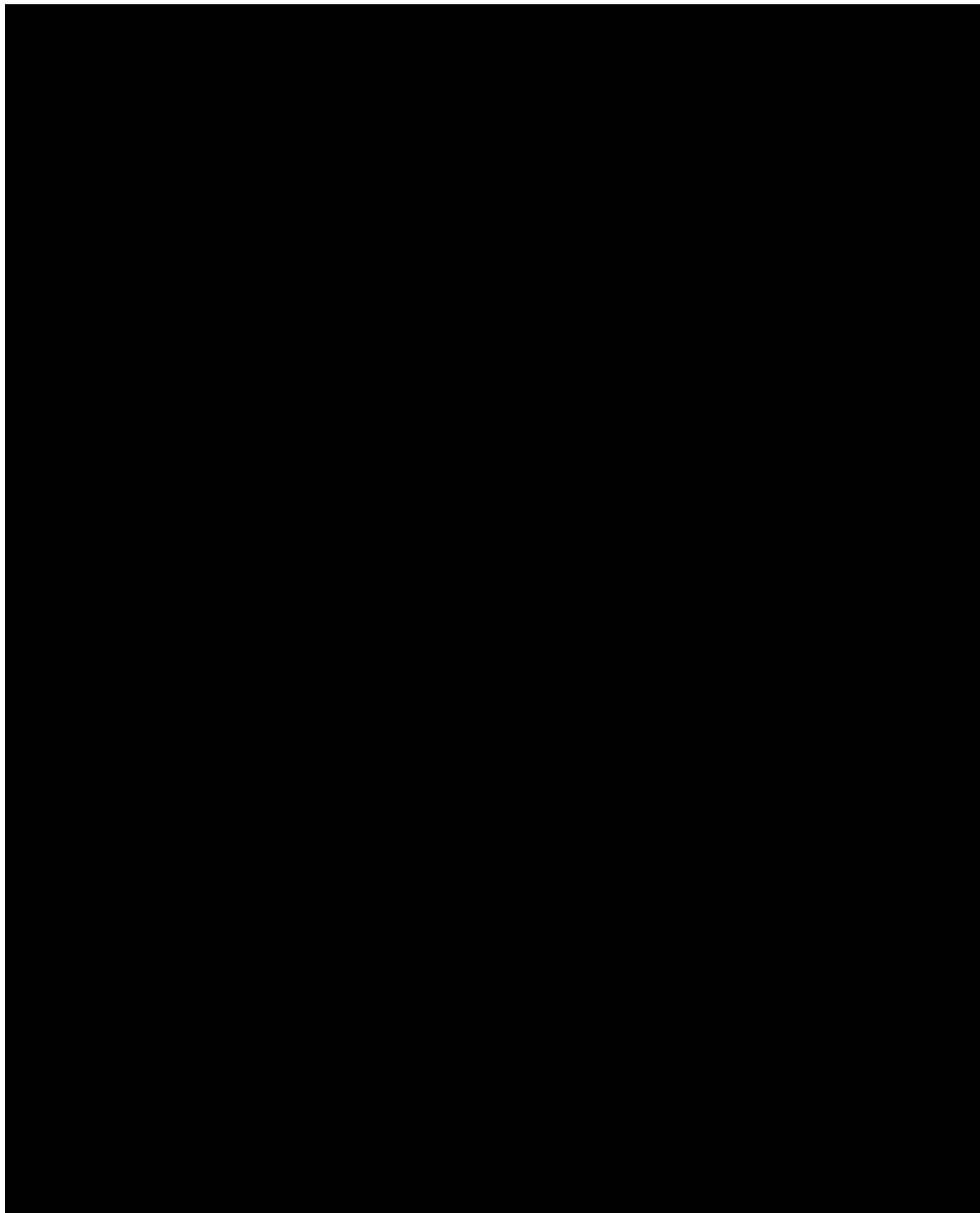
For all software components directly in the NG911 call path, the Contractor and all Subcontractors shall have a process to evaluate, release, and deploy critical security patches within 72 hours of the patch's public availability. This process shall be rehearsed on a regular cadence, and rehearsal results shall be shared with the State.

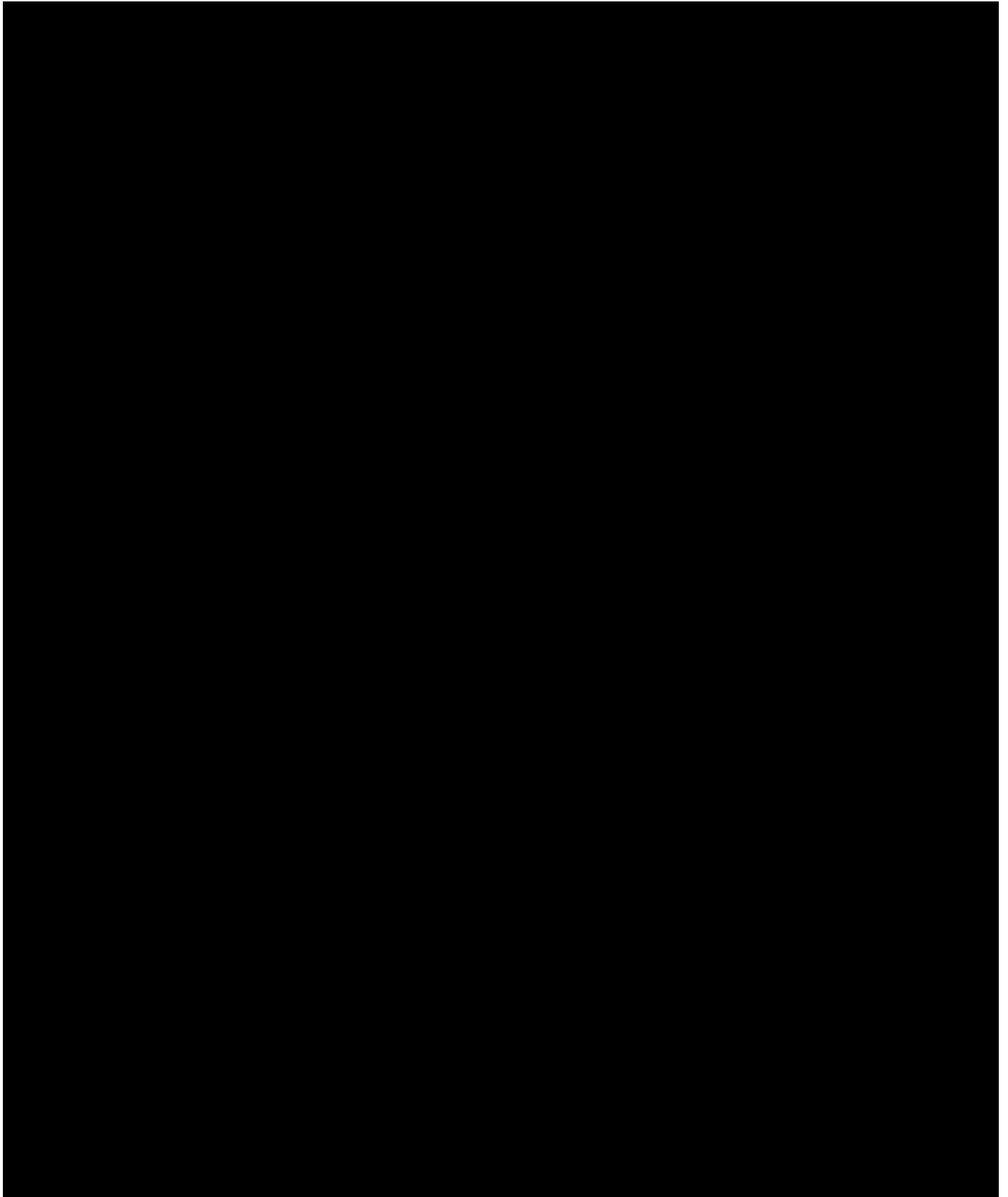
When a trouble ticket or outage results in a software bug, a discrepancy report, or a required system change to prevent recurrence, the Contractor shall maintain an online, State-accessible log showing each item, severity, affected components, current status, workaround (if any), and the target fix version 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.*

Response:





5.8.5.4. Software Updates and Improvements

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.*

Response:

Allerium's process for software upgrades and improvements is twofold. The first part is the development process for creating and testing software releases. The second part is the deployment of that software in the production system.

Scheduled Software Releases

Frequency

At a minimum, we provide two software releases per year that build on the underlying system code. Allerium provides point releases to address specific field issues on a quarterly basis unless we deem the issue significant enough to warrant an immediate point release. We execute all software releases per our ISO-certified development and release process and include a contingency rollback plan. We schedule all upgrades with the customer and provide release notes before implementation.

Decision-Making Processes

Scheduled releases usually contain a combination of feature enhancements and defect resolutions. Allerium determines the specific content of either kind of release by way of discussions with Allerium customers, industry adoption and preparedness for new features, targeted enhancements to existing features, and the severity and scope of the defects under consideration.

Defect-Resolution Software Releases

Frequency

We deploy releases on an as-needed basis. Given our rigorous development and pre-integration testing, the frequency of software defects is low.

Decision-Making Processes

Allerium's product organization works with the software development, systems engineering and operations teams to review the defects and prioritize the candidate items for a given release. Candidate defect criteria to determine defect resolution include:

- Customer impact,
- Source and scope of the defect,
- Severity of the defect, and
- Whether a temporary fix is available.

Based on the review by the teams, we include defect resolutions in quarterly point releases or bi-annual releases to address the targeted defects. We execute all software releases per our ISO-certified development and release process and include a contingency rollback plan.

Formal Process for Updates/Fixes/Improvements

Testing, Validation & Risk Mitigation

Prior to production deployment, all changes undergo structured validation in Allerium's dedicated lab environments. Test results are formally documented and attached to the IBOP record within the ITSM system to ensure technical completeness and operational readiness.

For complex or higher-risk modifications,

- Cross-functional Change Advisory Board (CAB) review is required.
- Director-level oversight is enforced for Level 1 and Level 2 changes.
- Client-facing Change Control Boards (CCB) may be convened when required by State governance.
- Vendor stakeholders are included in coordination discussions when applicable.

To further strengthen risk prevention, CAB meetings are held twice weekly to provide timely review of increasing change volume and complexity. This enhanced cadence reduces backlog risk, improves scrutiny, and minimizes change-related service disruptions.

Structured Approval & Oversight

Approval authority scales according to risk and impact:

- Routine operational updates may be completed within ITSM workflow.
- Moderate to high-impact changes require CAB review.
- Vendor-initiated maintenance impacting shared infrastructure is incorporated into the CAB review process when appropriate.
- Emergency changes follow an expedited Emergency IBOP process with shortened approval timelines and post-implementation review.

The Change Manager chairs and facilitates all CAB sessions, ensuring:

- Complete documentation and approvals prior to review
- Structured evaluation of technical quality and operational readiness

- Cross-functional accountability
- Vendor coordination when applicable
- Formal decision recording and follow-up tracking

This governance model ensures transparency, accountability, and alignment across Engineering, Operations, NOC/SOC, vendors, and program leadership.

