Intrado Life & Safety, Inc. Response to State of Nebraska RFP 6262 Z1 Option C

TECHNICAL PROPOSAL

June 3, 2020

Intrado Life & Safety, Inc.
All rights reserved.
Confidential and Proprietary.

Copyright and Trademark Notice

© 2020 Intrado Life & Safety, Inc.
All rights reserved.
Intrado® and the logo forms of Intrado are trademarks and/or service marks of Intrado Corporation in the United States, other countries, or both and may be registered therein. All trademarks used herein are the property of their respective owners.

Corporate Ownership

Requests for proposals may be fulfilled by Intrado Life & Safety, Inc.; Intrado Life & Safety Solutions Corp.; or Intrado Life & Safety Canada, Inc.

Non-Disclosure

The information contained in this document and provided to the Customer by Intrado Life & Safety is Intrado Life & Safety Corporate Confidential in its entirety. This designation restricts the disclosure to a third party of any information herein and other terms and conditions under the terms of a Non-Disclosure Agreement between Intrado Life & Safety and the Customer, if applicable.

Open Records Act Request

Customer will immediately advise Intrado Life & Safety in writing of any Open Records Act requests as it may relate to this proposal or any information contained herein.

Evaluation Purposes Only

Intrado Life & Safety's evaluation herein is based on its 9-1-1 knowledge and expertise, but is dependent upon information provided to Intrado Life & Safety on behalf of the Customer. As such, the information contained herein is intended for Customer evaluation purposes only.

Intrado Life & Safety Legal Notice

Intrado Life & Safety, Inc. provides the unregulated elements of the proposed service offering as set forth herein and in accordance with the final executed agreement between the parties. Intrado Safety Communications, Inc. provides the regulated elements of the service offering as set forth herein and in accordance with the applicable Intrado Safety Communications, Inc. Tariff, service offering, or other similar document governing the regulated elements in the subject state.

Contents

CORPORATE OVERVIEW 1
TECHNICAL APPROACH 14
A. UNDERSTANDING OF THE PROJECT REQUIREMENTS 14
B. PROPOSED DEVELOPMENT APPROACH 18
C. ATTACHMENT C - TECHNICAL REQUIREMENTS OPTION C 25
D. PROPOSED HIGH-LEVEL PROJECT PLAN 339
E. SCHEDULE FOR THE LIFECYCLE OF THIS PROJECT 339
FORM A: BIDDER PROPOSAL POINT OF CONTACT 340
REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM 341
ADDENDUMS FROM THE STATE OF NEBRASKA 342
SECTIONS II – IV 343
II. TERMS AND CONDITIONS 343
III. CONTRACTOR DUTIES 353
IV. PAYMENT 361

TABLE OF FIGURES

FIGURE 1: NG9-1-1 DIVISION ORG CHART AND REPORTING STRUCTURE 12
FIGURE 2: NGCS INGRESS/EGRESS 15
FIGURE 3: ESINET I3 CORE FUNCTIONS 16
FIGURE 4: TYPICAL IMPLEMENTATION TIMELINE 18
FIGURE 5: SOLUTION LIFECYCLE 19
FIGURE 6: DEFENSE IN-DEPTH SECURITY ARCHITECTURE 78
FIGURE 7: MONTHLY INCIDENT REPORTS 83
FIGURE 8: DEFENSE IN-DEPTH SECURITY ARCHITECTURE 100
FIGURE 9: A9-1-1 NETWORK MONITORING 105
FIGURE 10: INCIDENT MANAGEMENT REPORT 137
FIGURE 11: PSAP EGRESS ARCHITECTURE OVERVIEW 177
FIGURE 12: DIVERSITY/REDUNDANCY WITH BGP THROUGH PSAP WAN 179
FIGURE 13: IPV4 AND IPV6 SUPPORT MODEL 184
FIGURE 14: A9-1-1 ROUTING CORE SITE ARCHITECTURE 193
FIGURE 15: END TO END A9-1-1 NGCS AND ESINET 198
FIGURE 16: CORE SITE ARCHITECTURE WITH FUNCTIONAL ELEMENTS 199

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

FIGURE 17: OSP CONNECTIVITY MODEL 200
FIGURE 18: A9-1-1 ESINET BORDER CONTROL FUNCTION 225
FIGURE 19: IPV4 AND IPV6 SUPPORT MODEL 231
FIGURE 20: A9-1-1 ESINET BORDER CONTROL FUNCTION 237
FIGURE 21: ESRP/PRF DIAGRAM 240
FIGURE 22: SPATIAL INTERFACE, ECRF, AND LVF 284
FIGURE 23: SPATIAL INTERFACE 287
FIGURE 24: SPATIAL INTERFACE 290
FIGURE 25: TRANSITIONAL STATE WITH LOCATION DATABASE COMPONENTS 299
FIGURE 26: GEOMSAG ERROR RESOLUTION 303
FIGURE 27: SAMPLE ALI RETRIEVAL REPORT 313
FIGURE 28: SAMPLE CDR REPORT 314
FIGURE 29: PSAP RESOURCE AVAILABILITY AND STATISTICS 320
FIGURE 30: PSAP OPERATION STATE AND SUBSCRIBED FEATURES 321

TABLE OF TABLES

TABLE 1: CHANGE MANAGEMENT EVENT TYPES 68
TABLE 2: ESCALATION PROCEDURES 70
TABLE 3: CHANGE MANAGEMENT CHANGE CATEGORIES 90
TABLE 4: CHANGE MANAGEMENT CHANGE CATEGORIES 96
TABLE 14: ESCALATION PROCEDURES 110
TABLE 5: MTBF AND MTTR 123
TABLE 6: MTBF AND MTTR 125
TABLE 7: INTRADO SEVERITY LEVELS 140
TABLE 8: INTRADO SEVERITY LEVELS 142
TABLE 9: INTRADO SEVERITY LEVELS 144
TABLE 10: INTRADO SEVERITY LEVELS 146
TABLE 11: INTRADO SEVERITY LEVELS 149
TABLE 12: INTRADO SEVERITY LEVELS 151
TABLE 13: CHANGE MANAGEMENT CHANGE CATEGORIES 165
TABLE 14: ESCALATION PROCEDURES 166

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

CORPORATE OVERVIEW

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.

Intrado Response: Comply.

Intrado Life & Safety, Inc. ("Intrado")
1601 Dry Creek Drive
Longmont, CO 80503

History of Incorporation and Name Changes

Intrado was incorporated as a Colorado company in July 1979 under the name SCC Communications, Inc.

Intrado was registered as a corporation in the State of Delaware in September 1993 as SCC Communications, Inc.

In 2001 the corporation's name was changed to Intrado Inc. through a filing with the State of Delaware.

Intrado, Inc.'s name was changed to West Safety Services, Inc. on 4/5/2016 through a filing with the State of Delaware.

West Safety Services, Inc.'s name was changed to Intrado Life & Safety, Inc. through a filing with the State of Delaware on 10/10/2019.

b. FINANCIAL STATEMENTS

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

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

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

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

Intrado Response: Understood and Comply.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado Financial Reports

Financial reports are provided in the *Proprietary Information* file included with this response.

Intrado Banking Reference

A banking reference is provided in the *Proprietary Information* file included with this response.

Intrado Description

Intrado Life & Safety, Inc. (formerly West Safety Systems, Inc. aka "Intrado") is a leading provider of 9-1-1 technology solutions for traditional phone companies, wireless carriers, satellite and cable operators, VoIP providers, and public safety and government agencies across North America. Backed by over 40 years of world-class network engineering focused on the needs of public safety, Intrado connects people to first responders - firefighters, law enforcement, ambulance services, and to the "first" first responders – the telecommunicators answering calls in public safety answering points (PSAPs). Our seamless, reliable, redundant, end-to-end infrastructure **enables** responding agencies to locate, route, transport and deliver emergency communications to help save lives.

Intrado, founded in 1979, is headquartered in Longmont, CO and has additional offices in the US and Canada, which employ more than 650 people.

Intrado Life & Safety enjoys long-standing partnerships with the nation's public safety agencies, telecommunications carriers and enterprise organizations, working through each of our divisions to provide comprehensive 9-1-1 availability around the clock wherever it is needed. Our systems and services touch millions of lives every day. We take that responsibility seriously.

- Intrado manages over 430M 9-1-1 transactions annually.
- The Intrado A9-1-1® network delivers over 35M NG9-1-1 calls annually, serving over 35 million citizens.
- Nearly 950 U.S. PSAPs are now utilizing-or are in the process of implementing-the Intrado A9-1-1 network.
- Since 2016, Intrado has facilitated more than 1.5B 9-1-1 transactions - more than 430 million 9-1-1 transactions annually.
- Intrado serves over 250 communications service providers including AT&T and CenturyLink.
- The Intrado VIPER® call handling system is installed in over 2,350 PSAPs globally, including four state-wide VIPER systems and five states with a hosted VIPER system.
- Intrado supports over 205 million transactions for E9-1-1 mobile routing and location requests.
- Intrado has over 290 million telephone number records under management.

Intrado manages the entire emergency response continuum, specializing in data management; innovative call handling equipment; highly-reliable, highly-available networks; highly accurate location identification; and a deep understanding of public and personal safety emergency response protocols. We continue to develop ground-breaking, i3 compliant Next Generation 9-1-1 (NG9-1-1) solutions.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado Corporation (formerly West Corporation), the parent company of Intrado Life & Safety, Inc., was founded in Omaha, Nebraska in 1986 and continues to maintain its headquarters in Omaha. Intrado Corporation is an innovative, cloud-based, global technology partner to clients around the world, while employing approximately 730 people in Nebraska. Intrado Corporation supports Omaha and Nebraska communities through financial donations as well as our employees donating time. Intrado Corporation's solutions connect people and organizations at the right time and in the right ways, making those mission-critical connections more relevant, engaging, and actionable – turning Information to Insight.

Intrado Corporation's omnichannel capabilities enable a vast array of essential solutions for a diverse client base that includes Fortune 1000 companies, state and local governments, along with small and medium enterprises in a variety of vertical industries. At the end of 2019, Intrado Corporation had approximately 6,960 full-time employees and approximately 1,160 part-time employees with sales and/or operations in the United States, Canada, Europe, the Middle East, Asia-Pacific, Latin America, and South America.

Intrado Corporation has grown and evolved organically and through acquisitions with a consistent focus on innovation. In 2019, Intrado Corporation received or delivered approximately 9 billion omnichannel messages, managed approximately 91 million conference calls and 57 billion telephony minutes, distributed over 200,000 press releases, and hosted over 40,000 webcasts and over 3,000 investor relations websites. Our platforms provide scale and flexibility, allowing us to provide a broad range of solutions, inclusive of innovative new offerings, to our diverse client base.

No condition is known to exist that would materially affect the viability or stability of the organization

c. CHANGE OF OWNERSHIP

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

Intrado Response: Comply.

Intrado does not anticipate any change in ownership in the twelve-month period following the proposal due date.

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.

Intrado Response: Comply.

The office location responsible for performance if Intrado is awarded a contract with the State of Nebraska follows.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado Life & Safety, Inc.
1601 Dry Creek Drive
Longmont, CO 80503

e. RELATIONSHIPS WITH THE STATE

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

Intrado Response: Comply.

Following are the contracts Intrado Life & Safety, Inc. has entered into with the State in the last five years.

- West Safety Services, Inc. ("West" aka Intrado Life & Safety, Inc.) contracted for GIS Services, Contract # 84625 O4, dated 12/27/18.
- West Safety Solutions Corp ("West" aka Intrado Safety Solutions Corp) contracted with the Nebraska Public Service Commission for ECaTS Services in an "Agreement for Services" (no contract number), dated 8/29/2019.

Intrado 's proposed subcontractor, Carrier Access, partners with CenturyLink to supplement the support structure for voice and data services at the State of Nebraska. Carrier Access assists with design, quotes, implementation, and ongoing support. These services are contracted by the State with CenturyLink and are public record should they be needed.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

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

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

Intrado Response: Comply.

No such relationship exists.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past five (5) years, all such instances must be described as required below. Termination

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

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

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

Intrado Response: Comply.

Intrado is subject to various lawsuits in the ordinary courses of its business, none of which is material to its business or applicable to the products or services in this proposal. However, note the following:

> Intrado and the FCC entered into a three-year Consent Decree on November 4, 2019 to resolve the FCC's investigation into an August 1, 2018 outage in 911 service. *See* West Safety Communications Inc., Order, FCC DA 19-1063 (rel. November 4, 2019), available at: https://docs.fcc.gov/public/attachments/DA-19-1063A1.pdf. The Consent Decree requires Intrado to pay a penalty and comply with a variety of compliance and reporting terms. Intrado's compliance effort is ongoing under this Consent Decree, which expires on November 4, 2022.

h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

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

The bidder should address the following:

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

ii. Contractor 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 Contractors above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

Intrado Response: Comply.

Today Intrado provides 9-1-1 database management and 9-1-1 call routing services to the majority of US-based telecommunications service providers including all major Incumbent Local Exchange Carriers (ILECs), Competitive Local Exchange Carriers (CLECs), Wireless Carriers, and VoIP Service Providers (VSPs).

Intrado in some way touches more than 95 percent of all 9-1-1 calls placed in the United States. Intrado's customers are involved in all aspects of 9-1-1, to include the thousands of public safety agencies that use Intrado Advanced 9-1-1 applications or call handling solutions. Intrado also provides 9-1-1 solutions to the majority of the fixed wireline carriers, wireless carriers, and VoIP service providers in the United States. Through this combined customer base, the 6,000+ public safety answering points (PSAPs) in the United States rely on Intrado for efficient 9-1-1 voice and data delivery.

Intrado has implemented and currently supports Next Generation 9-1-1 ESInet solutions that process live 9-1-1 calls today, across the United States.

Intrado has successfully deployed Next Generation 9-1-1 ESInet solutions for the States of Arizona, Delaware, Washington, Minnesota, Hawaii, and Vermont, and to PSAPs in California, Florida, Louisiana, Nevada, North Carolina, Pennsylvania, and Utah.

Intrado Life & Safety Experience

State of Delaware

Intrado was the primary bidder for the State of Delaware solution providing A9-1-1 Routing, ALI, and TXT29-1-1. The project was completed within budget and is still live. The table below shows sites and implementation dates.

Site	Scheduled Completion	Actual Completion
Kent County Department of Public Safety	3/17/2016	4/7/2016
Dover Police Dept	3/9/2016	4/5/2016
New Castle Emergency Operations Center	6/8/2016	6/29/2016
Newark 911 Center	4/21/2016	6/2/2016
Wilmington 911 Center	4/7/2016	5/17/2016
University of Delaware	5/12/2016	5/10/2016
Rehoboth 911 Center	2/17/2016	2/19/2016

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Sussex County Emergency Operations Center	2/17/2016	2/19/2016
Seaford 911 Center	12/10/2015	1/26/2016

Through this implementation the following lessons were learned.

- When planning testing there should be a discussion with PSAP about their standard operations to maximize the deployment of positions while reducing impact
- Some equipment can still be added to the positions after they are cutover to allow for positions to be stood up quicker and not slow down the process on equipment that is not critical.
- Relationships and processes with the carriers were greatly strengthened as a large project to connect all carriers to create a robust ingress network was implemented

State of Delaware Contact Information

See the *Proprietary Information* file submitted with Intrado's response.

State of Hawaii

Intrado was the primary bidder for the State of Hawaii solution providing A9-1-1 Routing, ALI, and TXT29-1-1. The project was completed within budget and is still live. Sites and implementation dates are listed in the table below.

Site	Scheduled Completion	Actual Completion
Hawaii County Fire	8/27/2013	9/3/2013
Hawaii Police Dept	8/27/2014	9/3/2013
Hickam Air Force Base	10/10/2014	10/24/2014
Honolulu EMS	10/8/2013	10/23/2013
Honolulu Fire Dept	10/8/2013	10/23/2013
Honolulu Police Dept	10/8/2013	10/23/2013
Kauai Police Dept	11/6/2014	11/6/2013
Maui Police Dept	1/30/2014	1/24/2014
Molokai Police Dept	1/21/2014	1/29/2014

Through the State of Hawaii implementation, the following lessons were learned.

- Clearer delineation of roles and responsibilities, and appropriate parties serving in those roles, especially as it relates to technical resources and onsite support
- The network design and technical solution and project schedule dates should be finalized prior to signing the contract.
- Test Numbers for Training – create a process for tracking upfront so it's not changed during middle of training
- Complete pre-migration testing prior to training to avoid impact to training

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Create documentation on how to connect IP vs. Analog for recording vendors

State of Hawaii Contact Information

See the *Proprietary Information* file submitted with Intrado's response.

Washoe County, Nevada

Intrado was the primary bidder for the County of Washoe, Nevada, providing A9-1-1 Routing, ALI, and TXT29-1-1. The project was completed within budget and is still live. Sites and implementation dates are found in the table below.

Site	Scheduled Completion	Actual Completion
City of Reno Emergency Communication	4/3/2012	4/9/2012
REMSA	4/6/2012	4/11/2012
Sparks Police Dept	4/4/2012	4/10/2012
Washoe County Sheriff-Incline Village	4/5/2012	4/11/2012

Through this implementation the following lessons were learned.

- Site surveys did not produce the level of detail that allowed team to prevent changes or modifications late in the timeline
- Include the ILEC in the data collection process to identify all the details required (pilot TNs)
- Explanation to PSAPs in advance of the data collection to note the need for accuracy and validation of the 'star code' list

Washoe County, NV Contact Information

See the *Proprietary Information* file submitted with Intrado's response.

Carrier Access Experience (Proposed Subcontractor)

State of South Dakota, August – October 2019

Carrier Access was a subcontractor working with CenturyLink engineers for the deployment of NG9-1-1 throughout the State of South Dakota. Carrier Access was tasked to correctly provision the ESInet/egress SIP MPLS network. Primary responsibilities are listed below.

- Thirty PSAPs each with primary and diverse MPLS circuits designed using last mile diversity through diverse LEC switches to diverse ENNI to Diverse CUGS and Diverse VIPERMECH systems.
- Highlands Ranch to Phoenix 2x10G OWS PTP / Highlands Ranch 2x10G WLA MPLS / Phoenix 2x10G WLA MPLS

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Quoted, engineered, ordered, project management of each circuit through hand off to Intrado
- Onboarding/Go-live completed with Intrado in February 2020
- Finished on time – Completed as scheduled.

State of South Dakota Contact Information

See the *Proprietary Information* file submitted with Intrado's response.

North Dakota Association of Counties, November 2019 - Ongoing

Carrier Access is subcontracting to CenturyLink for the deployment of NG9-1-1 for the North Dakota Association of Counties. Carrier Access is tasked with the following responsibilities.

- Engineering, ordering, project management of ESInet/egress SIP MPLS Network – currently pending completion
- Miami data center Ethernet circuits 50M x 2 with diversity / Longmont PDC Ethernet circuits 50M x 2 with Diversity
- Point-to Point infrastructure circuits between Fargo, ND and Phoenix data center x 2 with end-to-end diversity
- Point to Point infrastructure circuit between Bismarck, ND and Phoenix data center
- Ethernet installs for Bismarck and Fargo ESInet infrastructure 10M x 2 at each with end-to-end diversity
- PSAP Ethernet installs for four sites x 2 with diversity

State of North Dakota Contact Information

See the *Proprietary Information* file submitted with Intrado's response.

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

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

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

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

Intrado Response: Comply.

Technical Project Manager

Intrado assigns a Technical Project Manager that will work with the State of Nebraska. The Technical Project Manager will collaborate with the State to manage the project plan and milestone schedule tailored to the needs of the State's requirements with mutually agreed-upon timeframes. Project management duties will include, and are not limited to:

- Assemble and chair the teams involved in the implementation
- Integrate the activities of all the State vendors/suppliers
- Manage, coordinate, and monitor the implementation activities
- Manage the change control process
- Identify risks and mitigate project obstacles
- Support quality and acceptance in all areas of the project
- Manage testing and coordinate compliance with test criteria
- Transition completed solution to the Intrado 24x7 support organizations
- Meet/exceed the State Department 's needs regarding documentation
- Schedule training
- Participate in the cutover readiness review
- Direct and monitor all cutover activities

Throughout the duration of project implementation, the Intrado Project Manager will keep the State informed of ongoing project status via regular project team meetings. Intrado prides itself on customer satisfaction and encourages the use of these project team meetings as a forum for continual feedback on Intrado's performance. With this feedback, the Project Manager can refine the implementation plan or take necessary action so that the final implementation meets the State's expectations.

Program Manager

Intrado assigns a Program Manager who is responsible for overseeing the implementation, communication, and ongoing support of the State of Nebraska implementation. The Program Manager functions as the primary point of contact for the State for all billing and reporting

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

questions as well as provides monthly/quarterly Customer reviews and functions as the State of Nebraska's first point of escalation. As needed, the Program Manager will be onsite with the State to ensure adherence to the specifications agreed upon. Intrado's Program Manager oversees the set of all project activities and decisions necessary to implement the new A9-1-1 system with a program management office and coordinated project teams. The Program Manager will provide continual communication to the State throughout all phases and has ultimate responsibility for successful project implementation and ongoing support. The Program Manager will update the State on frequent status calls to ensure the State is continually up to date on all aspects of the implementation and their service. Most importantly, the dedication of this resource in partnership with the State's personnel allows the Intrado solution to seamlessly change to meet the State's needs.

Director, Service Delivery

The Director of Service Delivery is responsible for overseeing the team of project managers and support staff that manages the successful implementation of A9-1-1 projects for the NG9-1-1 Business Unit. This role works closely with our partners and customers on project oversight, coordinates deployment requirements with internal technical managers, and advises on technical solutions as needed. Responsibilities include personnel management, project prioritization and reporting, escalation management, process development, and assessment of product development requests

Customer Team Director

Intrado provides a designated Customer Team Director who is responsible for coordinating and delivering ongoing customer and account management (Day-2 Operations) through the term of the purchased services as well as for the overall customer experience, contractual obligations and success of the project .

Resumes

Intrado is providing resumes for the following roles for the Nebraska implementation.

- Intrado Senior Technical Project Manager
- Intrado Program Manager
- Intrado Director of Service Delivery
- Intrado Customer Team Director
- Carrier Access Manager, 911 Network Deployments

Resumes are located in the *Proprietary Information* file provided with Intrado's response.

Organization Structure

The Service Delivery organization consists of two groups – the PSAP Deployment team and the Ingress team. The PSAP Deployment team is responsible for the implementation of NextGen solutions from contract signing through go-live. They manage the project plan, interface with all project team members, status calls, equipment ordering and installation, PSAP circuit ordering and turn up, data collection and provisioning, testing, scheduling, and the go-live cut event. The Ingress team works on interconnect agreements as needed with LECs and facilitates ingress

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

network design conversations. They also manage inbound and outbound SS7 and IP orders for LSR connectivity as well as inbound for OSPs and end offices both pre and post PSAP go-live.

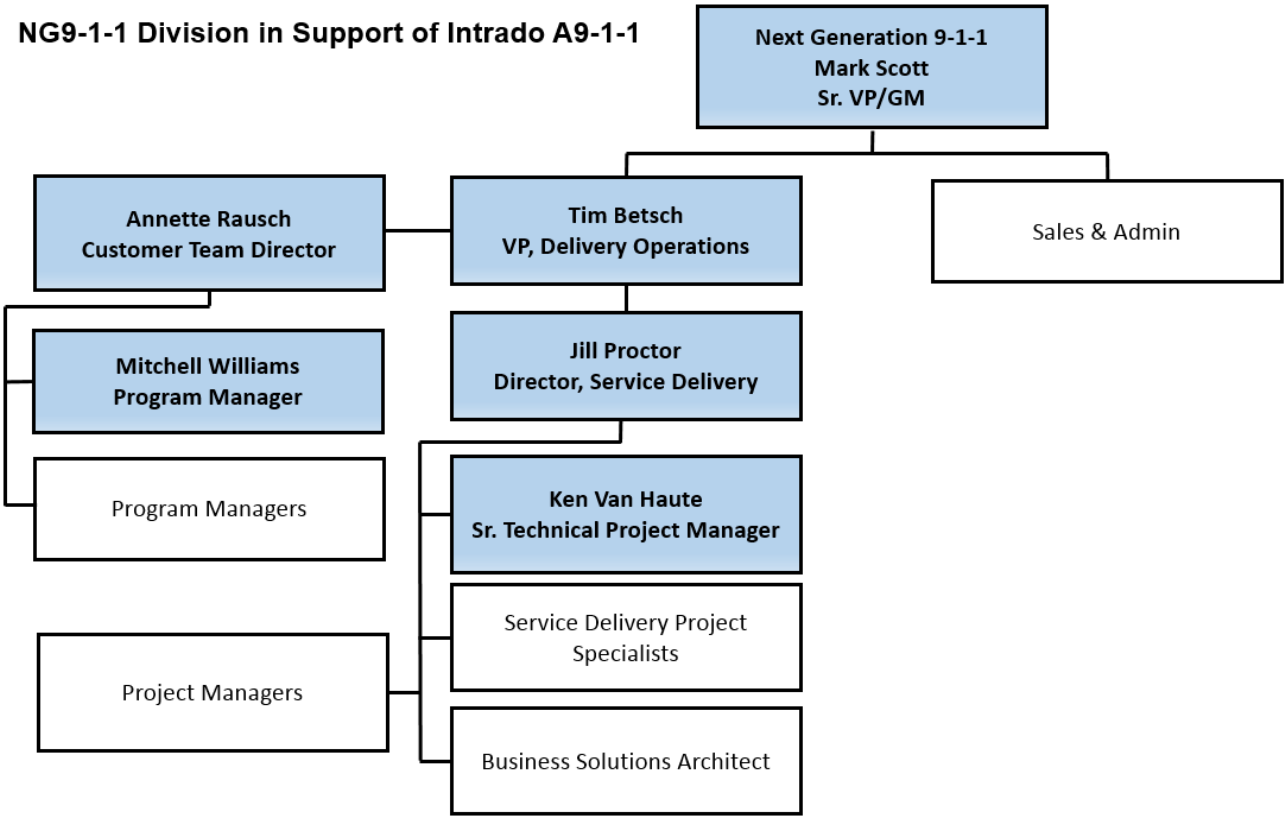

Figure 1: NG9-1-1 Division Org Chart and Reporting Structure

j. SUBCONTRACTORS

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

i. name, address, and telephone number of the subcontractor(s);
ii. specific tasks for each subcontractor(s);
iii. percentage of performance hours intended for each subcontract; and
iv. total percentage of subcontractor(s) performance hours.

Intrado Response: Comply.

i. Corporate Address

Carrier Access Inc.
1275 Northwest 128th Street Suite 205
Clive, Iowa 50325
515 987 9200

Satellite Office

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Carrier Access Inc.
2821 East 10th Street, Suite #6
Sioux Falls, South Dakota 57103
605 215 8185

ii. Carrier Access will perform the following tasks:

- Project Management - NG9-1-1 Core Network Deployment, Contracting, Order Management, Installation Coordination.
- Carrier Access will also manage post installation billing for all MPLS circuits, SD WAN solutions, and Broadband connections with each individual Carrier.
- Carrier Access will consolidate all network related invoices and send one comprehensive bill to Intrado monthly.

iii. Carrier Access will use approximately 15% of the performance hours intended for the contract.

iv. Carrier Access will use approximately 15% of the performance hours intended for the contract.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

TECHNICAL APPROACH

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

a. Understanding of the project requirements;
b. Proposed development approach;
c. Attachment C - Technical Requirements Option A, B, and/or C;
d. Proposed high-level project plan
e. Schedule for the lifecycle of this project; and
f. Cost Proposal

Intrado Response: Comply.

Please see document *RFP 6264 Z1 Intrado Life and Safety Inc Cost Proposal Option C ESInet and NGCS revision three.xlxs* for "f. Cost Proposal".

Proprietary information is found in *RFP 6264 Z1 Intrado Life and Safety Inc Option C Technical Proposal_Proprietary Information.docx.*

All other sections are contained within this document.

a. Understanding of the project requirements

Intrado Response: Understands and complies.

Intrado fully understands the project requirements as described within this RFP. Intrado has been an innovator in NG 9-1-1 for more than 25 years–deploying and supporting the first Wireless Phase 1, Phase 2, VoIP and Mobility voice solutions as well as supporting the first true NG9-1-1 transitional and i3 solutions in the nation. Many proven standards (processes, procedures, applications, and functionalities) were not only deployed but also formalized and FOA'd by Intrado resources and solutions.

Intrado is excited for the opportunity to continue and evolve our partnership with the State of Nebraska by deploying and supporting Next Generation 9-1-1 transitional and i3 services. By selecting Intrado the State will benefit from proven, best-in-class 9-1-1 services as well as the interoperability and interconnectivity of applications already deployed with intrado GIS and ECaTS products.

Intrado has deployed and/or supports services to multiple statewide solutions and hundreds of 9-1-1 PSAPs. Advanced 9-1-1 services include, IP-based selective routing, MPLS Text routing and delivery, i3 geo-spatial routing and call delivery, MPLS-based private ESInets, alternative and default routing scenarios, and a robust, highly available and redundant routing infrastructure. In addition, Advanced 9-1-1 service is data rich with online CDRs, detailed call traces, system KPI performance, and resource utilization statistics. The network and applications are fault tolerant, easily extensible, and reliable.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

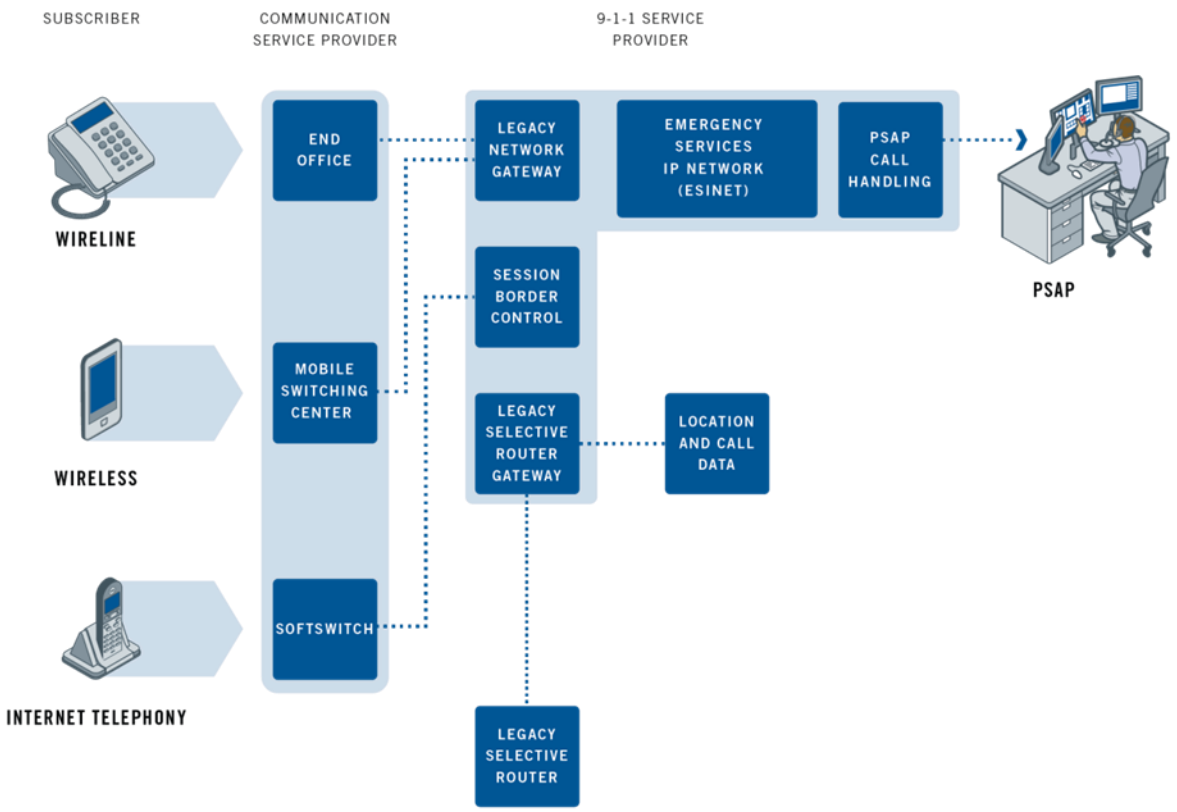

Figure 2: NGCS Ingress/Egress

TDM and IP Aggregation

Intrado is proposing a cost-effective solution for regional TDM connectivity into the Next Generation A9-1-1 infrastructure. The solution will allow for 9-1-1 Service Providers or OSP end offices to interconnect with two regional LNG locations located within the State of Nebraska. From that point, the calls are distributed to diverse IP interconnection points that provide geographic, hardware, and software redundancy with no single points of failure.

Intardo also supports and encourages ingress to the A9-1-1 service via IP. IP enables multiple benefits such as directly receiving the location of the caller with the call. Intrado offers two types of interfaces for IP ingress; full i3 and pre-i3 for carriers not yet ready to send an i3 formatted call. Intrado currently supports multiple OSPs with IP ingress into its Next Generation routing systems.

IP ingress is economically attractive in that it will accelerate an OSP’s ability to connect directly with the A9-1-1 system, thereby eliminating legacy 9-1-1 ILEC fees and long haul TDM circuits to the LNGs.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

i3 Capabilities and GIS Readiness

Intrado has designed an infrastructure which truly aligns with or exceeds current industry capabilities. The solution is i3-compliant and provides full end-to-end i3 protocols and functions. As we know through experience, not all local jurisdictional PSAPs and Originating Service Providers may be ready to deploy an end-to-end solution. Intrado has created an infrastructure that is not only based on i3 definitions, but also is planned for “real world” experiences.

If an OSP is not ready to provide all i3 functions, A9-1-1 is still capable of geospatially routing the call using the PSAP’s GIS data sets. This solution is NENA-compliant using the LNG LIF function for location retrieval during call processing. Alternatively, if a PSAP is not ready for i3 routing and call delivery, A9-1-1 is designed to reformat the call during call processing so that the PSAP’s legacy equipment can accept it. This allows each PSAP to transition to i3 at its own pace.

Intrado understands that the State may not want or have the capability to “flip a switch” and make all PSAPs immediately i3-ready. We have designed a service that is transitional and flexible enough to allow the State of Nebraska to do what you want on your terms.

Intrado’s solution adeptly supports multiple i3 transition scenarios. Intrado’s portfolio includes a robust set of GIS tools and services to support data preparation for geospatial routing to this end. For regions where the State’s GIS data is i3 ready, Intrado will assist the region to ensure that the data is accurately and appropriately validated to be used for routing, geospatial map displays and CAD.