Communication & Stakeholder Transparency

Allerium utilizes an automated notification platform supporting user-defined escalation tiers and multi-channel delivery (email, SMS, and voice). Notification preferences are established during implementation and may be modified at the State's request.

Stakeholders receive:

- Advance notice for scheduled changes
- Pre-work emergency notifications when applicable
- Vendor maintenance coordination notifications when third-party systems are involved
- Post-implementation confirmation
- Escalation updates if abnormal conditions are detected
- This structured communication model ensures that States, PSAPs, designated third parties, and vendor partners maintain continuous situational awareness.

5.8.6. Spares and Inventory

5.8.6.1. Spares

8.6. Spares and Inventory

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.*

Response:**Spares Overview**

Allerium implements a comprehensive tiered spares program for each of its NG911 markets that initially resolves around redundancy. Multiple call paths are generally used to reduce or eliminate single points of failure.

Critical spares are identified during the engineering phase. Some of these, through relationships with our major vendors, are available through a 24-hour replacement program as part of our maintenance contracts with them.

Other equipment is sourced from our vendors and kept at strategic locations throughout the market, to help reduce MTTR.

Lastly, failure analysis is conducted post-implementation to identify high rate of failure devices so inventory levels can be adjusted and / or additional sparing options can be considered.

Describe the spares program, including stocking levels, locations, and technician access time

Allerium provides a tiered response to sparing. Maintenance contracts with our major vendors provide 24-hour replacements for some of the larger critical equipment. Other gear is identified and placed at a number of climate-controlled storage depots with each of them no more than 60-90 minutes away from the field technicians. In addition, analysis is done of failed component type and quantity so inventory levels can be adjusted, and potential additional options can be evaluated.

Sparing quantities are typically a percentage of deployed assets, increasing as deployment and maintenance activities grow and tracked by using an in-house asset inventory system (Remedy).

Explain any State role in spare stocking or access

Any state facilities that might be strategically placed and offer 24-hour access and secure storage could be made depot locations. This could offer locations closer to PSAP locations which would reduce time to access spares.

Show how sparing maintains required MTBF/MTTR to achieve 99.999% availability

The diverse nature of engineering design is the primary factor to MTBF / MTTR availability. Localized sparing, however, offers added redundancy by placing critical gear near where it is potentially needed. This coupled with a robust field support and dispatch policy helps ensure timely identification and replacement of failed equipment.

5.8.6.2. Spare Inventory at Data Centers

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.*

Remainder of page intentionally blank

Response:

Spare Inventory at Data Centers Overview

Allerium's comprehensive sparing program for data center locations starts during the initial engineering design and is centered around diversification. Multiple call paths generally help to eliminate single points of failure.

Identified critical inventory is spared in a tiered approach, with some equipment available for 24-hour replacement through relationships with our major vendors and other equipment stored on-site.

On-site critical spare inventory at each data center.

Data center sparing needs are identified during the engineering process. Some of this is spared through partnerships with our major vendors. Other items are sourced based on a percentage of deployed assets and kept at each data center.

Identification/documentation of inventory.

Each spare item is asset tagged and tracked via our in-house management system (Remedy). This tool helps us to identify quantities, failure rates and re-order points.

Additions based on repair frequency/type.

Initial sparing levels are a percentage of deployed assets. Failures of this equipment, either in a data center or field environment, are analyzed for frequency and replenishment timeframes to identify if any adjustments are needed. This can result in an increase in our sparing quantity, evaluation of alternate vendors, or other arrangements.

Replenishment for repeated malfunctions/failures.

Any identified high failure items are put under review for mitigation. This can result in added quantities kept on site and/or alternate vendors being identified. Often this is done in tandem with our engineering team to determine if any design or other changes are needed to reduce the frequency of events.

5.9. Value Add and Optional Services [Project Requirements and Scope of Work, Section E.9]

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.

Response:

Allerium has described its optional CHE services and optional ESInet and NGCS backup system below.

Additionally, Allerium has included an option for geospatial professional services. Based on our experience, delays in deployment and/or difficulties with ongoing maintenance have come about due to data not being ready and maintained for geospatial call routing. We recommend that geospatial professional services be employed to ensure no delays in the implementation process and to, likewise, ensure proper GIS maintenance.

5.9.1. Call Handling Equipment (CHE) Services

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.

Response:

Allerium has had tremendous success in delivering similar Guardian call handling solution implementations as those desired by the State of Nebraska. Within the State of South Carolina, a hosted Guardian system has been successfully supporting 46 remote PSAPs with 322 positions for several years, and more and more PSAPs are being brought on-line every month. The solution can grow as needed to accommodate the additional positions to deliver a similar call handling experience for all PSAPs.

This expertise in deploying highly reliable, ESInet ready NG9-1-1 call handling solutions has also been brought to bear in the State of Ohio, which boasts a similar Guardian offering.

Other statewide deployments include the states of Vermont, Maine, New Hampshire, and Rhode Island, and Allerium has also engaged with the provinces of New Brunswick and Prince Edward Island in Canada to provide a Guardian solution in a similar manner.

Allerium would be pleased to further discuss the needs of the State of Nebraska as it evolves its NG9-1-1 solution.

Overview

The Guardian system is a powerful and flexible public safety call handling solution, designed to open standards, and is IP from the core to the telecommunicator user interface. Guardian is a modular and scalable platform, designed specifically for public safety, and provides a seamless migration from legacy emergency communications to NENA i3 standards. The Guardian solution can be deployed in a multitude of configurations—ranging from traditional stand-alone systems and geographically diverse configurations to hosted configurations—all designed to meet the needs of today's 9-1-1 customers. The Guardian NG9-1-1 communication system is also provisioned with standardized interfaces to external systems, including CAD systems, logging recorders, PBXs, ALI databases and other ancillary systems.

Guardian is constructed entirely from off-the-shelf components. All components are rigorously tested by Allerium before being certified for use in the Guardian solution.

The proposed solution includes no single point of failure that will result in any loss of functionality. The system uses demonstrated best practices of replication, redundancy and diversity to deliver mission-critical levels of system availability.

Allerium delivers an innovative approach to NG9-1-1 by offering a versatile and easy to use Guardian NG9-1-1 platform. The Guardian offers a portfolio of public safety appliances and applications that have been developed according to i3 NENA 08-003, providing a simplified means of interfacing with any NENA compliant system. The architecture is flexible to adapt and scale to new functionality that will be implemented and standardized in the future.

The solution manages IP calls end to end while supporting legacy interfaces to allow for a phased migration from legacy to new IP technology solutions.

Allerium is a leader in using IP-based interfaces between its NG9-1-1 solution and other 9-1-1 systems. Allerium has all the required serial interfaces to CAD, ALI, Map, etc., but has also implemented these interfaces over direct IP links. In addition to having both serial and IP interface options, Allerium can manipulate the data being sent over these links. Manipulation of the ANI/ALI and location information format allows the Guardian system to adjust to any specific requirements of CAD/Map systems. This dual capability of flexible connection type with data manipulation ensures the system interfaces optimally with existing and future sub-systems.

Deployment Options

Hosted Configuration

In addition to its IP-based architecture the Guardian NG9-1-1 core supports multi-tenant operation which makes it ideal for hosted deployment. In a hosted solution, Guardian is configured for autonomous operation of multiple PSAP tenants. Although everyone shares common back room equipment, each PSAP is unique and determines how calls to their PSAP are routed and handled under normal circumstances and backup scenarios. The solution offers significant cost savings and a state of the art NG9-1-1 system that lets the PSAPs continue to operate independently.

One of the greatest advantages of a hosted solution is that it eliminates Selective Router boundary transfer issues. All calls being handled by the system can be easily and rapidly transferred, including the callers ANI, to positions at any of the hosted PSAPs, regardless of service boundaries.

In fact, based on interoperability agreements between hosted agencies, neighboring PSAPs can be mapped as resources on one another's workstations, facilitating one-button transfer for backup or alternate routing in overflow conditions.

Another advantage of a shared core is the ease and economy of implementing a regional disaster recovery backup PSAP. If a PSAP goes down for any reason, telecommunicators can log into the system from an alternate location, and access their 9-1-1 trunks and administrative resources as though sitting at their usual PSAP workstation.

In a hosted NG9-1-1 core scenario, a primary Guardian core supports multiple tenant PSAPs. Each tenant PSAP manages their telecommunicator positions, configuration and local call routing, yet share the same Guardian system with the primary host PSAP and other tenant PSAPs. Tenant PSAPs need not purchase expensive equipment and software. Incoming calls are processed at the host's primary core and sent to the tenant PSAPs. For example, a tenant PSAP operating on a legacy infrastructure can answer and respond to a call from an IP platform.

Typically, in a Hosted NG9-1-1 configuration, the Guardian core equipment is installed at the primary PSAP host location. It can be configured to be geo-diverse if required. Figure 67 shows a hosted solution at a single location, and Figure 70 shows a geo-diverse hosted solution.

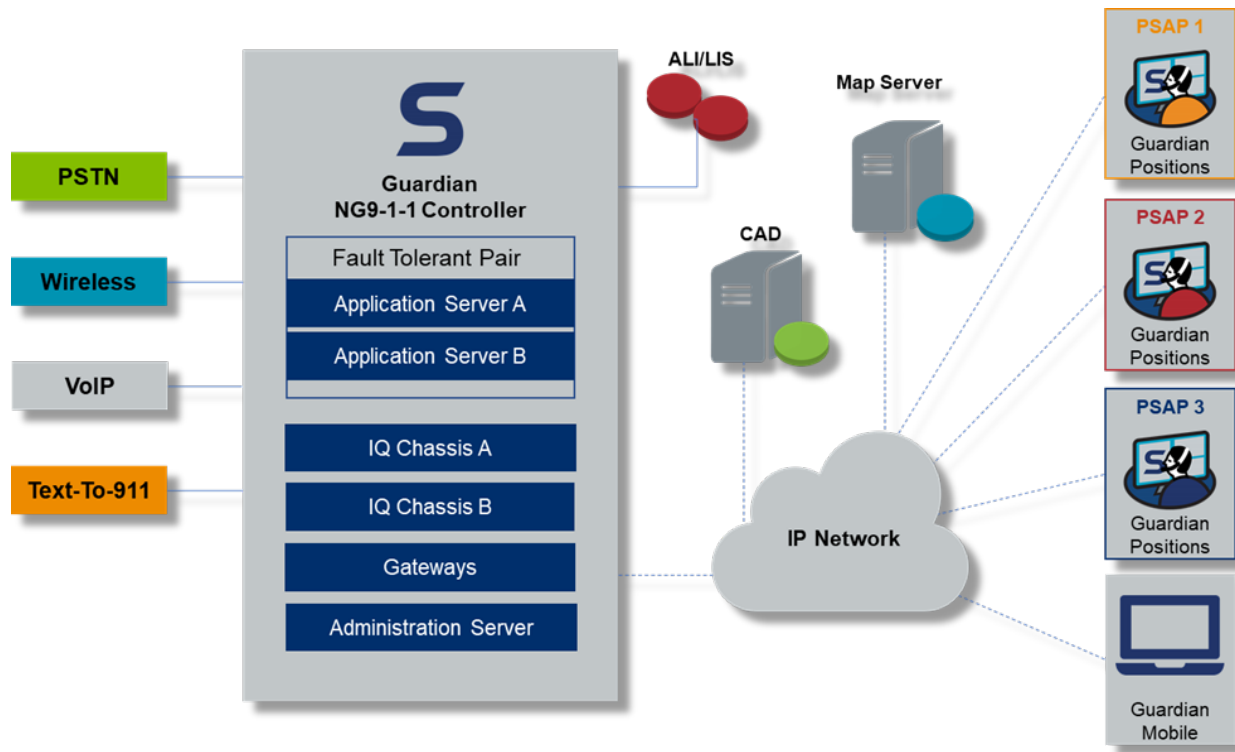


Figure 67. Typical Hosted Guardian NG9-1-1 Solution (Single Location)

Standalone Configuration

A standalone Guardian NG9-1-1 core is normally configured to host and support a single PSAP and is located in the equipment room at a single location. A number of call taking positions are connected to it requiring only a single IP connection. The number of positions supported depends on the configuration and the call distribution scheme required.

Figure 68 shows a typical Guardian standalone configuration.

In the standalone configuration, incoming trunks and circuits are diversified between Side A and Side B interfaces. Data is automatically replicated between the two sides. However, a single administration and maintenance application allows the operation of both sides as a single system. The complete redundant system is normally racked in a single cabinet but can be split into two cabinets upon customer request.

The system supports analog emergency trunks, analog administrative circuits, SIP connections (VoIP) and digital interfaces (T1, ISDN). It supports NENA legacy interfaces to ALI circuits and CAD systems, and also supports next generation ALI over IP (NENA AQS).

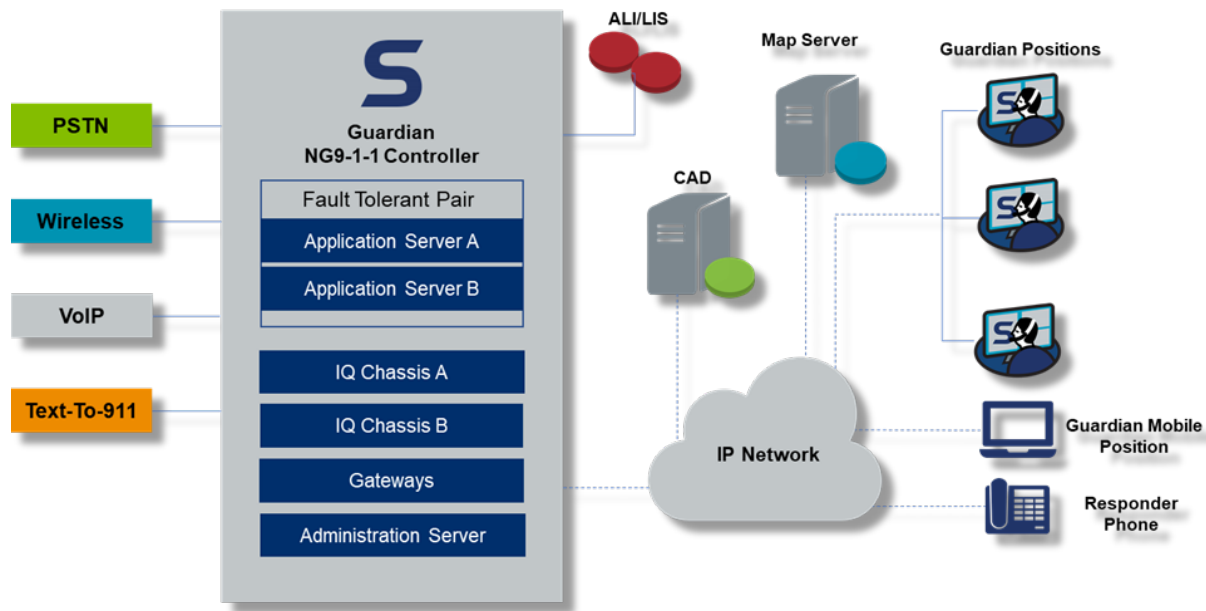


Figure 68. Standalone Guardian NG9-1-1 System

Geo-Diverse Configuration

Due to its IP-based architecture, the two sides of a Guardian NG9-1-1 core can reside in different geographic locations. It has been designed such that each site can operate on different IP networks therefore simplifying network design; the only requirements are adequate bandwidth (100 Kbps per position, trunk or administrative circuit) and latency (< 150 ms).

A typical deployment scenario consists of a primary site that is normally in operation and a backup site that goes into operation in the event of overflow, or when the primary can no longer operate. Since Guardian has been designed to be Active/Active, telecommunicator positions can be located at both sites and connect to either side depending on operational.

Figure 69 shows a typical geo-diverse Guardian NG9-1-1 core configuration where call processing occurs on a pair of application servers, Side A and Side B, that reside in different locations.

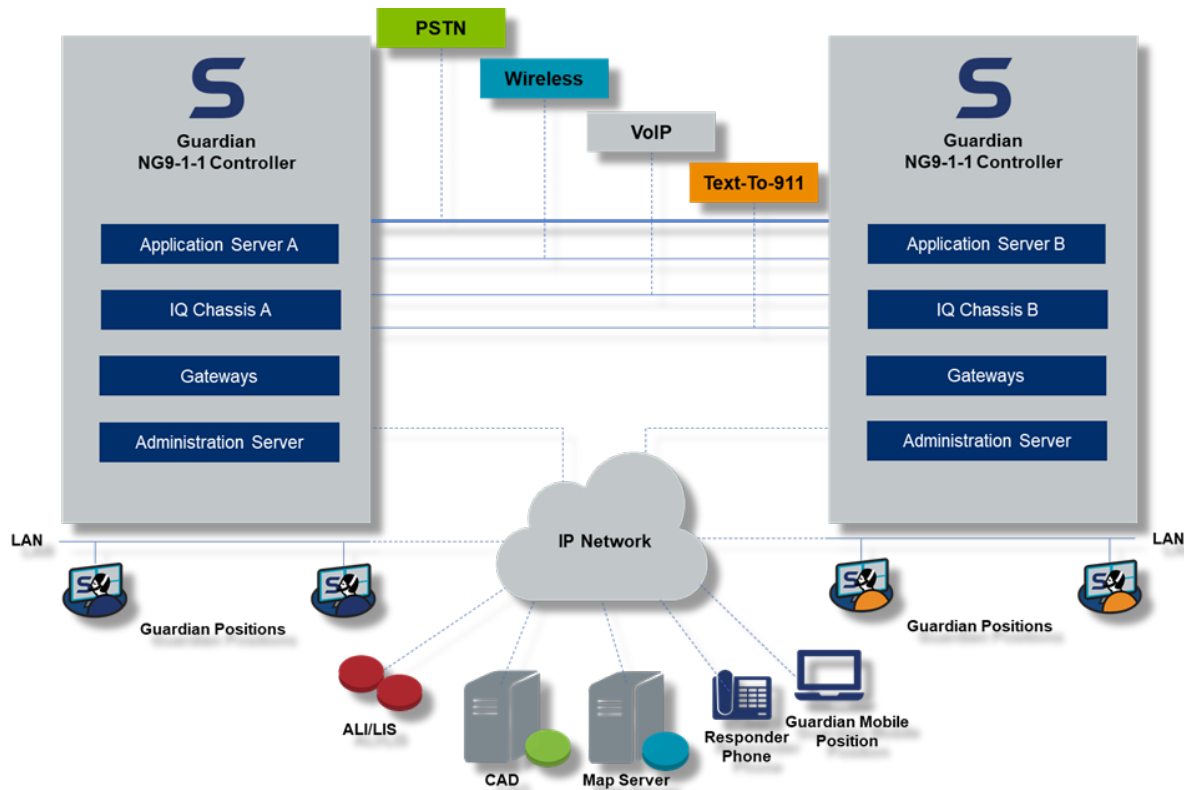


Figure 69. Typical Geo-Diverse Guardian NG9-1-1 System

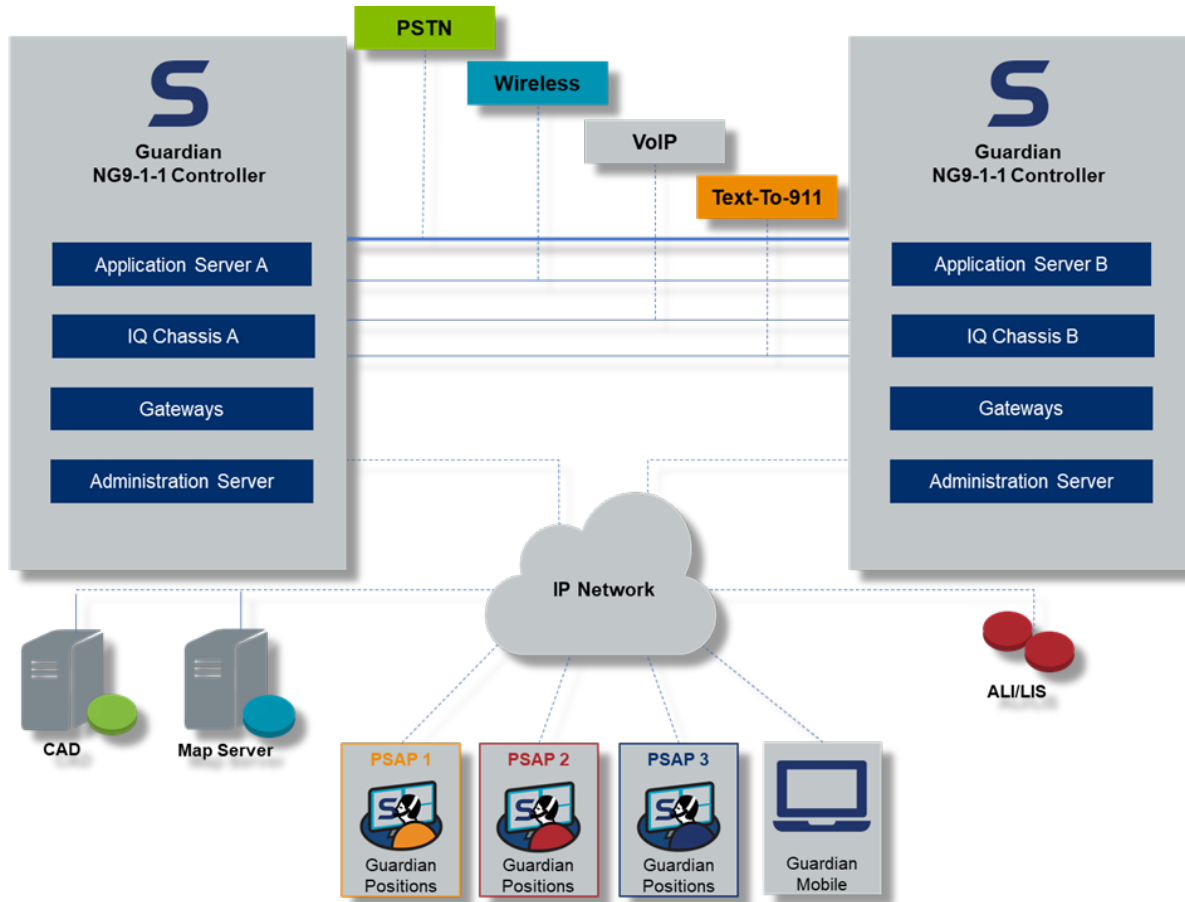


Figure 70. Typical Hosted Guardian NG9-1-1 Solution (Geo-Diverse)

Guardian Workstation

The core of every PSAP is a great call taking workstation. The Guardian Workstation brings IP to the desktop and delivers a new level of performance for responding to all types of calls. Guardian Intelligent Workstation interfaces with Computer Aided Dispatch, voice recording, video, Short Message Service, and Instant Messaging. Call takers can handle 9-1-1, administrative, enterprise PBX, 211, 311, 511, and 711 lines all in a unified environment.