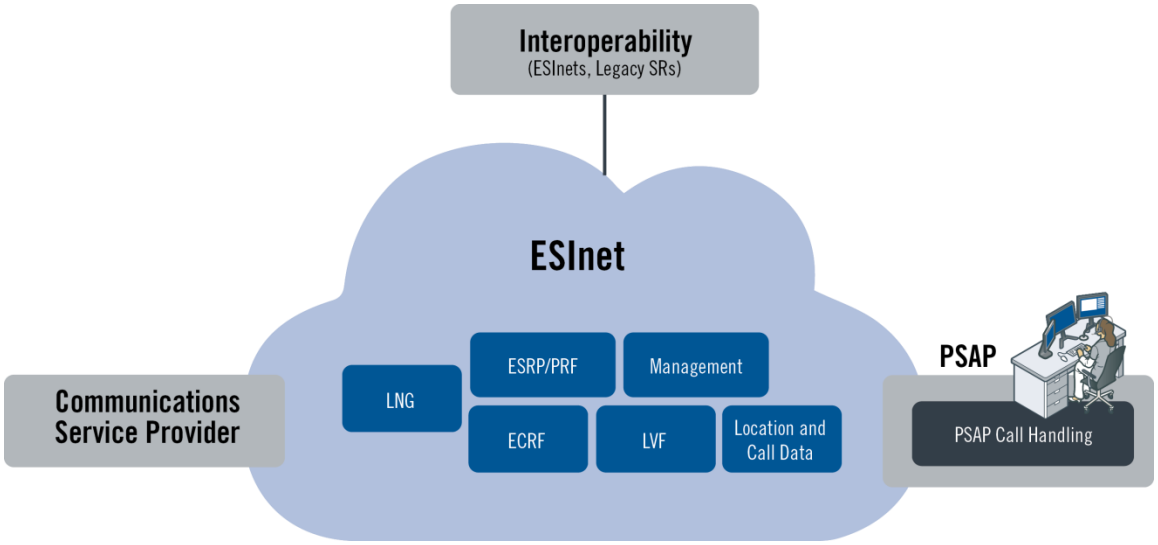

Figure 3: ESInet i3 Core Functions

Project/Program Management

During implementation of services, Intrado provides a dedicated Project Manager who will work with the State of Nebraska. The Intrado implementation Project Manager is responsible for all implementation-related activities including creation and management of the implementation

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

project plan with the State of Nebraska and coordinating activities with OSPs such as establishing connectivity and test/migration schedules. The project plan includes specific detail about interoperability testing and considerations with OSPs, CPE vendors, Legacy providers and neighboring ESInets.

Intrado also provides a designated Program Manager who is responsible for coordinating and delivering support through the term of the State of Nebraska's purchased services. The Intrado Program Manager is the single point of contact for the State of Nebraska and assists with all billing and reporting questions as well as provides monthly/quarterly Customer reviews and functions as the State of Nebraska's first point of escalation.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

b. Proposed development approach

Intrado Response: Comply.

Intrado Life & Safety, Inc. employs a solution lifecycle implementation methodology to ensure that all project areas of change are properly defined, designed, integrated, and deployed. The solution lifecycle implementation methodology has been developed and refined based on experience and the lessons learned migrating hundreds of systems to Next Generation 9-1-1. The methodology provides a blueprint for managing system migration and includes a project plan, templates, examples, diagrams, forms, and project communications. These project tools are tailored during the Solution Definition phase to address the specific attributes of each Next Generation system implementation and then refined during the subsequent project phases.

The Intrado Solution Delivery Lifecycle (SDLC) approach to plan, configure, network engineer, implement, test, document, train, and support Intrado services follows the Intrado time-proven Solution Delivery methodology. The lifecycle begins with Solution Definition and Architecture activities. During these initial phases, the joint Intrado and Customer team members verify system application and implementation requirements, refine the solution architecture, and finalize the plan for solution deployment. Following Definition and Architecture phases, the team orders, installs, configures, tests, and trains users on Customer-facing solution components as part of solution integration and deployment effort. Following successful deployment, the maintenance phase begins.

The figure below provides a high-level illustration of the implementation that Nebraska can expect.

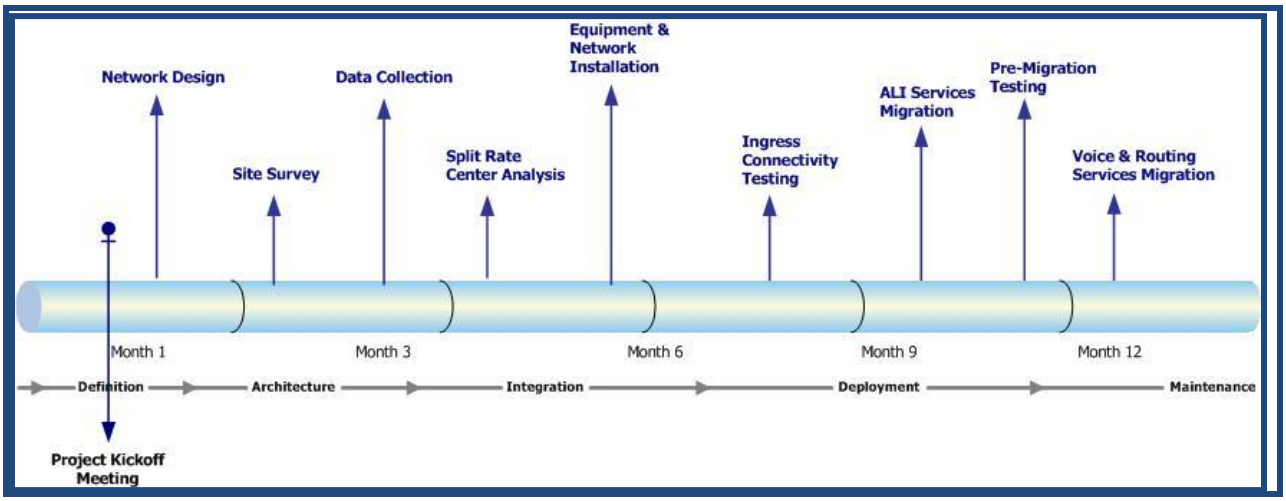

Figure 4: Typical Implementation Timeline

The project supports the Emergency Services Authority and PSAPs in transition to Intrado services and in the migration to i3. The project team will also work with the State of Nebraska on the following designs and plans:

- ESInet design and implementation including call overflow and management

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Text and Enhanced Data traffic analysis and demand
- GIS routing data implementation and deployment plans

The primary goal of the lifecycle methodology is that the project aligns with overall Customer expectations, and is tailored to fit the needs of the State of Nebraska.

Figure 5: Solution Lifecycle

The Project Plan phases are described below.

Solution Definition

The first phase in the solution lifecycle is the Solution Definition phase, which begins with the kickoff and alignment process and is critical to the overall success of the 9-1-1 initiative. During this process, key members of the joint project team unite to identify roles, responsibilities, critical success factors, project challenges, elaborate on specific strategies and project options, confirm project scope, and finalize plans to expedite solution delivery plans and resources. The proposed solution is reviewed in order to align each primary stakeholder with a common vision and strategy for unified team design and planning.

The Intrado team conducts current systems, processes, and site studies to more clearly understand the current system and user environment, allowing the team to plan the most effective migration path to the new system.

Solution Architecture

During the Solution Architecture phase, the detailed solution design is finalized based on confirmed requirements. During this phase, the team analyzes the current systems, operations, and operational procedures, identifies the human factors needs, considers implementation options, and with the Customer, commits the detailed solution design and implementation schedule.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Stakeholder participation to identify processes and standard operating impact is critical in this process to support a successful integration of the new system. It is vital that current procedures, connectivity, and routing policies are examined so that the appropriate practices are carried forward to the new system environment. Examples of important areas to consider include load balancing philosophies and default routing rules.

Initial planning for connectivity from the telephone service providers to the Points of Interconnection (POI) also begins in the architecture phase. Key solution architecture planning activities include:

- Detailed solution design and schematics (onsite, site-to-site, site-to-Intrado, firewalls, routers, etc.)
- ESInet and IP specifications
- Originating service provider connectivity specifications
- Physical requirements (e.g., equipment room design, floor loading)
- Call transfer requirements
- Training plan and schedule
- Refined project plan and timeline

Solution Integration

During the Solution Integration phase, the components of the solution, including processes, applications, servers, network components, and data flow, are engineered and readied for deployment. All network, regional, and Customer premises components are delivered, and the equipment rooms and other facilities are readied.

Coordination with wireline, wireless, and VoIP telephone service providers is an essential part of this stage to plan for the 9-1-1 services management transition. Originating service providers receive all necessary information and detail to obtain connectivity to the Intrado systems and the service provider's connectivity to the POIs is engineered and ordered.

Working closely with stakeholder groups, the project team designs customized provisioning plans (including incoming trunk route plans, bridge lists, and dialing plans). Additionally, the documentation and training developers customize the user and process documents and various training courseware, if needed, to meet the needs of the State of Delaware.

Solution Deployment

During the Solution Deployment phase, all network components and equipment connectivity is validated and acceptance tests are performed, metrics tracking, reporting is initiated, and training is provided. After complete non-live call testing, the system begins supporting live 9-1-1 traffic.

In preparation for deployment and in partnership with the State of Nebraska, the Intrado Project Manager finalizes the cutover plan, including procedures for notification concerning schedule specifics.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Prior to the commencement of cutover, the project team members will hold a cutover meeting with the State of Nebraska and the telephone service providers. The purpose of this meeting is to discuss the progress of activities and the cutover readiness.

PSAP training is provided in accordance with the detailed training rollout plans. The system will then undergo a system acceptance test and quality walkthrough. Once complete, and in agreement with the State of Delaware a live-traffic cutover will then commence. Once live traffic has moved to the system, the maintenance period begins.

Solution Maintenance

The Solution Maintenance phase begins once live traffic is transferred onto any part of the system. During this phase, Intrado provides ongoing tiered support services to monitor service level performance, manage help desk requests, escalate support procedures, and support the State of Nebraska to reach the highest level of operational excellence. The solution support team is in place to receive, analyze, and rectify problems and information requests throughout the term of the contract.

Program and Project Managers

Intrado provides a designated Program Manager who is responsible for coordinating and delivering support through the term of the State of Nebraska's purchased services. The Intrado Program Manager is the single point of contact for the State of Nebraska and assists with all billing and reporting questions as well as provides monthly/quarterly Customer reviews and functions as the State of Nebraska's first point of escalation.

The Intrado Program Manager is responsible for overall Customer service management that includes:

- Scheduling and facilitating kickoff meeting and status updates
- Coordinating Intrado resources
- Ongoing project management for the duration of the Statement of Work (SOW)
- Writing and maintaining all Intrado methods and procedures that affect Intrado operations and its interface with the Customer, OSPs, and PSAP operations

During implementation of services, Intrado provides a dedicated Project Manager who works with the State of Nebraska. The Intrado implementation Project Manager is responsible for all implementation related activities including creation and management of the implementation project plan with the State of Nebraska and coordinating activities with OSPs such as establishing connectivity and test/migration schedules.

The implementation Project Manager is an integrated partner with the Program Manager and meets with the Customer on a periodic basis to review the status of implementation and completion of implementation tasks against target timeframes as described within the integrated project plan.

Considering the State's needs and the constraints of the OSPs serving the State, the Intrado Project Manager creates an Implementation Project Plan and milestone schedule tailored to the

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

needs of the State's operations with mutually agreed-upon time frames. Project management duties will include, and are not limited to:

- Assemble and chair the teams involved in the implementation
- Integrate the activities of all applicable Nebraska PSAP vendors/suppliers
- Manage, coordinate, and monitor the implementation activities
- Manage the change control process
- Identify and escalate project obstacles
- Support quality and acceptance in all areas of the project
- Coordinate compliance with test criteria
- Transition completed solution to the Intrado 24x7 support organizations
- Meet/exceed the State's needs regarding documentation
- Schedule training and meet/exceed the PSAPs' needs
- Participate in the cutover readiness review
- Direct and monitor all cutover activities

Throughout the duration of the project implementation, the Intrado Project Manager will keep the Commission and the PSAPs apprised of ongoing project status via regular project team meetings. Intrado prides itself on customer satisfaction and encourages the use of these project team meetings as a forum for continual feedback on Intrado's performance. With this feedback, the Intrado Project Manager can refine the implementation plan or take necessary action so that the final NG 9-1-1 solution implementation meets the State's and the PSAPs' expectations.

Communication Plan

Intrado's communication plan is put into action immediately through preparation and facilitation of a project kickoff meeting. Following the kick-off meeting, the Intrado Project Manager facilitates ongoing implementation planning, design, and requirements definition meetings with the State and the affected telephone service providers to ensure successful and timely implementation.

During the maintenance period, the Program Manager facilitates regularly scheduled operations meetings and periodic formal reviews with the State to monitor general status and trends, receive customer performance reviews and obtain customer feedback, and address any questions or concerns.

Post Deployment

The Intrado Program Manager manages the ongoing maintenance of the A9-1-1 services through the life of the contract. Beginning with ALI migration, as each end office re-homes to the A9-1-1 solution, and continuing through the term of the contract, the Program Manager oversees all aspects of Intrado's full suite of maintenance services for all components of the solution, including:

- Data Integrity Services

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

  - Service Order Processing
  - Master Street Address Guide (MSAG) Management
  - Emergency Service Number (ESN) and ALI Response format management
  - Error correction for data content, MSAG, LNP, ANI/ALI Discrepancy, and No Record Found (NRF) errors
  - Special Services, including: data extracts, reconciliations, and audits
- Routing Services
  - I3 Routing Management
  - Provisioning support for routing, star code assignment, transfer, and other configurable attribute changes
- Originating Service Provider Management
  - Outstanding error management
  - Deployment of new Originating Service Providers (OSPs)
  - Support of end office and Mobile Switching Center (MSC) re-homes
  - Assistance in wire center overlap issue resolution
- System, Network and Hardware monitoring, maintenance, upgrades, and support

Maintenance Plan

Intrado monitors and manages its mission critical solutions 24x7x365. Intrado's trained personnel monitor numerous components of the solution's use and periodically review, make recommendations, and perform actions so that the systems and customer solutions are functioning at optimum efficiency.

When changes to the system are required, the scope of these changes typically falls under one of the following maintenance scenarios:

- Configuration changes
- Software hot fix introduction
- Software upgrade (for example, service packs providing enhancements or new features)
- For each of the above scenarios, the maintenance procedure may be applicable to:
- A specific facility or application component
- All facilities and application components

Maintenance of the Intrado-managed ESInet is done with no scheduled downtime. Intrado schedules planned events for routine maintenance in ways that 9-1-1 operations are not impacted. A notification of the upcoming event will be sent to Nebraska and/or the PSAPs as applicable. Intrado fully staffs and manages planned events with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. Intrado event team personnel will keep the PSAP and/or Nebraska informed of

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

event progress. Intrado adheres to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado will include the required back-out time within the scheduled maintenance time frame.

Monitoring, Support, Maintenance, and Availability

Intrado provides continuous system support to each network element and application supplied by Intrado. Intrado has a Network Operations Center (NOC) that is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage the Intrado ESInet and associated services. When a potential or actual Customer-affecting issue is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established Intrado processes that are ISO 9001:2000-compliant for immediate escalation, notification, resolution, and reporting.

Availability

The Intrado services maintain the highest system availability. Intrado embraces and creates all offerings based upon a "no single point of failure" principle, using a fully redundant, multi-carrier, multi-protocol network linking all Intrado network elements and PSAPs within the ESInet. Intrado facilities and nodes are equipped with physically redundant data communications and power equipment so that any component can be maintained without overall service impact. Buildings and supporting facilities such as generators, fuel, and entrance demarcations require card access and are monitored 24 hours a day by security personnel.

The Intrado evolution to i3 will incorporate the Intrado philosophy that is guided by a set of public safety class service standards. Recognizing that opportunities continually arise to introduce new features and functionality into our 9-1-1 systems, the distributed architecture used by Intrado Advanced 9-1-1 offers increased ability to accommodate growing and varied workloads in a modular fashion. New system features offer compelling advantages, such as access to new information, increased interoperability, higher efficiency, or expected cost savings. Proposed system changes and new features are stringently evaluated in the public safety context so as to not introduce weakness, inefficiency, or unpredictability into the systems. Each feature is designed, implemented, and operated in a manner befitting 9-1-1's critical role in the safety of the general public.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

c. Attachment C - Technical Requirements Option C

Bidders are instructed to complete a Matrix for Emergency Services Internet Protocol (IP) network (ESInet). Bidders are required to describe in detail how bidder's proposed solution meets the conformance specification outlined within each Requirement. The matrix is used to document and evaluate bidder's response to the requirements.

The matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. PSC will consider any such response to the requirements in this RFP to be non-responsive and the bid may be rejected. The narrative should provide The Public Service Commission (PSC) with sufficient information to differentiate the bidder's business solution from other bidders' solutions. Bidder shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details shall be provided in the same paragraph as the requirement. Bidder shall not include pricing information in the description and shall not refer the reader to pricing.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the matrix as provided by PSC. Failure to maintain these elements may render the bid non-responsive and result in for rejection of the bidder.

The bidder's response to each of the below requirements shall include an indication on the level of compliance that can be met. (Complies, Complies Partially, Complies with Future Capability, Does Not Comply) Bidder shall respond by placing an "X" in only **one** checkbox per requirement. Failure to complete this process properly will be treated the same as "Does Not Comply," and may result in the rejection of the response form.

1. Complies: Bidder's proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, generally available, and successfully deployed. Responding with "Complies" or "Complies with Future Capability" shall mean the bidder's solution meets or exceeds the requirement regardless of any comments included as additional information.

2. Complies Partially: Bidder's proposal addresses the RFP requirements through another method that currently is developed and available for implementation (i.e., shall be generally available), or the solution complies with some, but not all of the requirements. Bidder is responsible for clearly explaining how the proposed solution does not fully comply.

3. Complies with Future Capability: The RFP requirements will be met with a capability delivered at a future date. This response shall include a calendar quarter and year in which the requirement will be met with a generally available product or service at no additional cost.

4. Does Not Comply: Bidder's proposal does not/cannot meet the specific RFP requirement.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Req Identifier	Requirement Description				
GEN-1	**General Requirements - Bidder Vision of NG911** The Commission is issuing this RFP for the purpose of selecting a qualified bidder that understands and can clearly demonstrate alignment with the industry's evolution to NENA i3 -compliant ESInet and NGCS solutions. Describe bidder's vision of NG911 and how bidder's vision aligns with NENA's i3 standard, bidder's approach to monitoring and supporting evolving standards and the bidder's level of involvement in standards development and Industry Collaboration Events (ICE).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

Intrado's Vision of NG9-1-1

Full end-state deployment of a NENA i3 compliant ESInet and NGCS solution will dramatically improve the efficiency of managing and delivering emergency calls, alerts and information to PSAPs and First Responders. Calls and IoT alerts will be delivered faster and in a very targeted manner to the appropriate resources. Policies will be easily managed for specific locations, call types, alert types, and media. Rules will be very refined for different operational states (e.g., in service, out of service, busy) and resource sharing with contiguous PSAPs. Device-based location will be delivered with the call for immediate location management and response. Additional information specific to the citizen and the location will also be delivered with the call for fast dispatch and resource assessments. The end-to-end fully meshed IP network will be resilient and inherently more redundant. The ESInet will carry PSAP traffic other than emergency calls; CAD-to-CAD, RDM, and administrative voice are examples of such traffic. Intrado is very excited about how quickly the Public Safety community is moving towards the NENA i3 end-state. Our citizens will greatly benefit from this evolution.

Intrado's Involvement and Approach to Monitoring and Supporting Evolving Standards

Intrado supports and works to advance the NENA i3 standard. We have multiple employees that support multiple NENA working groups including CS-EIDO Conveyance, CS-i3 Architecture, ASC-EIDO, DS-Interface Specification Development, SS&R Cloud Services, and SS&R-IoT/Apps.

Intrado Participation in Industry Collaboration Events (ICE)

Intrado is an active participant in NENA's Industry Collaboration Events for system interoperability. Intrado has participated in the NENA ICE 2, ICE 4, ICE 5, ICE 6, ICE 7, and ICE 8 events.

During the ICE 2 event Intrado tested their VIPER and Power 911 systems.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado participated in the ICE 4 event, held at the AT&T Center for Learning in Irving, Texas in November 2011. Intrado tested its solutions to demonstrate i3 interoperability in a multi-vendor NG9-1-1 environment. The areas of focus for Intrado's i3 interoperability testing included the following functional elements as part of its i3 solution: • Emergency Call Routing Function (ECRF) • Location Validation Function (LVF) • PSAP Call Processing Equipment (VIPER®) – PSAP CPE • Other products tested included IPSR, ESRP, i3 PSAP, ECRF, LVF, and PRF. At ICE 5 during the week of October 15, 2012 Intrado successfully tested our SMS Text to 9-1-1 (TXT29-1-1) solution which includes our Emergency Text Gateway product along with the Power 911 product. The ICE 6 event was focused on comprehensive end-to-end functionality, interaction between vendor elements (external interfaces) and interoperability testing. Intrado participated with its VIPER and Power 911 systems as well as with its LIS/LDB solution. Most recently at ICE 7, Intrado tested its Additional Data Repository (ADR) and Location (LIS) products. NENA ICE 8, which Intrado participated in with the Intrado VIPER and Power 911 systems, demonstrated interaction of Logging and Recording vendors on an i3 system. Intrado will continue to participle in the upcoming ICE events in that they play an important role in enabling and accelerating the transition from today's legacy 9-1-1 systems to Internet Protocol (IP)-based next-generation 9-1-1 networks and NGCS.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-2	**Proprietary Solutions and Standards** 1. Describe any use of proprietary standards, interfaces, or protocols in bidder's proposed solution. 2. Describe any patented technology in the proposed solution, who owns the patent and describe any licensing arrangements. Disclose any technological limitations, in the response.	X			
	Bidder Response: **1.** The Intrado solution, A9-1-1, does not employ any proprietary standards, interfaces, or protocols in our network design. All standards, interfaces, and protocols used are industry standard. **2.** Proposer represents that it has all intellectual property rights to provide the offered solution. There are no technical limitations based on patents or other intellectual property rights.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-3	**System and Network Architecture** The Commission is seeking a Public Safety Grade Next Generation 911 System. System and network architecture, including the design and deployment of interface functions and security measures, shall comply with current NENA i3 requirements as established in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards for the NENA i3 Solution. Describe how the solution meets or exceeds the requirements in Section V.D.1.b. of the RFP.	X			

Bidder Response:

The solution presented within this response complies with the NENA-STA-010.2-2016 and NENA detailed functional interface standards for the NENA i3 solution. Below is a summary of how Intrado meets the requirements as referred to in V.D.1.b of the RFP.

Reliability

There are many contributing factors, both physical and logical, that lead to a public safety grade, reliable 9-1-1 infrastructure. The main components include, but are not limited to

- Geographic diversity of the Core and local PSAP equipment and applications
- Diverse and redundant network architecture
- Secure facilities and protected infrastructure
- Active adherence to, and participation in, industry standards
- Extensive lab integration and ongoing testing/validation

Availability

The Intrado A9-1-1 solution achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. All functions necessary for call processing are deployed in a highly available configuration and duplicated across core sites and LNGs. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability.

The NGCS and ESInet components are designed and configured for continuous operation. A9-1-1 availability is calculated from the time an outage begins that impacts call processing ability, until such time that the call processing ability is restored.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	All network routing infrastructure is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology. The Intrado A9-1-1 solution implements a design of redundancy upon redundancy. Individual processing elements are redundant at each core site and core sites are redundant to each other. The failure of any given component at a core site will not prevent that core site from processing 9-1-1 calls. If a dual failure does occur at a single core site, or a single core site somehow becomes unavailable, calls are processed at the alternate geographically diverse core site—giving the solution multiple levels of redundancy. Each core site can process any 9-1-1 call. The core sites are geographically distributed across the United States and a unique regional disaster will not remove the ability for the Intrado A9-1-1 solution to process 9-1-1 calls, assuming telecommunication transport services for the impacted region are operable. The core routing and intelligence of the solution provides the State with immediate scalability in call routing and data delivery. The Intrado core network and NG9-1-1 services are designed to support very large volumes with geographic diversity of core processing centers. The end result is an infrastructure that is public safety grade with respect to capacity, reliability, scalability, and redundancy. The Intrado geographically distributed solution ensures high availability in the event of regional service impacting events or disasters. The solution consists of the following high availability components: • Geographically redundant core processing sites • Local and redundant Aggregation Sites for TDM call ingress and egress. • Flexible and redundant points of interface for IP ingress. • Ethernet Private WAN for “any-to-any” Ethernet networking between Core and Aggregation Sites. • Redundant and logically diverse connection facilities from the A9-1-1 NGCS core sites to the Public Safety Answering Point (PSAP) for delivery 9-1-1 calls. Core Sites work in an active-active mode; calls are distributed across all core sites. The architecture is more than capable of processing all the 9-1-1 calls for the state of Nebraska; therefore, there is no need for NGCS capacity supplementation as the Nebraska PSAPs on-board to Intrado A9-1-1 service.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Core Sites work in an active-active mode; calls are distributed across all core sites. The architecture is more than capable of processing all the 9-1-1 calls for the State of Nebraska; therefore, there is no need for NGCS capacity supplementation as the Nebraska PSAPs move to the Intrado A9-1-1 service. Intrado will conduct major and minor planned and critical unplanned events for all NG9-1-1 Services, system maintenance, or upgrades that may impact any of the customer PSAPs. Intrado event team personnel will keep the customer informed of event progress. Intrado adheres to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado will include the required back-out time within the scheduled maintenance time frame. **Security** Secure communications are retained through the following measures, as recommended in NENA-INF-015.1-2016, Section 3.2: **a) Rivest–Shamir–Adleman (RSA)-based public-key cryptography using X.509 certificates to authenticate elements, agencies and agents. Mutual authentication must exist between both ends of a communication.** Intrado manages credentialing and issuing digital certificates to help ensure protection and security as defined within section 6 of NENA-STA-010.2-2016. Intrado verifies credentialed devices or that carriers are authorized access in the following manner: • Client certificates are issued by a trusted Certificate Authority (CA) are required in order to access I3 services • Intrado validates all x.509 certificates with a trusted, key signing, CA All systems utilize the highest capabilities of protection and authentication available, including IPSec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification. **b) An eXtensible Access Control Markup Language (XACML)-based data rights management (DRM) system to control authorization.** Intrado's dual-factor Authentication, Authorization, and Accounting (AAA) System uses XAMCL to control access to all IEN Voice administrative functions based on section 6.5 of the NENA-STA-010.2-2016. **c) Advanced Encryption Standard (AES)-based encryption to provide confidentiality**

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	The solution employs AES 256 encryption-in-transit on our own networks and on networks not under our direct control. Encryption is achieved either using SSL/TLS or IPSEC. Intrado uses AES encryption for data in-transit while crossing untrusted networks, e.g., outside the secure Intrado boundary-controlled network. AES encryption is also used to encrypt all “data at rest” inside the secure Intrado network, and no data is stored “at rest” in the Intrado DMZ network region **d) Secure Hash Algorithm (SHA)-based, digest-based digital hashing to provide integrity protection** All Intrado systems that participate in secure inter-machine, client-server, and user administrator transactions do so under the protection of SHA secured session control. **e) Digital Signature (Dsig)-based digital signatures to provide non-repudiation** Where applicable, we support Dsig to ensure the authenticity of data we receive from customers, as well as Dsig sign data we originate and transfer to the customer. **Network Traffic Restrictions** All data navigating the A9-1-1 system and data access is strictly for public safety use as required in NENA-STA-010.2-2016. Commercial and non-public safety data and access is prohibited from sharing the system.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

GEN-4	**General Requirements – Capacity- Initial Design and Deployment** The bidder's initial design and deployment of the ESInet and NGCS elements, including all components and physical network segments, shall provide capacity that will support current and planned ESInet traffic and usage that occurs as a result of data sharing in, and between, all participating PSAPs, the Commission, and designated support agencies. Additionally, the system and network design shall allow for 50 percent traffic and usage growth for the life of the contract. All current and potential core functions and applications shall be considered, e.g., call-handling systems, CAD, logging, GIS data, streaming media, real-time text (RTT), IP traffic, traffic management systems, communications systems, and incident management systems. Describe how bidder's solution will meet or exceed the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado has investigated the existing call volumes for the state of Nebraska, including the busy hour (10x of normal operations), and has confirmed that the A9-1-1 solution can successfully process the traffic under both normal and non-redundant conditions. A9-1-1 is capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. Intrado can easily scale IP capacities through network port size increases, horizontal scaling of core routing systems, and simple provisioning processes, eliminating the need for additional network buildouts, and enabling customers to increase capacities within a few weeks vs. months. Intrado will work with the State for capacity planning and to mutually agree on ordering timeframes. This methodology provides the State with a cost-effective solution in the near term and allows for growth based on coordinated agreements.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-5	**Capacity - Scalable Deployment** As the Commission migrates toward a fully compliant NG911 environment, additional PSAP functions will transition to the systems and network. The bidder's systems and network solution shall be designed and deployed in a way that is easily scalable, with the capability to grow in both capacity and coverage without disruption in service. Describe in detail how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Our solution provides a fully compliant and readily scalable environment in the existing LNG and ESInet core infrastructure. Currently our aggregation gateways used to ingress 9-1-1 traffic operate with redundancy at each location and are configured on 100mb Ethernet circuits. We run bandwidth capacity at 60% of the total capacity available The A9-1-1 network is easily capable of bandwidth growth at each network element, existing end sites, and future end sites without sacrificing reliability of the solution. The solution is capable of interconnecting to other national- and/or state-level ESInets via open standards-based interfaces. The A9-1-1 network is deployed with a 2N redundancy model; each remote site is provisioned with at least twice as much bandwidth as is required to serve the total number of voice trunks provisioned at the site. The network core is IP and is capable of adjusting bandwidth to meet changing needs easily, quickly, and with minimal operational impact. The IP network transport used by A9-1-1 will initially be baselined to the specified network bandwidth requirements of the PSAP. The PSAP can deploy additional bandwidth over the required baseline at any time. The A9-1-1 IP network is also proactively monitored for capacity trends that indicate the need for growth of the ESInet. As the needs of the State grow, local PSAP connectivity bandwidth will be scaled up or down by a change order process or through procedures as defined in the SLA and/or contract.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 1	**Security - Cybersecurity** For the purposes of this RFP, cybersecurity (security) is considered to be the established systems and processes focused on protecting computers, networks, programs, and data from unintended or unauthorized access, modification, or destruction. **Security Requirements and Standards** The security requirements established in applicable standards listed in Section V.D.1. Table 1 of the RFP apply equally to all elements of the system requested in this RFP, including but not limited to components located in the following building types: 1. Data centers; 2. Network-housing structures ; and, 3. Regeneration sites and other buildings housing any element or device that is part of the overall system. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Due to the complexity of the i3 NG systems and the challenges of continuously tracking compliance across numerous and constantly changing compliance frameworks, we first adhere to Intrado security requirements and the NENA Security for Next-Generation 9-1-1 Standard (NG-SEC). Additionally, due to the critical nature of the infrastructure in supporting the 9-1-1 call processing environment, we track alignment to the NIST Cybersecurity Framework and applicable areas of the FBI CJIS Security Policy. To ensure ongoing compliance, our Governance Risk Compliance (GRC) program includes annual reviews of applicable control requirements through internal controls assessments and audits. Our environments undergo periodic review by an independent third-party at least every three years. Intrado-specific policies that govern ESInet and NGCS environments and operations include: Facilities General Security Requirements, Access Control Process, Badge Control Process, Information Security Policy, Safe Work Environment Policy and Infrastructure and Information Policy. Intrado documents policy and procedure training and record completion. Information security incidents are reported, escalated, and managed with the Incident Management Procedure. An appropriate log and audit trail of each security incident is created and maintained. The A9-1-1 ESInet implements a highly secure, private IP-managed network built to withstand aggressive attacks. All inbound and outbound traffic interactions are with pre-vetted entities and use IPSEC key exchange between controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. Intrado employs a defense-in-depth security strategy where multiple levels of security are in place to provide security and protect sensitive information. Such controls include stateful packet inspection firewalls (host and network based), intrusion detection systems (IDS) / intrusion prevention systems (IPS), Access Control Lists (ACLs), Role-based Access control, multi-factor				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	authentication, strong encryption, and anti-virus and anti-malware including email and host. Furthermore, Intrado protects its systems with build standards, patch management, and regular vulnerability scans. Sensitive data is housed in data centers with logical and physical access controls. All hardware and software elements go through stringent release management processes that incorporate thorough testing and scans before deployment to production systems. Development environments are separate from production and production data is not used in development and system test environments. Inter-zone traffic is restricted to only the necessary protocols/destination and data that transits un-trusted networks (leaves Intrado custody) pass through applications or communication channels with encryption to safeguard confidentiality and integrity. A9-1-1 network segments are capable of processing all traffic, but administratively deny protocols identified as a threat or that otherwise fall outside of pre-defined parameters. These mechanisms include routing tables and/or Access Control Lists (ACLs). A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution. **Vulnerability Management Program** Intrado understands the importance of a well-established cyber security strategy, and therefore, has established a multi-tiered vulnerability management program, which incorporates the following components: • Hardened configuration management and baseline inventory • Pre-deployment and major change scans • Passive vulnerability monitoring • Quarterly external vulnerability scans • Annual penetration testing The foundation of the Intrado vulnerability management program is the establishment of baseline, hardened security configurations and identification of assets operating within the ESInet environment. Prior to initial implementation into the production environment and upon major modifications, individual component vulnerability scans are performed, ensuring baseline security configurations have been met and no vulnerabilities will be introduced into production. In addition to implementation and modification scans, a passive, network-based vulnerability management solution is deployed in the A9-1-1 system, allowing real-time, ongoing monitoring of the environment in a less intrusive manner than traditional port-based vulnerability scans. Data from network monitoring can be correlated with the centralized security