The Guardian Intelligent Workstation is an extremely powerful next generation 9-1-1 call taking position designed to maximize the effectiveness of call taking. The intuitive graphical user interface allows call takers to quickly assess, prioritize and handle wireline, wireless and VoIP calls. All calls, regardless of network of origin, are transported and processed as VoIP calls within the Guardian system - with identical speed and accuracy.

Available Equipment

The workstation solution consists of the following available equipment:

- Workstation with keyboard and mouse
- Monitor(s)
- Integrated dual instant recall recorder (IRR)

- Position Audio Control (PAC II) which supports three modes of operation:
 - 9-1-1 call taking
 - Radio integration
 - External radio integration.
- Handset or headset
- 24 or 48-button keypad
- SMS, MMS and video support

Available Features

While not a comprehensive list, the following outline some of the features available on the Guardian workstation:

- Automatic call distribution (ACD)
- TDD/TTY/Real-Time Texting (RTT)
- Text-to-911 and Text-from-911
- Call hold
- Speed dialing
- Contact list
- Status bar
- Abandoned call capture
- Virtually unlimited conferencing
- Intelligent transfers
- Automatic redial
- Translation/transcription
- Automatic call/text back
- Full support of ESInet call delivery (as well as legacy if and as required)
- Support for images and video
- Full suite of interfaces for CAD, logging recorders, ancillary systems such as RapidSOS, etc.
- Intuitive and completely configurable graphical user interface (see Figure 71 and Figure 72)
- Mapping (see Figure 73)



Figure 71. Typical Graphical User Interface Layouts (Sheet 1 of 2)

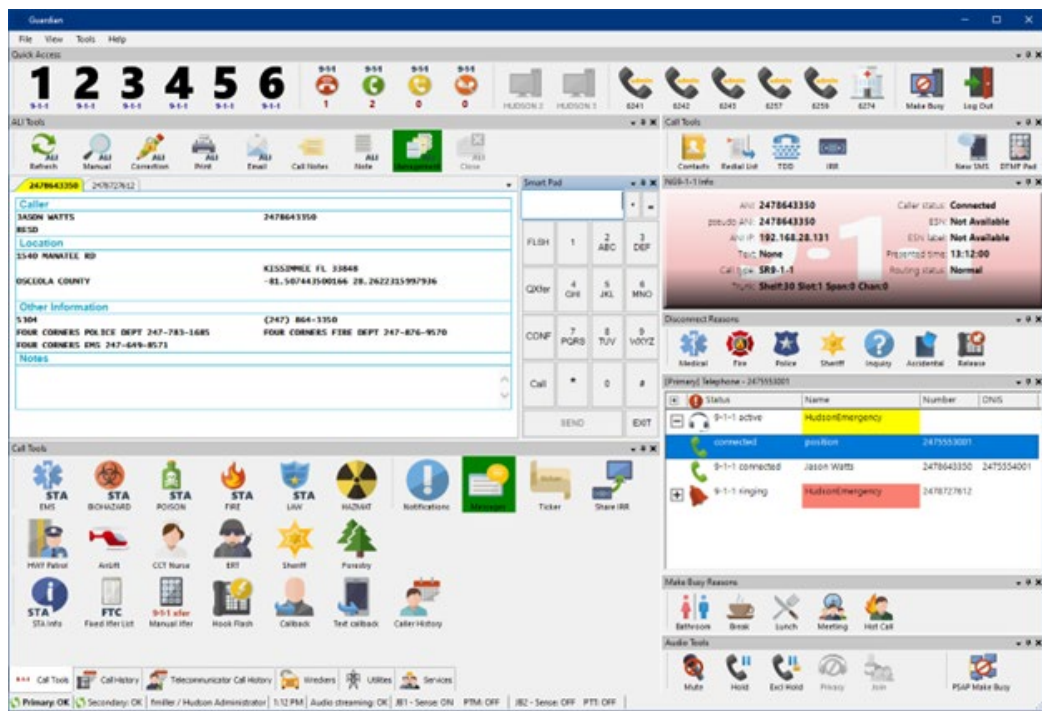


Figure 72. Typical Graphical User Interface Layouts (Sheet 2 of 2)

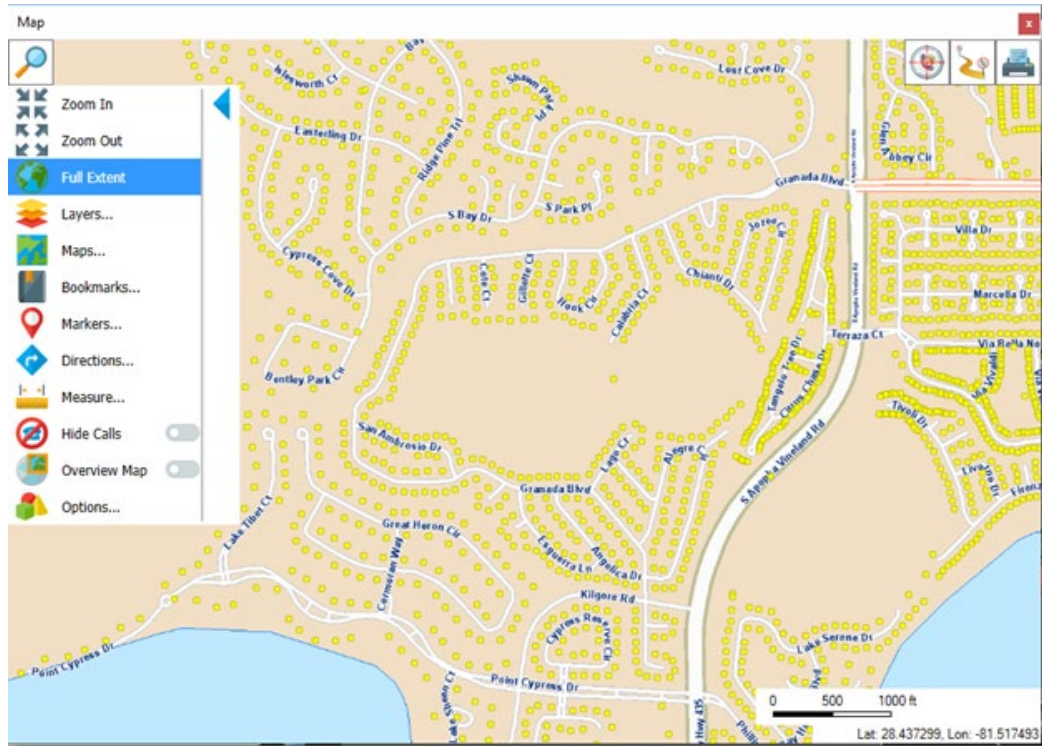


Figure 73. Map Display with Main Menu Opened

System Architecture

The Guardian Next Generation 9-1-1 system hardware components are carrier grade and engineered to offer a 99.999% system reliability. The system is configured with no single point of failure, ensuring that no single event would result in any loss of functionality. A pair of application servers (Side A and Side B) operates in an active/active mode, as a virtual pair. System information is automatically replicated between each server and synchronized by the software.

Guardian workstations are dynamically controlled by the core equipment and if a failure of either server is detected or network connectivity is compromised the position will automatically switch to the available server.

Component Failure

The Guardian solution has been designed with multiple layers of redundancy, offering no single point of failure. The Guardian system will deliver 99.999% availability using demonstrated best practices of replication, redundancy and diversity to deliver mission-critical levels of system availability.

- **Replication:** At the core of the proposed solution are two continuously available application servers which deliver 99.999% availability – one on side A of the system and one on side B. The servers operate in active/active mode. Data is replicated between the two servers, ensuring equal data availability. Either server is capable of supporting the required call processing capacity.
- **Redundancy:** All vital modules are deployed redundantly to ensure that failure of a module does not result in system downtime or loss of system functionality.

- **Diversity:** Telecommunication circuits are distributed across multiple interface modules, ensuring only a minor and temporary decrease in system capacity in the unexpected event that an interface module fails (until the module is replaced).

Replication is used to maintain the two sides in synchronicity.

The system's Side A – Side B architecture is designed such that failure of a major component does not result in system downtime. Furthermore, system maintenance and/or upgrades can be performed without downtime. The system's reaction to the failure of a major component is described below:

- **Application Servers:** The Side A – Side B architecture ensures that failure of an application server does not result in the loss of active calls or system functionality. Either server is capable of supporting all system call processing; failure of a server does not result in a loss of calls or system functionality. If the system detects a problem with the Primary side's application server, telecommunicator positions will automatically be moved over to the Secondary side.
- **VoIP Switching Modules:** The solution is configured with a redundant pair of VoIP Audio Switching Modules. One VoIP module can support the system entire audio switching requirements. Failure of a VoIP module does not result in loss of calls or system functionality. If the system detects a problem with the Primary side's VoIP Module, telecommunicator positions will automatically be moved over to the Secondary side.
- **Administration Server:** Failure of the administration server does not have an impact on call processing, however, system administrative capability will temporarily be restricted.
- **MIS Server:** Failure of the MIS server does not have an impact on call processing, however, system administrative capability will temporarily be restricted.
- **Guardian Workstation:** The failure of a telecommunicator position results in a minor and temporary reduction in system capacity i.e. one less telecommunicator position but does not result in the loss of active calls or system functionality. Calls that are active at a telecommunicator workstation will not be lost, instead they will be maintained by the system and returned to the call queue.
- **Media Gateway:** The system can be configured with multiple gateways distributing administrative circuits – Media gateways offer the best survivability strategy for traditional circuits. By diversifying circuits across multiple gateways, the potential impact of a failed gateway is minimized. In the event of a gateway failure, there will be an isolated loss of capacity, affecting only those legacy circuits associated with that particular gateway, until the gateway is replaced. There will be no loss of system functionality.
- **Emergency Gateway:** The system can be configured with multiple gateways distributing emergency circuits – Emergency gateways offer the best survivability strategy for traditional circuits. By diversifying circuits across multiple gateways, the potential impact of a failed gateway is minimized. In the event of a gateway failure, there will be an isolated loss of capacity, affecting only those legacy circuits associated with that particular gateway, until the gateway is replaced. There will be no loss of system functionality.
- **Ethernet Switch:** The system will be configured with multiple diversified Ethernet switches to minimize the impact of a failure. The precise impact of a switch failure is dependent

upon the devices connected to a particular switch. All critical redundant components will be connected to two switches. Failure of one switch will not result in the loss of call processing capability.

Functionality

In the standalone configuration, incoming trunks and circuits are diversified between Side A and Side B interfaces. Data is automatically replicated between the two sides - however a single administration and maintenance application allows the operation of both sides as a single system. The complete redundant system is normally racked in a single cabinet but can be split into two cabinets upon customer request or for geo-diverse implementations.

5.9.2. ESInet and NGCS Backup System

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.

Remainder of page intentionally blank

Response:

The Allerium service provides several alternate/backup systems and routes to increase availability in the service. The most practical approach to increase redundancy is to provision a path outside of the normal ESInet. That path can be an unrelated physical path (for instance, a wireless circuit when the primary circuits are on fiber) or across the PSTN, the most direct route to avoid crossing the ESInet or requiring the CHE to be available. For clarity, we have described the overall operation of the service with regards to alternate and backup routing with more detail below.

Network Failure

In the event that the CHE is available but network issues are prevalent, the following routing will take place (dependent on each site's pre-provisioned planning):

1. **Network Convergence:** Each PSAP site is provided with at least two, with the possibility of three, ESInet circuits. Network convergence will occur in under one second if any of the circuits to the site become unavailable. Calls will not be dropped, and the convergence is transparent to all members of the call.
2. **Alternate Routing to PSTN:** If all circuit paths to the PSAP are unavailable, the pre-provisioned alternate routing plans that exist in the PRF rules will come into play. Alternate routes include the ability to reroute the calls away from the ESInet and onto the public telephone network (i.e., the PSTN). Call delivery will then occur from the NGCS to the PSAP through the PSTN until the ESInet has recovered.
3. **Alternate Routing to Another PSAP:** If the PSTN is not provisioned as a desired alternate path, then the NGCS will route the call to a pre-provisioned alternate PSAP.

Call Handling Equipment Failure

Similar to the NGCS/ESInet service, the CHE provides multiple solutions for call delivery if the primary CHE equipment is unavailable, including:

1. **CHE Side-B:** For PSAPs that have deployed with a geo-redundant Guardian Side A / Side B configuration, the surviving “side” of the CHE is available to process incoming calls.
2. **Guardian CHE Survivability Controller:** Allerium provides a Survivability Controller which is available as a separate system deployed at the PSAP to ensure call continuity if the PSAP so elected the solution. The Survivability Controller is located at remote PSAPs which behaves as a third node (node C) in the Allerium architecture. Provisioning is done at the core as normal and replicated to the Survivability Controller, mirroring the exact system resources as the host controller (e.g., usernames and passwords, system contacts and resources, and screen layouts). The purpose of the Survivability Controller is to allow remote PSAPs to continue operations when they become isolated from the host controller (i.e., network outage). For the Survivability Controller to function properly, trunks and lines should terminate locally at the remote PSAP. Currently, this holds true for admin lines, which trunks terminate at the host controller. An activity will take place to redirect those trunks back to remote PSAP locations. To fully benefit from the Survivability Controller’s design which includes displaying ALI, at least one ALI circuit should terminate at the remote PSAP locations. Trunk, line and ALI circuits will be coordinated through local providers.

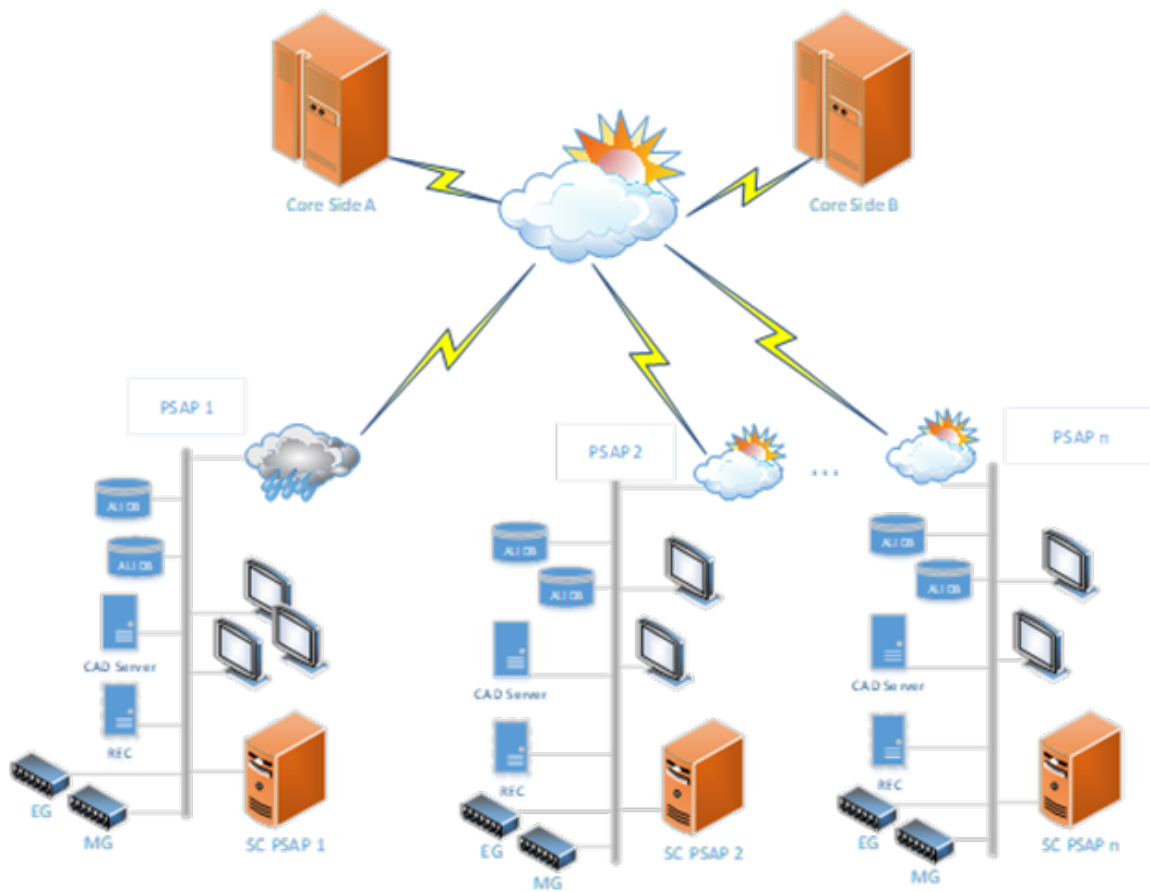


Figure 74. Sample Guardian Survivability Controller Design

5.10. Use Case Examples for Use with Response [Project Requirements and Scope of Work, Section E.10]

5.10.1. Instructions

10. Use Case Examples for Use with Response

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.

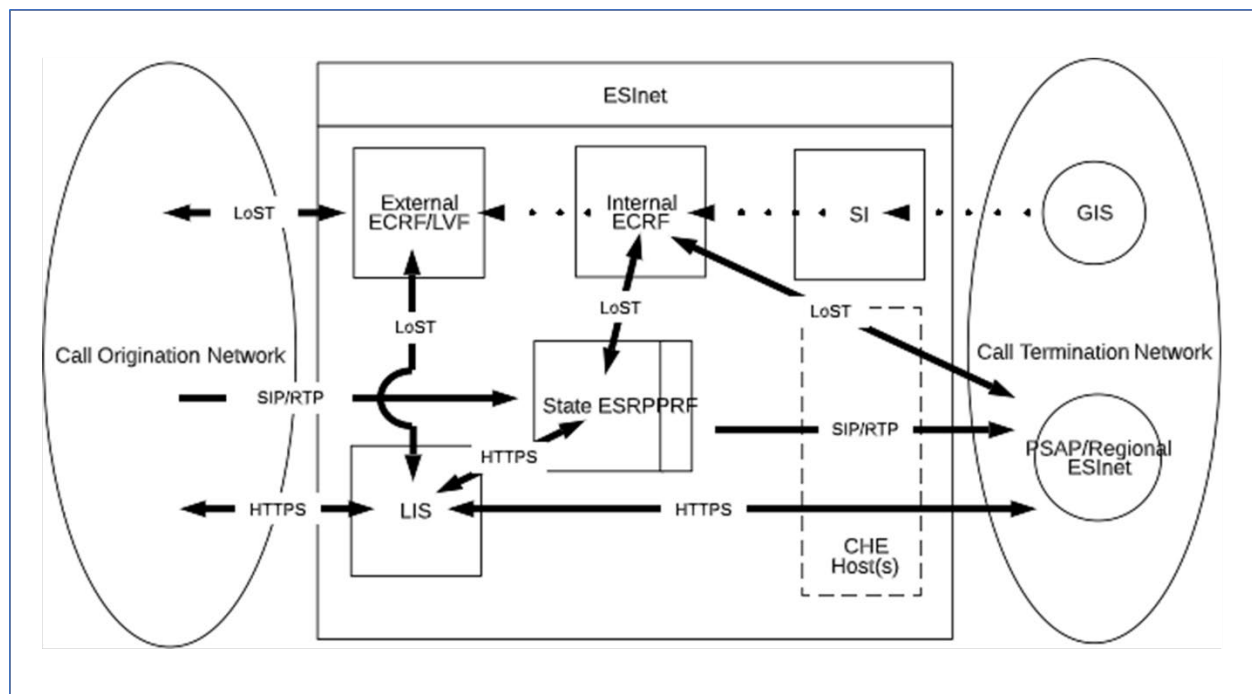


Figure 3: High-level NENA i3v3 Architecture

Remainder of page intentionally blank

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.
 - o 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.
 - o 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.
 - o At each functional element, a description of how the interface between the functional elements will be utilized.

- o 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.*
- o 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.*
- o Identify how systems operate in a “normal” state.*
- o Identify how systems operate in an “abnormal” condition.*
- o 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.*
- o Identify how DDoS and TDoS events are mitigated.*
- o 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.*
- o Identify how databases operate.*
- o Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.*
- o Explain how logging is collected and accessed for legacy CDR and i3 logging.*
- Describe how calls may be transferred between NG PSAPs.*
- o 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.*
- o 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.*
- o Describe how transfers are logged and how the data is logged.*
- o Discuss the data that is transferred to the receiving PSAP.*
- o 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.*
- o 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.*
- o 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.*

Remainder of page intentionally blank

Response:

Meeting the Depicted Functionality

Allerium has been deploying NG9-1-1 services for 15 years and has completed over a dozen statewide and large regional deployments. In addition, we provide 9-1-1 routing services to two of the three largest carriers, and provide service, in one fashion or another, to nearly every PSAP of the 5000+ PSAPs in the United States. To date, none of the deployments are designed in the way the above diagram depicts. While the diagram does represent a possible future state and is in alignment with the overall NENA i3 design, please consider the following narrative as the actual deployment approach.

The diagram below illustrates the reality of how NG9-1-1 deployments are completed. The two RED-outlined components (the External ECRF/LVF and the LIS) are not implemented in this fashion today.

The External ECRF is positioned here as an interface for OSPs to query with LoST to determine routing. In reality, we work with each OSP to create point-to-point connectivity with them. Therefore, in Nebraska, we will identify each OSP that provides service today and will work with them to provision circuits to our points of ingress/interconnection (POIs), which aren't shown here, to provide either IP or legacy-based traffic ingress. This diagram does not show the POI functionality, but it is a core function of the deployment and creates a direct connection to the OSPs. With the direct connection, the OSPs do not query the ECRF for routing instruction.