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	information and event management (SIEM) solution, providing real-time analysis of security events across the infrastructure. The Intrado vulnerability management program also incorporates quarterly vulnerability scans from outside the network by a third-party security contractor, focused on identifying weaknesses in external interfaces that could potentially be susceptible to attack from outside parties. Finally, an annual penetration test is performed by a third-party, in order to provide an independent review and assessment of the security defenses deployed to protect A9-1-1 and the life mission critical services it supports. Throughout the process, identified vulnerabilities are classified using industry-standard scoring for rating levels of critical, high, medium and low, with remediation timeframes established. Because of the complex nature of the A9-1-1 system, multiple factors are considered to determine the true risk associated with identified vulnerabilities. Layered onto the vulnerability management program, is an established Patch Management process, ensuring the timely identification, evaluation, testing and implementation of vendor released patches. Following a regular patching process acts to limit the number and severity of vulnerabilities within the operational environment.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 2	**Security Plan** A comprehensive security plan is a critical component of the Nebraska's NG911 network solution. Describe the security plan, including the 1. mitigation; 2. monitoring; 3. alerting and incident-response processes; and 4. provide information on specific hardware components and software systems incorporated in the proposed security plan. The proposed solution's security plan is required to utilize the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) and Task Force on Optimal PSAP Architecture (TFOPA) best practices.	X			
	Bidder Response: Policies and procedures are used to manage the operating environment and overall security plan. Policies are crafted according to industry requirements and best practices including CSRIC best practices and compliance with the vast majority of the NENA NG-SEC standard. Policies exist that govern ESInet establishment and operation of the A9-1-1 Routing service, including but not limited to: Facilities General Security Requirements, Access Control Process, Badge Control Process, Ethics policies, and Information Security Policy Safe Work Environment Policy and Infrastructure and Information Policy. Policy and procedure training is documented and training completion is recorded. Policy and Procedures are owned and managed by specific line organizations responsible for the relative area of concern. Information security incidents are reported, escalated and managed with the Incident Management Procedure, with an appropriate log and audit trail of each security incident is created and maintained. Intrado's cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technologies. The A9-1-1 infrastructure is built to withstand sophisticated attacks. A9-1-1 is a secured and private IP managed network. All inbound and outbound traffic interactions are with pre-vetted entities, utilize well defined protocols and traverse controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. Intrado employs a defense-in-depth security strategy where multiple levels of security are in place to provide security and protect sensitive information. Such controls include but are not limited to stateful packet inspection firewalls (host and network based), intrusion detection systems (IDS) / intrusion prevention systems (IPS), ACLs, Role-based Access control, multi-factor authentication, strong encryption, and anti-virus and anti-malware including email and host. Furthermore, systems are protected with build standards, patch management, and regular vulnerability scans.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Sensitive data is housed in data centers with logical and physical access controls. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. Development environments are separate from production and production data is not used in development and system test environments. Inter-zone traffic is restricted to only the necessary protocols/destination and data that transits un-trusted networks (leaves A9-1-1 custody) pass through applications or communication channels with encryption to safeguard confidentiality and integrity. A9-1-1 network segments are capable of processing all traffic, but administratively deny protocols identified as a threat or that otherwise fall outside of pre-defined parameters. These mechanisms include routing tables and/or Access Control Lists (ACLs). A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution. **Logging and Monitoring** Intrado will provide 24x7x365 logging and monitoring of the State's 9-1-1 service and equipment. For security purposes, Intrado does not allow outside vendor/customer access to monitoring equipment. Intrado will provide real-time reporting capabilities as well as access to the NOC for real-time updates on the health of the service and equipment. Intrado provides 24x7x3657 monitoring and incorporates Denial of Service mitigation tools into the solution. Intrado monitors the core network for traffic anomalies and shared resource consumption thresholds to protect the core network and ensure that traffic storms do not impact the performance of other customers. Intrado monitors and audits all aspects of the network for threats from a variety of sources. Net flow statistics and packet level capture and forensics are continuously performed. In addition, network hosts and security infrastructure provide logging through a centralized Security Information and Event Management (SIEM) solution, providing real-time analysis, event correlation, and alerts across the A9-1-1 system. This capability assists in troubleshooting and anomaly resolution as well as providing assurance of reliable performance. Information Security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. **Incident Response** In the event of an unplanned outage, or intermittent outage of a system, network component, or application that has the potential to cause an adverse impact to production services, Intrado immediately engages the Incident Command System (ICS), which is based on the FEMA Incident Command Structure. The incident team, led by a qualified incident commander and supported by Intrado technical and operations resources, evaluates the information received, determines

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	the problem statement, categorizes the problem severity level, and manages/works the incident until the incident objectives are met. Incident Management personnel are trained in incident command with courses provided by the Emergency Management Institute, a FEMA-sponsored Emergency Management Course as well as ITIL framework. Incident Management is available 24x7x365. Intrado implements and tests its Incident Management Plan on a regular basis and conducts audits and reviews and/or walk through exercises of its continuity plans at least annually. Information gathered feeds into a continuous improvement cycle as part of the maintenance and review process. **DDoS / TDoS Mitigation** The network infrastructure is built to withstand sophisticated attacks (including DDoS, TDoS) by means of a defense in depth strategy. We employ high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/Application availability is safeguarded with clustering and load balancing techniques. Furthermore, our security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, IDS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress. The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or Access Control Lists (ACLs). We continually investigate and upgrade with new advances in protective technology with tools such as Intrusion Detection Systems (IDS). The solution incorporates physical, network, and application security principals. Traffic between Core processing sites and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) is route- and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution. The A9-1-1 solution deploys firewalls and other network security devices and software to protect against inbound network threats on the servers that support the A9-1-1 service. The NOC also employs a regularly scheduled patching process to protect against the effects of malware. Computing devices are subjected to thorough security scans so that there are no malware elements present. Access to processing elements is restricted to authorized personnel. Network connections from solution components are limited to those connections needed for operation and maintenance. Physical and network

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	access to production components is restricted to those that have an operational responsibility, and all activity is audited and monitored. All development environments are fully separate from production environments. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. **Hardware Components and Software Systems in the Security Plan** The A9-1-1 NOC/SOC uses multiple tools and techniques to track performance and fault management activities. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to HP OpenView, which is used to present a single pane of glass to the A9-1-1 NOC. OpenView uses the HP Operations Manager (OM) module, which monitors systems and applications using agents and provides SNMP trap and syslog receiver capabilities, and the HP Network Node Manager (NNMi) network monitoring software module based on SNMP. These systems also provide ICMP and SNMP trending and threshold alarming. The A9-1-1 NOC also uses the following tools: • CIMRaN is used immediately following an incident to provide a call impact report that identifies calls, callback numbers, PSAPs, state carriers and associated CDRs in a report that can be distributed to the customer. This report is generated within minutes following an incident. • Netscout is used for network troubleshooting and analysis. The Intrado A9-1-1 system utilizes many mechanisms for event tracking and alerting. Systems leverage syslog and SNMP traps for event / fault notifications. Application hosts also utilize embedded agents which communicate directly with our monitoring platforms. Systems are monitored by use of SNMP polling and application health-checks. All systems are provisioned for fault, performance, and configuration monitoring / management.

Any additional documentation can be inserted here:

SEC 3	**Security Compliance Matrix** Describe how the proposed solution addresses compliance in each of the following categories in NENA 75-502, NENA NG-SEC Audit Checklist.

Category

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

1. Senior Management Statement
2. Acceptable Use Policy
3. Authentication/Password Policy
4. Data Protection
5. Exception Request/Risk Assessment
6. Hiring Practices
7. Incident Response
8. Information Classification and Protection
9. Physical Security
10. Compliance Audits & Reviews
11. Network/Firewall/Remote Access
12. Security Enhancement Technical Upgrade
13. Technical Solutions Standards
14. Wireless Security

Bidder Detailed Response:

1. Senior Management Statement – The Intrado Information Security Program Policy specifies the development, implementation, assessment, authorization, and monitoring of the IT security program.

Key Components

Intrado has appointed the following Information Security (InfoSec) roles:

- **Chief Information Officer (CIO)**: responsible for the overall management, direction, and security of Intrado's information assets.
- **Vice President (VP) of Information Security**: accountable for coordinating, developing, implementing, and maintaining an enterprise Information Security Program, including engaging resources to help deliver the mission; provides management briefings to the CIO on a regular basis.
- **Information Security Steering Committee (ISSC)**: responsible for overseeing security initiatives, policies, and related documentation; assists the VP of InfoSec with successfully implementing policies and controls across the enterprise.

Intrado applies a risk-based approach to holistically evaluate threats and design security measures that address compliance requirements and align with business goals.

Intrado InfoSec defines, publishes, maintains, and disseminates security instructions in the form of policies, controls, standards, processes, procedures, and guidelines to employees and relevant external parties. These materials establish the ground rules by

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

which Intrado operates and safeguards its data and information systems by reducing risk and minimizing the effect of potential incidents.

InfoSec has established an information security workforce development and improvement program, including Annual Security Awareness Training.

2. Acceptable Use Policy – The Intrado Acceptable Use Policy requires employees, and where applicable, contractors and third-party users, to apply information security in accordance with the established policies and standards; this includes acceptable usage of technology and software approved for business purposes.

Key Components

• Practices zero tolerance for malicious activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon, including hacking, circumventing access controls or security controls, and creating or exploiting vulnerabilities

- Fairly applies sanctions and corrective actions to employees who are found to have violated Intrado InfoSec policies
- Reports employees found to have violated local, state, Federal, and/or international law(s) to the appropriate authorities.
- Revokes physical and logical access rights and associated materials and property (e.g., passwords, badges, keys) upon termination of employment or change of responsibilities

3. Authentication/Password Policy – The Intrado Access Control Policy ensures that access to Intrado information systems and information is controlled based on business and security requirements and is maintained and removed in a timely manner.

Key Components

Intrado defines access requirements and manages access according to business and security requirements. Methods include:

- Identifying account types (e.g., individual, group, systems, application, guest, and temporary)
- Enforcing standard user access profiles for common job roles
- Establishing conditions for group membership
- Identifying authorized users of information systems and specifying access privileges

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Requiring appropriate approvals for requests to establish accounts
- Establishing, activating, modifying, disabling, and removing accounts
- Authorizing, monitoring, and deactivating the use of guest and temporary accounts
- Reviewing accounts periodically
- Incorporating relevant legislation and contractual obligations

Intrado employs the principle of least privilege (PoLP), which is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work.

Intrado defines requirements for passwords, including length, complexity, display, history, locking, sharing, expiration, reset, disclosure, storage, and encryption.

Intrado manages access identification and authentication using appropriate technology and established processes, including access control lists, session timeouts, and multi-factor authentication.

4. Data Protection – The Intrado Data Security and Privacy Policy defines requirements to protect data privacy at rest and in transit.

Key Components

Intrado searches Sensitive Personally Identifiable Information (SPII) and Personally Identifiable Information (PII) for unstructured data and addresses any anomalies prior to processing the data.

Intrado monitors for evidence of unauthorized exfiltration or disclosure of information.

Intrado specifies where information can be stored, including:

- Minimizing instances of storing data classified as “restricted” or “confidential”
- Storing data on Intrado systems or systems hosted by Intrado-approved vendors
- Prohibiting storage of “restricted” and “confidential” data on privately-owned (non-company owned) devices or media

Intrado secures the technology utilized for external data transfers.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

In accordance with the Applicable Laws, Intrado defines and enforces requirements for data retention, including Personal Information:

- Intrado does not retain Personal Information in a form which permits identification of data subjects for longer than is necessary for the purposes for which such Personal Information was collected or for which it is further processed .
- In some cases, Intrado may be required by local, state, Federal, and/or international laws to retain certain categories of Personal Information (e.g., traffic and location data) for a different period for purposes of investigation, detection, and prosecution of crime, or on general grounds of national or state public security.

5. **Exception Request/Risk Assessment** – The Intrado Risk Management Policy ensures that risk analysis is performed throughout the Intrado information system and data management life cycle, and that controls are applied commensurate with the risk, data classification, compliance requirements, and business needs.

Key Components

Intrado documents and implements a formal risk assessment process to identify, evaluate, and manage risks to an acceptable level. Risk assessments include the evaluation of multiple factors that may threaten security as well as the likelihood and impact from a loss of confidentiality, integrity, and availability of information and systems.

Risk management processes are monitored, reported, and reviewed across the organization at least annually or when environmental, operational, or technical changes arise that may impact the confidentiality, integrity, or availability of information resources.

6. Hiring Practices – The Intrado Information Security Human Resources Policy ensures that employees, contractors, and third-party users are suitable for the roles for which they are being considered, to reduce the risk of fraud, theft, or misuse of facilities.

Key Components

Prior to employment, Intrado:

- Screens individuals requiring access to organizational information and before authorizing access
- Reasonably verifies an applicant's identity and employment history
- Conducts background checks in accordance with relevant laws, regulations, and ethics; such checks may include drug screens and reviewing motor vehicle driving records, credit histories, and criminal records

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

During onboarding, Intrado:

- Requires that employees, contractors, and third-party users agree and sign the terms and conditions of their employment contracts, which shall include their responsibilities for information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.
- Ensures that individuals requiring access to organizational information and information systems sign appropriate confidentiality or non-disclosure agreements (NDAs) prior to being granted access

During employment, Intrado:

- Provides employees with Security Awareness Training
- Requires employees, and where applicable, contractors and third-party users, to apply information security in accordance with the established policies and standards; this includes acceptable usage of technology and software approved for business purposes
- Practices zero tolerance for malicious activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon, including hacking, circumventing access controls or security controls, and creating or exploiting vulnerabilities
- Fairly applies sanctions and corrective actions to employees who are found to have violated Intrado InfoSec policies
- Reports employees found to have violated local, state, Federal, and/or international law(s) to the appropriate authorities.
- Revokes physical and logical access rights and associated materials and property (e.g., passwords, badges, keys) upon termination of employment or change of responsibilities

7. **Incident Response** – The Intrado Security Incident Management Policy establishes the approach for security incident response, investigation, and communications.

Key Components

Intrado provides incident response personnel with training on their roles and responsibilities with respect to information systems, including annual refresher training.

With respect to incident reporting, Intrado:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Uses automated tools and logical controls where possible to identify and report on potential and known events
- Requires personnel to report known and suspected security incidents to Intrado incident response personnel as quickly as possible
- Communicates security incident information to external authorities and/or stakeholders in a timely manner as required
- Trains employees, contractors and partners in incident reporting expectations and requirements
- Tracks incident details involving security incidents

Intrado maintains an Incident Response Plan (IRP), which provides the company with a roadmap for implementing its incident response capability. Intrado reviews the IRP at least annually and distributes it to all incident response personnel. Intrado's incident response capabilities include:

- Identifying the specific system(s) involved in a security incident
- Alerting company-defined personnel of the incident using a secure method of communication
- Containing the affected information system(s)
- Identifying and containing other information systems that may have been subsequently compromised
- Collecting evidence

Intrado uses knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.

8. Information Classification and Protection – Intrado identifies and tracks information classifications and security categories at every phase of the systems development life cycle (SDLC). Data collections are assigned a classification based on data type, including but not limited to:

- Customer Proprietary Network Information (CPNI)
- Payment Card Industry (PCI) Data

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Protected Financial Information (PFI)
- Protected Health Information (PHI)
- Public Information
- SPII

9. Physical Security – The Intrado Physical and Environmental Security Policy minimizes risk to Intrado information systems and data by addressing applicable physical security and environmental concerns.

Key Components

Intrado controls physical access to facilities that house Intrado information, information systems, and/or personnel in order to prevent unauthorized physical access, damage, and interference to information and information processing facilities. This includes:

- Verifying and enforcing physical access authorizations for all physical access points not designated as publicly accessible
- Controlling entry to facilities containing information systems using physical access devices or mechanisms (e.g., badges, keys, combinations) and/or guards
- Implementing role-based physical access to buildings, facilities, secured areas, and resources
- Maintaining a list of individuals with authorized access to facilities containing information systems and issuing authorization credentials for facility access; the access list is reviewed periodically and individuals who no longer require access are removed from the list
- Ensuring that onsite personnel and visitor identification (e.g., badges) are revoked, updated when access requirements change, or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned, disabled, or changed
- Granting visitor access for specific and authorized purposes, providing visitors with instructions on security requirements and emergency procedures, and issuing visitor badges that are visually distinct from personnel badges
- Restricting unescorted access to personnel with required security clearances, formal access authorizations, and validated need for access

Intrado has designed and applied controls for protecting personnel and information systems against damage from natural disasters, civil unrest, malicious attack, or accidents. This includes:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Conducting annual risk assessments, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

10. Compliance Audits & Reviews – The Intrado Compliance Policy ensures that the existence and communication of appropriate safeguards in order to protect sensitive business data against loss, unauthorized access, or disclosure, in accordance with applicable statutory, regulatory, and contractual compliance obligations.

Key Components

Intrado records are required to be protected from loss, destruction, falsification, and unauthorized access, modification, or release.

Intrado performs periodic reviews to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Intrado managers are responsible for ensuring compliance with security requirements for their functional area.

11. Network/Firewall/Remote Access – The Intrado Operations Security Policy safeguards the confidentiality, integrity, and availability of Intrado's information and information systems by ensuring the documentation, maintenance, and availability of operating procedures.

Key Components

Intrado has developed a Security Concept of Operations (CONOPS) for information systems; the CONOPS is reviewed and updated periodically and contains at a minimum:

- How the organization intends to operate the systems from the perspective of information security
- A description of groups, roles, and responsibilities for the logical management of information systems

Intrado maintains key architectural information on each critical information system that includes at a minimum:

- External interfaces, including the information being exchanged across the interfaces and the protection mechanisms associated with each interface
- User roles and the access privileges assigned to each role

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Unique security requirements
- Types of information processed, stored, or transmitted by information systems and any specific protection needs in accordance with applicable local, state, and Federal laws
- Restoration priority of information or information system services

Intrado segregates conflicting duties and areas of responsibility to reduce the risk of unauthorized or unintentional modification or misuse of assets. No single person shall be able to access, modify, or use assets without authorization or detection.

Intrado logically or physically separates development, test, and operational environments and controls those environments to reduce the risks of unauthorized access or changes to the operational system.

Intrado controls the installation of software on operational systems to reduce the risk of corruption to operational systems.

Intrado develops, documents, and maintains under configuration control a baseline configuration standard for all authorized information systems and software in the enterprise.

Intrado implements detection, prevention, and recovery controls to protect against malware, and provides appropriate user awareness.

Intrado manages and controls networks to protect information systems and information, including information in transit. Intrado uniquely identifies and authenticates network devices that require authentication mechanisms, before establishing a connection, that, at a minimum, use shared information (i.e., media access control [MAC] or Internet Protocol [IP] address) and access control lists to control remote network access.

All systems (excluding approved exceptions) that handle information, accept network connections, or make access control (authentication and authorization) decisions shall record, retain, and export audit-logging information to Intrado-approved repositories.

12. Security Enhancement Technical Upgrade – The Intrado System Development, Acquisition, and Maintenance Policy ensures that information systems (developed or purchased) incorporate security controls throughout the SDLC and defines the protection requirements for data used for testing.

Key Components

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado considers security at every stage of an information system's life cycle (e.g., feasibility, planning, development, implementation, maintenance, retirement, and disposal) in order to:

- Ensure conformance with all appropriate security requirements
- Protect enterprise data
- Facilitate efficient implementation of security controls
- Prevent the introduction of new risks when the system is modified
- Ensure proper removal of data when the system is retired

13. Technical Solutions Standards – The Intrado Vendor Security Program Policy establishes guidelines for assessing, mitigating, monitoring, and reviewing the risks associated with vendor management.

Key Components

Intrado InfoSec reviews vendors in relation to the services provided and the level of access granted to Intrado facilities, systems, and data. This includes vendors providing:

- Contractors (long-term or temporary)
- Services that require establishing a connection between the Intrado network and the third-party (vendor) network
- A technology or product that will be installed in, or connected to, the Intrado network
- Services that involve the transport or destruction of paper or technology containing Intrado data
- A technology or product that will be resold by Intrado

Intrado conducts a Vendor Business Impact Analysis, which gathers basic data about the vendor and the services being provided, and then assigns a risk ranking.

- Intrado performs a vendor risk analysis on all new vendors and annually on vendors with a risk ranking of "high" or "extreme."
- Intrado InfoSec reviews all Master Service Agreements (MSA) with vendors with a risk ranking of "high" or "extreme.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

The Intrado Change Management Policy establishes the change management requirements and expectations for Intrado automated information assets and software.

Key Components
Change requests undergo a formal review and approval process, as follows:

- Requestors document and present change requests
- Resource owners approve change requests
- Programmers and end users test the change prior to implementation
- Appropriate personnel implement the change into the production environment

Intrado bases change management processes and decisions on assigned information classifications and security categories. Intrado identifies and establishes security rules and quality assurance processes for the development of software and systems.

Intrado examines and controls configuration changes made to the enterprise, whether code or infrastructure, to ensure all invested parties are aware of enterprise changes, all risks introduced by changes are known and mitigated, and the changes are approved at the appropriate level.

The Intrado network change management process ensures application service transactions are protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, and unauthorized message duplication or replay.

14. Wireless Security – While the core of our solutions does not incorporate direct wireless access, wireless security is covered as part of the Intrado Cryptography Policy, which ensures that appropriate cryptographic safeguards are in place to protect Intrado data against loss, unauthorized access, or disclosure.
Key Components
Intrado has established and documented encryption and key management strategies in compliance with applicable laws and regulations, including the encryption of:

- User passwords and credentials
- Data transmissions within and outside of the Intrado network, including wireless transmissions

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- CDs and DVDs
- Non-console administrative access and remote access to privileged functions
- Multi-factor authentication of remote users

In addition, end user devices (e.g., laptops, workstations) are encrypted when the device is imaged or reimaged. Mobile devices shall only access Intrado systems through approved software.

Any additional documentation can be inserted here:

	Predictive Analysis and Monitoring Describe solution's capabilities to provide predictive analysis and modeling to combat security threats.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SEC 4	Bidder Response The Intrado solution provides predictive analysis and modeling to combat security threats as described below. Security Information and Event Management (SIEM) analysis is a daily task of our Security Operations Center. Network hosts, including all call processing elements and security infrastructure, provide logging through a centralized SIEM solution, providing real-time event correlation, predictive analysis and alerts across the A9-1-1 environment. Information Security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. We deploy heuristic analysis, a method employed to detect previously unknown computer viruses, as well as new variants of viruses. Heuristic analysis is an expert-based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. In addition to performing continuous network traffic monitoring, we perform annual external and internal penetration testing of our critical systems and infrastructure. We maintain in-house tools and expertise to conduct penetration testing and work with nationally recognized penetration test providers to achieve third party assurance.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 5	**Credentialing Process** Solution shall provide a process so that devices and carriers outside the IP network shall not have credentials, per NENA-STA-010.2-2016. Provide details regarding how the solution ensures that devices and carriers outside the IP network are not provided credentials.	X			
	Bidder Response: Interactions between the ECRF and the ESRP are secured within the ESInet. Interactions with external ECRFs, a third-party LIS or ADR or the PSAP CPE will use digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA), once available. Until that time, Intrado Life & Safety will manage credentialing and issuing digital certificates for its assets to help ensure protection and security. This mechanism will also be used for PSAP access to systems within A9-1-1, including access to the LIS interface, ADR interface and ECRF. While it is possible to deploy ECRF/LVFs in such a manner that they assume a common public identity for devices and carriers outside the ESInet that do not have credentials, this is not a standard deployment within the A9-1-1 solution. At such time that non-credentialed transactions are required, we will consider providing these capabilities as an optional service. At no time will ECRFs used for call routing or PSAP determination of responders provide un-credentialed access due to the potential for Denial of Service (DoS) attacks impacting their critical functions. Following are devices and/or protocols used to restrict access. • A9-1-1 uses a security border API gateway for I3 data traffic. This device controls access to its services by using client trusted certificates. • Session Border Controllers (SBC) are used for all SIP and SIP related communications. Intrado verifies credentialed devices or that carriers are authorized access in the following manner: • Client certificates issued by a trusted Certificate Authority (CA) are required in order to access I3 services such as LIS, ADR and ECRF. • The trusted CA is currently provided by Intrado. Intrado will use the authorized NENA PCA vendor once they roll out their program. • The IP address of any far end SIP endpoint must be provisioned in the SBC.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	○ The endpoint is also required to send all traffic to a uniquely assigned IP: port combination on the SBC. ○ All SIP signaling is done over direct connections or VPNs. ○ IP connections to the ESInet are only allowed by vetted OSP's and/or data sources. ○ Connectivity to the ESInet is only by signed and approved agreement with data encapsulated by IPSEC MPLS VPN.

Any additional documentation can be inserted here:

SEC 6	**Third-Party Security Audits** Bidder shall allow for annual third-party security audits at the request and cost of the Commission. Describe bidder's current process for third party security audits.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Security audits are performed internally and by third-party vendors on a regular (yearly) basis. Audits specifically requested and initiated by the State shall be added to this schedule upon request.	X			

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 7	**Physical Security** All structures outside the Commission's control that will house components of the ESInet and NGCS shall have security and access-control systems that ensure that only duly authorized individuals can access the areas housing the Commission's systems and network equipment. Any workstations or other equipment connected to, or capable of accessing, the ESInet and NGCS systems shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the Commission's systems similarly shall be protected. Identify any elements that are not under the direct control of the bidder, and a description of the building's security and access-control systems shall be provided.	X			
	Bidder Response: We use various procedures to help ensure physical security in our data centers, including controlling, monitoring, and recording physical access to facilities where client servers and other equipment reside. We provide complete physical security for our locations, with a special emphasis on security of the data centers and other sensitive areas. Our physical security controls include: • Access policies and procedures • Access control system • Employee access procedures • Visitor procedures • Contractor access procedures • Building security • Data center security • Global Client Support Center (GCSC) security • Onsite 24x7 guards Additional controls include: • Multi-factor authentication for physical data center access • Closed circuit TV monitoring				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Access logs
	• Quarterly review of access list
	
	Our automated access control system uses electronic badge readers, biometric hand scanners, and PIN keypads to control and monitor access to Intrado buildings and data centers. Security guards monitor the facilities and maintain a 24X7 physical presence at each data center, and the system logs access and sends alerts if entrances are left ajar.
	
	We limit access to the data centers to only those employees who require access to perform their job functions. We lock the data center server racks and allow access only to persons who have proper authorization.
	
	Access to other buildings, including lobby entrances, also requires an electronic access badge. As an additional measure, we use strategically located video cameras to record and monitor activity, both within and outside buildings and workspaces, in addition to having uniformed security personnel conducting regular rounds throughout facilities.
	
	Local and remote monitored Power and Environmental controls (built at least to an N+1 methodology) include:
	
	• HVAC
	• Fire detection and suppression systems
	• Diverse commercial power feeds
	  ○ Standby generator systems
	  ○ Dual Uninterruptible Power Supply (UPS)
	  ○ Grounding architecture
	  ○ Commercial power contingency arrangements
	
	We limit access to the data centers and Customer Support Centers to only those personnel who require access to perform their job functions. We lock the data center server racks and allow access only to personnel who have proper authorization.
	
	In addition, Intrado:
	
	• Ensures all Information Resources intended for use by multiple users are located in secure physical facilities with access restricted to authorized individuals only.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Monitors and records access to the physical facilities containing Information Resources intended for use by multiple users in connection with Supplier's performance of In-Scope Work. • Physically secures any area where In-Scope Information is accessible to prevent access by unauthorized persons.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	General Requirements – Network Operations Center (NOC)/Security Operations Center (SOC)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 1	**Centralized NOC/SOC** All services and components deployed and interconnected as part of the solution shall be monitored 24 hours a day, 7 days a week, 365 days a year (24 x 7 x 365) by a centralized Network Operations Center (NOC) and Security Operations Center (SOC). These functions may be in separate buildings or combined in a single building located in the continental United States.	X			
	NOC/SOC Interoperability Contractor shall have the ability to communicate, troubleshoot and connect with other vendors NOCs should there be a different ESInet and NGCS provider. In addition, the Contractor shall interface with the NOCs that support the regions throughout the state. This shall include ebonding of the ticket systems to support transparency throughout the troubleshooting process.	X			
	NOC/SOC Operations Model Provide documentation including organizational structure and procedures that describe bidder's 1. NOC/SOC operations model, 2. Continuity Of Operations Plan (COOP), 3. problem and change management systems, 4. reporting systems, 5. escalation plan, and 6. conformance with best practices (Information Technology Infrastructure Library (ITIL) or equivalent methodology)) for service-delivery management. The Contractor shall confirm the requirement compliance of any interconnected network utilized by the Contractor not previously identified to the Commission.	X			
	Bidder Response: **Centralized NOC/SOC** The A9-1-1 solution maintains its own Network Operations Center (NOC) from our secure, self-sustaining facility in Longmont, CO. The NOC operates 24x7x365 and provides proactive, real time monitoring of the solution. The NOC leverages highly sophisticated monitoring tools to make sure the systems and networks are maintained to the highest quality and availability. We deploy heuristic analysis, a method employed to detect previously unknown computer viruses, as well as new variants of viruses. Heuristic analysis is an expert-based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	We perform annual external and internal penetration testing of our critical systems and infrastructure. We maintain in-house tools and expertise in order to conduct penetration testing and work with nationally recognized penetration test providers to achieve third party assurance **NOC/SOC Interoperability** Intrado interacts with multiple resolution centers and NOC/SOCs with multiple vendors for various solutions. Intrado has integrated eBonding ticketing exchange for automatic logging and notification of system events. These same systems are available to be used with outside NOCs. Intrado will work with the State on when and through what process (automated or otherwise) the State desires to be notified of various systems' status. **NOC/SOC Operations Model** **1. NOC/SOC operations model** The Intrado Network Operations Center (NOC) is staffed 24x7x365 and is located at Intrado headquarters in Longmont, Colorado, with back-up facilities available for disaster recovery scenarios. The NOC is staffed with highly trained 9-1-1 professionals, currently averaging over nine years of dispatch experience in a PSAP. This unique skill set, coupled with Intrado's refined logging and reporting functionality, means that Intrado's call agents are highly equipped and prepared to handle and supervise emergency service calls. In addition, Intrado's NOC personnel are trained to field questions received from PSAPs or first responders. Tier 1 support will engage Tier 2 and Tier 3 support personnel to resolve high-priority tickets and alarms. In situations where the Originating Service Provider(s) need to be engaged for troubleshooting, the NOC will contact the appropriate wireline, wireless and/or VoIP carriers to initiate the troubleshooting process for full turn-key, 24x7x365 support. Remote monitoring of network and computer performance is conducted to provide statistical data on the number of alarms received and reported based on severity. Monitoring tools to capture the elements of a complex end-to-end service environment include HP Openview for monitoring all network elements, data communications, computer systems, databases, remote facility environments and the applications themselves. Multiple network management components monitor IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. NOC staff can monitor the complex dependencies among these managed elements and alert the appropriate group for interpretation. This provides a method to immediately notify designated personnel of any system failures or performance degradations. Delivery of monitoring reports, including bandwidth utilization and connectivity, are provided as mutually agreed upon during contract negotiations.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	All Intrado network elements are monitored with SNMP at the Intrado NOC. This includes LNGs, ESRPs, ECRFs, BCFs, and PSAP site equipment. Intrado monitors and tracks net flow statistics and performs packet level capture and forensics at the A9-1-1 core sites. Intrado currently operates multiple network and systems monitoring applications across multiple networks and in multiple physical locations. There are currently two varieties of monitoring systems in use at Intrado. One provides a “single pane of glass” for network and system status. This provides SNMP trap and syslog receiver capabilities. These systems also provide ICMP and SNMP trending and threshold alarming. The second type of system provides packet capture, display, and troubleshooting capabilities. Since the underlying network is IPSEC encrypted, SNMP v2 is a fully validated secure method for monitoring the network. Intrado performance monitoring systems have the ability to either retrieve data upon request or publish pre-defined reports based upon the specific needs of the requestor which are then delivered electronically. These reports can be either real-time or historical and the views are based on the actual state of infrastructure. The performance monitoring system supports trend reports that provide short-term and long-term trend plots of imminent violations and customized reports for fault, performance, threshold, and informational messages. To provide consistent levels of service, the NOC maintains a full suite of operations metrics and statistics. The NOC tests and implements new products, performs updates to existing products, and is responsible for creating and archiving production system backups. The Intrado NOC personnel have all had extensive FBI background checks conducted prior to employment. The NOC provides continuous system support and monitoring 24x7x365 to each ALI node supplied by Intrado and to the database management system. Intrado also monitors all PSAP connections into the ALI nodes at the application level. Intrado staffing in the NOC is second to none in the industry with Tier 0 through Tier 2 support staff on duty 24x7x365. The following are key highlights for the NMS (HPOV): • The five state levels from HPOV are as indicated: Critical, Major, Minor, Warning and Normal • We provide notification to the 24x7x365 NOC via a Java GUI referred to as the browser by HPOV • We provide notification by email and SMS • Notification levels are defined by the supporting entity • We are capable of alarm suppression by time, quantity and a combination for reducing alarm notifications

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- For example we can say, no more of a certain alarm for the next 30 minutes or we can say send me duplicate alarms every 5 minutes

- Alarms we typically process are SNMP traps, local agents and polling
  - A monitored system sends us a trap upon the observation of a predefined event in a monitored service
  - Agents run local to the monitored service and do logfile analysis, process analysis, and performance analysis
  - Polling occurs to monitor for availability of service

The polling and local agent analysis intervals vary by device, but typically range from 5 seconds to 5 minutes as defined by the supporting team of that device.

Intrado's advanced monitoring system, Intrado Sentry Monitoring, is a real-time network monitoring solution. Sentry provides enhanced maintenance monitoring and management for both cloud based, and PSAP premise network and equipment. Sentry provides immediate notification of any defined irregular behavior, including faults, exceeding performance thresholds or predicted failures. A Sentry console and local clients communicates system information to the Sentry system and can support Intrado centralized management for several to thousands of Sentry locations with a full range of remote support capabilities. Sentry offers a comprehensive suite of reporting and notification tools to help identify/resolve problems with Intrado call handling solutions, including

- Monitoring Capabilities
  - Serial Data Taps
  - Contact Closures
  - Agent Monitor
  - Cluster Monitor
  - Event Alarm
  - Event Collector
  - Exchange Monitor
  - File Monitor
  - FTP Monitor

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	○ TCP Port Monitor ○ Performance Alarm ○ Ping Monitor ○ POP3 Monitor ○ Process Monitor ○ SMTP Monitor ○ SNMP Object ID Monitor ○ SQL Monitor ○ Page Monitor ○ SNMP Receiver • Notification Methods ○ Alarm Panel ○ Alert ○ Beep ○ Network Message ○ Pager ○ Play Sound File ○ Post Web Form ○ Command Script ○ SNMP Trap ○ SNMP OID ○ Historical reporting of previous faults

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Trend analysis of faults, response and repair times
- Knowledgebase for documenting failure mode history
- Instructions for problem resolution
- Maintenance activity log
- Maintenance mode to prevent nuisance alarms during upgrades
- Full access level control
- Remote terminal access
- Remote computer access
- Web services
- Archive and data warehousing.
- Improved response time to alarm conditions
- Reduced time to resolve alarm conditions
- Increase equipment availability
- Reduced maintenance costs.

2. Continuity Of Operations Plan (COOP)

Intrado provides life-critical services supporting 9-1-1 and public safety and is strongly committed to continuous, sustained readiness of its applications, systems, networks, and processes 24x7x365. Intrado's business and service continuity plans, geographically diverse and redundant systems, and incident management processes and plans provide confidence that continuous operations will be sustained through planned or unplanned events.

Service Continuity Planning Steps

1. *Risk Assessment*

Intrado business and service continuity risk assessment addresses naturally occurring and facility affecting events, as well as system interruptions. Processes in place address interactive management of events designed to support continuous

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

functioning of 9-1-1 systems and enable personnel to continue to perform through specific incident conditions. Intrado's robust incident command system is used for any type of business interruption.