Regarding the LIS, the diagram indicates that the LIS is part of the ESInet, adjacent to the other NGCS functional elements. In reality, the LIS is an OSP-provided function, outside of the NGCS, and is rarely in place today (with the exception being a LIS service we provide to VoIP customers). Realizing this, NENA describes a transitional element called the location database (LDB). The function of the LDB is to operate as a location database that accepts legacy inputs (such as SOI file updates) but also "speaks" NENA i3. The LDB is necessary until such time that every OSP has their own LIS database, which would reside in either a) the OSP's network directly, or b) in another network where the LIS is deployed as a service (e.g., the LIS Allerium provides to our VoIP customers). The diagram does not represent this situation accurately, despite it being the reality in every NGCS deployment today (not just Allerium's deployments, but for every NGCS provider).

The remainder of the diagram is accurate and deployed as shown. Our response addresses this in the remainder of this section.

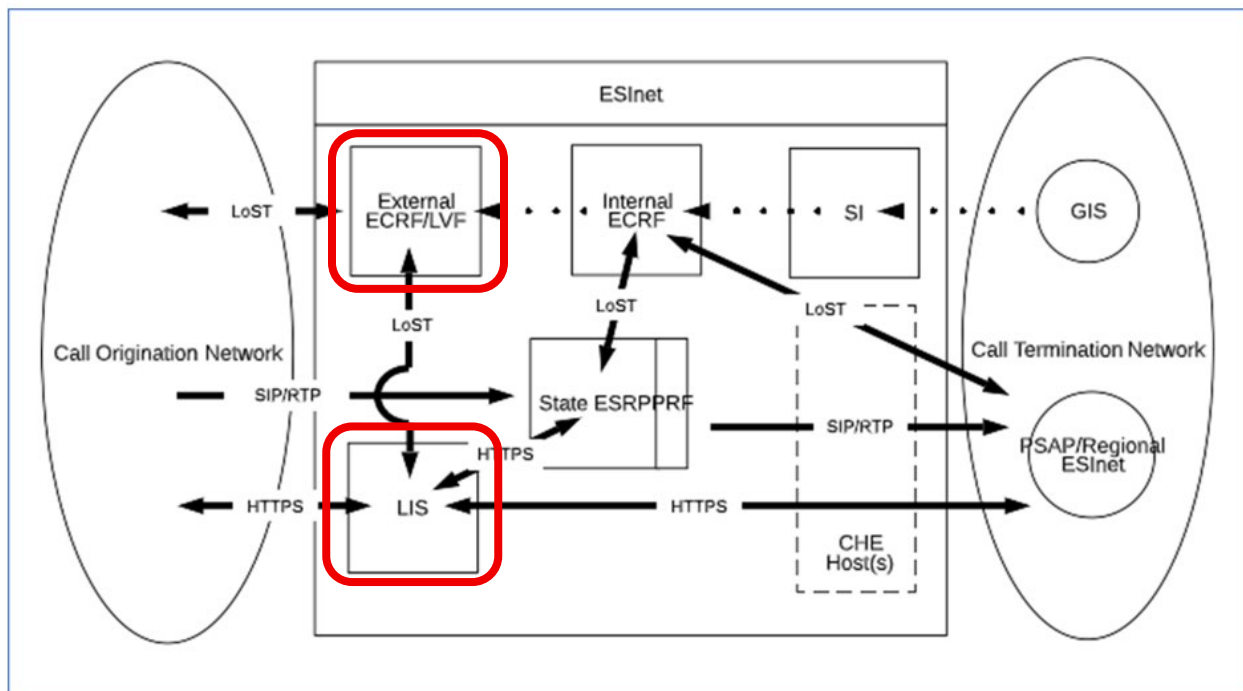


Figure 75. High-Level Future Architecture

Traffic Flows from the Call Origination Network through the Core to the PSAP

Allerium describes many different connection and call routing scenarios in our provided interface control documents (ICDs). For instance, “Emergency Call Origination” is outlined in detail and provides details for:

- URN format
- SIP URI values
- Route headers
- CBN and Identity values
- Geolocation headers
- Call-Info headers
- PIDF-LO treatment

Each section of the ICD is similar, with nearly 200 pages of detail provided for the State's review. For readability, general traffic flow will be discussed here but we welcome the State's interest in the ICDs.

Traffic flow, as it relates to the provided diagram above, starts in the OSP network and is delivered to the NG9-1-1 network in one of two manners - by SIP/RTP or through legacy TDM. Both functions exist at the POI location, which will either ingress the SIP/RTP directly or convert the TDM to SIP/RTP in a gateway. The call will then transit a SBC/BCF for security before being processed in the NGCS functional elements. The ESRP is the primary element, as depicted, which will query the location database (typically a LDB as described, or a LIS in a future state) to retrieve location information. Once a location is known, the ESRP will send a LoST query to the ECRF, which will use the provided location to determine the proper PSAP (next-hop URI) for delivery and return that identifier to the ESRP. The ESRP will use the policy routing function (PRF) and policy routing rules (PRRs) to determine if the identified PSAP is able to receive the call, and in normal operation the call will then be sent, via SIP INVITE) to the PSAP. Once accepted, RTP (the voice packets) will begin to flow to the PSAP and the path will be managed via the ESInet to ensure connectivity is maintained. When the call is finished, a BYE message is sent and the call is "torn down" through a SIP call termination process.

This call routing can better be described through ladder diagrams, of which here is one example for i3-compliant call delivery of a legacy (TDM) call.

All functional elements within our span of control are managed by our NSOC for monitoring and incident management. If any element experiences an error condition, a trap is generated and sent to the NSOC for investigation. Likewise, we have a variety of alarm conditions, threshold alerts, and process mapping alerts that occur for various possible error conditions.

Allerium is responsible, as the prime for the call ingress network (starting from the POI), the NGCS elements, and the ESInet (ending at the PSAP LAN edge). We offer an end-to-end management approach to eliminate "finger pointing" in our deployments. If the State or PSAPs need assistance, the NSOC is available 24x7x365.

Additional details regarding the call path, error conditions, alternate routing, connection protocols, and a host of other information is available in the provided ICDs.

System Performance Expectations

The entire NG9-1-1 deployment is scaled appropriately for the task at hand. For instance, at our POI locations we provide ports for each carrier to connect to at least two POI locations (physical capacity) and burstable licensing in our SBCs to accommodate every position in the state, simultaneously, to be on a call (licensing capacity). Bandwidth is provisioned to be non-blocking, with the various QoS and management strategies discussed throughout this response. Transaction capacity is load-tested in the lab prior to any deployment and far exceeds the call volume of the entire state for any one NGCS core - and with three cores all operating in active/active mode the transactional capacity is well above any possibility for congestion.

Allerium's ICDs go into detail on various abnormal conditions, including:

- Unexpected SIP INVITE dual messages
- Short-call (CANCEL) call handling
- Unexpected BYE received
- Unsupported or Unknown SIP Message
- Unexpected call transfer scenarios
- Catastrophic failure call routing

While each of the above (and more) are detailed in the ICDs, a general description of "abnormal" conditions and call flows is provided here. Generally speaking, each functional element is provisioned with a series of fallback options, with each option being specific to the element. For instance, if the ESRP tries to deliver a call to a PSAP and the PSAP does not answer, a Ring No Answer call scenario is invoked. The RNA scenario is pre-provisioned for every PSAP in that each PSAP will have selected, through the on-boarding process, an alternate treatment method in this case. Typical treatments include queuing the call, admin line treatment, and alternate PSAP treatment.

Implementing Security Across the System

Allerium implements a multi-layered approach to security, which we have described in the security section of this RFP response. As it relates to these specific security requirements, however, our service is designed with a zoned security model across the entire system. We implement four security zones, with the NGCS residing in a "trusted" zone and all other systems, including the PSAPs, operating in various levels of "untrusted" zones. In particular, the NGCS core, in its trusted zone, implements border control to enter/exit the trusted zone on the way to the PSAP. A secure tunnel is built between the NGCS core zone and the PSAP, with certificates, to ensure all traffic is encrypted between zones. This approach ensures security while maintaining performance guarantees.

As it relates to the DDoS and TDoS, we have separate mechanisms to deal with both possibilities. For DDoS, we place all externally-facing IPs in the "DMZ" untrusted zone so that external interfaces are kept to a bare minimum (typically for provisioning activity, report retrieval, and location data maintenance). If a DDoS event is detected by our cybersecurity applications and/or SMEs, we have a cloud-based DDoS mitigation service that diverts known "bad" traffic away from the externally facing applications.

For TDoS mitigation we have the technical ability to block devices/numbers that initiate the attack. Knowing that TDoS mitigation carries the risk of blocking valid 9-1-1 traffic, we always ask the State to define the policies that block 9-1-1 traffic in the system. We look forward to working on these policies with the State.

Delivering 9-1-1 Data to the Logging & Reporting System

Allerium's service includes internal logging and external log delivery. Logging and reporting can be described as these three related actions:

- Internal logging of call detail records (CDR) and elements
- Providing external logging/reporting functions a log stream of transactions
- Media recording (as a voice logger)

The internal logging and recording works in two ways, with call transaction detail records (TDRs) being collated into CDRs as one aspect and the other being logging and recording of service elements. CDR data collection is near-real-time (the only delay is waiting for the call to complete to finish the CDR collection) with the CDRs being automatically sent to a Splunk database for processing. The CDRs are then used for reporting, troubleshooting, and external reporting solutions like 911 Logix, who we use regularly in our own deployments. In addition to CDRs, each element in the service logs transactions and details relevant to that element (for instance, the ESRP logs ring no answer (RNA) events). System level events are logged in syslog servers dedicated to that task.

As mentioned, and as proposed here, we stream CDRs to external reporting engines as well. In the case of 911 Logix, we provide a stream of CDRs from the Splunk database to the MIS system. This stream of data is then used in generating the dashboard view of events.

Finally, as described in this proposal, we provide a NENA i3-compliant logger as part of the service to capture media/voice traffic. The voice logger has a dedicated interface for access while the internal transactional logging can be accessed through the Splunk database using internal MIS systems. Allerium has partnered with Equature for the voice logging functionality. Additional information regarding the voice logger is provided below:

- **Call Recording Flow:** When a 911 call is established through the ESInet (BCF → ESRP → BCF → PSAP), a BCF or Bridge, or call-handling equipment acts as a Session Recording Client (SRC) and initiates a SIPREC session with Equature's Logging Service Session Recording Server (SRS). The SRC delivers a copy of all call media (voice, video, text) to the Logging Service in real-time without impacting the call path.
- **Database Operation:** Equature stores call metadata in a Microsoft SQL Server database and media files on local SSD storage at the customer site. All data is indexed for rapid retrieval. The database maintains referential integrity between call records, media files, transcripts, AI classifications, and associated metadata (ANI, ALI, PIDF-LO, CAD data).
- **Local Recording:** For PSAPs that choose local recording, Equature servers are deployed on-premise at the PSAP. The server captures all media locally, performs AI processing via the Nexus cloud, and stores all recordings on local storage — maintaining full data sovereignty.