2. *Service Continuity Strategy*

Intrado is strongly committed to providing essential business processes, systems, and networks on a 24x7x365 basis and is well prepared for possible disruptions and disasters. As a critical public safety service provider, Intrado has in place a robust business and service continuity program designed to prevent or mitigate service disruptions and support rapid response to loss or impairment of crucial business functions or infrastructure. To address potential risks, Intrado utilizes:

- Redundant, Geographically Diverse Systems – Systems are in place for 9-1-1 critical path (ALI) and are being implemented for additional Intrado systems and networks. Intrado continues to add geographic diversity to platforms to reduce the impact on 9-1-1 call delivery in the event of loss of a system or network.
- Incident Management – In the event of an unplanned outage or intermittent outage of a system, network component, or application that has the potential to cause an adverse impact to production services, Intrado immediately engages the Intrado Incident Command System, which is based on the FEMA Incident Command Structure. The incident team, led by a qualified incident commander and supported by Intrado technical and operations resources, evaluates the information received, determines the problem statement, categorizes the problem severity level, and manages/works the incident until the incident objectives are met.
- Business and Service Continuity, Disaster Recovery, and Emergency Procedures – Intrado has established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to Intrado facilities or systems, including:
    - Building emergency procedures (e.g. bomb threat, earthquake, power failure, tornado, and flood)
    - Data center risks (e.g. water, flood, power, electrical, and fire)
    - Security Risks (e.g. information and network security, physical security)
    - Building evacuations
    - Pandemic
    - Inclement weather
    - Building disasters

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

3. *Implementing Risk Reduction and Recovery Measures*

Intrado's essential processes, systems, and networks supporting 9-1-1 traffic are designed and deployed to accommodate possible disruptions and disasters to any given element or data center and support 24x7x365 continuous operation. In the event of unplanned system or network outages, this diversity allows for Intrado 9-1-1 systems to continue operating while Incident Management processes are engaged to identify and resolve issues so that redundancy is fully restored.

4. *Developing Plans and Procedures*

Intrado's continuity plans cover critical application and infrastructure components, including services provided to and on behalf of our customers. At least one copy of the continuity plans is maintained offsite in secure storage, available 24x7x365. Key personnel possess encrypted electronic copies of business continuity information, updated regularly. Intrado conducts reviews and updates of continuity data and plans at least annually. Certain continuity plan functions are exercised on an on-going basis, such as Incident Management, which is utilized for all planned and unplanned events. Intrado is well prepared and practiced for contingencies and has communications protocols and processes in place to notify personnel, customers, vendors, suppliers, and regulatory bodies in support of Intrado applications, systems, and network components. Continuity plan materials include:

- Essential functions and personnel
- Employee emergency contact information
- Building emergency procedures
- Contractor/Vendor contact procedures
- Crisis communication plans
- Specific scenario response procedures
- Customer contact and notification
- Life mission critical system recovery processes

5. *Testing Service Continuity Plans*

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado implements and tests its Incident Management Plan on a regular basis and conducts audits and reviews and/or walk through exercises of its continuity plans at least annually. Information gathered feeds into a continuous improvement cycle as part of the maintenance and review process.

6. *Service Continuity Plan Maintenance*

Intrado conducts a maintenance review of its continuity plans at least annually. In this review, which is coordinated by the overall plan owner, the interdependent plan owners identify, validate, implement, and document changes to the plan components.

3. problem and change management systems

Intrado utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well best-in-class tools for Change Management, including the use of ServiceNow Change Management Module. Depending on the type of change, changes are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

Intrado changes are submitted to a Change Advisory Board (CAB), a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of project and product stakeholders or their representatives. Intrado manages all aspects of change management through the CAB approval process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

There are four change event types:

Minor Change (Severity 4 Change)	A cosmetic flaw or minor problem to a component of the application that does affect usability or functionality
Planned Event	Any upgrade, enhancement, or configuration change to a production system or network. A planned event has a minimum of five (5) business days to submit an event plan to the Intrado CAB.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Emergent Event	An upgrade, enhancement, or configuration change to a production system or network that requires attention in less than five (5) business days.
Incident Change	In progress or imminent issue has been identified that requires immediate action. Does not require that the change go through the same process as a planned event. All incident changes are documented for tracking purposes and reviewed.

Table 1: Change Management Event Types

For a planned or emergent event to receive approval there must be an event plan submitted to the Intrado CAB. The event plan must include a step-by-step guide of changes being made and clearly state the impact of each change. All event plans must also include a detailed validation plan and back-out plan in compliance with implementation plan standards and approved by the CAB stakeholders. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA. Intrado will provide written notification and release content, when applicable, to the State.

If the event is closed as unsuccessful and the back-out plan was enacted, the issues which caused the event to be unsuccessful are documented. A new event plan and subsequent change must be submitted for re-approval by the Intrado CAB.

Intrado CAB also documents and stores each event for tracking and reporting purposes. Intrado CAB logs all planned and emergent event change requests on events that are both approved and declined. Intrado also reviews and issues Reason for Outage (RFO) reports when outages occur.

In addition to planned and emergent events, Intrado also maintains a problem management system for tracking and reporting trouble. Intrado provides a service portal for opening trouble tickets, change requests and checking status of existing items. Intrado can also provide monthly trouble reports showing tickets opened, resolved and unresolved.

Intrado also utilizes the Incident and Problem Management modules of ServiceNow, which allows for tracking of break/fix issues as well as any resulting Problem Management requests.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado utilizes ServiceNow for managing service events. The Change Management module tracks changes system hardware and software versions. Upgrade events can be tracked via the Change Management module to establish a full version history of the system. ServiceNow ServiceNow is utilized to create and track service requests/tickets, group similar tickets into problems for further analysis, record the original hardware and software for each site, and track changes to hardware and software by site. Service requests can be initiated either via a phone call to the Intrado Help Desk or by utilizing the online Service Request Module (SRM). SRM allows a user to log on and request service via a web portal. The user can also view previous requests and their current statuses as well as closed requests. Users are typically configured to only be able to view and open requests for their respective PSAPs. However, users can be configured to see a broader set of PSAPs such as an entire region or even statewide. Multiple tickets can be grouped together as a “problem” in ServiceNow to trigger additional investigation of observed trends. The problem will be reviewed by Level 2 or 3 support and possibly engineering. Once a resolution to a problem is identified proper corrective action, if any, can be taken. When a customer is set up in ServiceNow, the equipment shipped to each PSAP is associated with the PSAP. This includes types of hardware and serial numbers. If maintenance requires the replacement of a position, the new serial number will be updated in the database. Similarly, the version of software that shipped with the system is recorded as well. When subsequent updates are performed, the new software version will be updated in the database. Such changes can be tracked via a change event or a maintenance ticket depending on the scope or nature of the change. **4. reporting systems** Intrado can provide reports from ServiceNow for incidents, changes, and problems that are open, pending, resolved etc. on weekly, monthly, and an annual basis if necessary. ServiceNow is utilized to create and track service requests/tickets, group similar tickets into problems for further analysis, record the original hardware and software for each site, and track changes to hardware and software by site. Service requests can be initiated either via a phone call to the Intrado Help Desk or by utilizing the online Service Request Module (SRM). SRM allows a user to log on and request service via a web portal. The user can also view previous requests and their current statuses as well as closed requests. Users are typically configured to only be able to view and

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

open requests for their respective PSAPs. However, users can be configured to see a broader set of PSAPs such as an entire region or even statewide.

Multiple tickets can be grouped together as a “problem” in ServiceNow to trigger additional investigation of observed trends. The problem will be reviewed by Level 2 or 3 support and possibly engineering. Once a resolution to a problem is identified proper corrective action, if any, can be taken.

5. escalation plan

The first step in the escalation process is always handled through the A9-1-1 Network Operations Center (NOC) and can be initiated at any time by requesting a NOC Supervisor. The NOC is staffed 7x24x/365 and a supervisor is always available to escalate an incident if necessary. Listed below are the current A9-1-1 escalation procedures.

Listed below are current A9-1-1 escalation procedures.

Table 2: Escalation Procedures

Escalation Intervals	Level	Responsibility
First Escalation SEV 1 - 2 Hours SEV 2 – 4 Hours SEV 3 – 6 Hours	NOC Manager	Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center
Second Escalation Customer Discretion	Area Manager or Delegate	Review status of ticket Monitor ticket progress Notify Director - when appropriate
Third Escalation Customer Discretion	Director	Status Customer Escalate as needed to partner centers Monitor ticket progress/ documentation Notify VP when appropriate
Fourth Escalation	Vice President	Ensure adequate resources are available and engaged for prompt resolution Update customer as appropriate Escalate as needed to appropriate levels

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	When escalating a problem, it is important to provide the following information: • Customer's name and telephone number • Active ticket number(s) • Trouble Location • Trouble description (e.g., out of service, service degraded, etc.) • The action or resolution requested **6. conformance with best practices (Information Technology Infrastructure Library (ITIL) or equivalent methodology)) for service-delivery management. The Contractor shall confirm the requirement compliance of any interconnected network utilized by the Contractor not previously identified to the Commission.** An escalation matrix is in place to ensure that Intrado utilizes industry standard processes, including adherence to the Information Technology Infrastructure Library (ITIL) and Federal Emergency Management incident management practices (FEMA).

Any additional documentation can be inserted here:

NOC/ SOC 2	**NOC/SOC - Remote Connectivity Required** Contractor shall provide any network connectivity required to support Contractor's NOC/SOC services. Describe any remote connectivity required by the solution including, but not limited to, Virtual Private Network (VPN), phone-home connection, and tech support remote access.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: All remote connectivity is included in the base services of the system. All remote locations (PSAP CHE host locations) are accessible through the dedicated IP connectivity included in this service. Any connectivity to the NGCS platform is available by dedicated Connectivity terminated to Intrado's NOC/SOC and also available through a secure VPN platform maintained by Intrado.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 3	**NOC/SOC - Network Security Monitoring and Management** **Security Management Solution** The bidder's security management solution shall control access to network resources in accordance with public safety network security best practices such as NIST, NENA and the FCC to prevent sabotage, service interruption (intentional or unintentional) and the compromise of sensitive information. Security management shall comply with security- and data-integrity standards listed in Section V.D.1. Table 1 in the RFP, to monitor users logging into network resources and to refuse access to those who enter inappropriate access codes. The proposed IP network and systems shall support standard security policies that may include the use of firewall rules, Access -Control Lists (ACLs), Virtual Local-Area Networks (VLANs), VPNs, and Transport Layer Security (TLS) protocols to control network traffic and access. The systems shall support the use of software to detect and mitigate viruses, malware, and other attack vectors. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: A9-1-1 adheres to NENA 75-001 (NENA Security for Next-Generation 9-1-1 Standard [NG-SEC]) and NENA 04-503 (PSAP Security), as applicable, and we track alignment to the NIST Cybersecurity Framework in addition to the applicable areas of the FBI CJIS Security Policy. The A9-1-1 solution supports centralized management of user permissions, rights, and security settings by designated administrators. The system administrators can use the application to manage user roles and privileges, including granular authentication, user profiles, and other security rights. The system can be configured so that wherever an authenticated user logs in, without regard to which workstation or which PSAP, all the user's rights, permissions and configurations follow that user. The proposed system is password-protected, so only properly credentialed, authorized users can use it. Security options can be configured according to user group. Administrators can create groups of user-assigned roles with associated user settings to be automatically applied when users are authenticated during log-in. All systems use the highest capabilities of protection and authentication available, including IPSec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification. Operating system and application protections are configured for segregation of duties, and strong password policies are enforced to ensure that password length and minimum change restrictions are followed. Strict auditing controls are enforced across the enterprise. Remote access to the A9-1-1 network is permitted providing that authorized users are authenticated, and privileges are restricted. Remote access is only permitted via equipment which utilizes an approved firewall, anti-virus protection, and strong authentication. Any connections over the Internet employ an authorized VPN client. Remote access to perform				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	systems administration tasks is achieved over Secure Shell (SSH). Intrado administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform the work. Intrado incorporates a robust strategy for identity management, and user access to Intrado web-based applications is protected through an identity management system. New users must complete a rigorous online registration process. Multi-factor authentication and role-based access control are used to restrict user access to Intrado's trusted resources. User access via the public Internet requires two-factor authentication, where one factor is provided through user name and password and the second factor is provided through a dynamic, randomly changing secure access code from an Intrado-provided security token. Users are configured in the identity management system, and linked to a specific security token and configured for access to a defined list of applications. A9-1-1 cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology. A9-1-1 infrastructure is designed to withstand sophisticated cyber-attacks. A9-1-1 is a secured and private IP managed network providing services for 9-1-1 call delivery. All inbound and outbound traffic interactions are with pre-vetted entities, use well defined protocols and traverse controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. Sensitive data is housed in data centers with logical and physical access controls. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough vulnerability scan testing. Corporate, development, and test environments are separate from production, and live production data is not used for development or testing purposes. Inter-zone traffic is restricted to only authorized personnel and the necessary protocols destinations used to support the management and applications of A9-1-1 with all other traffic implicitly denied by way of redundant and diverse session border controllers and firewalls. A9-1-1 infrastructure is built to withstand sophisticated attacks by means of a defense-in-depth strategy. A9-1-1 employs high availability systems with redundancy at geographic, carrier, circuit, power, application, and system levels. System/Application availability is safeguarded with clustering and load balancing techniques. The security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, IDS, multi-factor authentication, strong encryption, encrypted data at rest, anti-virus/anti-malware, vulnerability, and patch management solutions. Traffic between core processing and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) are route-secure and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of A9-1-1.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado employs a regularly scheduled patching process to protect against security vulnerabilities and the effects of malware. Computing devices are subjected to thorough security scans for malware elements. Physical, network, and application access to production components is restricted to personnel that have a direct operational responsibility, with all activity audited and monitored. The Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage A9-1-1 associated services and connectivity to the network. When a potential or actual customer-affecting issue is defined and determined to be an incident, the Incident Administration team is engaged by the NOC. The team uses established processes that are ISO 9001:2015-compliant for immediate escalation, notification, resolution, and reporting. All buildings, NOC and Data Center access are monitored by 24x7 security and access control systems. Security Information and Event Management (SIEM) analysis is a daily task of our Security Operations Center. We have deployed a SIEM tool for log aggregation and consolidation from multiple machines and for log correlation and analysis. Info security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. We deploy heuristic analysis, a method employed to detect previously unknown computer viruses, as well as new variants of viruses. Heuristic analysis is an expert-based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. We perform annual external and internal penetration testing of our critical systems and infrastructure. We maintain in-house tools and expertise in order to conduct penetration testing and work with nationally recognized penetration test providers to achieve third party assurance.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 4	**NOC/SOC - Connected Systems Compliance** Any system that connects to an IP network shall be required to comply with listed standards in Table 1, including security standards, and demonstrate compliance through an initial and recurring audit. **Security Reports and Recommendations** Contractor shall provide, within 30 days of the end of each calendar month, security summary reports and recommended improvements on a monthly basis (at a minimum), including incidents and incident response; building, facility, and network access reports, including failed attempts; and updates or changes to security systems and software. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: If selected by the State of Nebraska, Intrado will work with the State to implement mutually agreed upon reporting as indicated in this requirement. The Next Generation 9-1-1 (NG9-1-1) solution adheres to industry standards, guidelines and recommendations including those of the NENA ESIND (ESInet Network Design) and meets the security criteria as defined in the NENA NG-SEC specifications for NG9-1-1 security. The standards listing included in Table 1 is quite extensive, and it should be noted the challenges to continuously monitor and track compliance across such an expansive listing of frameworks, standards and specifications. Intrado is engaged with, and play active roles in, industry associations that develop standards applicable to NG911, including NENA, APCO, ATIS, FCC, PCIA, and TIA. Due to the complexity of the solution and the afore mentioned challenges of continuously tracking compliance across numerous and constantly changing compliance frameworks, we adhere to the security requirements and the NENA Security for Next-Generation 9-1-1 Standard (NG-SEC). In addition, our overall information security program is based upon the requirements of the ISO/IEC 27001 international standard. And due to the critical nature of the infrastructure in supporting the 9-1-1 call processing environment, we track alignment to the NIST Cybersecurity Framework in addition to the applicable areas of the FBI CJIS Security Policy. To ensure ongoing compliance, our Governance Risk Compliance (GRC) program includes annual reviews of applicable control requirements through internal controls assessments and audits. In addition, the environment undergoes periodic review by an independent third-party, at least every three years. Intrado has a robust operational and incident security management process including an incident response team. Access to facilities is managed with card readers, security camera surveillance, and 24x7 security personnel. Intrado has implemented a central logging system that captures authorized and unauthorize attempts to access the environment and maintains an ITIL-based change management system for managing changes to the production environment.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 5	**NOC/SOC – Connected Systems Compliance** **Support for Similar Solutions** Provide details concerning how bidder provides security monitoring and management for similarly deployed production solution. Provide details, including drawings, which explain how the proposed solution meets or exceeds the above requirements.	X			
	Bidder Response: Intrado's cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology (COBIT). CenturyLink's next generation emergency services network is a secured and private IP managed network. All inbound and outbound traffic is through well-defined and controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. Intrado employs a defense-in-depth security strategy to protect sensitive information. Such controls include, but are not limited to stateful packet inspection firewalls (host and network based), IDS/IPS, ACLs, Role-based Access control, two-factor authentication, encryption, and AV (email and host). Furthermore, systems are protected with build standards, patch management, and regular vulnerability scans. Sensitive data is housed in our data centers with logical and physical access controls. Development environments are separate from production and production data is not used in dev or SQA. Data transits untrusted networks (leaves Intrado custody) through applications or communication channels with encryption to safeguard confidentiality and integrity. The A9-1-1 infrastructure (illustrated in the figure below) is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. Intrado employs high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/application availability is safeguarded with clustering and load balancing techniques. Furthermore, A9-1-1's security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

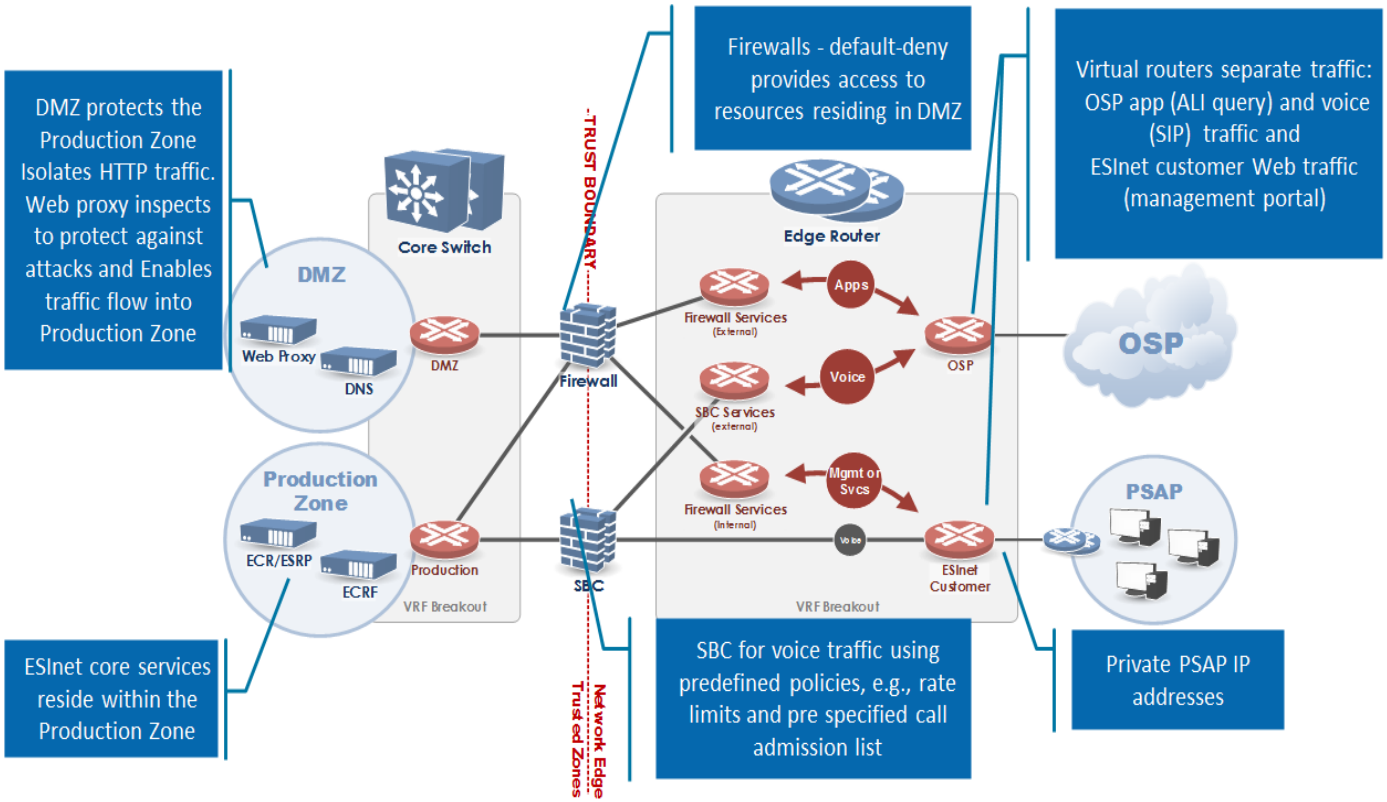

Figure 6: Defense in-depth Security Architecture

The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or Access Control Lists (ACLs). Intrado continually investigates and upgrades with new advances in protective technology with tools such as Intrusion Detection System (IDS).

The solution incorporates physical, network, and application security principals. Traffic between Core processing sites and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) is route- and protocol-secure. A combination

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution. Intrado's A9-1-1 deploys firewalls and other network security devices and software to protect against inbound network threats on the servers that make up the proposed ESInet. The NOC also employs a regularly scheduled patching process to protect against the effects of malware. Computing devices are subjected to thorough security scans so that there are no malware elements present. Access to processing elements is restricted to authorized personnel. Network connections from solution components are limited to those connections needed for operation and maintenance. Physical and network access to production components is restricted to those that have an operational responsibility, and all activity is audited and monitored. All development environments are fully separate from production environments. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 6	**NOC/SOC - Physical Access Monitoring and Management** Contractor shall track and log all physical access to structures housing IP network components serving the Commission or have the capability to obtain access logs for structures not under immediate control of the bidder. Reports may be requested and shall be made available for review upon request. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Provide a detailed explanation of bidder's processes and procedures for logging physical access to ESInet /NGCS components, and how the bidder's solution generates the required reports.	X			

Bidder Response:

Intrado maintains an information security policy derived from the ISO 27000 suite of standards and observes practices and standards accordingly. Intrado has implemented controls that address the policy concerns of the NENA 75-001 NG-SEC security standard. This standard comprehensively identifies a variety of security measures, including physical security safeguards, badge and biometric access controls, observing Principle of Least Privilege, Operating System hardening, IDS/IPS, firewalls, adhering to Information Security Best Practices, stringent change management processes, Security Incident Response capability based on the FEMA Incident Command System.

Intrado controls physical access to facilities that house Intrado information, information systems, and/or personnel in order to prevent unauthorized physical access, damage, and interference to information and information processing facilities. This includes:

- Verifying and enforcing physical access authorizations for all physical access points not designated as publicly accessible
- Controlling entry to facilities containing information systems using physical access devices or mechanisms (e.g., badges, keys, combinations) and/or guards
- Implementing role-based physical access to buildings, facilities, secured areas, and resources
- Maintaining a list of individuals with authorized access to facilities containing information systems and issuing authorization credentials for facility access; the access list is reviewed periodically and individuals who no longer require access are removed from the list
- Ensuring that onsite personnel and visitor identification (e.g., badges) are revoked, updated when access requirements change, or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned, disabled, or changed

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Granting visitor access for specific and authorized purposes, providing visitors with instructions on security requirements and emergency procedures, and issuing visitor badges that are visually distinct from personnel badges • Restricting unescorted access to personnel with required security clearances, formal access authorizations, and validated need for access Intrado has extensive physical security controls at our data center sites. This includes badge access to general security environments along with multi factor authentication requirements for more secure areas including network egress points. Access to the Miami data center is controlled via WORK VISIT tickets opened with Equinix. Intrado can demonstrate access to those components via WORK VISIT tickets for Miami and logs from door readers and Access Log books at entry for Longmont.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 7	**NOC/SOC - Incident Management System** The bidder's incident management system shall log all support requests, both from users and those automatically generated. 1. Provide examples of monthly reports detailing tickets opened, pending, resolved, and closed. 2. Provide a matrix outlining Service Impact Levels in a detailed response, to include notification times and response times.	X			
	Bidder Response: In case of a service interruption and/or outage, our team has instituted Incident Management processes and procedures for dealing with various severity levels during the course of an incident. Our incident response tools include use of the Incident Command System (ICS), which is housed within our Ticketing System. The ICS is modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute for major incidents. The ICS processes include resolution, documentation of any incident, communications, and post- event analysis. Incidents overall, regardless of level of severity, are tracked within our ticketing system, which also provides broadcast messaging available for real-time updates and status of ongoing service affecting issues that may impact the A9-1-1 solution. Incident Management personnel are trained in incident command with courses provided by the Emergency Management Institute, a FEMA-sponsored Emergency Management Course as well as the ITIL framework. Incident Management is available 24 hours a day, 7 days a week. Intrado utilizes the Incident and Problem Management modules of ServiceNow, which allows for tracking of break/fix issues as well as any resulting Problem Management requests. All support requests from users and those automatically generated are logged. **1.** Samples of monthly reports can be found below.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Figure 7: Monthly Incident Reports

Within ServiceNow, if the customer is set up to e-Bond or use the Customer Management Portal they would have access to a customer dashboard that would enable them to see any open requests and the status of each of those requests within the system.

2. A table outlining Service Impact Levels, including notification and resolution times is below.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Table 1: Intrado Severity Levels

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major	Customer is able to access the system, or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado will conduct major and minor planned and critical un-planned changes for all A9-1-1 system maintenance or upgrades that may impact customers. Intrado will manage and complete events with a trained ESInet change management team facilitating the change implementation, monitoring, and communication through the length of the event. Intrado adheres to stringent internal event plan processes and procedures which include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado will include the required back-out time within the scheduled maintenance time-frame.

Intrado utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well as best-in-class tools for Change Management for managing changes to the service. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management. Generally speaking, there are two classes of ESInet maintenance e.g., standard and emergency.

- **Standard:** Intrado will provide a schedule of standard maintenance windows for activities defined below as: level 4 standard and level 3 normal.
- **Emergency:** Where reasonably practicable, Intrado will give the State of Nebraska 24 hours' notice of the need for the maintenance and a summary of the potential impact. Emergency maintenance may occur at any time.

Table 2: Change Management Event Type

Change Event Type	Definition	Notification
Level 4 - Standard	A planned maintenance event that is a low risk and repeatable change that occurs frequently. Repeatable Change plans / MOPs have been established. Example: PSAP Network failover testing (pre-production), replace a failed disk drive within an array.	Courtesy notification will be provided for standard changes directly affecting A9-1-1. These notifications will not require customer approval.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Level 3 - Normal	A planned maintenance event or upgrade, potentially partial- or full-service impacting. Normal changes are categorized according to risk and impact. Change Plans for events requiring the Customer's support will be reviewed with Intrado prior to the scheduled date. Example: Router replacement, PSAP activation, A9-1-1 software upgrade.	Target timeframe to be provided minimum of 45 days in advance to Customer. Detailed schedule with date, time, and duration to be provided a minimum of 30 days in advance.
Emergent - Emergency	A change that resolves a problem deemed critical to business continuity and for which a workaround is not sufficient. An issue considered high risk and has a potential for an immediate threat to the production environment. Example: A router issue that has the potential to affect voice delivery.	The risk posed by the issue may not allow Intrado to provide advance PSAP notification for this type of event. Intrado shall notify PSAP customers as soon as a need for maintenance is identified. Every effort will be made to provide as much advanced notification as possible for issues anticipated to result in a Severity 1 or Severity 2 service disruption. For issues not anticipated to result in a Severity 1 or Severity 2 service disruption, notification shall be no less than twenty-four (24) hours.

Depending on the type of change, changes are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

For a Planned or Emergent Event to receive approval there must be a change plan submitted to the CAB. The change plan must include a step-by-step guide of changes being made and clearly state the impact of the change. All change plans must also include a detailed validation plan and back-out plan in compliance with implementation plan standards and approved by the CAB Stakeholders. All event resources are clearly listed and verified ahead of time. New application

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	code is never to be loaded without it being officially released by QA. Intrado will provide written notification and release content (when applicable) to the jurisdiction(s). If the event is closed as unsuccessful and the back-out plan was enacted, the issues which caused the event to be unsuccessful are documented. A new change plan and subsequent change must be submitted for re-approval by the CAB. The CAB also documents and stores each change for tracking and reporting purposes. The CAB logs all planned and emergent change requests on events that are both approved and declined. We also review and issue Reason for Outage (RFO) reports when outages occur. For Normal, Emergency, and Expedited changes, a change request is submitted to the CAB. The request must include a step-by-step guide of changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment. We will provide written notification and release content (when applicable) to the State. The result of each change is tracked and available for future reference in our system whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues which caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the CAB. If the change was successful with deviation, this is also tracked with the deviations documented. Intrado uses a suite of interlinked management tools for Incident, Problem and Change Management, which allows for tracking of break/fix issues as well as any resulting Problem Management requests. This tool suite and built-in ITIL best practices enable us to understand and minimize risk while making IT changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs processes by allowing changes to be evaluated for their benefits and risks and considering all impacts. We have scheduled maintenance time frames for non-emergency events. If we have an emergency item, we will alert the customer using a standard process. The customer has options on the modality of this communication (i.e. text, email, etc.) The Intrado Service Manager will provide advance notice of maintenance events. For questions during the maintenance window, the customer should contact the A9-1-1 NOC. The A9-1-1 maintenance window is 12am-6am per time zone (Tuesday-Thursday), unless otherwise agreed to in order to resolve service impacting issues. Changes affecting multiple time zones will be completed between 12am-6am CT. Intrado

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Customer PSAPs may require maintenance at the PSAP to be done outside of this maintenance window, in which case Intrado will coordinate an appropriate time to perform maintenance at the PSAP. In addition to managing planned and emergent events, we maintain a problem management system for tracking and reporting trouble. Intrado provides a service for opening trouble tickets, change requests, and checking status of existing items e.g., tickets opened, resolved and pending.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 8	**NOC/SOC - Change Management System** **Change Management Review System** Describe bidder's change management system and the ability to provide the Commission's program manager and designated PSAP representatives with the ability to review proposed change requests and the client approval process. The Contractor shall provide monthly reports detailing change tickets opened, pending, resolved, and closed.	X			

Bidder Response:

Intrado utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well as best-in-class tools for Change Management, including the use of the ServiceNow Change Management Module.

Intrado will conduct major and minor planned and critical un-planned events for all A9-1-1 system maintenance or upgrades that may impact customers. Intrado will manage and complete changes to the service including aggregation sites, core call routing complexes, PSAP equipment maintenance, circuit maintenance, and software upgrade events, with a trained ESInet event management team facilitating the change implementation, monitoring, and communication through the length of the event. Intrado adheres to stringent internal event plan processes and procedures which include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado includes the required back-out time within the scheduled maintenance time-frame.

Change Requests very widely in terms of scope and complexity, dependent upon the type of change. Change Requests with largest potential impact are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. Intrado manages all aspects of Change Management through the Change Management Process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

Depending on the type of change, changes are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT service continuity management. Generally speaking, there are two classes of ESInet maintenance e.g., standard and emergency.

- **Standard:** Intrado will provide a schedule of standard maintenance windows for activities defined below as: level 4 standard and level 3 normal.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- **Emergency:** Where reasonably practicable, Intrado will give the Commission and any affected PSAPs 24 hours notice of the need for the maintenance and a summary of the potential impact. Emergency maintenance may occur at any time.

There are five categories of changes.

NORMAL*	This change indicates a low risk and repeatable change that occurs frequently. Once it is deemed appropriate (3 successful) Change plans/MOPs are in place, a template will be built so the change can be entered as a Standard Change for future usage negating the need for a normal change. This change type does not require CAB approval.
NORMAL	Normal changes are often categorized according to risk and impact to the organization. By definition a normal change will proceed through all steps of the change management process, including the CAB for approval.
POST-DATED	This change should be utilized for unplanned work, resulting from a critical incident ticket and/or Major Incident.
EMERGENCY*	By definition an Emergency* change will proceed through all steps of the change management process and will be reviewed by the executive CAB unless there is a valid business reason to bypass the 48 hour advance submittal time frame.
EMERGENCY	Utilized for a change that resolves a problem deemed critical to business continuity and for which a workaround is not sufficient. Examples are a router that could put voice delivery at risk and has a potential for an immediate threat to the production environment and /or to be a major impact to Business or Customer. Emergency changes are approved at an Emergency Executive CAB.

Table 3: Change Management Change Categories

For a Planned or Emergent Event to receive approval there must be an event plan submitted to the CAB. The event plan must include a step-by-step guide of changes being made and clearly state the impact of the change. All event plans must also include a detailed validation plan and back-out plan in compliance with implementation plan standards and approved by the CAB Stakeholders. All event resources are clearly listed and verified ahead of time. New application code is never

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	to be loaded without it being officially released by QA. Intrado will provide written notification and release content (when applicable) to the jurisdiction(s). For Normal, Emergency, and Expedited changes, a change request is submitted to the CAB. The request must include a step-by-step explanation of the purposed changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment. The result of each change is tracked and available for future reference in our ServiceNow Change Management Module whether it was successful or unsuccessful. If the change or event is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the CAB. If the change was successful with deviation, this is also tracked with the deviations documented. The CAB also documents and stores each event for tracking and reporting purposes. The CAB logs all planned and emergent event change requests on events that are both approved and declined. We also review and issue Reason for Outage (RFO) reports when outages occur. We have scheduled maintenance time frames for non-emergency events. If we have an emergency item, we will alert the Commission and affected PSAPs using a standard process. The State can choose the modality of this communication (i.e. text, email, etc.) The Intrado Service Manager will provide notice of maintenance events. Intrado maintains open communication with its partners about all changes through weekly reports that detail upcoming changes. These reports clearly outline proposed changes and allow for input and thorough understanding of what change is occurring, why it is occurring, and what potential impacts might be seen during the change event. Intrado welcomes partner feedback during this process to minimize impact on the end users. For questions during the maintenance window, the State should contact the Intrado NOC. All events are formally closed out and communicated via email upon completion of the event. An event will either be closed as successful or would be backed out and rescheduled with proper information given. The A9-1-1 maintenance window is 12am-6am per time zone (Tuesday-Thursday), unless otherwise agreed to in order to resolve service impacting issues. Changes affecting multiple time zones will be completed between 12am-6am CT.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Customer PSAPs may require maintenance at the PSAP to be done outside of this maintenance window, in which case Intrado will coordinate an appropriate time to perform maintenance at the PSAP. In addition to managing planned and emergent events, we maintain a problem management system for tracking and reporting trouble. Intrado provides a service for opening trouble tickets, change requests, and checking status of existing items e.g., tickets opened, resolved and pending.