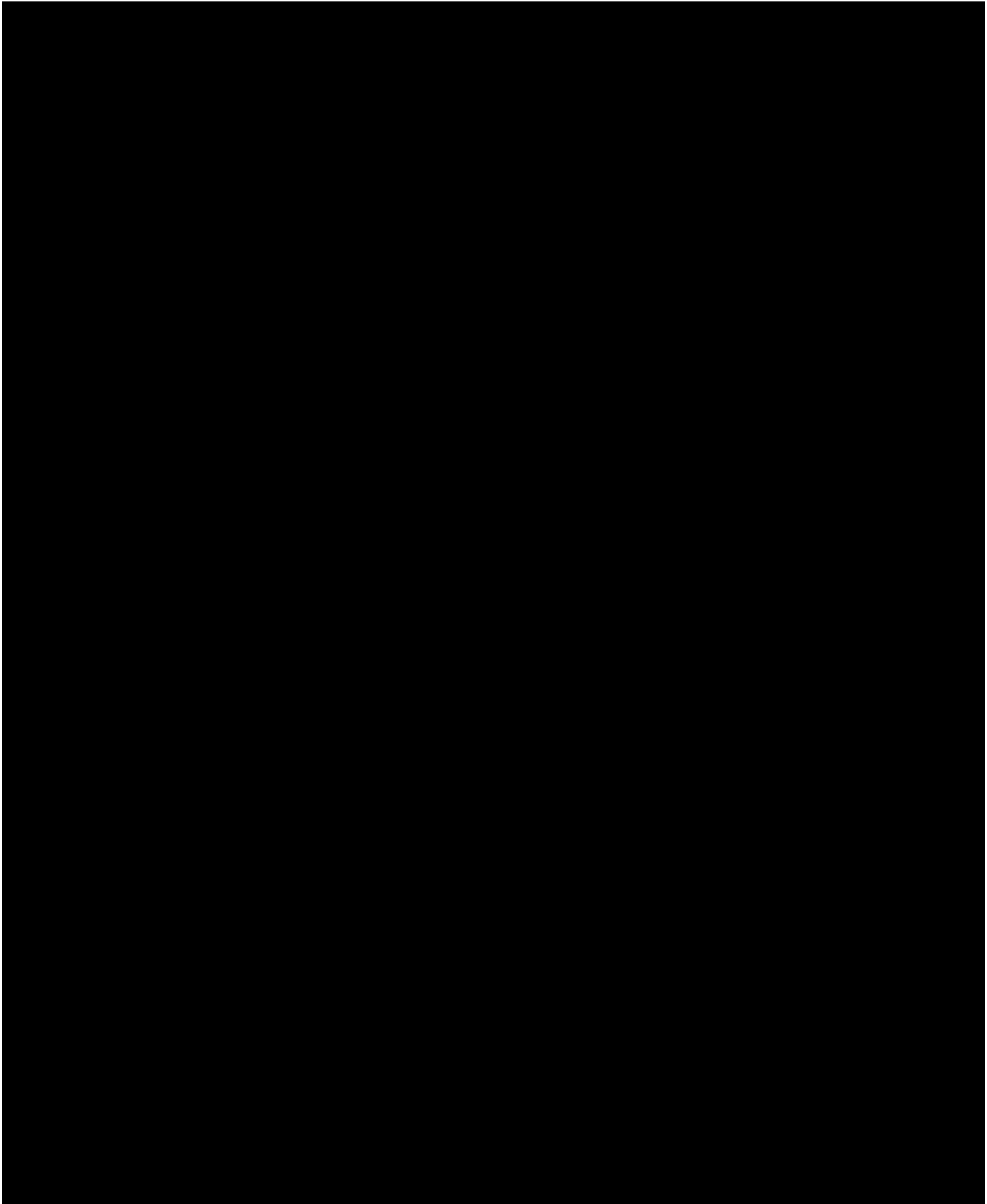
- **Hosted Recording:** For PSAPs that prefer hosted recording, Equature supports centralized logging service deployment where media is delivered to a State-hosted or cloud-hosted Logging Service instance via SIPREC over the ESInet.
- **Legacy CDR and i3 Logging:** Equature supports both legacy CDR-style reporting (call detail records with timestamps, ANI, duration, device) AND full i3 logging (structured LogEvents per NENA-STA-010.3). Legacy PSAPs connecting through an LPG receive the same level of recording; the Logging Service normalizes all data into the i3 format for unified retrieval.
- **Transfer Logging:** When calls transfer between PSAPs, Equature's Logging Service captures the complete transfer chain. Each leg of the call is recorded with SIP signaling data including History-Info headers, reason codes, and transfer targets. The Scenario Replay feature in ViewPoint allows supervisors to reconstruct the entire multi-leg call as a single incident timeline.

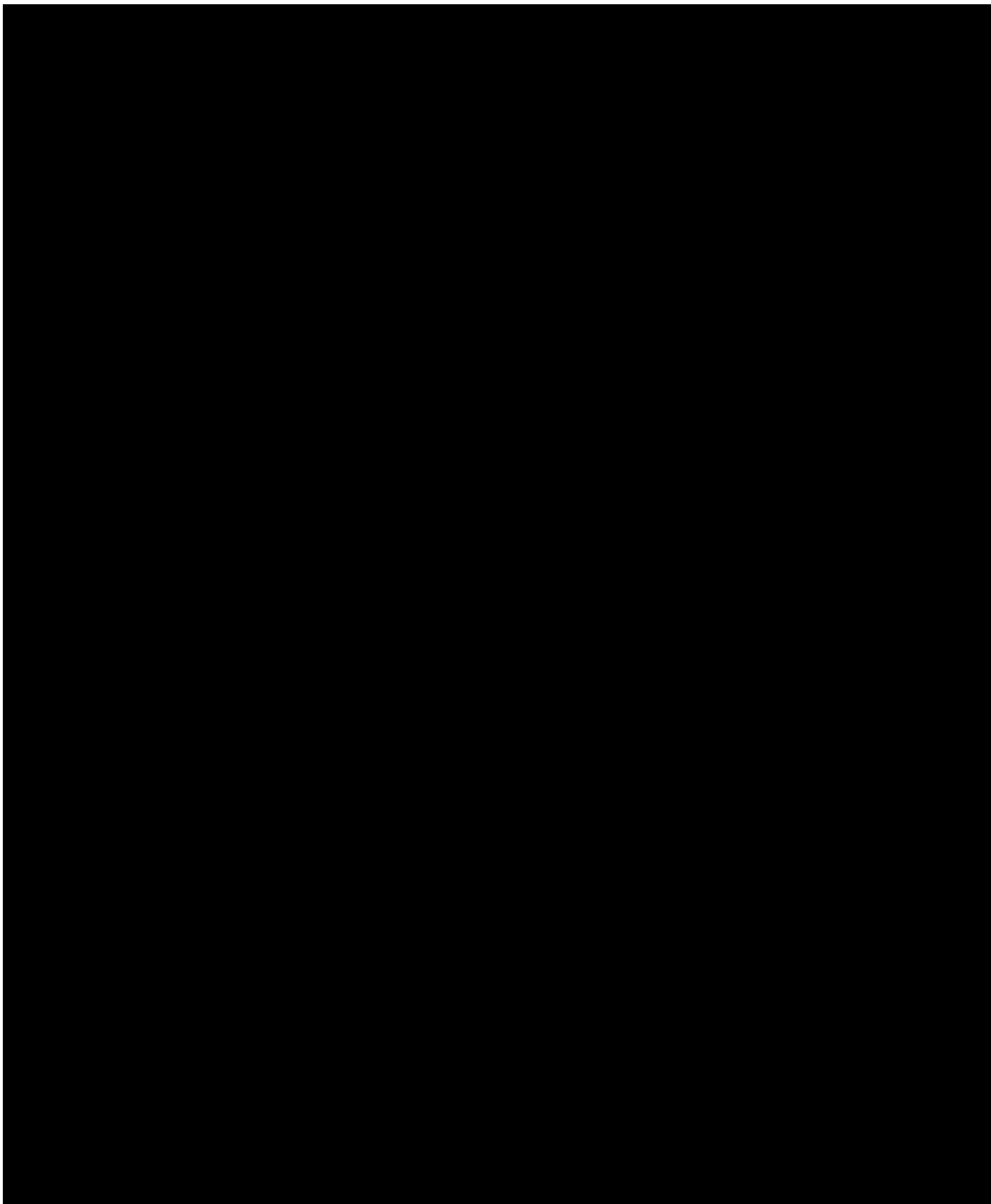
Transferring Calls between NG PSAPs

When discussing call transfers, there are multiple scenarios depending on the ESInet, PSAP, legacy network, and neighboring ESInet interconnections. In this scenario, we'll explain a call transfer from the Allerium ESInet to an adjacent non-Allerium ESInet. Additional scenarios can be found in the System Interconnect for OSPs, ESInets, and SRs ICD attached as documentation.

For a successful ESInet-to-ESInet transfer from an i3-compliant PSAP served by the Allerium NGCS platform, the transfer request must include the destination ESInet PSAP URI. This information is sent in a REFER to the Allerium NGCS platform from the PSAP.

The following answer is ALLERIUM CONFIDENTIAL-PROPRIETARY INFORMATION.





A forest guide for ECRF has not been deployed. The Incident Data eXchange (IDX) EIDO standard has been issued by NENA but not widely adopted. Allerium NGCS is currently monitoring adoption to support NENA i3 compliant entering and leaving transfers with updated location in the EIDO.

“Span of Control,” Gaps & Limitations

When a call remains "within the system" as stated here, Allerium assumes that to mean that the call remains within the span of control of the aggregation service, the NGCS, or the ESInet, or a combination thereof. In that case, the only practical area that would limit success would be at the PSAP locations. If a PSAP host does not have diverse entrances for network then a limitation would exist in that a "backhoe incident" could interrupt traffic to that PSAP. If the State chooses to implement a tertiary wireless connection, that issue is mitigated. Other avenues for mitigation would include moving one circuit from an overhead to underground access, for instance. Additionally, the ESRP/PRF will automatically reroute traffic to a surviving path if circuits are interrupted to the destination PSAP.

Other limitations exist, but they are outside the span of control of Allerium. Examples would include the OSP ingress network, provided by the OSP, and issues upstream of those circuits in the OSP network itself. Similarly, in a host/remote deployment like the regional deployments in the state, issues between the host and the remote PSAPs (be they logical or physical) could impair traffic, but those are, again, outside of Allerium's span of control.

To summarize what is in our span of control, we have proposed:

- Three data centers—all running in active/active mode—to provide NGCS functions. The data centers are in Council Bluffs, Dallas, and Raleigh, meaning low latency options while also providing data centers on separate power grids and with geographic separation.
- Two POI locations for the ingress of traffic. Each POI is capable of interconnection to legacy selective routers, legacy OSPs, and IP-based OSPs. The POI functionality is in accordance with the FCC report and order regarding OSP ingress.
- A truly diverse, fiber-based, MPLS network that underpins our ESInet. The ESInet is designed for scalability and availability. Fast convergence times and appropriate non-blocking bandwidth sizing ensure excellent voice characteristics.

5.10.2. Additional Examples

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.