Any additional documentation can be inserted here:

NOC/ SOC 9	**NOC/SOC - Change Management System** **Change Management Tools** Provide detailed descriptions of any other tools bidder intends to use to provide access to the change management system, such as web portals and client software.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado utilizes the Change, Incident, Problem Management, and Knowledge modules of ServiceNow, which allow for tracking of all new and existing change requests as well as any resulting break/fix issues or problem management requests. The goal of having all these modules in one unified system is to complete change requests as quickly and efficient as possible in a prioritized fashion. Having one system allows for easier tracking and linking of events, simplifying the process for our resources and allowing for clear communication with our partners. In addition to managing planned and emergent events, we use ServiceNow for tracking and reporting trouble. Intrado provides a service for opening trouble tickets, change requests, and checking status of existing items e.g., tickets opened, resolved, and pending. In addition, Intrado can offer e-Bonding to the State's NOC if they meet the requirement of an API.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 10	**NOC/SOC – Change Management System** **Change Testing and Training Environment** A non-production ESInet replica / NGCS replica, test lab, or similar system shall be established to test, and exercise proposed upgrades, third-party interfaces, and applications prior to release in live production. This system also could be leveraged for training purposes. Provide detailed descriptions of how the solution satisfies this function in the change management process.	X			

Bidder Response:

We employ rigorous steps to technically and operationally review all new hardware, software and patch releases end-to-end. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. The testing program includes the following elements.

- Test plans developed in conjunction with equipment and software vendors.
- Labs that mirror the production architecture and operating environment.
- Coordination with vendors to address any problems related to new product or software releases.
- Oversight of the First Office Application (FOA) of all newly introduced hardware or software releases.
- Provides Approval for Use and certifies new hardware or software release upon successful completion of FOA soak period.

Intrado offers an i3 CPE test lab program. As part of this program, Call Handling vendors, NG Service Providers, Originating Service Providers, and Additional Data Providers can test with Intrado's A9-1-1 lab to validate i3 interoperability before going into production.

Changes can be application software upgrades, third party software upgrades, or new/upgraded hardware. During the standard change testing process, Intrado maintains a production-like Testing/SQA environment in which any and all changes are verified. The testing of new changes initially is manual to validate/verify feature interaction, and then automated. Intrado performs automated testing every night in the Testing environment to ensure that as changes are made that the existing feature base is not impacted. The test automation test suite continuously grows as new features are added.

Intrado provides mechanisms that allow test calls to be directed to a CPE training deployment in production. These calls are marked as test calls and do not impact any metrics reporting. For Ingress Service Providers and CPE Providers, Intrado provides a dedicated Customer Integration Lab (CIL) that said providers can test and validate their systems with the Intrado A9-1-1 Routing systems.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NORMAL	**NOC/SOC – Change Management System** **Change Management Process** 1. Outline bidder's proposed change management process. The ITIL change management standard methods and procedures are preferred. 2. Include a description of the process for notifying the Commission and affected PSAPs. Notification shall be made no less than ten (10) business days in advance of the change, except in emergency situations, in which case notification shall be provided immediately. 3. Include explanation of solution's Fault, Configuration, Accounting, Performance, and Security (FCAPS) procedures. 4. Provide a detailed explanation describing how the proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.	X			

Bidder Response:

1. Intrado utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework, as well best-in-class tools for Change Management, including the use of ServiceNow Change Management Module. Depending on the type of change, changes are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

There are five categories of changes:

Change Category	Description
NORMAL*	This change indicates a low risk and repeatable change that occurs frequently. Once it is deemed appropriate (3 successful) Change plans/MOPs are in place, a template will be built so the change can be entered as a Standard Change for future usage negating the need for a normal change. This change type does not require CAB approval.
NORMAL	Normal changes are often categorized according to risk and impact to the organization. By definition a normal change will proceed through all steps of the change management process, including the CAB for approval.
POST-DATED	This change should be utilized for unplanned work, resulting from a critical incident ticket and/or Major Incident.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

EMERGENCY*	By definition an Emergency* change will proceed through all steps of the change management process and will be reviewed by the executive CAB unless there is a valid business reason to bypass the 48 hour advance submittal time frame.
EMERGENCY	Utilized for a change that resolves a problem deemed critical to business continuity and for which a workaround is not sufficient. Examples are a router that could put voice delivery at risk and has a potential for an immediate threat to the production environment and /or to be a major impact to Business or Customer. Emergency changes are approved at an Emergency Executive CAB.

Table 4: Change Management Change Categories

For Normal, Emergency, and Expedited changes, a change request is submitted to the CAB. The request must include a step-by-step guide of changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment. We will provide written notification and release content (when applicable) to the State.

The result of each change is tracked and available for future reference in our ServiceNow Change Management Module whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues which caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the CAB. If the change was successful with deviation, this is also tracked with the deviations documented.

Intrado also utilizes the Incident and Problem Management modules of ServiceNow, which allows for tracking of break/fix issues as well as any resulting Problem Management requests.

2. Intrado meets weekly to discuss all changes to the production environment. As soon as a change is vetted and authorized to move forward the Intrado Program Management team will add it to the week status report that would be sent to Nebraska for review. All normal change events would be scheduled to meet the requirement of 10 business days, unless the event is deemed to be Emergent or Emergency event. All change events are sent to partners as soon as possible and are not held to notify at the minimum requirements.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	3. FCAPS, a network management framework created by the International Organization for Standardization (ISO), categorizes the working objectives of network management into five levels: the **F**ault-management level, the **C**onfiguration level, the **A**ccounting level, the **P**erformance level, and the **S**ecurity level. The levels are described below: • **Fault Management** - network problems are found and corrected. Potential future problems are identified and steps are taken to prevent them from occurring or recurring. With fault management, the network stays operational, and downtime is minimized. • **Configuration Management** - network operation is monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. At this level, inventory of equipment and programs is kept and updated regularly. • **Accounting Management** aka allocation level - devoted to distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the cost of operation. The Accounting level is also responsible for ensuring that users are billed appropriately. • **Performance Management** - is involved with managing the overall performance of the network. Throughput is maximized, network bottlenecks are avoided, and potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement. • **Security Management** - the network is protected against hackers, unauthorized users, and physical or electronic sabotage. The confidentiality of user information is maintained where necessary or warranted. Security systems also allow network administrators to control what each individual authorized user can (and cannot) do with the system. **4.** Conformance to Information Technology Infrastructure Library (ITIL) framework and best practices allows us to understand and lessen risks while making changes, as well as enabling the environment to be reliable, and predictable. Intrado utilizes and follows ITIL and FCAPs processes in order to evaluate changes for their benefits and risks and consider all impacts.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 12	**NOC/SOC - Network Management System** **System and Network Management Software** Software packages are widely available for capturing, analyzing, and reporting the network's health based on the Simple Network Management Protocol (SNMP) traffic it receives. Provide the name and description of the management software that will be implemented including all functional modules associated with it (e.g., reporting, backup, and IP address management).	X			

Bidder Response:

The A9-1-1 NOC/SOC uses multiple tools and techniques to track performance and fault management activities. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to HP OpenView, which is used to present a single pane of glass to the A9-1-1 NOC. OpenView utilizes the HP Operations Manager (OM) module, which monitors systems and applications using agents and provides SNMP trap and syslog receiver capabilities, and the HP Network Node Manager (NNMi) network monitoring software module based on SNMP. Visual alerts are available 24x7x365 to the A9-1-1 NOC. These systems also provide ICMP and SNMP trending and threshold alarming.

The A9-1-1 NOC also utilizes the following:

- Riverbed Steel Central suite of tools is used for Network Configuration collection/management, and IP network performance tracking and reporting.
- BlueCat Proteus IP Address Management (IPAM) solution is the IP Management tool; it enables us to design, deploy, reconfigure, and maintain the IP address inventory of all devices in the network, production, and lab environments.
- CIMRaN is used immediately following an incident to provide a call impact report that identifies calls, callback numbers, PSAPs, state carriers and associated CDRs in a report that can be distributed to the customer. This report is generated within minutes following an incident.

Netscout is used for network troubleshooting and analysis.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 13	**NOC/SOC – Network Management System** **NMIS Interworking with Elements and Services** Provide a detailed explanation and associated drawings explaining how the proposed solution interworks with all of the various elements and services of the proposed systems and network elements.	X			
	Bidder Response: Intrado's cyber security policies, standards, and guidelines are compliant with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology (COBIT). Intrado's next generation emergency services network is a secured and private IP managed network. All inbound and outbound traffic is through well-defined and controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. Intrado employs a defense-in-depth security strategy to protect sensitive information. Such controls include, but are not limited to stateful packet inspection firewalls (host and network based), IDS/IPS, ACLs, Role-based Access control, two-factor authentication, encryption, and AV (email and host). Furthermore, systems are protected with build standards, patch management, and regular vulnerability scans. Sensitive data is housed in our data centers with logical and physical access controls. Development environments are separate from production and production data is not used in dev or SQA. Data transits untrusted networks (leaves Intrado custody) through applications or communication channels with encryption to safeguard confidentiality and integrity. The A9-1-1 infrastructure, illustrated in the figure below, is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. Intrado employs high availability systems with redundancy at geographical, carrier, circuit, power, application, and system levels. System/application availability is safeguarded with clustering and load balancing techniques. Furthermore, A9-1-1's security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, both ingress and egress.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

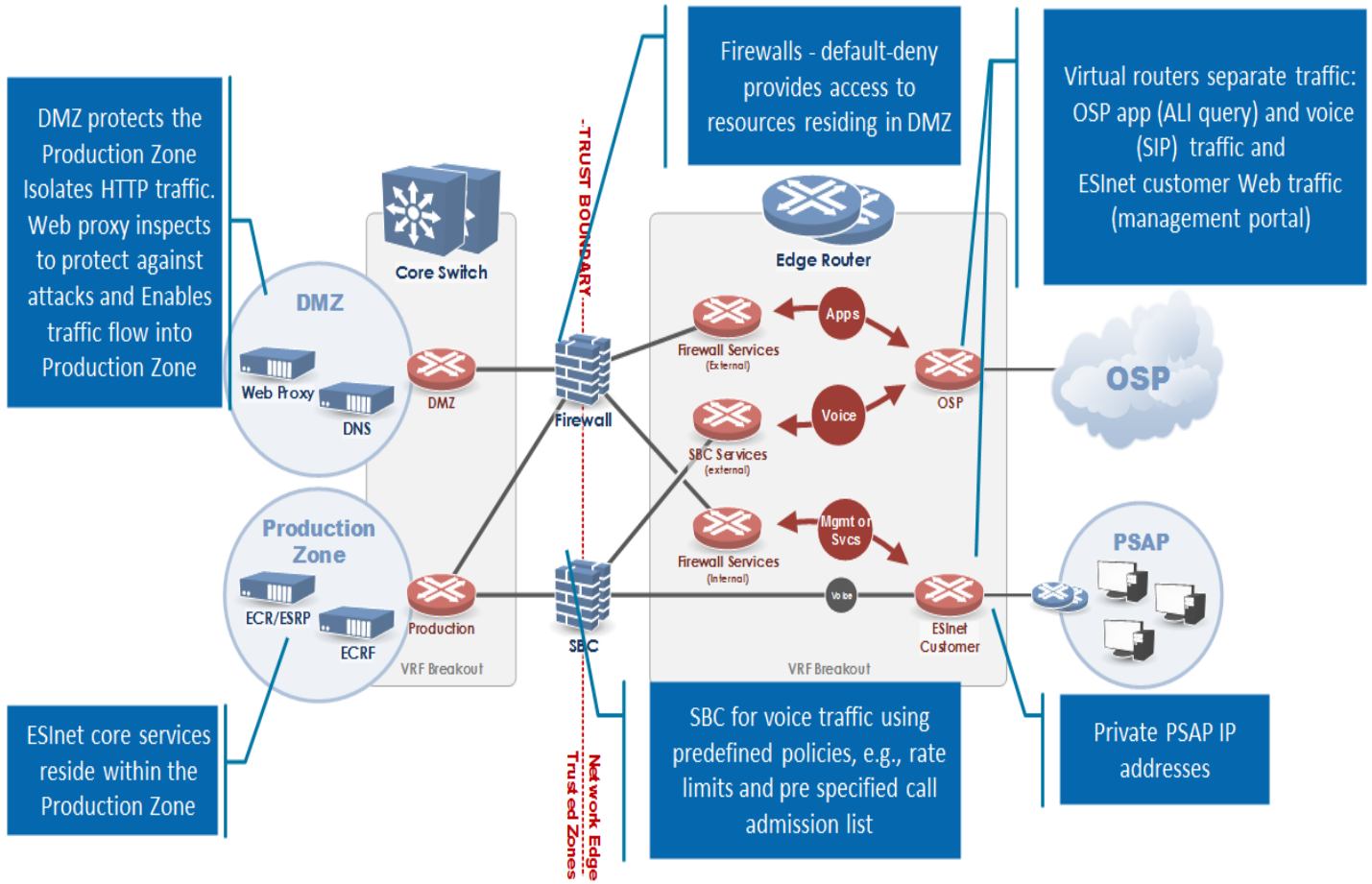

Figure 8: Defense in-depth Security Architecture

The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or Access Control Lists

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	(ACLs). Intrado continually investigates and upgrades with new advances in protective technology with tools such as Intrusion Detection System (IDS). The solution incorporates physical, network, and application security principals. Traffic between Core processing sites and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) is route- and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution. Intrado's A9-1-1 deploys firewalls and other network security devices and software to protect against inbound network threats on the servers that make up the proposed ESInet. The NOC also employs a regularly scheduled patching process to protect against the effects of malware. Computing devices are subjected to thorough security scans so that there are no malware elements present. Access to processing elements is restricted to authorized personnel. Network connections from solution components are limited to those connections needed for operation and maintenance. Physical and network access to production components is restricted to those that have an operational responsibility, and all activity is audited and monitored. All development environments are fully separate from production environments. All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 14	**NOC/SOC - Network Event Logging** **System and Network Event Logging and Reporting** The network management system shall capture real-time and historical tracking of network and system events, as well as event resolution of the IP network and attached systems. This is for logging errors and statistical information related to the health of the network and attached systems. Events shall include, but are not limited to, hardware (power, processor, interface cards, ports), software (operating system errors, database errors, application errors and failures), network (Quality of Service (QoS), Mean Opinion Score (MOS), jitter, latency, and packet loss)). The events recorded in this section are not related to the event logging of 911 requests for service as part of NGCS Option B requirement NGCS 13 Event Logging. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: A9-1-1 utilizes many mechanisms for event tracking and alerting. Systems leverage syslog and SNMP traps for event / fault notifications. Application hosts also utilize embedded agents which communicate directly with our monitoring platforms. Systems are also monitored by use of SNMP polling and application health checks. All systems are provisioned for fault, performance, and configuration monitoring/management. Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause intervention if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites uses IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the best IP path for IP packet transport. The A9-1-1 solution achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. All functions necessary for call processing are deployed in a highly available configuration and duplicated across Core sites and LNGs. Transactions or call traffic divert to available components on failure or degradation of Service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NOC/ SOC 15	**NOC/SOC - Network Event Logging Management System Interface to Incident Management System** This system should be part of, or interfaced with, the bidder's incident management system, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract and provide copies of the data to the Commission on request, and at the end of the contract. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado has integrated e-Bonding ticketing exchange with its partners for automatic logging and notification of system events. Historical trouble ticket information is retained for six months duration after the ticket is closed at which point it is transferred to archive. Intrado agrees to provide copies of the data to the Commission on request, and at the end of the contract.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NOC/ SOC 16	**NOC/SOC - Network Event Logging Interfacing Between Solutions** Provide a detailed explanation and associated drawings explaining bidder's processes, tools, and procedures for interfacing with the bidder's monitoring solutions.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The A9-1-1 NOC/SOC uses multiple tools and techniques to track performance and fault management activities. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to HP OpenView, which is used to present a single pane of glass to the A9-1-1 NOC. OpenView utilizes the HP Operations Manager (OM) module, which monitors systems and applications using agents and provides SNMP trap and syslog receiver capabilities, and the HP Network Node Manager (NNMi) network monitoring software module based on SNMP. Visual alerts are available 24x7x365 to the 9-1-1 NOC. These systems also provide ICMP and SNMP trending and threshold alarming.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

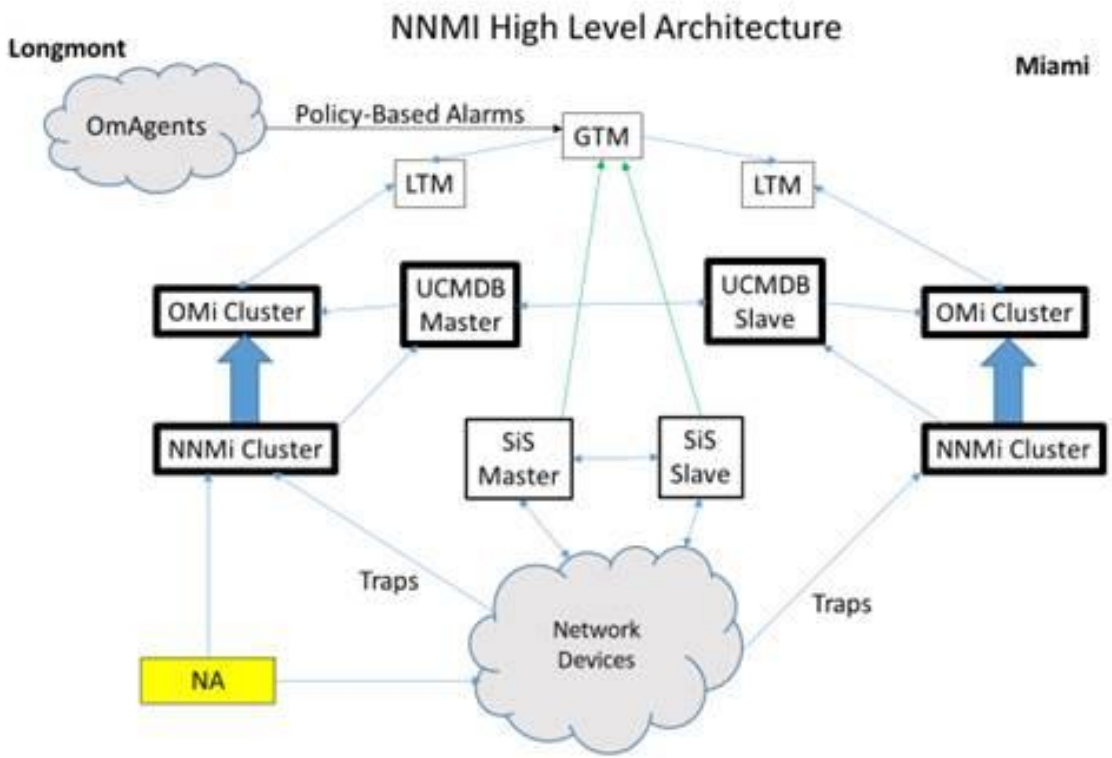

Figure 9: A9-1-1 Network Monitoring

The A9-1-1 NOC uses e-Bonding as the mechanism for communicating alarms and reports.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NOC/ SOC 17	**NOC/SOC - Access to Technical Staff** 1. Detail the procedures by which bidder communicates with technical personnel from participating subcontractors, the Commission, and the participating PSAPs. 2. Specify the level of assistance required from such technical personnel to resolve service-related issues.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: **1.** Intrado will communicate with technical personnel from any participating suppliers, the State of Nebraska, and PSAPs through phone calls and ticketing system applications. A dedicated toll-free number is available for the State, PSAPs, and participating suppliers to utilize for reporting and obtaining/providing status on A9-1-1 ESInet issues. Intrado provides a web-based ticketing system for use by our customers as well and a ticketing interface tool between Intrado and our participating suppliers. **2.** The level of assistance required from technical personnel specified above to resolve service-related issues is expected to be minimal.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 18	**NOC/SOC - Notification** Specify how the bidder's NOC informs the Commission and the affected PSAPs or their designees of problems with the network, scheduled service and maintenance outages, and upgrades. Include all methods of notification used. Notifications for scheduled maintenance or outages shall be made no less than ten (10) business days in advance, except for emergency situations in which case, notification will be given immediately. Tickets related to the services delivered to subcontractors shall be forwarded automatically. Notification shall be provided via multiple communications means to the Commission and applicable PSAPs. Entities requiring notification may change, depending on the alarm or incident. Provide a detailed explanation explaining how the solution meets or exceeds the above requirements, including the methods of communications used.	X			
	The Intrado team will conduct major and minor planned and critical un-planned events for all NG9-1-1 services, system maintenance, or upgrades that may impact the NG9-1-1 Customer PSAPs. Intrado fully manages and completes these events with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado includes the required back-out time within the scheduled maintenance time frame. As described above, Intrado will schedule all typical maintenance and upgrades no less than ten business days out, unless the event is deemed critical. Intrado has the ability to e-Bond tickets to allow for automatic forwarding and tracking of updates. All events would be sent on the weekly event tracker that Intrado sends out. Communication on any emergency or incident work would be sent out by the Intrado NOC or Incident team and regular updates would be sent out via GroupCast notifications.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 19	**NOC/SOC - Executive Dashboard** Contractor shall provide a web-based executive dashboard or similar tool, providing near real-time visibility of network status displayed geographically with service impact levels color-coded. Open ticket status shall be available to users through this dashboard. Describe how the solution meets or exceeds the above requirement.	X			

Bidder Response:

Intrado provides an executive dashboard, available through the Intrado portal, which allows for a PSAP-specific display of network availability based on PSAP specific ESInet IP connectivity status. This status is displayed in a color-coded format which allows for an easy and immediate understanding of the PSAPs current available network. Additionally, each PSAP profile displays a geographic representation of the PSAP 9-1-1 authoritative boundary.

As part of the data gathering and implementation phase of the project, Intrado will work with the PSAP on configurable display attributes and preferences on design layout.

Access to the Intrado customer ticketing system is also available through this portal.

The Intrado Customer Management Portal (CMP) provides participating PSAPs and approved personnel 24x7x365 access to real-time KPIs including call detail records for voice, MSRP and RTT calls, detailed call traces, PSAP trunk utilization, health (activity) of call processing resources, route lists, policies, and PSAP operational status through a secure, web-based portal. Call detail records and the call trace provide the user with all of the pertinent information for each call.

The CMP allows user profiles to be set up for both local (for a single PSAP) and regional (multiple PSAPs under the same jurisdictional authority) views for multi-jurisdictional coordination. CMP uses dual factor authentication to keep sensitive data secure and only accessible by authorized resources.

Example information that the CMP provides includes:

- Operation State of PSAP(s)
  - Current status
  - History of changes in status including who made the change and when
  - Resource Counts (available TDM trunks or IP Contacts)
  - Operation State color-coded with indications for In Service/Out of Service
- PSAP Route Lists: Primary, Alternative, Abandonment, Backup
- Fixed Transfer/Bridge List for Legacy PSAPs

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Statewide PSAP Directory Call Detail Records provide PSAPs information including alternately routed calls, i3 to ESN fallback, and transferred/conferenced calls.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 20	**NOC/SOC - Escalation Procedures** 1. Outline a detailed regional-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. 2. Describe how discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed. These procedures shall be maintained and accessible via an online portal. This escalation notification process shall be integrated with the notification processes described above, based on the problem reported.	X			

Bidder Response:

1. The first step in the escalation process is always handled through the A9-1-1 Network Operations Center (NOC) and can be initiated at any time by requesting a NOC Supervisor. The NOC is staffed 7x24x/365 and a supervisor is always available to escalate an incident if necessary. Listed below are the current A9-1-1 escalation procedures.

Table 5: Escalation Procedures

Escalation Intervals	Level	Responsibility
First Escalation SEV 1 - 2 Hours SEV 2 – 4 Hours SEV 3 – 6 Hours	NOC Manager	Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center
Second Escalation Customer Discretion	Area Manager or Delegate	Review status of ticket Monitor ticket progress Notify Director - when appropriate
Third Escalation Customer Discretion	Director	Status Customer Escalate as needed to partner centers Monitor ticket progress/ documentation Notify VP when appropriate
Fourth Escalation	Vice President	Ensure adequate resources are available and engaged for prompt resolution Update customer as appropriate Escalate as needed to appropriate levels

When escalating a problem, it is important to provide the following information:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Customer's name and telephone number • Active ticket number(s) • Trouble Location • Trouble description (e.g., out of service, service degraded, etc.) • The action or resolution requested **2**. In the event an issue requires further attention, a full list of available team members and chain of command will be provided. A dedicated Program Manager will be assigned and, in the event an escalation is required, can be contacted if proper attention is not assigned in accordance with agreed upon severity levels. The Program Manager can assist through the process and ensure the proper personnel are contacted. The Program Manager will be the primary contact for SLA disputes and, as needed, will go through the same chain of command for review within Intrado.

Any additional documentation can be inserted here:

NOC/ SOC 21	**NOC/SOC -Statement on Standards for Attestation Engagement Number 16** Bidder shall demonstrate compliance with the Statement on Standards for Attestation Engagements Number 16 (SSAE 16). The applicable report from an SSAE 16 engagement is the Service Organization Controls 1 (SOC 1) report. 1. If bidder is proposing services, provide a detailed explanation of how bidder has complied with SSAE 16 for similar solutions, and how this would be implemented with the Commission's NG911 implementation. 2. Provide with the detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
				X	
	Bidder Response: Intrado has not performed a SOC 1 review. Intrado will comply with the Statement on Standards for Attestation Engagements Number 16 and provide SOC 1 reports (see *Proprietary Information* file.). Once the review and report are completed, we will immediately remedy any gaps identified and provide a detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 22	**NOC / SOC - Configuration Backup and Restoration** 1. The bidder shall deploy and provide detailed descriptions of bidder and any subcontractors' capabilities to automatically or routinely back up configuration data and define the conditions under which the configuration of network elements, such as routers or switches, will be restored, and the process that will be used. A reporting process shall confirm regularly scheduled (e.g., monthly, quarterly) backup and restoration, and provide sufficient details on backup and restoration activity. 2. Describe the bidder's abilities to perform on-demand backups, such as at the end of a successful configuration change. A reporting process shall confirm on-demand backup and restoration and provide sufficient details on backup and restoration activity. 3. Describe bidder's COOP as it applies to the NGCS and delivery of 911 traffic via IP network to the respective host locations. 4. Provide a detailed explanation and any associated drawings explaining how the proposed processes and procedures provide the ability to manage these configuration backup and restoration processes in a manner that has no negative impact on the total Commission ESInet and NGCS solution.	X			
	Bidder Response: **1.** A9-1-1 network configuration tools provide version control and "rollback" functionality to all network elements, with backups of all network configuration performed daily. This allows the restoration of previously "known good" configurations or timely restoration of stored configurations in the event of equipment failure or disaster recovery. Using the above process, our network configuration management tools perform the following functions: • Detect and report on configuration policy violations or configuration backup failures to ensure compliance with corporate standards. • Use configuration and command templates, custom scripts, and configuration changes to provide consistent implementation of network configurations across similar site types. • Simultaneously modify configurations, change community strings, update ACLs, and block MAC addresses across many devices. • Compare start-up and running configuration files to troubleshoot device configurations issues. • Automatically check all network elements for changes and perform backup for all changed network device configurations on a daily or ad hoc basis, as needed.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado can provide reports confirming regularly scheduled daily backup and restoration files archived and provide additional details on backup and restoration activity as required. Intrado can provide copies of all data upon request. **2.** Intrado can provide reports confirming on-demand backup and restoration files archived and provide additional details on backup and restoration activity as required. Intrado can provide copies of all data upon request. **3.** Intrado provides life-critical services supporting 9-1-1 and public safety and is strongly committed to continuous, sustained readiness of its applications, systems, networks, and processes 24x7x365. Intrado's business and service continuity plans, geographically diverse and redundant systems, and incident management processes and plans provide confidence that continuous operations will be sustained through planned or unplanned events. <u>Service Continuity Planning Steps</u> *1. Risk Assessment* Intrado business and service continuity risk assessment addresses naturally occurring and facility affecting events, as well as system interruptions. Processes in place address interactive management of events designed to support continuous functioning of 9-1-1 systems and enable personnel to continue to perform through specific incident conditions. *2. Service Continuity Strategy* Intrado is strongly committed to providing essential business processes, systems, and networks on a 24x7x365 basis and is well prepared for possible disruptions and disasters. As a critical public safety service provider, Intrado has in place a robust business and service continuity program designed to prevent or mitigate service disruptions and support rapid response to loss or impairment of crucial business functions or infrastructure. To address potential risks, Intrado utilizes: • Redundant, Geographically Diverse Systems – The A9-1-1 architecture is located in geographically diverse and redundant data centers in Longmont, Colorado and Miami, Florida. • Incident Management – In the event of an unplanned outage, or intermittent outage of a system, network component, or application that has the potential to cause an adverse impact to production services, Intrado immediately engages the Incident Command System, which is based on the FEMA Incident Command Structure. The incident team, led by a qualified incident commander and supported by technical and operations resources, evaluates the information received, determines the problem statement, categorizes the problem severity level, and manages/works the incident until the incident objectives are met.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Business and Service Continuity, Disaster Recovery, and Emergency Procedures – Intrado has established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to our facilities or systems, including:
  - Building emergency procedures (e.g. bomb threat, earthquake, power failure, and flood
  - Data center risks (e.g. water, flood, power, electrical, and fire)
  - Security Risks (e.g., information and network security, physical security)
  - Building evacuations
  - Pandemic
  - Inclement weather
  - Building disasters

3. Implementing Risk Reduction and Recovery Measures

Intrado's essential processes, systems, and networks supporting 9-1-1 traffic are designed and deployed to accommodate possible disruptions and disasters to any given element or data center and support 24x7x365 continuous operation. In the event of unplanned system or network outages, this diversity allows for Intrado 9-1-1 systems to continue operating while Incident Management processes are engaged to identify and resolve issues so that redundancy is fully restored.

4. Developing Plans and Procedures

Continuity plans cover critical application and infrastructure components. At least one copy of the continuity plans is maintained offsite in secure storage, available 24x7. Key personnel possess encrypted electronic copies of business continuity information, updated regularly. Intrado conducts reviews and updates of continuity data and plans at least annually. Certain continuity plan functions are exercised on an on-going basis, such as Incident Management, which is utilized for all planned and unplanned events.

Intrado is well prepared and practiced for contingencies and has communications protocols and processes in place to notify personnel, customers, vendors, suppliers, and regulatory bodies in support of our applications, systems, and network components. Continuity plan materials include:

- Essential functions and personnel

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Employee emergency contact information • Building emergency procedures • Contractor/Vendor contact procedures • Crisis communication plans • Specific scenario response procedures • Customer contact and notification • Life mission critical system recovery processes *Testing Service Continuity Plan* Intrado implements and tests its Incident Management Plan on a regular basis and conducts audits and reviews and/or walk through exercises of its continuity plans at least annually. Information gathered feeds into a continuous improvement cycle as part of the maintenance and review process. *Service Continuity Plan Maintenance* Intrado conducts a maintenance review of its continuity plans at least annually. In this review, which is coordinated by the overall plan owner, the interdependent plan owners identify, validate, implement, and document changes to the plan components. **4.** Network configuration management tools automatically check all network elements for changes and perform backup for all changed network device configurations on a daily basis and may be performed on-demand, as needed. Network configuration management tools have been implemented with geo-diversity in place.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NOC/ SOC 23	**NOC/SOC - Third-Party Management** The Commission is seeking the optimum value provided by best-of-class products and services integrated as part of the total IP network solution. This may present a situation where no single manufacturer or supplier can provide a public safety-grade, unified NOC/SOC accountable for all components, products, and services that comprise the Commission's total IP network solution. Consequently, the Commission may find it beneficial to have a third party provide that overarching NOC/SOC service. A third-party NOC/SOC provider may be responsible for functioning as an umbrella for monitoring all of the Contractor's products and services, including collaboration with the Contractor's NOC/SOC. To facilitate that capability, the third-party NOC/SOC shall have a view into all elements that are under SLAs. Bidder's NOC/SOC NMIS and/or incident-tracking tools shall have the ability to perform eBonding, which enables bidirectional data synchronization. 2. Provide a detailed narrative discussing bidders experience in providing access to third-party NOC/SOC, overarching support as well as for each of the requirements in Third-Party NOC/SOC Support below.				
	Bidder Response: Intrado has many available options for interconnectivity and interoperability between Intrado and third-party systems. Intrado has been subcontracting for multiple telecommunication companies over past 25 years, so many technical and communication processes and procedures are already established with existing partners and third-party providers. Change management, ticket management, e-Bonding, SNMP data, and shared portals are all solutions that have been deployed in the past to support external NOC/SOCs, and Intrado looks forward to defining and establishing requirements and solutions to support this future service. Understanding that formal requirements have not been requested – including connectivity requirements, interoperability specifications, and SLAs, Intrado does not currently have the data required to fully estimate resource needs. If and when the State of Nebraska decides to move forward with this requirement, Intrado will take a very active role to identify, support and deploy the required services.				

1. In support of the Commission's consideration of such an option, bidder shall indicate the compliance level of experience in providing access to third-party NOC/SOC overarching support, as related to the requirements identified in the table below.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Change management processes	X			
Coordinating and managing trouble tickets to resolution from bidder and multiple suppliers.	X			

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly).	X			
Notification processes for bidder and suppliers, and any other entities or people designated by the Commission.	X			
System alarm access in the form of SNMP or syslog data.	X			
Experience and processes for interworking of multiple public safety data system suppliers.	X			

Any additional documentation can be inserted here:

SLA 1	**General Operations - Service Level Agreements** **System Capacities and Performance** 1. Provide capacity levels of each element of the IP Network This may be in terms of busy-hour calls, network bandwidth, or any other applicable measure. The proposed solution shall be capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. 2. Specify lead times required to increase capacities on each element of the IP network.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: **1.** Each A9-1-1 location is deployed with a minimum of two 100MB IP Network connections, each of which is capable of providing adequate bandwidth for the traffic of the entire location in the event of redundant path failure. IP Network bandwidth is continuously monitored for these links and will be augmented when a link reaches a sustained threshold in excess of 60% of utilization. In the case of Legacy Network Gateway aggregation sites, the ingress DS0 quantity is also tracked and factored into augmentation plans. Each connection is designed to handle 100% of traffic between the ingress aggregation sites and the call processing data centers should one link become compromised. The proposed solution is capable of handling current and planned IP traffic. The solution can be easily augmented to support 50 percent capacity growth over the term of the contract. **2.** All network connectivity is provided on Gigabit Ethernet links with sub-rated ports provisioned. This deployment methodology provides for a quicker turnaround of bandwidth increases and allows Intrado to augment bandwidth with lead times far quicker than the typical time of 60-90 days.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 2	**Service Level Agreements - System Performance** **Network Latency** Specify the guaranteed maximum latency across the backbone network under a full-load condition, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			
	Bidder Response: A9-1-1 network latency is a monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less between the core processing sites and the PSAP end points under full load conditions. Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause intervention if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites uses IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the optimal IP path for IP packet transport. Network performance reports will be available through the A9-1-1 Customer Management Portal.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 3	**Service Level Agreements - System Performance** **Point of Presence (POP) to POP** Specify the guaranteed maximum latency from interconnection facility to interconnection facility, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			
	Bidder Response: A9-1-1 POP-to-POP network latency is a monthly average roundtrip transmission of fifty (50) milliseconds or less. Packet loss, latency, and jitter are measured at each ingress and egress point of presence. Predicted MOS thresholds are established to alert and cause remediation if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites uses IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the best IP path for IP packet transport.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 4	**Service Level Agreements - System Performance** **POP to Endpoints** Specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			
	Bidder Response: A9-1-1 network latency is a monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less between the core call processing sites and the PSAP end points. Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause remediation if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites use IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the optimal IP path for IP packet transport. Network performance reports will be available through the A9-1-1 Customer Management Portal.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 5	**Service Level Agreements - System Performance** **Mean Opinion Score (MOS)** Bidder shall guarantee, in the response, a consistent MOS of 4.0 or better across all network links transporting media streams from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Edge routers in the A9-1-1 network continually test quality from the edge of the network to the core call processing sites by sending a stream of synthetic RTP packets across the tunnels that traverse the MPLS networks. This is done with the Cisco IPSLA tool set. This testing is controlled by the remote site routers; all testing is generated by these routers towards routers at the core sites, which then change the sequence number and timestamp on each synthetic RTP packet and is then retransmitted back to the remote site router. This generates a 4-second long stream of RTP towards the mGRE interface on a core edge router, using the same codec used for the voice application. 100 packets are sent with an interval of 40ms. The test restarts after five seconds (each test is padded with an extra second to avoid overlapping tests). The test results are quite detailed; results for RTT, unidirectional latency, jitter, and packet loss are all generated. The IPSLA engine then derives both Impairment Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values from these results. Additionally, Intrado actively monitors the network's quality using the industry standard Mean Opinion Score (MOS) that automatically alarms on the router if the MOS score dips below a specific value. When this occurs, the router will automatically shut down the route that is having an issue and route all traffic over the redundant IP path. Major alarm notifications regarding the MOS score issue are paged out to the Network Engineering 24x7 on call staff. MOS reports will be available to the PSAP via the Customer Management Portal.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 6	**Service Level Agreements - System Performance** **Packet Loss** Specify the guaranteed maximum end-to-end packet loss across the network. This specification also shall include any loss characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: Intrado engineers its ESInets to keep the packet loss budget under 2.5 percent. Our ESInets are also designed without oversubscription. Packet loss of less than 1 percent should be achievable. Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause remediation if they are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites uses IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the best IP path for IP packet transport. Packet loss reports will be available to the PSAP via the Customer Management Portal.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 7	**Service Level Agreements - System Performance** **Network Latency** Specify the guaranteed maximum end-to-end network latency across the network. This specification also shall include any latency associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: A9-1-1 network latency is a monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less between the core call processing sites and the PSAP end points under full load conditions. All carriers used to provide transport services for the solution will be required to meet this minimum requirement in order to be utilized. Packet loss, latency, and jitter are measured at each core site. Predicted MOS thresholds are established to alert and cause remediation if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites use IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the optimal IP path for IP packet transport. Network performance reports will be available through the A9-1-1 Customer Management Portal.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 8	**Service Level Agreements - System Performance** **Jitter** Specify the guaranteed maximum end-to-end jitter across the network. This specification also shall include any jitter characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: Jitter shall not exceed twenty (20) milliseconds. A9-1-1 currently uses a 40 ms jitter buffer for all voice calls. This means that all voice packets have been treated such that minimal end point jitter buffering would be needed (typically much less than 20 ms). Packet loss, latency, and jitter are measured at each core site. Thresholds are established to alert and cause remediation if thresholds are exceeded. IP packet characteristics are used to establish production acceptance criteria and are available for trouble shooting problems. In addition, the dual transport paths between any two sites uses IP packet characteristics via Cisco's IP Service Level Agreements (IPSLA) functionality to determine the best IP path for IP packet transport. Jitter reports will be available via the Customer Management Portal.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 9	**Service Level Agreements - System Performance** **Network Traffic Convergence** Specify convergence protocols and the estimated or guaranteed network convergence time (less than 54 ms) of IP traffic at any point within the proposed solution, including how convergence information will be gathered, calculated, and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: Technologies such as MPLS fast-reroute are used to re-converge within 54ms upon detection of end-to-end circuit failures at the physical layer (optical/electrical). Fast-Reroute, along with similar rapid-convergence technologies, are used throughout the Intrado solution to ensure the network converges within the timelines specified. Understanding that Fast-Reroute is a network configuration, this functionality will not vary. If issues occur, the Intrado Network Team captures logs and run calculations on a case-by-case basis. Monthly reports can be provided to the Commission and/or PSAPs.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 10	**Service Level Agreements - System Performance** **Mean Time to Repair (MTTR)** Specify the MTTR characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTTR information will be gathered, calculated and provided to the Commission and affected PSAPs.	X			

Bidder Response:

The MTTR characteristics are listed in the table below, where the following abbreviations are used:

- Life and Mission Critical Services (LCMS)
- Business Critical Services (BCS)
- Business Essential Services (BES)
- Business Support Services (BSS)
- Unsupported Business Services (UBS)

Table 6: MTBF and MTTR

Service Class	MTBF (Service)	MTTR (Service)
LMCS	>5 years	<2 minutes
BCS	>1 year	<4 hours
BES	>3 months	<40 hours
BSS	>1month	<3 days
UBS	Unspecified	Unspecified

MTTR information is gathered as part of the process for responding to Severity Level 1, 2, 3 and 4 incidents. The time to repair would be based upon the time from the beginning of the incident ("beginning" of the incident should be the "point of detection/discovery" as defined by the FCC) to the time in which the service became functional again. Reporting is provided on a monthly basis and can be delivered electronically.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 11	**Service Level Agreements - System Performance** **Mean Time Between Failures (MTBF)** Specify the MTBF characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTBF information will be gathered, calculated and provided to the Commission and affected PSAPs.	X			

Bidder Response:

MTBF characteristics are commensurate with the appropriate level of service at which the system is functioning i.e., systems in the call path are Life and Mission Critical Services (LCMS) while peripheral systems are considered Business Critical Services (BCS). The MTBF characteristics are listed in the table below, where the following abbreviations are used:

- Life and Mission Critical Services (LCMS)
- Business Critical Services (BCS)
- Business Essential Services (BES)
- Business Support Services (BSS)
- Unsupported Business Services (UBS)

Table 7: MTBF and MTTR

Service Class	MTBF (Service)	MTTR (Service)
LMCS	>5 years	<2 minutes
BCS	>1 year	<4 hours
BES	>3 months	<40 hours
BSS	>1month	<3 days
UBS	Unspecified	Unspecified

Based on our public safety experience, Intrado has found that measuring Service Availability from a call processing perspective is more applicable and relevant to 9-1-1 service vs. traditional methods of calculating availability thru MTBF and MTTR measures.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado believes that the most relevant measure of service availability is evidenced by uninterrupted, reliable 9-1-1 call routing and delivery to the PSAPs. A9-1-1 availability is calculated from the time an outage begins that impacts call processing ability, until such time that the A9-1-1 call processing ability is restored. This includes all A9-1-1 downtime for the end-to-end service. This report will be made available on a monthly basis to the State of Nebraska. Maintenance of and upgrades to the A9-1-1 solution are done with no scheduled downtime. We schedule planned events for routine maintenance in ways that 9-1-1 operations are not impacted. A notification of the upcoming event will be sent to the customer as applicable. Planned events are fully staffed and managed with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. The Intrado team will conduct major and minor planned and critical un-planned events for all NG9-1-1 Services, system maintenance, or upgrades that may impact the NG9-1-1 Customer PSAPs. Intrado fully manages and completes these events with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado includes the required back-out time within the scheduled maintenance time frame. Standard 9-1-1 availability as described in this response will be supported for all services offered in the A9-1-1 solution. A9-1-1 is engineered for 99.999 availability. Intrado would like to point out that availability for the network is valid for diverse and redundant connectivity into the PSAP or third-party providers network. Any connectivity provided outside of the diverse/redundant connectivity provided by Intrado is not guaranteed.

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 12	**Service Level Agreements - System Performance** **Network Reliability** Network reliability is defined as the ability for system end-points to effectively communicate with each other, and all associated data and information is exchanged in usable formats. An IP-based network looks at reliability as an overall redundancy design, rather than component by component. Specify in the response the overall reliability service level of the IP network, including all bidder-provided components and facilities.	X			
	A9-1-1 achieves 99.999% service reliability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. Each i3 element has multiple instances within a single core to provide redundancy for that core. The same redundant configuration is replicated at each of the geo-diverse core sites. The Aggregation sites use the same design approach of redundancy within each individual site mirrored at the other sites. All vital system components are protected through the use of redundant modules to eliminate any single point of failure. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability. A9-1-1 components are designed and configured for continuous operation. Core sites include redundant network transport and redundant network interfacing elements to ensure optimal operation and availability. Network interfacing elements include switches, routers, SBCs, firewalls, and other security devices. All network routing infrastructure is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology. The A9-1-1 network implements a design of redundancy upon redundancy. Individual processing elements are redundant at each Core Site and Core Sites are redundant to each other. The failure of any given component at a Core Site will not prevent that Core Site from processing 9-1-1 calls. If a dual failure does occur at a Core Site, or a Core Site somehow becomes unavailable, calls are processed at another Core Site. Any Core Site can process any 9-1-1 call. The Core Sites are geographically distributed across the United States and a regional disaster will not remove the ability for A9-1-1 to process 9-1-1 calls, assuming telecommunication transport services for the impacted region are operable.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 13	**Service Level Agreements - System Performance** **Network Availability** 1. Specify the service level offered as a percentage of time when the service is available, and the maximum period of total outage before remedies are activated. Availability is defined as MTBF/(MTBF+MTTR). 2. Include how system availability information will be gathered, calculated and provided to the Commission and affected PSAPs.	X			
	Bidder Response: **1.** The A9-1-1 network Service availability is 99.999% The A9-1-1 network starts with the ingress point of interface and ends with the Intrado router at the location that houses the PSAP's CHE. **2.** A9-1-1 availability is calculated from the time the outage begins that impacts call delivery, until such time that call delivery ability is restored. This includes all Intrado A9-1-1 downtime for the end-to-end service. Availability reports will be available via the Customer Management Portal.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 14	**Service Level Agreements - System Performance** **End-of-Support Equipment** Contractor shall proactively replace, at Contractor's expense, any hardware that has reached end of support (EOS) no later than 90 calendar days prior to the manufacturer's EOS date. All equipment must be new and of current manufacture, not refurbished. Describe your procedures for End-of-Support Equipment.	X			
	Bidder Response: Components within the Intrado A9-1-1 solution are periodically renewed to enable PSAPs to operate on the most modern communications technology during the life of the contract. Intrado maintains and monitors all equipment and software within the solution, and it is Intrado's commitment to replace End of Support (EOS) equipment prior to the EOS published date by the vendor. Intrado will replace any faulty equipment at no additional cost to the jurisdiction that is not a direct result of negligence of on-site PSAP personnel. All equipment is new and of current manufacture; refurbished equipment is not used.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 15	**Service Level Agreements –** **SLAs for Incident Management** The Commission requires the Contractor to establish processes and procedures for supporting a NOC/SOC that can rapidly triage and manage reported network incidents. Bidder shall develop an ITIL compliant severity-level scale that includes levels one through four, with level one being the most severe incident. The top two levels shall capture all incidents affecting the level of service of one or more end-points. Include a description of incident severity-level attributes, including response and resolution times for each severity level, and how response and resolution times are measured.	X			

Bidder Response:

Intrado uses industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework, and our severity scale is compliant with the ITIL processes and standards. The response/resolution times below are initiated (measured) from the point of Discovery. Discovery occurs when Intrado is notified about the specific Incident. This could occur through automated means such as alarms, or through external means such as customer/third party notification.

Table 3: Intrado Severity Levels

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 16	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Outage Summary and Lessons Learned** Provide a summary of FCC reportable outage situations that interrupted 911 service to bidder's clients over the past three years, where 911 calls were not delivered or not delivered to the appropriate PSAP as a result of the issue. The response shall include the deployment type (legacy, ESInet, and NGCS), month, year, duration, number of PSAPs or population impacted, number of PSAPs or population served by the impacted system, impacted system, and lessons learned from each outage. **Regulatory Compliance** Contractor shall comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract.	X			

Bidder Response:

Outage Summary and Lessons Learned

Intrado and the FCC entered into a three-year Consent Decree on November 4, 2019 to resolve the FCC's investigation into an August 1, 2018 outage in 911 service. *See* West Safety Communications Inc., Order, FCC DA 19-1063 (rel. November 4, 2019), available at: https://docs.fcc.gov/public/attachments/DA-19-1063A1.pdf. The Consent Decree requires Intrado to pay a penalty and comply with a variety of compliance and reporting terms. Intrado's compliance effort is ongoing under this Consent Decree, which expires on November 4, 2022. Deployment type (legacy, ESInet, and NGCS), month, year, duration, number of PSAPs or population impacted, number of PSAPs or population served by the impacted system, impacted system, and lessons learned are available at the link.

Regulatory Compliance

Intrado Life & Safety, Inc. will comply with all applicable rules and regulations throughout the term of the contract.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 17	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Outage Notification** Contractor shall notify the Commission and affected PSAPs within a maximum 30 minutes of discovering an event or outage that may impact 911 services. All events that meet criteria for local, state, or federal reporting shall also be completed by the Contractor. At the time of initial notification, the Contractor shall convey all available information that may be useful in mitigating the effects of the event or outage, as well as a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. The Contractor is responsible for coordinating data gathering, troubleshooting and reporting on behalf of subcontractors. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: In case of a service interruption and/or outage, Intrado has instituted Incident Management processes and procedures for dealing with various severity levels during the course of an event. Intrado's incident response tools include use of the Incident Command System (ICS). Intrado's ICS is modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post- event analysis. Intrado manages incidents and provides customers with up to the minute notification and status of ongoing service affecting issues that may impact the Intrado solution. Intrado personnel are trained in incident command by Emergency Management Institute, a FEMA sponsored Emergency Management Course. This course is a prerequisite to Incident Management training and part of the certification program. Each Incident Commander (IC) is certified prior to leading an Incident without supervision. Trainees must complete the mentoring program and have successfully managed mocked incidents along with supervised incidents. Incident Management is available 24x7x365. Intrado will notify the Commission and affected PSAP(s) within 30 minutes for all critical outages and would follow guidelines on communication timelines on lower severity incidents. Intrado will provide as much detail as possible during Incident communication, including a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. Intrado currently utilizes reporting functionality that details Incident Management and time on response upon detection and can be shared with the State for reporting on SLA requirements.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 18	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Status Updates** The Contractor shall communicate any updated status information to the Commission and affected PSAPs no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 911 service is restored. This information shall include the nature of the outage, the best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected operations. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The Intrado Incident team is well versed in this type of communication as it is already in place for our customers today. The Intrado NOC and Incident Management team currently utilize several methods including GroupCast communication to send out updates during outages. An update will be provided at a minimum every two hours with all the latest information that Intrado has, including best-known cause, scope, and ETA on restoration. Intrado sends updates as frequently as we have them and does not wait for the minimum frequency to provide updated information.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 19	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Reason For Outage (RFO) Reporting** Following the restoration of normal 911 service, Contractor shall provide a preliminary RFO report to the Commission and affected PSAPs no later than three (3) calendar days after discovering the outage. An in-depth RFO report, including a detailed root-cause analysis, shall be provided to the Commission and affected PSAPs no later than ten (10) calendar days after discovering an outage. 1. Describe how bidder will comply with the notification and reporting requirements above. 2. Describe the NOC/SOC tools and techniques at bidder's disposal to ensure that bidder's various subcontractor perform troubleshooting and post-event analysis and provide associated reports.	X			
	Bidder Response: **1.** Intrado has a Problem Management team that meets after each major outage to break down and review outages. Root cause is identified, and lessons learned outlined to minimize the probability of repeat occurrences. This information is shared with our partners and will be available for the State of Nebraska. A preliminary RFO will be provided within three days after discovering the outage, although information that early may be very limited due to resource constraints. A thorough RFO report would be provided within the 10-day timeline. Intrado pulls together senior leadership and resources from all applicable groups for Incident and Outage reviews and provides detailed written reports containing root cause analysis and actions items to address any shortcomings identified. **2.** Our technical teams use all available reporting tools and system monitoring during our review process to provide a second-by-second breakdown of what was seen in the network during an outage. The modules in Service Now, including Change, Incident, Problem Management, and Knowledge, provide our teams with insight into any planned changes and analyze any correlation between changes in the system and impacted service.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 20	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **PSAP Notifications** Outage notifications and follow-up analysis of outages are a critical element to understanding overall system health and preventing future service interruptions. Having awareness of issues that exist in a neighboring PSAP provides valuable insight into potential issues that may begin impacting another PSAP's operations. The Commission' is seeking an outage notification service that allows for each PSAP to elect the outage notification types and PSAPs for which it will receive outage notifications, outage updates and RFO reports. A web portal for authorized users to select/deselect outage notifications is required. Provide a detailed description of how bidder will support such an outage notification service.	X			
	Bidder Response: Intrado will have an online portal that Nebraska and all sites will be able to access and customize their notification preferences by selecting or deselecting which outages/programs for which they would like to receive communication. The online portal will be available for sites to access at their convenience and update their preferences as they may change.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 21	**Service Level Agreements –** **Media Contact** 1. Contractor shall provide a 24 x 7 spokesperson who will be available for media contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs. **Government & Regulatory Contact** 2. Contractor shall provide a 24 x 7 representative who will be available for government and regulatory contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs Describe bidder's experience in providing both a Media Contact and Government & Regulatory Contact for similar contracts.	X			
	Bidder Response: Intrado has extensive experience in government and regulatory policy related to 9-1-1 outage reporting and service delivery In addition to understanding all State and Federal policies and regulations that govern 9-1-1 outage reporting, the Intrado RGA organization is involved at the national level with the Federal Communications Commission (FCC), National Association of Regulatory Utility Commissioners (NARUC), and ATIS work group initiatives related to outages, outage rules and development of improved Best Practices that will aid in minimizing the risk of 9-1-1 outages. **Media Contact** Intrado's spokesperson information for media contact for outage of 9-1-1 services is located in the *Proprietary information* file. **Government & Regulatory Contact** The Intrado Government and Regulatory Affairs (RGA) team has dedicated staff that is available on a 24x7 basis to respond to regulatory and governmental needs when an unfortunate outage occurs. Intrado has maintained this dedicated staff for over 25 years. Intrado's Government and Regulatory contact information is located in the *Proprietary information* file.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 22	**Service Level Agreements –** **SLA Violations** An SLA violation shall have occurred whenever: A. The Contractor fails to meet any single performance level; or, B. The average of any single performance item over the preceding two-month period fails to meet the service level stated in response to requirements SLA 1 through SLA 22. Contractor shall deliver an SLA violations report to the Commission on a monthly basis. **SLA Reporting** Provide a detailed description of how bidder measures and reports incidents, including immediate notifications and regularly scheduled reports. SLA results shall be delivered to the Commission on the 10th business day of the month. The report shall include all performance items identified in the bidder's proposal and documented in contract negotiations.	X			
	Bidder Response: **SLA Violations** Intrado will work with the State on summarizing and reporting on the agreed upon SLAs. **SLA Reporting** Intrado supplies SLA reporting via our web-based reporting tool which provides real-time/near real-time data viewing. This report can be pulled in summary and delivered to Nebraska by the 10th business day of each month. A sample of the information available in these reports can be seen below.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Incident Management Report

Privileged and Confidential Attorney Client Communications - Do Not Copy or Distribute

Call Summary Click to [Hide]

Total Number of Calls for Live PSAPs (excludes Test Calls)	828
Number of Calls not delivered due to incident (Fast Busy or dead air)	**0 (0%)**
Number of Calls that were Abandoned	97 (11%)
Number of Calls with > 6 secs Call Setup Time (Not EWCR)	0 (0%)
enwdcoec ECMC - Total Number of Calls	415
enwdcoec ECMC - Number of Calls not delivered due to incident (Fast Busy or dead air)	**0 (0%)**
enwdcoec ECMC - Number of Calls that were Abandoned	47 (11%)
enwdcoec ECMC - Number of Calls with > 6 secs Call Setup Time (Not EWCR)	0 (0%)
miamflec ECMC - Total Number of Calls	413
miamflec ECMC - Number of Calls not delivered due to incident (Fast Busy or dead air)	**0 (0%)**
miamflec ECMC - Number of Calls that were Abandoned	50 (12%)
miamflec ECMC - Number of Calls with > 6 secs Call Setup Time (Not EWCR)	0 (0%)

Call Details

	enwdcoec	miamflec
Number of Calls that were Site Redirected	0	0
Number of Calls Successfully Site Redirected	0	0
Number of Calls Failing Site Redirection (possible dead air to caller)	**0 (0%)**	**0 (0%)**
Number of Failed Calls (possible dead air to caller; destination unknown - Notify All)	**0 (0%)**	**0 (0%)**
Number of Calls that failed in delivery to a PSAP	0	0
Number of Calls to a PSAP that failed but alternate routed successfully	0	0
Number of Calls to a PSAP that failed and caller heard Fast Busy	**0 (0%)**	**0 (0%)**
Number of Calls to a PSAP that encountered an error but delivered successfully	1	0
Number of Calls to a PSAP that were not delivered due to resource constraints (Traffic Busy)	0	0
Number of Calls that failed to be bridged	**0**	**0**
Number of Calls that encountered an error but bridged successfully	1	0

Figure 10: Incident Management Report

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 23	**Service Level Agreements –** **SLA Violation Financial Remedies** Contractor shall provide financial remedies to the Commission for each event in which service levels are not maintained. The Commission requires that all of the Contractor's network facilities, devices, and services will be measured on a rolling, 12-month calendar. Failure to meet SLAs shall be measured per service-affecting outage. Financial remedies shall be assessed for failure to meet SLAs. For service-affecting incidents, a 10 percent (10%) discount shall be accessed against the Monthly Recurring Charge (MRC) applicable to the source of the failure, whenever the initial period of resolution is exceeded. If the resolution period length of time doubles, then the discount shall increase to 20 percent of the MRC. If the resolution period length of time quadruples the initial period, then 50 percent of the MRC shall be assessed. The amount related to the damages is to be credited to the invoice for the month immediately following the violation. Bidder shall include how uptime information will be gathered, analyzed and provided to the Commission.	X			
	Bidder Response: Intrado will work with the State to provide appropriate service assurances in the forms of Service Level Agreements (SLAs). Intrado will utilize its internal metrics system for system performance and subtract out any outage times from the monthly total availability. Intrado will keep a rolling spreadsheet that will be provided to Nebraska that shows the cumulative availability statistics along with outage times for all previous months. All applicable outages will be clearly tallied with cumulative totals identifying if SLAs were met or missed. The ongoing monthly and yearly totals will be readily available for both parties to view as each month's new report is calculated and sent out.				

Any additional documentation can be inserted here

Operational Scenarios
Safeguards shall be established to minimize the impact of human or system error. Describe bidder's risk-mitigation and issue-resolution strategies for the following hypothetical scenarios:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 1	**Scenario 1** At 0300 hours, a series of SBC alarms previously unseen by the NOC staff on duty begin to increase in volume and frequency. At 0330, multiple critical alarms are received. At 0345, a few PSAPs start reporting garbled audio while others report an inability to obtain location information. At 0600, some PSAPs are reporting that they have not received a call in the last 15 minutes.	X			

Bidder Response:

This situation is managed as a Critical (Severity 1) incident, ensuring expedited resolution.

The steps taken follow.

- Review alarms for indication and correlation of customer specific or SBC events (0300).
- If SBC specific alarms indicate critical errors that necessitate rerouting of traffic manually, complete a High Availability (HA) redirection on the SBCs. This activity moves traffic away from potentially impacted interface.
- (0330) If critical alarms are SBC-related and continue after the switch over, evaluate if they are PSAP-specific or specific to one of the redundant SBCs per Core. If SBC-specific alarms are still persistent, move SBC experiencing issues completely out of path.
- (0345) Reports of garbled voice – The NGCS allows for voice to be evaluated post call. This capability would be utilized by the NOC engineer to evaluate both ingress and egress voice traffic to look for commonalities. If a common route is identified, the NOC engineer would remove route from service and notify customer and appropriate vendors.
- Evaluate the circuit connectivity, location information is completed by ALI lookup from ANI or held query over an I3 interface and indicates a potential local or common circuit issue in the PSAP area.
- (0600) Look for calls to the reported PSAPs. The NOC makes test calls from the application out to the PSAP to recreate the issue. If no calls are coming in this indicates the problem resides with ingress path; that would indicate the previously report issues are a separate issue. Next step would be identify/isolate circuit and busy out the trunks associated with that circuit. Report ingress 26 codes/IP Circuit ID to carrier for repair. Previous steps for 0330 – 0345 would identify the problem on the egress side.
- In each of these scenarios the NOC would be working directly with the customer ensuring open communications and joint troubleshooting is occurring.

*It should be noted that the alarms from 0300 may or may not be related to the garbled audio issue beginning at 0345.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Restoration and Resolution Timeframes

Intrado will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 8: Intrado Severity Levels

Root Cause Analysis Report

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Root Cause Analysis (RCA) report for Critical (Severity Level 1) or Major (Severity 2) service disruptions will be available following the resolution of a Critical (Severity 1) or Major (Severity 2) service disruption outlining the conditions that caused the trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

- Date/Time of the start of the service disruption.
- Date/Time of service restoration.
- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s).
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues)	Immediate	30 min-2 hrs	15 min

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria			
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 9: Intrado Severity Levels

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 2	**Scenario 2** All originating service providers in the state are connected directly via Signaling System Number 7 (SS7) protocol to the bidder's LNGs that serve the PSAPs in Nebraska, as well as others outside the Commission's footprint. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. One of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of the prior day's logs, it is found that the two surviving LNGs only are processing 2,000 calls each.	X			

Bidder Response:

This situation is managed as a Critical (Severity 1) incident, ensuring expedited resolution.

The technical resources will be working to restore the catastrophic failure – as well as working the possible redundant infrastructure issues. This response focuses on the immediate need to restore the OSPs traffic to full capacity. Those steps are listed below.

- If failure is at the LNG, investigate if OSPs are experiencing a route selection temporary failure. Work to identify and evaluate potential for OSPs not load sharing traffic between LNGs.
- Contact Ingress OSP providers to verify alternate route configuration is correctly provisioned
- Contract Ingress OSP providers to verify redundant circuit/bandwidth availability
- Complete Test calls with OSPs to verify proper failover and bandwidth
- Test and verify internal LNG network failover
- Investigate additional alternate paths for ingress into the infrastructure.

This incident would be initially designated as a Major (Severity 2) routing services are impaired issue, but upon review would change the classification to a Critical (Severity 1). Once the perceived call volume mismatch is detected Intrado will, until proven otherwise, assume that calls were/are being impacted by this outage.

Restoration and Resolution Timeframes

Initial Classification: Intrado will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Updated Classification: Intrado and its subcontractors will apply immediate and sustained effort, 7x24, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 10: Intrado Severity Levels

Root Cause Analysis Report

A Root Cause Analysis (RCA) for Critical (Severity 1) or Major (Severity 2) service disruptions will be available following the resolution of a Critical (Severity 1) or Major (Severity 2) service disruption outlining the conditions that caused the

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

- Date/Time of the start of the service disruption.
- Date/Time of service restoration.
- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s)
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues)	Immediate	30 min-2 hrs	15 min

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria			
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 11: Intrado Severity Levels

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 3	**Scenario 3** As part of normal data-maintenance procedures, the bidder has uploaded six minor recent changes. The bidder's Quality Assurance/Quality Integrity (QA/QI) process provides a discrepancy report detailing 15,000 errors resulting from the updated file.	X			
	Bidder Response: The Intrado Spatial Interface (SI) is built to deal with this exact scenario. GIS submissions will be provided via the SI. Intrado utilizes the Enterprise Geospatial Database Management System (EGDMS) to allow customers to both submit data and view reports. EGDMS will not provision GIS Data updates to production systems (ECRF/LVF) for any polygon layer if there is a critical error found. In other words, all polygon layer updates must be 100% error free to proceed to production. For polygon, road centerline and address points submissions, there are safeguards in place for feature count deviation. In the event that there was an omission of GIS data features from one upload to the next, and the omission resulted in a percentage change above the tolerance defined for each layer, the upload is held until Intrado i3 GIS Analysts review and approve the submission. Critical errors identified in the road centerline and address points are identified in the upload summary report and detailed error shape files, and should be corrected as soon as possible after the report is received. For the above scenario, call routing would never be affected, since the SI is designed to know when there is a problem and stops the changes from being committed to the ECRF. ECRF will continue to utilize the existing data within its database until the errors are corrected and resubmitted to the EGDMS.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 4	**Scenario 4** At 0700, the NOC has received an alarm reporting loss of connectivity for a single path to Host A. At 0705, the NOC contacts Host A to confirm the loss of connectivity. The PSAP has found that the link lights are off, but the system appears to be operational. At 0725, the redundant link appears to be bouncing for Host A. At 0900, the PSAP is reporting a decrease in typical call volume.	X			
	Bidder Response: As part of normal operations, The NOC actively monitors all paths between PSAPs and the core processing locations. When a path or device fails, the NOC sees alarms and begins troubleshooting. All alternate and paths for PSAP connectivity are pre-tested during integration and turnup. Any issues with failover will be addressed prior to turning the PSAP live. The presumed response of the NGCS vendor of Scenario 4 differs from how Intrado would institute mitigation. At 7:25, the team's priority would be to evaluate if there is any risk of 9-1-1 call or data degradation. Since the redundant path is not reliable (bouncing), and although the system is configured to do this in an automated fashion, the recommendation to force automated failover of all calls would be made. This would allow for reduced failover timing and/or other possible unforeseeable impacts. This situation would be worked at the highest priority with an Incident Commander and team assigned to work the issue to resolution. Intrado would continue to work troubleshooting the issue from a circuit perspective and verify with internal test calls to the effected PSAP. Once a single link was brought back into service, a joint decision would need to be made by Intrado and the PSAP on whether or not to bring the PSAP back up one-sided, understanding the previous instability. In a typical environment, although not preferred, a one-sided solution is temporarily acceptable. For this particular situation and the history of one-sided issue with possible call impacts, a real-time decision would need to be made. Tools (call tracing, MOS evaluation, and test call validation) will be critical in determining next steps. This incident would be initially designated as a Major (Severity 2) routing services are impaired issue, but upon review would change the classification to a Critical (Severity 1) severely impacted. Once the perceived call volume mismatch is detected Intrado will, until proven otherwise, assume that calls were/are being impacted by this outage. **Restoration and Resolution Timeframes** Intrado and its subcontractors will apply immediate and sustained effort, 7x24x365, until a final resolution is in place. All reasonable efforts will be made to provide a temporary workaround within two (2) hours and permanent resolution with a target of twenty-four (24) hours of the issue being detected.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 12: Intrado Severity Levels

Root Cause Analysis Report

A Root Cause Analysis (RCA) for Severity Level 1 or 2 service disruptions will be available following the resolution of a Severity Level 1 or 2 Service Disruption outlining the conditions that caused the trouble, the corrective action taken, and any corrective action plans to prevent future occurrences of the trouble. This report will include the following:

- Date/Time of the start of the service disruption.
- Date/Time of service restoration.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Date/Time of service resolution.
- Date/Time service disruption was detected.
- Associated Ticket Number (s)
- Number of customers impacted.
- Actual number of calls impacted.
- Functionality lost during the service disruption.
- Corrective action(s) (completed and future as applicable).
- City(ies) and state(s) where failed equipment is located.
- City(ies) and/or county(ies) and state(s) impacted, as applicable.

Severity Level	Description	Response Time	Customer Resolution Time	Status
Critical (Severity 1)	Any outage or condition that results in: • Loss of 9-1-1 call processing • End office or Remote Switch isolation from 9-1-1 network for 10 or more minutes • Loss of end office to 9-1-1 tandem circuits • Loss of ANI / ALI to a PSAP for 15 or more minutes (excludes CPE or customer PSAP issues) • PSAP isolation for 10 or more minutes. Excluding troubles at PSAP and reroute successful with both ANI/ALI. • Any fault condition meeting FCC reportable criteria	Immediate	30 min-2 hrs	15 min
Major (Severity 2)	Customer is able to access the system or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Minor (Severity 3)	Customer is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent (Severity 4)	Customer has an informational request or questions of a general nature concerning the overall product suite functionality, or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours

Table 13: Intrado Severity Levels

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
PM 1	**Project Management and Ongoing Client Management Services** **Project Management Methodology** 1. Describe bidder's project management methodology and support structure. 2. Describe the daily, weekly, and monthly interactions during the migration. 3. Include a proposed high-level project plan. 4. Include a schedule for the through implementation of this project.	X			

Bidder Response:

1. The Intrado approach to plan, configure, network engineer, implement, test, document, train, and support A9-1-1 services implementation follows Intrado's recommended and time-proven solution lifecycle progression methodology for projects of this type. Intrado has successfully deployed Next Generation 9-1-1 ESInet solutions for the States of Arizona, Delaware, Washington, Minnesota, Hawaii, and Vermont, and to PSAPs in California, Florida, Louisiana, Nevada, North Carolina, Pennsylvania, and Utah. In addition:

- The Intrado A9-1-1® network delivers over 35M NG9-1-1 calls annually, serving over 35 million citizens.
- Nearly 950 U.S. PSAPs are now using-or are in the process of implementing or are preparing to implement -the Intrado NGCS/ESInet solution.
- Since 2016, Intrado has facilitated more than 1.5B 9-1-1 transactions - more than 430M 9-1-1 transactions annually.
- Intrado serves over 250 communications service providers for routing and call delivery to the PSAP including AT&T and CenturyLink.
- Intrado supports over 205 million transactions for E9-1-1 mobile routing and location requests.
- Intrado has over 290 million telephone number records under management in its location databases.

Considering the State's needs and the constraints of the OSPs serving the State, the Intrado Project Manager creates an Implementation Project Plan and milestone schedule tailored to the needs of the State's operations with mutually agreed-upon time frames. Project management duties will include, and are not limited to:

- Assemble and chair the teams involved in the implementation
- Integrate the activities of all applicable PSAP vendors/suppliers
- Manage, coordinate, and monitor the implementation activities
- Manage the change control process

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- Identify and escalate project obstacles
- Support quality and acceptance in all areas of the project
- Coordinate compliance with test criteria
- Transition completed solution to the Intrado 24x7 support organizations
- Meet/exceed the State's needs regarding documentation
- Schedule training and meet/exceed the PSAPs' needs
- Participate in the cutover readiness review
- Direct and monitor all cutover activities

Throughout the duration of the project implementation, the Intrado Project Manager will keep Nebraska and the PSAPs apprised of ongoing project status via regular project team meetings. Intrado prides itself on customer satisfaction and encourages the use of these project team meetings as a forum for continual feedback on Intrado's performance. With this feedback, the Intrado Project Manager can refine the implementation plan or take necessary action so that the final NG 9-1-1 solution implementation meets the State's and PSAPs' expectations.