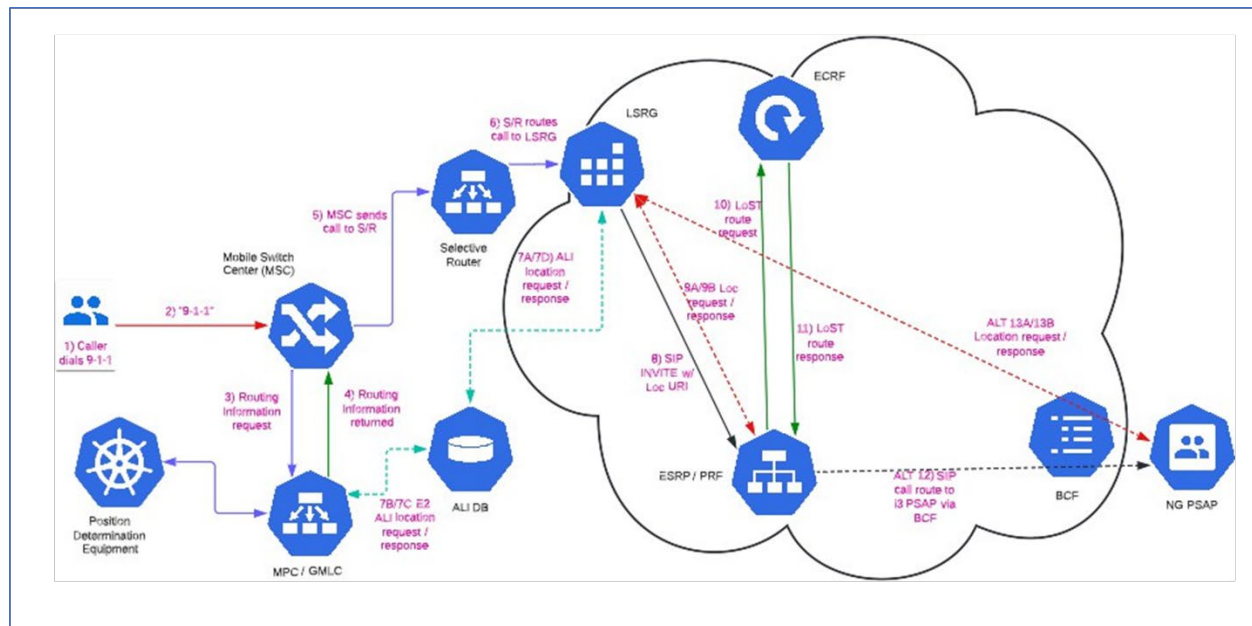


Figure 4: NENA Call Flow Scenario 1

Remainder of page intentionally blank

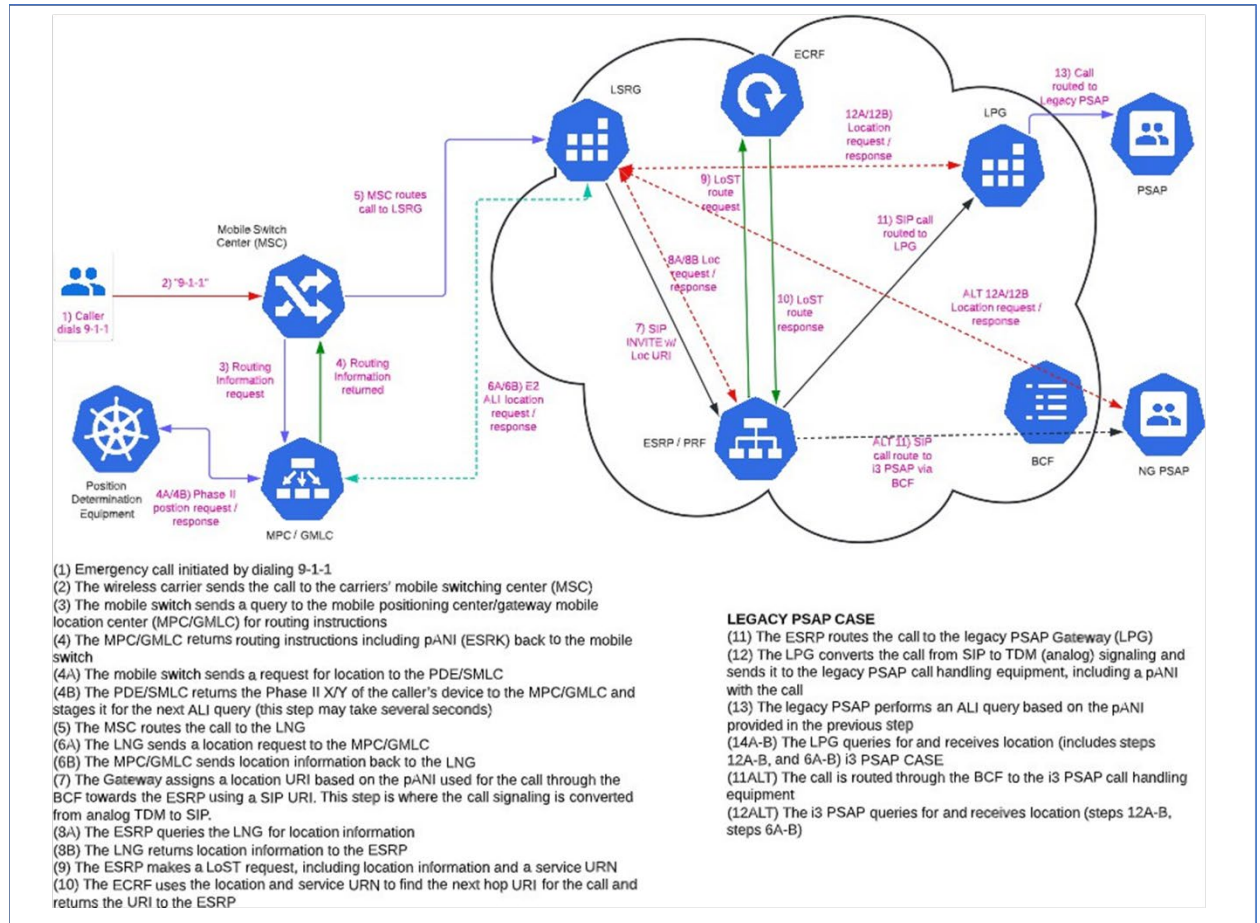


Figure 5: NENA Call Flow Scenario 2

Remainder of page intentionally blank

Response:

Allerium has included various explanatory diagrams that meet the intent of this section. Those diagrams are found throughout this response, as well in our ICD and technical documentation provided with this response.

6. Cost Proposal [Proposal Instructions, Section A.6]

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.

Response:

Allerium's complete Revised Cost Proposal Addendum 2 is included with our proposal in Excel format with additional information featured in our Additional Cost Information file.

7. Terms [Proposal Instructions, Section A.7]

7. 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.

Response:

Terms Table

Allerium’s technical terms and conditions table with initials is included below.

Docusign Envelope ID: D3394E19-E6CF-4DC2-BE14-D4F3ECF24F23

Proposal Instructions

A. SOLICITATION RESPONSE SUBMISSION

7. 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.)
RFP Section "Executive Summary"		
RFP Section "Project Requirements and Scope of Work," Subsection A. PROJECT OVERVIEW AND BACKGROUND INFORMATION		
RFP Section "Project Requirements and Scope of Work," Subsection B. SCOPE OF WORK		
RFP Section "Project Requirements and Scope of Work," Subsection C. WORK PLAN AND PROJECT PLANNING		
RFP Section "Project Requirements and Scope of Work," Subsection D. DELIVERABLES AND DELIVERABLE APPROVAL PROCESS		
RFP Section "Project Requirements and Scope of Work," Subsection E. TECHNICAL		

Page 1 of 3

Figure 78. Terms Table (Page 1 of 3)

Docusign Envelope ID: D3394E19-E6CF-4DC2-BE14-D4F3ECF24F23

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.)
REQUIREMENTS, E.1. ESInet Requirements through E.3.2. Core Data Services INITIAL: 		
	RFP Section E. TECHNICAL REQUIREMENTS, Subsection E.3.2.1. Mapping Data Service INITIAL: 	At this time, our solution does not include a fully deployed Mapping Data Service (MDS) as defined in NENA-STA-010.3. This position is deliberate and reflects the broader realities of the NG911 GIS environment. While the MDS construct is well-defined within the NGCS architecture, its successful execution depends on a stable, mature, and consistently stewarded nationwide GIS data supply chain—an ecosystem that is still actively evolving.
RFP Section “Project Requirements and Scope of Work,” Subsection E. TECHNICAL REQUIREMENTS, E.3.2.2. MSAG Conversion Service (MCS) INITIAL: 		
	RFP Section E. TECHNICAL REQUIREMENTS, Subsection E.3.2.3. Geocode Conversion Service (GCS) INITIAL: 	Allerium’s solution can provide a compliant Geocode Service and the necessary protocol details if required. However, in practice, we have seen that most CAD and mapping applications already provide this service, thus making it unnecessary in the NGCS. Please note that limited implementation details are provided within the standard.
RFP Section “Project Requirements and Scope of Work,” Subsection E. TECHNICAL REQUIREMENTS, E.3.3. PSAP-Facing Services through E.10.2. Additional Examples		

Page 2 of 3

Figure 79. Terms Table (Page 2 of 3)

Docusign Envelope ID: D3394E19-E6CF-4DC2-BE14-D4F3ECF24F23

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.)
RFP Section "Procurement Procedures," Subsections A. GENERAL INFORMATION through BB. DEBRIEFINGS RFP Section "Proposal Instructions," Subsections A. SOLICITATION RESPONSE SUBMISSION through C. PROPRIETARY INFORMATION RFP Section "Glossary" RFP Section "Intent to Award" RFP Section "Solicitation Conference" Appendix A: Cost Proposal Template Appendix B: Technical Matrix INITIAL: 		

Page 3 of 3

Figure 80. Terms Table (Page 3 of 3)

Similar Documents for Incorporation into the Contract

Allerium has included the following sample documents as appendices:

- Sample master sales agreement (MSA) for hosted services as Appendix 10: Sample MSA
- Sample statement of work (SOW) as Appendix 11: Sample SOW
- Sample call handling end user license agreement (EULA) as Appendix 12: Sample CHE EULA

Per the Executive Summary's Overview of Contracting Process information within the RFP, Allerium welcomes the opportunity to collaborate with the State to formulate a final SOW based on the RFP's Project Requirements, RFP's Scope of Work, and Allerium's response.

8. Contractual Agreement Form [Proposal Instructions, Section A.8]

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.

Response:

Allerium's completed and signed Contractual Agreement Form is included below.

Docusign Envelope ID: D3394E19-E6CF-4DC2-BE14-D4F3ECF24F23

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.

____ 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. § 71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED MANUALLY IN INK OR BY DOCUSIGN

BIDDER:	NextGen Communications, Inc.
COMPLETE ADDRESS:	2401 Elliott Avenue, Suite 100, Seattle, WA 98121
TELEPHONE NUMBER:	206-792-2000
FAX NUMBER:	206-792-2001
DATE:	4/15/2026
SIGNATURE:	 Signed by:
TYPED NAME & TITLE OF SIGNER:	0436B8E49C0744A Jeff Robertson, President of Allerium Business Segment

Figure 81. Contractual Agreement Form