This solution lifecycle begins with project definition and solution architecture activities. During these initial phases, the joint Intrado and Nebraska team members verify system application and implementation requirements, refine the solution architecture, finalize the plan for solution deployment, and notify and assist telephone service providers in planning for the migration. Following definition and architecture phases, Intrado orders, installs, configures, tests, and trains users on customer-facing solution components as part of solution integration and deployment effort. Following successful deployment, the maintenance phase begins. The primary goal of the lifecycle methodology is that the project aligns with overall customer expectations and is tailored to fit the needs of Nebraska.

2. Intrado's communication plan is put into action immediately by the Project Manager through preparation and facilitation of a project kickoff meeting attended by stakeholders and the Intrado project team . Following the kick-off meeting, the Intrado Project Manager facilitates ongoing implementation planning, design, and requirements definition meetings with the State and the affected telephone service providers to ensure successful and timely implementation. Depending on the phase of the project, the Project Manager will provide either a bi-weekly or weekly status report. In addition, there will be

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	bi-weekly or weekly (depending on the phase) conference calls with minutes distributed. Email correspondence will be used as well as phone calls as necessary, which will be followed up with written documentation. During the maintenance period, the Program Manager facilitates regularly scheduled operations meetings and periodic formal reviews with the State to monitor general status and trends, receive customer performance reviews and obtain customer feedback, and address any questions or concerns. **3.** The primary goal of the Project Plan is that it aligns with overall customer expectations and is tailored to fit the needs of the State. During this process, key members of the joint project team unite to identify roles, responsibilities, critical success factors, project challenges, elaborate on specific strategies and project options, confirm project scope, and finalize plans to expedite solution delivery plans and resources. The proposed solution is reviewed in order to align each primary stakeholder with a common vision and strategy for unified team design and planning. A proposed high-level Project Plan is included in the *Proprietary Information* file submitted with Intrado's response. **4.** All activities in the Project Plan have a proposed date assigned to them, with linked dependencies. The proposed schedule is part of the high-level Project Plan included in the *Proprietary Information* file submitted with Intrado's response.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
PM 2	**Project Management and Ongoing Client Management Services** **Post-Deployment Client Management** Describe the post-deployment client management service, including client management reports, executive briefings and the fielding of ad hoc support requests.	X			

Bidder Response:

Post Deployment Client Management

The Intrado Program Manager manages the ongoing maintenance of the A9-1-1 services through the life of the contract. Beginning with ALI migration, as each end office re-homes to the A9-1-1 solution, and continuing through the term of the contract, the Program Manager oversees all aspects of Intrado's full suite of maintenance services for all components of the solution, including:

- Data Integrity Services
  - Service Order processing, including PAD installation, SIP enablement and Session Augmentation.
  - Master Street Address Guide (MSAG) management
  - Emergency Service Number (ESN) and ALI Response format management
  - Error correction for data content, MSAG, LNP, ANI/ALI Discrepancy, and No Record Found (NRF) errors
- Special Services, ad-hoc support requests including (but not limited to): non-Intrado equipment upgrades (CHE), PSAP location moves, special even support, data extracts, reconciliations, and audits
- Routing Services
  - i3 Routing management
  - Provisioning support for routing, star code assignment, transfer, and other configurable attribute changes
- Originating Service Provider Management
  - Outstanding error management
  - Deployment of new Originating Service Providers (OSPs)

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	○ Support of end office and Mobile Switching Center (MSC) re-homes ○ Assistance in wire center overlap issue resolution • System, Network and Hardware monitoring, maintenance, upgrades, and support Intrado has a Communication Management process that is followed. Depending on the phase of the project, the Intrado Program Manager will provide either a bi-weekly or weekly status report. In addition, there will be bi-weekly or weekly (depending on the phase) conference calls with minutes distributed. Email correspondence will be used as well as phone calls as necessary, which will be followed up with written documentation. Throughout the duration of the contract, the Intrado Program Manager will keep the PSAP and State representatives apprised of ongoing project status via regular project team meetings. During the maintenance period, the Program Manager facilitates regularly scheduled operations meetings and periodic formal reviews with the customer to monitor general status and trends, receive customer performance reviews and obtain customer feedback, and address any questions or concerns. Intrado prides itself on customer satisfaction and encourages the use of project team meetings as a forum for continual feedback on performance. With this feedback, the Intrado Program Manager can refine the implementation plan or take necessary action so that the final NG 9-1-1 solution implementation and management meets the customer's expectations. Schedule is maintained using Microsoft Project and cost monitoring is done using Oracle Applications for actual/to-date information and a combination of Microsoft Project and Microsoft Excel for Estimate-To-Complete (ETC) information.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 1	**General Requirements – Training** **Comprehensive Training** Contractor shall provide comprehensive training to designated Commission representatives responsible for varying layers of network/system monitoring and system maintenance. Describe bidder's training program for system implementation and ongoing operation and maintenance, including but not limited to the following topics: 1. user-configurable elements; 2. NOC/SOC procedures; 3. escalations; 4. trouble reporting; 5. help desk portal; 6. executive dashboard; and, 7. service monitoring tools. Training shall be available at the user level and delivered to the PSC and each region (up to 10) and also the train-the-trainer level (up to 25 individuals).	X			
	Bidder Response: Intrado provides extensive training packages to support the rollout of the NG9-1-1 system products and services. Through detailed analysis and review processes, the specifications and methodologies for technical and non-technical requirements have been selected so that training courses and materials are tailored to suit the specific system and minimize operational impact on the end users and staff. Intrado also provides appropriate training to Originating Service Providers to supplement OSP support information available on line. The Intrado training plan for the State is progressive in nature. The sequence of courses leads the trainees from a generalized overview to a more comprehensive understanding of the components within the A9-1-1 system, respective to each user's area of responsibility. Training sessions are designed to allow trainees to understand and effectively interact with Intrado and the web-based tools to maximize benefits of the system and tools for the State. This is achieved by integrating well-designed technical documentation, practice exercises, and instruction into the overall training experience. Intrado will provide a comprehensive set of training materials for each trainee. Among others, the following topics are covered: • User-configurable elements • NOC/SOC procedures • escalations • trouble reporting				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• help desk portal • executive dashboard, Customer Management Portal, 9-1-1NET, etc. • service monitoring tools *Standard Customer Training* Intrado provides A9-1-1 training to State-designated users. These classes are offered in a web-conference style, allowing the attendees to receive the full benefits of an instructor-led program without the additional cost of travel and lodging. Optionally, Intrado can provide on-site and/or customized training at an additional fee. *Supplemental Training* Intrado is committed to maintaining current training activities and documentation and providing additional training as needed. As technology continues to develop over the duration of the contract, supplemental training is critical to introduce users to new and enhanced services. Intrado views the State as a partner in overseeing the quality of the training and making ongoing recommendations for improvement. *Optional Training* Intrado will work with the Commission to scope, design, develop, and deliver any additional A9-1-1 training desired by the State, including pertinent optional classes or training as it becomes available.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 2	**General Requirements – Training Attendees and Curriculum** 1. Describe the number and types of attendees required to attend training, training curriculum, number of training attendees included in the proposed price, and the duration of the training program per attendee (expressed in hours per day and number of days), as well as the location of the training and whether such training is available online or onsite. Preference is given to training that can be conducted in an onsite setting for attendees. 2. Provide Examples of the proposed training plans. 3. Provide a sample of the training materials to be used. Training classes shall be recorded for future reference and training of new Commission and PSAP employees.	X			

Bidder Response:

1. Different class size arrangements can be discussed with the customer; however, we recommend small groups so that participants can closely interact during the course and support each other after the session. Intrado will work with the Commission to establish training details, such as number of attendees, a date, time, venue, and training for both initial training and subsequent training as new systems, features, and services are deployed. Intrado will provide the training materials in advance of each training session for review and approval by the Commission.

Training sessions typically include an overview of Intrado systems including the IP selective router and ALI management systems, training on all PSAP-facing applications such as the Customer Management Portal (CMP), web-based EGDMS, Spatial Interface, 9-1-1NET, reporting tools, feature options and configurations, and problem reporting and escalations. Intrado will work with Commission to mutually agree on the topics to be covered as part of PSAP information sessions. Training sessions are usually web-based and provided “train-the-trainer” style, although we can provide on-site and/or customized training for an additional fee. The training schedule will be contingent upon the project timeline, impact of training on departmental operations, and trainer availability. Intrado will work with Commission to agree on the topics to be covered as part of PSAP information sessions. All training details will be mutually agreed upon during contract negotiations.

2. & 3. Please see the attached sample Training documents below. All training materials for the State of Nebraska will be customized in conjunction with the Commission and PSAPs for the State’s specific implementation.

A9-1-1 NOC_CMP Training Schedule.p

A9-1-1 CMP 6.2 Demo Outline_Samp

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	CMP Introduction and Navigation.mp4

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRAR 1	**General Requirements – Service, Repair and Advance Replacement** The Commission shall not be responsible for the replacement and maintenance of hardware and software required to provide the NGCS or ESInet connectivity provided as part of the bidder's solution. The Contractor shall resolve all faults or malfunctions at no additional cost to the Commission. **Support Maintenance** 1. Describe in detail bidder's 24 x 7 x 365 maintenance support for the life of the contract. 2. Describe bidder's understanding of public safety maintenance windows and associated notification processes. 3. Describe bidder's problem resolution and change management processes, the supporting systems, and adherence to best practices, such as those described in the ITIL version 3 or most current version.	X			

Bidder Response:

As a managed service, the A9-1-1 solution minimizes the need to constantly maintain, upgrade, and administer complex hardware and software and maximizes the ability to focus on public safety. This 9-1-1 network services model consistently renews key components to enable PSAPs to operate on the most modern communications technology and eliminates the service development and deployment bottlenecks present in legacy solutions. During the life of the contract, Intrado will maintain and monitor all equipment and software within the NGCS solution. Intrado will replace any faulty equipment (that wasn't a direct cause of negligence of on-site PSAP personnel) at no additional cost to the State.

Support Maintenance

1. All aspects of the A9-1-1 architecture are designed to be extremely resilient and redundant, allowing call traffic to continue in case of a failure at one or more pieces of hardware, software, or network infrastructure. This also allows repair to take place without further impacting PSAPs or call delivery. Disaster recovery plans have been created for each aspect of the A9-1-1 infrastructure, with on-call available resources and replacement hardware to quickly restore impacted systems.

Intrado will conduct major and minor planned and critical un-planned changes for all A9-1-1 maintenance or upgrades that may impact customers including hardware service, repair, and replacement. A9-1-1 utilizes the Change Management module of ServiceNow for managing changes to the service including aggregation sites, core call routing complexes, PSAP equipment maintenance, circuit maintenance, and hardware and software versions. Intrado will manage and complete these events with a trained ESInet change management team facilitating the change implementation, monitoring, and communication through the length of the event. Intrado adheres to stringent internal event plan processes and procedures which include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

The Solution Maintenance phase begins once live traffic is transferred onto any part of the system. During this phase, Intrado provides ongoing tiered support services to monitor service level performance allowing the State of Nebraska to reach the highest level of operational excellence. The solution support team is in place to receive, analyze, and rectify problems and information requests throughout the term of the contract.

A designated customer Program Manager is provided who is responsible for coordinating and delivering support through the term of the customer's purchased services. The Program Manager is the single point of contact for the Commission and PSAPs and assists with all billing and reporting questions as well as provides monthly/quarterly customer reviews and functions as the State's first point of escalation.

The Program Manager is responsible for overall customer service management that includes:

- Scheduling and facilitating kickoff meeting and status updates
- Coordinating resources
- Ongoing project management for the duration of the Statement of Work (SOW)
- Writing and maintaining all methods and procedures that affect Intrado operations and its interface with the customer, carriers, and PSAP operations

During implementation of services, Intrado provides a dedicated Project Manager who works with the customer. The implementation Project Manager is responsible for all implementation-related activities including creation and management of the implementation project plan with the customer and coordinating activities with carriers such as establishing connectivity and test/migration schedules.

The implementation Project Manager is an integrated partner with the Program Manager and meets with the customer on a periodic basis to review the status of implementation and completion of implementation tasks against target timeframes as described within the integrated project plan.

2. Maintenance of the A9-1-1 solution is done with no scheduled downtime. We schedule planned events for routine maintenance in ways that 9-1-1 operations are not impacted. A notification of the upcoming event will be sent to the customer as applicable. Planned events are fully staffed and managed with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event.

The Intrado team will conduct major and minor planned and critical un-planned events for all NG9-1-1 Services, system maintenance, or upgrades that may impact the NG9-1-1 Customer PSAPs. Intrado fully manages and completes these

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	events with a trained event management team, facilitating the change implementation, monitoring, and communication through the length of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado includes the required back-out time within the scheduled maintenance time frame. The A9-1-1 maintenance window is 12am-6am per time zone (Tuesday- Thursday), unless otherwise agreed to in order to resolve service impacting issues. Changes affecting multiple time zones will be completed between 12AM-6AM CT. Customer PSAPs may require maintenance at the PSAP to be done outside of this maintenance window, in which case Intrado will coordinate an appropriate time to perform maintenance at the PSAP Maintenance and repair of those elements of the ESInet and interconnections owned, operated, installed or controlled as part of the solution will be provided by Intrado. Intrado will provide on-site support for all A9-1-1 Equipment including removal and disposal. Intrado will provide all necessary resources to successfully perform and complete the maintenance. **3.** A 24x7x365 NOC dedicated to 9-1-1 call delivery services supports the A9-1-1 network, core services, and equipment. Intrado utilizes industry standard processes, including adherence to Information Technology Infrastructure Library (ITIL) framework as well as best-in-class tools for Change Management, including the use of the ServiceNow Change Management Module. Intrado will conduct major and minor planned and critical un-planned events for all A9-1-1 system maintenance or upgrades that may impact customers. Intrado will manage and complete changes to the service including aggregation sites, core call routing complexes, PSAP equipment maintenance, circuit maintenance, and software upgrade events, with a trained ESInet event management team facilitating the change implementation, monitoring, and communication through the length of the event. Intrado adheres to stringent internal event plan processes and procedures which include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. Intrado includes the required back-out time within the scheduled maintenance time-frame. Change Requests very widely in terms of scope and complexity, dependent upon the type of change. Change Requests with largest potential impact are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. Intrado manages all aspects of Change Management through the Change Management Process including availability, capacity, configuration, incident, problem, release, service-level and IT Service continuity management.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Depending on the type of change, changes are submitted to a Change Advisory Board (CAB) for approval. The CAB is a committee that makes decisions regarding whether or not a change should be implemented. The Change Advisory Board consists of executive stakeholders or their representatives. We manage all aspects of change management through the Change process including availability, capacity, configuration, incident, problem, release, service-level and IT service continuity management. Generally speaking, there are two classes of ESInet maintenance e.g., standard and emergency.

- **Standard:** Intrado will provide a schedule of standard maintenance windows for activities defined below as: level 4 standard and level 3 normal.
- **Emergency:** Where reasonably practicable, Intrado will give the Commission and any affected PSAPs 24 hours notice of the need for the maintenance and a summary of the potential impact. Emergency maintenance may occur at any time.

There are five categories of changes.

Change Category	Description
NORMAL*	This change indicates a low risk and repeatable change that occurs frequently. Once it is deemed appropriate (3 successful) Change plans/MOPs are in place, a template will be built so the change can be entered as a Standard Change for future usage negating the need for a normal change. This change type does not require CAB approval.
NORMAL	Normal changes are often categorized according to risk and impact to the organization. By definition a normal change will proceed through all steps of the change management process, including the CAB for approval.
POST-DATED	This change should be utilized for unplanned work, resulting from a critical incident ticket and/or Major Incident.
EMERGENCY*	By definition an Emergency* change will proceed through all steps of the change management process and will be reviewed by the executive CAB unless there is a valid business reason to bypass the 48 hour advance submittal time frame.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

EMERGENCY	Utilized for a change that resolves a problem deemed critical to business continuity and for which a workaround is not sufficient. Examples are a router that could put voice delivery at risk and has a potential for an immediate threat to the production environment and /or to be a major impact to Business or Customer. Emergency changes are approved at an Emergency Executive CAB.

Table 14: Change Management Change Categories

For a Planned or Emergent Event to receive approval there must be an event plan submitted to the CAB. The event plan must include a step-by-step guide of changes being made and clearly state the impact of the change. All event plans must also include a detailed validation plan and back-out plan in compliance with implementation plan standards and approved by the CAB Stakeholders. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA. Intrado will provide written notification and release content (when applicable) to the jurisdiction(s).

For Normal, Emergency, and Expedited changes, a change request is submitted to the CAB. The request must include a step-by-step explanation of the purposed changes being made and clearly state the impact of the change. These changes must also include a detailed validation plan and back-out plan in compliance with implementation plan standards. All event resources are clearly listed and verified ahead of time. New application code is never to be loaded without it being officially released by QA and validated in our test environment.

The result of each change is tracked and available for future reference in our ServiceNow Change Management Module whether it was successful or unsuccessful. If the change is closed as unsuccessful and the back-out plan was enacted, the issues that caused the event to be unsuccessful are documented. A change plan and request must be submitted for re-approval by the CAB. If the change was successful with deviation, this is also tracked with the deviations documented.

If the event is closed as unsuccessful and the back-out plan was enacted, the issues which caused the event to be unsuccessful are documented. A new event plan and subsequent change must be submitted for re-approval by the CAB.

The CAB also documents and stores each event for tracking and reporting purposes. The CAB logs all planned and emergent event change requests on events that are both approved and declined. We also review and issue Reason for Outage (RFO) reports when outages occur.

We have scheduled maintenance time frames for non-emergency events. If we have an emergency item, we will alert the Commission and affected PSAPs using a standard process. The State can choose the modality of this communication (i.e. text, email, etc.)

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

The Intrado Service Manager will provide notice of maintenance events. For questions during the maintenance window, the State should contact the Intrado NOC.

The A9-1-1 maintenance window is 12am-6am per time zone (Tuesday- Thursday), unless otherwise agreed to in order to resolve service impacting issues. Changes affecting multiple time zones will be completed between 12AM-6AM CT. Customer PSAPs may require maintenance at the PSAP to be done outside of this maintenance window, in which case Intrado will coordinate an appropriate time to perform maintenance at the PSAP.

In addition to managing planned and emergent events, we maintain a problem management system for tracking and reporting trouble. Intrado provides a service for opening trouble tickets, change requests, and checking status of existing items e.g., tickets opened, resolved and pending.

Escalation

We will notify the specified single point of contact in writing concerning scheduled release installations. Acknowledgement of notification is required from the customer. Intrado will send an email notification to the customer at the start and end of the pre- arranged maintenance interval. Listed below are the current A9-1-1 escalation procedures.

Table 15: Escalation Procedures

Escalation Intervals	Level	Responsibility
First Escalation SEV 1 - 2 Hours SEV 2 – 4 Hours SEV 3 – 6 Hours	NOC Manager	Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center
Second Escalation Customer Discretion	Area Manager or Delegate	Review status of ticket Monitor ticket progress Notify Director - when appropriate
Third Escalation Customer Discretion	Director	Status Customer Escalate as needed to partner centers Monitor ticket progress/ documentation Notify VP when appropriate

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Fourth Escalation	Vice President	Ensure adequate resources are available and engaged for prompt resolution Update customer as appropriate Escalate as needed to appropriate levels

When escalating a problem, it is important to provide the following information:

- Customer's name and telephone number
- Active ticket number(s)
- Trouble Location
- Trouble description (e.g., out of service, service degraded, etc.)
- The action or resolution requested

Intrado understands the requirement for integration and information sharing to the Customer for service management support. Intrado will work with the Commission to develop an appropriate integration design, plan, and MOP for information sharing.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 1	**General Requirements – Software Release Policy** **Scheduled Releases** **Frequency of Scheduled Releases** 1. Describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release. 2. Include a current 1 of feature updates and additions with projected release by quarter and year.	X			
	Bidder Response: **1.** Defects: Upon discovery and communication by the customer of a software defect, a ticket (change request) is created and reviewed by a cross-functional team. A disposition is typically made within 3 weeks, but within days if not hours for a critical issue. . A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. The frequency of defect resolution software releases is driven to some extent by the nature of the defect. 'Must fix' defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will make the fix available within 6 months or sooner. Defects characterized by the customer as minor will be prioritized in partnership with the customer. The decision-making processes involved in selecting which software defects to fix is done in partnership with the customer. All defects are assessed, managed, and scheduled by the Intrado Change Control Board. Critical and Major defects are managed as soon as discovered and communicated by the customer. The initial solution may be a manual process. A long-term solution will be with the next ESInet platform code release. Minor defects are reviewed within three weeks of discovery and communication by the customer. The solution will be ranked against other defects and enhancements and road-mapped appropriately. Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has installed in production, we will follow up with the customer to make sure the issue has been resolved. Features: The decision-making processes involved in selecting which software features to build and release are based on standards updates, customer input, technical innovations with direct benefit to Public Safety and overall market demand. The advances in Public Safety are accelerating and Intrado is organized to respond quickly to advances that benefit how citizens requiring assistance are supported. Intrado typically releases a set of new capabilities and/or features quarterly.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Feature Release Testing Process

The following information describes our product release cycle.

Deployment

The Deployment phase consists of a series of release candidates and testing until the system is considered complete and ready to launch:

- A first build may be provided from the branch(es) and become release candidate #1. This build goes through a limited testing cycle (for example, smoke tests).
- Finalize regression testing, as needed (System Team).
- Release candidate #1 is sent to the Deployment/Operations team.
- The cycle above is repeated (RC#2, RC#3, etc.) until no critical bug is found.
- Training is given to the deployment team, if applicable.
- User documentation and release notes are finalized.
- Marketing datasheets are updated and provided to customers.

Ready to Deploy

The Ready to Deploy milestone is reached when no critical bugs are found in the release candidate currently in testing. At this point, the release candidate is provided and the release is complete.

2. The A9-1-1 product roadmap with NG 9-1-1 features considered for the next three years can be found in the *Proprietary Information* file submitted with Intrado's response.

Figure 1: Intrado A9-1-1 Roadmap

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 2	**General Requirements – Software Release Policy** **Maintenance Releases** Describe the frequency of defect-resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.	X			
	Bidder Response: Upon discovery and communication by the customer of a software defect, a ticket (change request) is created and reviewed by a cross-functional team. A disposition is typically made within three weeks or sooner depending upon the severity of the issue. A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. The frequency of defect resolution software releases is driven to some extent by the nature of the defect. 'Must fix' defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will typically make the fix available within 6 months if not earlier. Defects characterized by the customer as minor will be prioritized in partnership with the customer. The decision-making processes involved in selecting which software features to provide are based on standards updates and market demand. A typical annual release schedule includes one major software release with up to two minor releases as required. The decision-making processes involved in selecting which software defects to fix is done in partnership with the customer. All defects are assessed, managed, and scheduled by the Change Control Board. Critical and Major defects are managed as soon as discovered and communicated by the customer. The initial solution may be a manual process. A long-term solution will be with the next ESInet platform code release. Minor defects are reviewed within three weeks of discovery and communication by the customer. The solution will be ranked against other defects and enhancements and road-mapped appropriately. Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has installed in production, we will follow up with the customer to make sure the issue has been resolved. The A9-1-1 solution is offered as a managed service; therefore, known issue and defects resolution are included at no cost. Enhancements could incur additional fees.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 3	**General Requirements – Software Release Policy** **Test Environment** Prior to install of new releases, bidder shall explain how Contractor replicates the production environment for software release testing to provide assurances that future software releases will not negatively impact PSAP operations.	X			
	Bidder Response: All Intrado releases of the A9-1-1 service are rigorously tested prior to installation in Intrado's Production Network. Software release are tested in multiple, exactly-replicated, Test and Pre-Production environments prior to deployment. These environments are comprised of the same hardware systems, e.g., OEM model/series number, CPU and memory generation, high availability/redundant server system complement. All new features are thoroughly tested, and vigorous regression testing, load and performance, and backwards compatibility are verified to ensure that no new bugs have been introduced. After SQA testing, additional deployment testing is performed in the Pre-Production labs. Here the MOP is tested to ensure the A9-1-1 i3/IP Selective Router Administrative team, who will perform the production installation, are familiar and practiced at performing the installation prior to the install event. During this time each phase of the install is executed as it will be performed, and any changes to the environment are verified and validated prior to finalizing the MOP.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 4	**General Requirements – Software Release Policy** **Access to Defect Tracking System** Contractor shall provide the Commission with access to the Contractor's defect tracking system for the Commission to track the progress of defect resolutions. **Software Defect Tracking Process** Provide a detailed description of the software defect tracking process and describe how bidder will provide training for no more than ten (10) Commission staff prior to Final Acceptance Testing.	X			
	Bidder Response: **1.** Intrado will provide monthly reports on defects to the Commission. The Commission can also use Intrado's software defect ticketing system (JIRA) at their discretion. Training will be provided. **2.** Upon discovery and communication by the customer, a ticket (change request) is created and reviewed by a cross-functional team with representatives from Engineering and Product and an Intrado Customer Representative. A disposition is typically made within 3 weeks or sooner depending upon the severity of the issue. A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. Intrado has a comprehensive defect tracking process as part of our defect tracking tool, Jira. Critical and Major defects are managed as soon as discovered and communicated by the customer. The initial solution may be a manual process. 'Must fix' but non-critical defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will typically make the fix available within 6 months if not earlier. Defects characterized by the customer as minor will be prioritized in partnership with the customer. The decision-making processes involved in selecting which software defects to fix is done in partnership with the customer. All defects are assessed, managed, and scheduled by the Change Control Board. Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has been installed in production, we will follow up with the customer to make sure the issue has been resolved.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 5	**General Requirements – Software Release Policy** **Software Defect Aging** Describe how service-affecting software defects are aged. If minor problems (from the Contractor's perspective) are not identified and resolved immediately, these minor problems can become major or critical problems. Describe in detail how/when this minor problem gets scheduled or automatically escalated, and the feedback mechanism in place for keeping the Commission informed.	X			
	Bidder Response: Intrado has a comprehensive defect tracking process as part of our defect tracking tool, Jira. Critical and Major defects are managed as soon as discovered and communicated by the customer. The initial solution may be a manual process. Intrado will utilize the Product Roadmap and the Service Enhancement Request process to track the status and prioritize the enhancement with other Product Roadmap improvements. 'Must fix' defects (call delivery impacting) are normally rolled into the release immediately following the time of discovery. This will typically make the fix available within 6 months if not earlier. Defects characterized by the customer as minor will be prioritized in partnership with the customer. Upon discovery and communication by the customer of a "minor" defect, a ticket (change request) is created and reviewed by a cross-functional team. A disposition is typically made within three weeks or sooner depending upon the severity of the issue. A disposition can range from 'no-action' required to immediate resolution required. Once a disposition is made; the ticket is slated against a specific release. The decision-making processes involved in selecting which software defects to fix is done in partnership with the customer. All defects are assessed, managed, and scheduled by the Change Control Board (CAB). Once a defect has been assigned to a release, we will communicate back to customer the timeline for defect resolution. Defects are reviewed on a periodic basis for changes in priority and coding/testing synergies. After a defect has been installed in production, we will follow up with the customer to make sure the issue has been resolved.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
DOC 1	**General Requirements – Documentation** The Contractor shall provide the Commission with all pertinent documentation for the ESInet and/or NGCS connectivity provided as part of the Contractor's solution as implemented, No more than 30 days after completion of the network construction, and update the Commission as configurations change over the term of the contract. The required documentation shall include the following: **1.** Detailed project plan; **2.** Escalation procedures; **3.** Circuit identification; **4.** Single points of failure; **5.** Network path diversity drawings into each PSAP; **6.** Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system; **7.** PSAP backroom as-built drawings; **8.** PSAP demarcation point drawings; and, **9.** All user interface training and reference materials. **Network As-Built Documentation** Upon implementation, Contractor shall provide a network or solution diagram that clearly depicts the Contractor's solution as implemented. The Contractor shall provide all documentation in agreed-upon electronic format via a Contractor-hosted web portal. Please describe how bidder's solution meets or exceeds this requirement.	X			
	Bidder Response: Intrado will provide appropriate documentation to the Commission as listed above. Intrado will provide each of the PSAPs with pertinent documentation for the ESInet and NGCS, and update the PSAPs as configurations changes. Intrado will author PSAP backroom as-built and PSAP demarcation point drawings. Intrado will provide customized migration plans for each PSAP that will be proactively utilized and managed by the Intrado Project Manager. Web-based, user interface reference materials will be provided along with a "leave behind" reference guide for each PSAP. Intrado will also provide user interface training on the web-based portal for accessing documentation and reviewing reports. Intrado will develop and maintain the operational procedure documentation required for the day-to-day interaction between the parties. **Network As-Built Documentation** Intrado will provide a network or solution diagram that clearly depicts the Contractor's solution as implemented. Documentation will be provided in agreed-upon soft copy format via the Customer Management Portal.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 1	**Emergency Services IP Network (ESInet)** **Diversity** The network shall be designed with diverse entrances (e.g., east-west entrances) into specified buildings that are part of the ESInet. This requirement shall apply to the core network sites, including data centers and PSAPs specified in Attachment A - PSAP Host End-Point Locations, Equipment List and Selective Router Locations. Primary and redundant links shall not share common routes, trenches, or poles. If last-mile facility or building construction is required, bidder shall so indicate. If this is not possible at a given location, indicate how bidder intends to provide redundant and resilient connectivity to that location. Describe how bidder's solution meets or exceeds the above requirement.			X	
	Bidder Response: Intrado has not been able to acquire a quote for the creation of new entrances into each region facility due to the turnaround for construction quotes. If chosen, Intrado will commit to providing quotes to the State, and implement (if desired) those network buildouts at 10% cost markup to cover management resources. Intrado does believe that the Intrado-proposed network solution will provide the necessary redundancy and diversity required for a 99.999% available system at a fraction of the costs it would take to buildout physical diverse entrances and laying new fiber-optic cable to redundant and diverse end offices.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

ESI 2	**Emergency Services IP Network (ESInet)** **Network Design** Bidder shall design the physical network using the most robust facilities available. Use of fiber-optics is the preferred method for connectivity due to available capacity (bandwidth) and increased reliability. Given the amount of fiber-optic facilities and interconnections between the fiber-optic networks in Nebraska, the ESInet design should include as much fiber as possible, not only on the transport side but on the access side as well. Describe the design of proposed network with specific details on connectivity.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado, along with our third-party provider, Carrier Access, has designed a solution which is not only highly available, redundant, and diverse, but also cost effective. In addition, the Intrado solution allows for extra redundancy and diversity by using the backend PSAP-side WAN as an alternate path to reach each CHE host location. **Regional Connectivity**				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

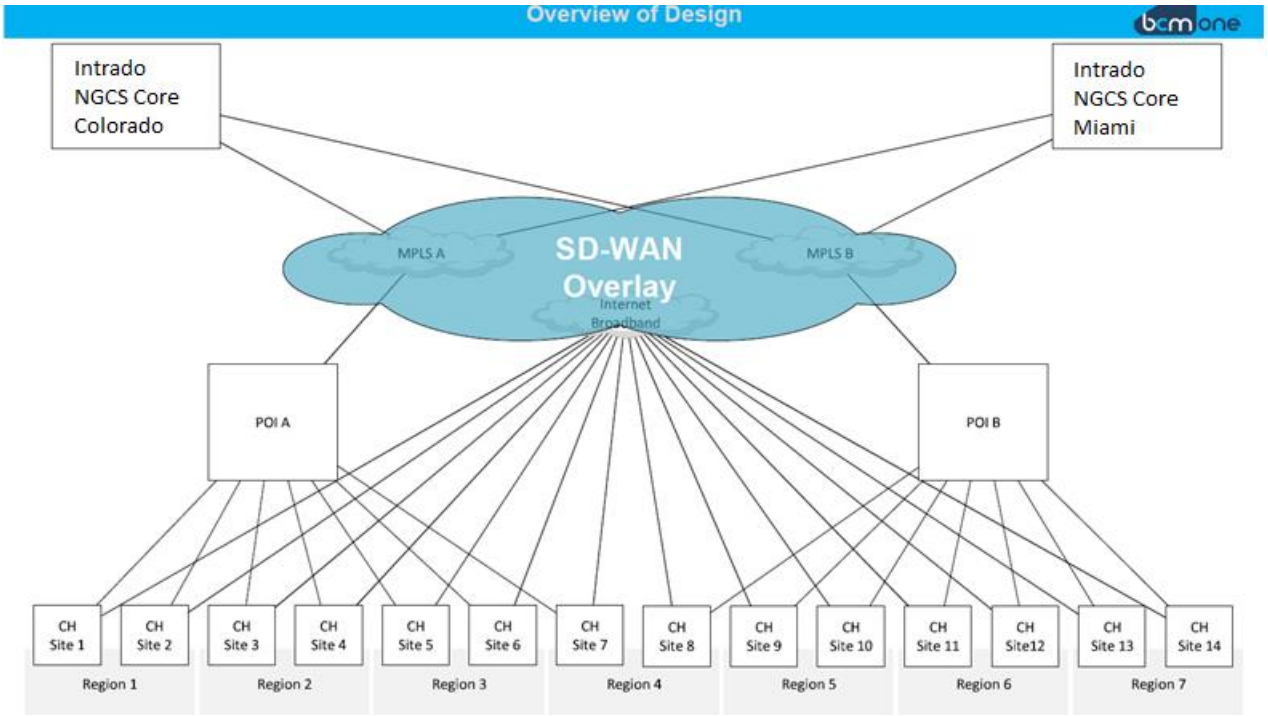

Figure 11: PSAP Egress Architecture Overview

As seen above, the methodology that would be deployed for the State of Nebraska is a combination of MPLS fiber into each CHE location, as well as an Internet broadband SD-WAN connection for redundancy and network diversity. This approach allows the State to gain the benefits of a fully available IP infrastructure, with high bandwidth connectivity (100 Mbps) at a fraction of the cost. This is a completely monitored and maintained service-based solution with Public Safety grade guaranteed uptime, latency, and jitter specifications.

The design includes:

- Primary fiber circuits to each location – with an SD-WAN MPLS overlay that is designed to be Active-Active. The SD-WAN overlay will provide additional resiliency by establishing an active-active topology, application routing, and

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	via packet duplication. This would route critical traffic over redundant paths which prevents jitter and latency from impacting communication. • a resilient, redundant core for the IP-based NG9-1-1 network without significant capital expense • PSAP connection diversity provided through multiple carrier host clouds In addition to the proposed network, Intrado will work with the PSAPs to create a network path through the already available and managed CHE WAN network. In this configuration, as long as the interconnectivity is up between the region's two host locations and the network allows for BGP to be utilized, a call will be able to be completed to each host, even if all direct connectivity from Intrado to a single host is lost.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

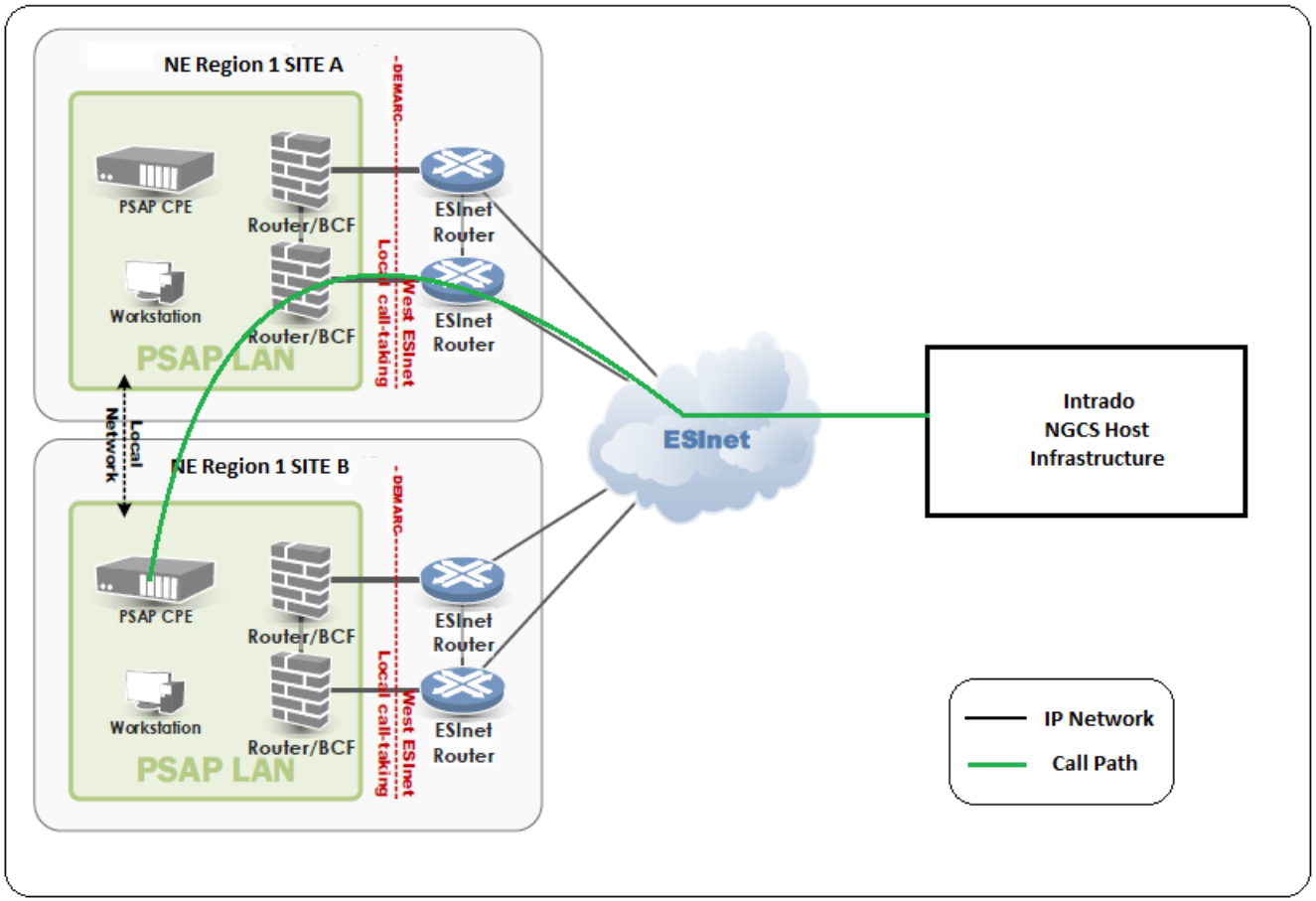

Figure 12: Diversity/Redundancy with BGP through PSAP WAN

Intrado believes that the methodology of using a combination of the MPLS fiber connection, as well as a fully available SD WAN connection in conjunction with utilizing the local network already running between the two regional CPE sites will give the State the required availability, redundancy, and diversity to provide a 99.999% available solution. In addition to the availability and robust infrastructure provided, the additional cost benefit and high bandwidth provided proves that the

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado solution is superior in providing a dependable, affordable solution that will grow with future technology for years to come.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 3	**Emergency Services IP Network (ESInet)** **No Single Points of Failure** The mission-critical ESInet shall be designed with no single points of failure. All equipment shall include redundant processors and power supplies and be supported by an uninterruptible power supply (UPS) system and alternate power source in a properly conditioned environment. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: The A9-1-1 solution has no single point of failure, positioning the State of Nebraska with a solid foundation to deploy future NG9-1-1 functions when they become available. A9-1-1 supports 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. Each i3 element has multiple instances within a single core to provide redundancy for that core. The same redundant configuration is replicated at each of the geo-diverse core sites. The Aggregation sites use the same design approach of redundancy within each individual site mirrored at the other sites. All vital system components are protected through the use of redundant modules to eliminate any single point of failure. Transactions or call traffic divert to available components on failure or degradation of service of a given functional component or a loss of a physical site. IP transport paths for critical service components are redundant and designed for multipath IP packet delivery so the failure of a given IP transport mechanism does not affect overall service availability. A9-1-1 components are designed and configured for continuous operation. Core sites include redundant network transport and redundant network interfacing elements to ensure optimal operation and availability. Network interfacing elements include switches, routers, SBCs, firewalls, and other security devices. All network routing infrastructure is designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an ingress aggregation site, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology. The A9-1-1 network implements a design of redundancy upon redundancy. Individual processing elements are redundant at each Core Site and Core Sites are redundant to each other. The failure of any given component at a Core Site will not prevent that Core Site from processing 9-1-1 calls. If a dual failure does occur at a Core Site, or a Core Site somehow becomes unavailable, calls are processed at another Core Site. Any Core Site can process any 9-1-1 call. The Core Sites are geographically diverse and a regional disaster will not remove the ability for A9-1-1 to process 9-1-1 calls, assuming telecommunication transport services for the impacted region are operable.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	The core routing and intelligence of the ESInet provides the State with immediate scalability in call routing and data delivery. The Core network and NG9-1-1 services are designed to support very large volumes with geographic diversity of the two core processing centers. The end result is an infrastructure that is public safety grade with respect to capacity, reliability, scalability, and redundancy. Data Center facility requirements address 24x7x365 secured physical access, secured floor space or locked equipment cabinets with controlled access, and monitoring and alarming for all facility elements, such as electrical, heating, cooling, etc. Data Centers include redundancy and diversity in electrical, to include power feeds and Uninterruptible Power Supplies (UPS). All the NGCS and network elements use dual power supplies so that a failure on the primary circuit will not disable the operation of the device.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 4	**Emergency Services IP Network (ESInet)** **IPv4 and IPv6 Support** All network equipment shall be new and of current manufacture at the time of implementation. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IpPv6 and have the capability to run dual protocol stacks. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: A9-1-1 will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards. All network equipment has the capability to utilize IPv4 and IPv6 addresses and is configurable to support dual stack operation. Whereas some components of internal systems only support IPv4; this will not be a limitation for this solution. When an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet Core strips down the IPv6 packet, removes the IPv6 header and adds the IPv4 header and passes it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. The IPv4 network and IPv6 interfaces are continuously monitored for availability and performance. This is accomplished with the use of a back-to-back user agent session border controller, rather than Network Address Translations (NATs). All devices within the network shall be assigned static addresses.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

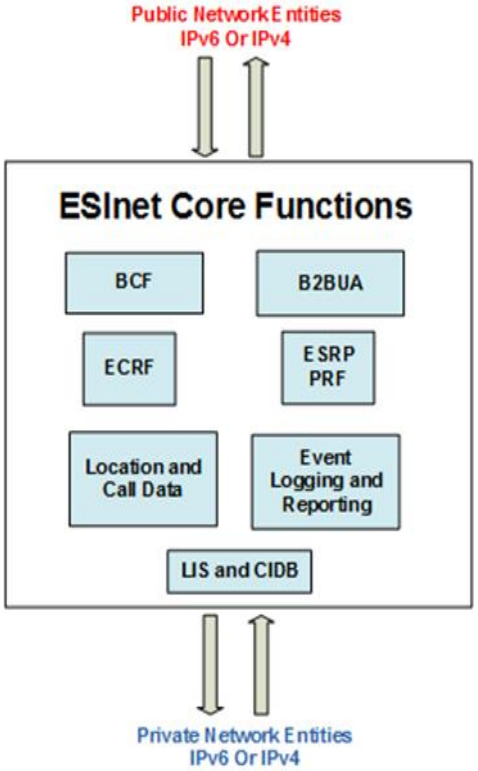

Figure 13: IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 5	**Emergency Services IP Network (ESInet)** **Open Standards** Open standards-based protocols shall be used, and the use of proprietary routing protocols is prohibited. **Resiliency** Resiliency, or fast failover, may be achieved through the use of the Bidirectional Forwarding Detection (BFD) protocol as defined in IETF Request for Comments (RFC) 5880 and RFC 5881, or other standards-based, non-proprietary methods. Describe how the bidder's solution will achieve resiliency.	X			

Bidder Response:

Open Standards

The A9-1-1 service provides a Next Generation 9-1-1 (NG9-1-1) solution that adheres to industry standards. The A9-1-1 solution system complies with NENA STA-010.2-2016 which in itself is based upon IETF RFCs such as SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), and IETF ECRIT best practices documents and ANSI standards. The A9-1-1 solution network architecture adheres to the guidelines and recommendations of the NENA ESIND (ESInet Network Design) A9-1-1 meets the security criteria as defined in the NENA NG-SEC specifications for NG9-1-1 security. The A9-1-1 service adheres to the NENA i3 standards for NG9-1-1 models and offers customers transition strategies to an NG9-1-1 end state while maximizing investment and leveraging existing network assets.

Intrado actively participates in developing new standards and we will support the NENA STA-010.2, the NENA Detailed Functional and Interface Standards for the NENA i3 solution (formerly NENA 08-003). Any time NENA documents conflict, an evaluation is done as to the direction of the industry and intent of the most recent standards documents. Intrado is committed to continued participation in the active NENA workgroups as well as in the annual NENA meetings where conflicts within NENA (and other) documents are discussed and resolved. Typically, the most recently issued documents or working drafts will take precedence over older NENA documents when determining a roadmap that will keep Intrado systems NENA i3-compliant.

The solution does not use proprietary routing protocols.

Resiliency

Intrado leverages the use of Bidirectional Forwarding Detection (BFD) on all network backbone links for fast failover purposes. Two LPGs are deployed to each CAMA-based PSAP for redundancy and failover. All supporting network routing infrastructure connected to the LPGs is designed and deployed in an N+1 model.

Intrado also uses Link Aggregation as a method of combining multiple physical network links into a single logical link. For example, two Network Interface Cards (NICs) are combined into one virtual/logical interface. The network and software

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	running across it recognize these two NICs as one virtual connection. If one goes down, the other handles the traffic. When one or more interfaces in a group fail, the software automatically detects the failure and rebalances the traffic across the remaining links without loss of data. Once the failed link has been restored, the system automatically reconfigures to use all active network links. This load balancing is transparent to the end user who experiences no downtime. A fault-tolerant NIC group eliminates the single points of failure. The fault-tolerant interface group provides dynamic failover access across multiple redundant connections to the network. When a bad cable, a lost link, or a failed adapter causes a failure on the primary NIC link, the intermediate driver software will switch to the secondary adapter.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 6	**Emergency Services IP Network (ESInet)** **Multicast Routing and Switching** Routers and switches must support multicast routing and switching. The applicable base protocols are Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: The A9-1-1 solution is capable of supporting multicast routing and switching. If multicast is enabled for an application, A9-1-1 will use the following base protocols; Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). Intrado has designed multiple solutions for end-to-end communication of non-NGCS applications and systems over the provided ESInet infrastructure. Multicast, although supported by the routers and switches, can introduce risks into a highly available and resilient 9-1-1 system. Additional supported options and configurations may be preferred and will be discussed with the state of Nebraska prior to implementing additional communication paths.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 7	**Emergency Services IP Network (ESInet)** **Quality of Service (QoS)** The network equipment shall support Quality of Service (QoS) marking for prioritizing traffic in the network using the Differentiated Services Code Point (DSCP) protocol. While the network can change DSCP values through rules, the values typically are set by the system or functional element that originates the traffic. Network routers and switches shall not be configured in such a manner as to change DSCP values set by originating functional elements. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: The proposed ESInet is a Quality of Service (QoS)-managed private IP network which can prioritize any type of IP traffic; voice, data, and multi-media. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. Quality of Service in the A9-1-1 network is performed through packet marking with Differentiated Services Code Point (DSCP) on ingress to the ESInet switch ports. In some cases, the voice equipment manages its own marking, and the router/switch honors these QoS settings. In others, the router/switch will override the DSCP marking with a more appropriate setting. The audio stream Real Time Protocol (RTP) is marked with “Expedited Forwarding”, the highest class of service available, so that it is treated like real-time media (e.g., voice). This is typically mapped to a priority queue. Signaling packets (SIP or Media Gateway Control Protocol [MGCP]) are placed in another queue, which will typically have a small but firmly-reserved portion of bandwidth.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 8	**Emergency Services IP Network (ESInet)** **ESInet Properties** The proposed ESInet shall be private, robust, scalable, secure, diverse, redundant, sustainable, and self-healing. Bidder shall propose a network solution for all host sites listed in Attachment A - PSAP Host End-Point Locations and any future identified regions throughout the term of the contract. Describe how the proposed system meets each of these individual requirements.	X			

Bidder Response:

Private – The A9-1-1 IP network uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission.

Robust – The solution delivers voice, data, text, image, video, and third-party data sources on a secure, robust multipurpose network. These technology changes will allow for vast improvements to the current system, including:

- more robust feature functionality
- enhanced survivability and resiliency
- increased quality of service
- faster call set-up time
- improved alignment with public expectation for text and data
- immense information sharing across PSAP and public safety jurisdictions
- seamless evolution with the technological advancements in modern communications
- significant adaptability to the unique needs of individual PSAPs and public safety jurisdictions

The Next Generation design creates an environment conducive to interoperability, flexibility, and innovation that will significantly enhance Public Safety agencies' abilities to communicate with each other and with the public and to effectively respond to emergency situations.

Intrado is committed to providing NextGen 9-1-1 solutions that adhere to industry standards. The solutions comply with NENA i3 models that offer customers transitional strategies from current legacy systems to NextGen 9-1-1. As new standards are ratified, Intrado will work diligently with standards bodies to develop, test and obtain certification (if available) of the new standards to meet our customer's needs. Intrado ensures that the i3 compliant network and call handling solutions will work with other i3 solution providers.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Scalable – The A9-1-1 service provides a fully compliant, scalable environment in the existing LNG and ESInet core infrastructure. Currently the LNGs operate with redundancy at each location and are configured at 20-40mb on 100mb Ethernet circuits or 40mb on 45mb DS-3 based circuits. Future configurations will include GIGE interfaces. Therefore, the bandwidth is expandable in a short timeframe with no need for a forklift upgrade. The A9-1-1 network is capable of bandwidth growth at each network element, existing end sites, and future end sites without sacrificing reliability of the solution. The solution is capable of interconnecting to other national- and/or state-level ESInets via open standards-based interfaces. The A9-1-1 model is deployed from a network perspective with a 2N redundancy model – each remote site is provisioned with twice as much bandwidth as is required to serve the total number of TDM voice trunks provisioned at the site. The network has the scalability to adjust bandwidth to changing needs easily, quickly, and with minimal operational impact. The bandwidth for each data center will support the bandwidth requirements and ease of future growth of the PSAP network. **Secure** – The MPLS VPN tunnels offer a stateful connection across the MPLS cores, so that both ends can quickly identify black holes or other network impairment. In addition, the tunnels are encrypted for security reasons, with AES 256-based IPSEC tunnel protection. Each router at a remote site has two tunnels built from that router over its attached MPLS network to the mGRE hub interfaces at each A9-1-1 core site. **Diverse** – The A9-1-1 solution is designed with diverse entrances into each core call processing facility and each aggregation site (e.g., data centers). The solution uses MPLS networking between sites and avoids commonality of physical or virtual networks utilizing alternate POPs in all designs. **Redundant** – The Intrado solution is a fully redundant, multi-carrier, multi-protocol Emergency Services IP network linking all of the solution's 9-1-1 network elements and PSAPs. Within each redundant node there are redundant network elements. Intrado facilities and nodes are equipped with physically redundant data communications and power equipment such that any component can be maintained without overall service impact. Network paths enter each facility via diverse facility transport paths and diverse points of interconnection. All Intrado solution components are functional redundant. Two carriers will be utilized in all paths where possible. It is common for last mile to not have diverse physical facilities available, dual entries into PSAPs, etc. Intrado will work with the State of Nebraska to identify and mitigate any such single path limitations. Intrado A9-1-1 Routing includes multiple layers of diversity and failover scenarios. The combination of diverse communication links and redundant components creates a highly available architecture. Inbound OSP communication

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	links are subdivided and connected to geographically separated media gateways which are connected by dual path MPLS links to geographically separate call processing complexes. The use of multiple MPLS carriers or instances also allows network equipment to fail away from a temporarily-impaired MPLS core. This can be a relatively common occurrence – small black hole events will occur from time to time within a single provider's MPLS core. These are typically too short in duration to disrupt TCP-based data services, but can cause dropouts and audio artifacts in voice (RTP) streams. In addition to creating redundancy at the hardware and circuit level, using multiple MPLS providers provides redundancy at the path level. To exploit this, remote site routers form routing relationships across the MPLS cores to the Intrado core site routers, and perform constant end-to-end quality testing – if a given path is found to be impaired, the network will switch to an alternate path over a different MPLS core, with minimal impact to active calls. The geographically separate call processing complexes have several components involved in processing of a given call. Each component at a call processing complex has redundancy and high availability within its own domain. The failure of any single component results in either a mated pair taking over or its geographic counterpart performing the processing of future calls. The Emergency Call Routing Function (ECRF) and Emergency Services Routing Proxy (ESRP) functions are highly redundant within each of the geographically diverse sites. There are multiple computers running these functions and the failure of any one or two of those computers do not affect calls in progress. Failure of a complete geographic Emergency Call Routing site results in all future calls being processed by the other geographic site and will still provide the total required call processing capacity requirement. The audio path of a given call is connected to a media server at each geographic call process site and the media server is a physically redundant fault tolerant platform. The failure of a component of the media server results in failover within the media server and no impact to calls in progress. If a call has been established through a media server and that entire media server becomes unavailable, the call will be terminated. All future calls will be directed through an available media server. The A9-1-1 Routing solution architecture is designed from the bottom up with redundancy and automated failover. Within the design, application level components are accessed via means that allow for a given function to be provided by more than one individual instance of a component. In additional, the redundancy and failover concepts are fundamental and exercised on a regular basis as part of the upgrade strategy that allows A9-1-1 Routing to be upgraded without any service availability impact. In addition to application component design, application protocols include regular communication verification and application path roll-over to redundant components upon recognizing the failure of an instance of a functional component.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Sustainable – The Intrado NG9-1-1 functions and services are extensible and scalable based on the component architecture approach and application server complex models. Ingress paths to end sites are expandable by adding IP network connectivity to each site and the NG9-1-1 functional components. Additional sites may be added to the network by connecting them to the ESInet cloud. The core i3 systems of the solution have high capacity Ethernet connectivity to the redundant MPLS carriers serving the state ESInet. The Emergency Call Routing Function (ECRF) and Emergency Call Routing Function (ESRP) components are designed to handle significantly more traffic than planned for Indiana, and their redundant and geographically distributed architecture provides a highly available application environment. Any requirements to increase capacity beyond initial deployment are strictly limited to business contractual agreement. The architecture elements, interworking protocols, and network connectivity lend themselves to expansion while still achieving high reliability processing. **Self-healing** – the Intrado A9-1-1 solution is self-healing as every PSAP has connectivity to the geographically-diverse NGCS core sites and diverse aggregation centers. Network connectivity is provided by Intrado MPLS network and is guaranteed to be diverse and redundant.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 9	**Emergency Services IP Network (ESInet)** **Special Construction** Bidder is responsible for any fees incurred through system commissioning, construction permits, make-ready costs, and other subcontracted activity. **Use of Existing Network Assets** There is already a microwave network in place that may be used as a backup network, as well as other local and state-owned network assets that may be suitable for inclusion in the ESInet. The final network design may make use of any of these facilities that are determined by the bidder to be suitable for inclusion in the ESInet. The bidder may support the router configuration necessary to make use of these facilities. **Network Design Documentation** Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end-state designs for the ESInet.	X			
	Bidder Response: **Special Construction** – Intrado has not been able to acquire a quote for the creation of new entrances into each region facility due to the timelines. If chosen, Intrado will commit to providing quotes to the State and implement (if desired) those network buildouts at 10% cost markup to cover management resources. Intrado does believe that the Intrado-proposed network solution will provide the necessary redundancy and diversity required for a 99.999% available system at a fraction of the costs it would take to buildout physical diverse entrances and lay new fiber-optic cable to redundant and diverse end offices. **Use of Existing Network Assets** – Intrado supports the use of additional redundancy and diversity the State may have to offer. Evaluations will need to be completed to determine the dependability of the network (public safety grade), demarc locations, delegation of responsibilities, and maintenance/escalation procedures. Intrado looks forward to understanding any/all possibilities of making the Nebraska ESInet a more available and reliable infrastructure. **Network Design Documentation -** Below is a high-level diagram of the network design for the State of Nebraska.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

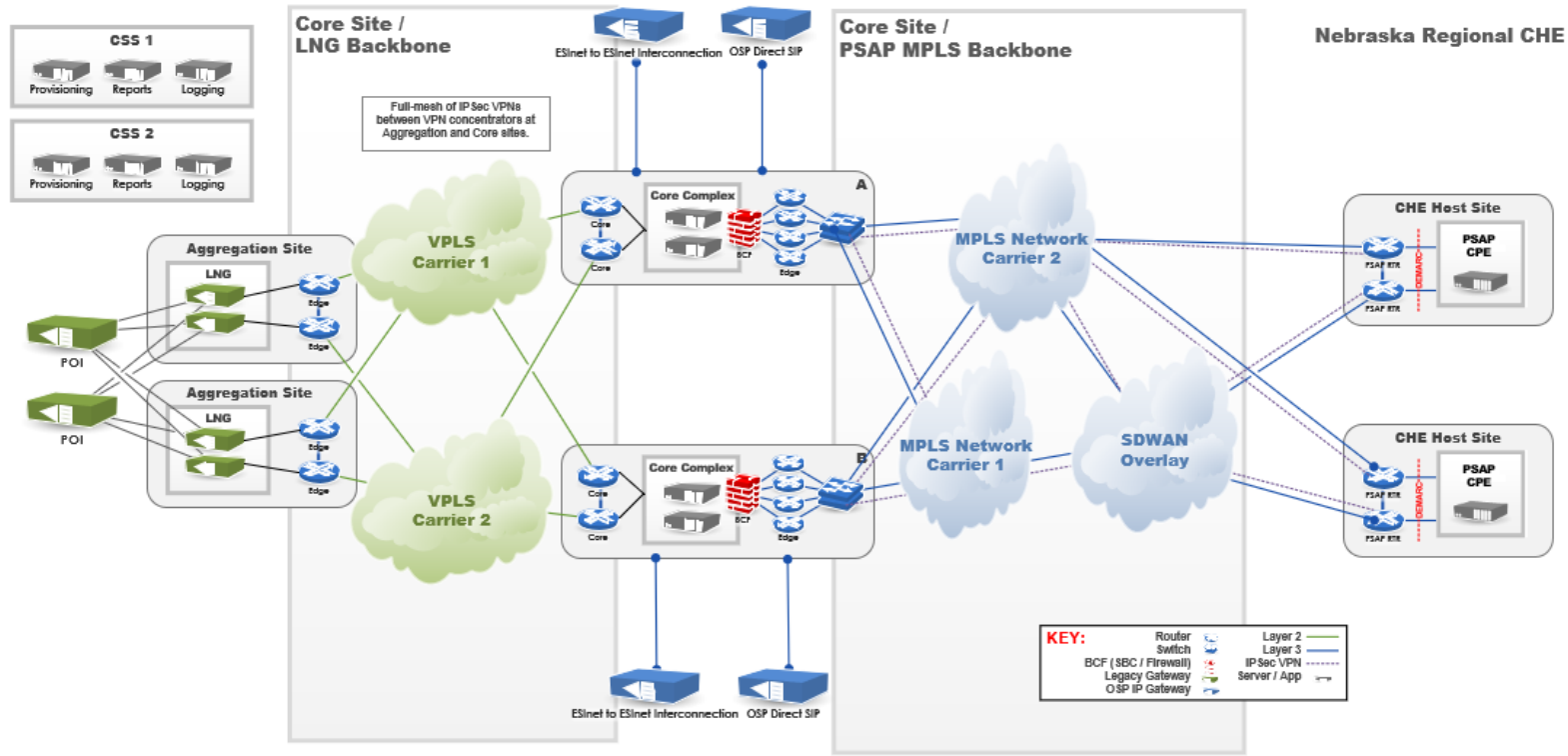

Figure 14: A9-1-1 Routing Core Site Architecture

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 10	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** Contractor shall provide an ESInet solution capable of interfacing with neighboring state and regional NG911 IP networks as they are established, and capable of transferring voice and data between PSAPs. Describe how the solution will meet these requirements.	X			

Bidder Response:

Seamless interworking between A9-1-1 and other neighboring ESInets that serve their clients with either IPSR (pre-i3) and/or a full i3 solution is accomplished by adhering to NENA standards. The below ESInet-to-ESInet specifications define interface specifications for both pre-i3 and i3 for maximum flexibility to exchange traffic with neighboring NG9-1-1 IP networks.

- *ESInet to ESInet Interface Specification SIP Basic_v.3.1*
- *ESInet to ESInet SIP Interconnection Specification i3_v.3*

The pre-i3 specification defines how Intrado will interface with an IPSR service that is not yet ready for direct ESRP to ESRP call management. This specification leverages direct dial telephone numbers to forward transfers and conferences to the appropriate PSAP.

The i3 specification defines how Intrado will interface with the Upstream Emergency Services Routing Proxy (U-ESRP) and Downstream ESRPs (D-ESRPs) in another Emergency Services IP network (ESInet). This interface is based on the requirements defined in the NENA i3 Functional and Interface Specification STA-010.2 (formerly 08-003) and related RFCs. Variations and exclusions from the NENA i3 specification are identified in the document. Intrado is an active participant in the NG911 Interstate Playbook commissioned by 911.Gov and managed by Mission Critical Partners. We have recently completed interoperability testing with another NG 9-1-1 service provider to support interstate transfers and conferences. Test results are available upon request.

Both specification documents are located in the *Proprietary Information* file submitted with the Intrado response.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 11	**Emergency Services IP Network (ESInet)** **Provide Network to Network Interface with Other IP Networks** **Connecting to Other IP Networks** At such time as neighboring ESInets and NGCS systems are able to interconnect and exchange traffic, Contractor shall establish such connections and provide routing and security to allow traffic to be exchanged with neighboring ESInets and NGCS systems, regardless of the respective vendors of those systems. Describe how the solution meets or exceeds the above requirement.	X			

Bidder Response:

The proposed A9-1-1 solution is a complete, end-to-end managed and hosted NG 9-1-1 solution that provides an i3 ESInet that is fully interoperable with neighboring non-Intrado ESInets as well as with legacy networks.

The Intrado solution provides interconnection to a variety of networks and physical locations. These include, as required, all 9-1-1 calls originating in the State of Nebraska, any/all data centers serving 9-1-1 traffic, any bordering legacy networks, or any bordering regional, state, or national ESInets using IP interconnection, assuming that ESInet follows all NENA i3 standards.

Connecting with Neighboring ESInet/NGCS Providers via IP

Seamless interworking between A9-1-1 and other neighboring ESInets that serve their clients with either IPSR (pre-i3) and/or a full i3 solution is accomplished by adhering to NENA standards. The below ESInet-to-ESInet specifications define interface specifications for both pre-i3 and i3 for maximum flexibility to exchange traffic with neighboring NG911 IP networks.

- *ESInet to ESInet Interface Specification SIP Basic_v.3.1*
- *ESInet to ESInet SIP Interconnection Specification i3_v.3*

The pre-i3 specification defines how Intrado will interface with an IPSR service that is not yet ready for direct ESRP to ESRP call management. This specification leverages direct dial telephone numbers to forward transfers and conferences to the appropriate PSAP.

The i3 specification defines how Intrado will interface with the Upstream Emergency Services Routing Proxy (U-ESRP) and Downstream ESRPs (D-ESRPs) in another Emergency Services IP network (ESInet). This interface is based on the requirements defined in the NENA i3 Functional and Interface Specification STA-010.2 (formerly 08-003) and related RFCs. Variations and exclusions from the NENA i3 specification are identified in the document.

Both specification documents are located in the *Proprietary Information* file submitted with the Intrado response.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado is an active participant in the NG9-1-1 Interstate Playbook commissioned by 911.Gov and managed by Mission Critical Partners. We have recently completed interoperability testing with another NG 9-1-1 service provider to support interstate transfers and conferences. Test results are available upon request. **Connecting with Neighboring ESInet/NGCS Providers via TDM** Intrado will use a NENA-compliant Legacy Selective Router Gateway (LSRG) to support egress, transfers and hand-offs from neighboring 9-1-1 Service Providers that do not have IP infrastructures. The LSRG provides gateway functionality between legacy SRs and i3 ESInets. Intrado also provides a PSTN gateway to reach entities that are not served by an ESInet.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 1	**Next Generation Core Services Elements (NGCS)** Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end state for the Commission's ESInet and NGCS, taking into account the hosts and PSAPs listed in Attachment A - PSAP Host End-Point Locations. The following functional elements and services be included: a. Originating Service Provider (OSP) Connectivity; b. Legacy Network Gateway (LNG); c. Border Control Function (BCF); d. Emergency Services Routing Proxy (ESRP); e. Policy Routing Function (PRF); f. Emergency Call Routing Function (ECRF); g. Location Validation Function (LVF); h. Spatial Interface (SI); i. Location Database (LDB); j. Discrepancy Reporting; k. Logging and Recording; l. Time Server; m. Alarm Integration; and, n Message Session Relay Protocol (MSRP). **Originating Service Provider (OSP) Connectivity** **Due Authorization** Bidder shall possess a certificate of public necessity to operate as a telecommunications provider in the state of Nebraska. The Contractor shall provide a copy of current certificate of public necessity prior to award of contract. **Identification of Service Providers Connected to the Legacy Selective Router** Contractor shall be responsible for identifying and for connecting all wireline, wireless, Voice over IP (VoIP), telematics, and other third-party service providers currently connected to the existing legacy selective router. Contractor shall be responsible for updating this information quarterly for the term of the contract. Bidder shall identify each service provider that will be utilized by Contractor..	X			
	Bidder Response:				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Intrado A9-1-1 Routing Core Site Architecture

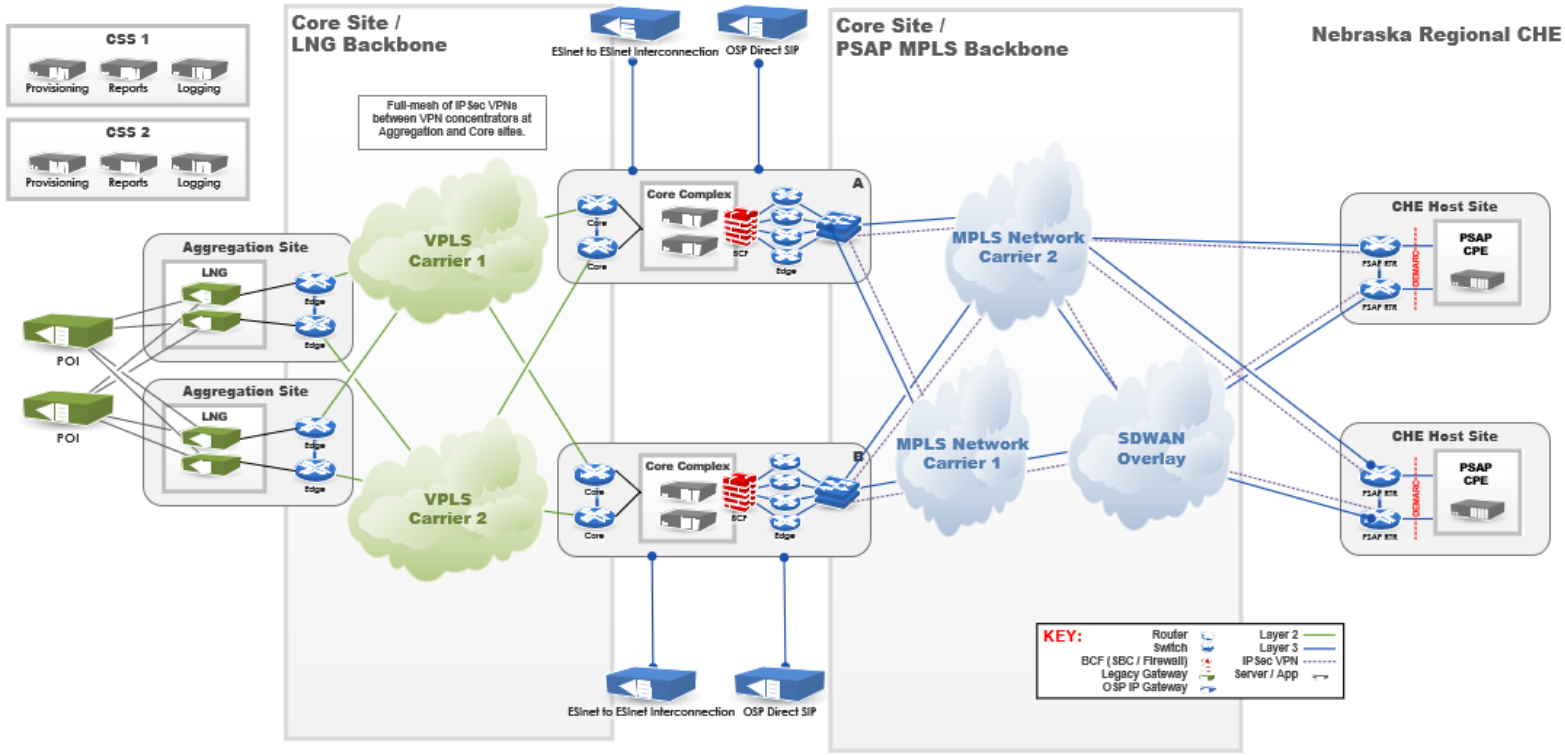

Figure 15: End-to-End A9-1-1 NGCS and ESInet

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

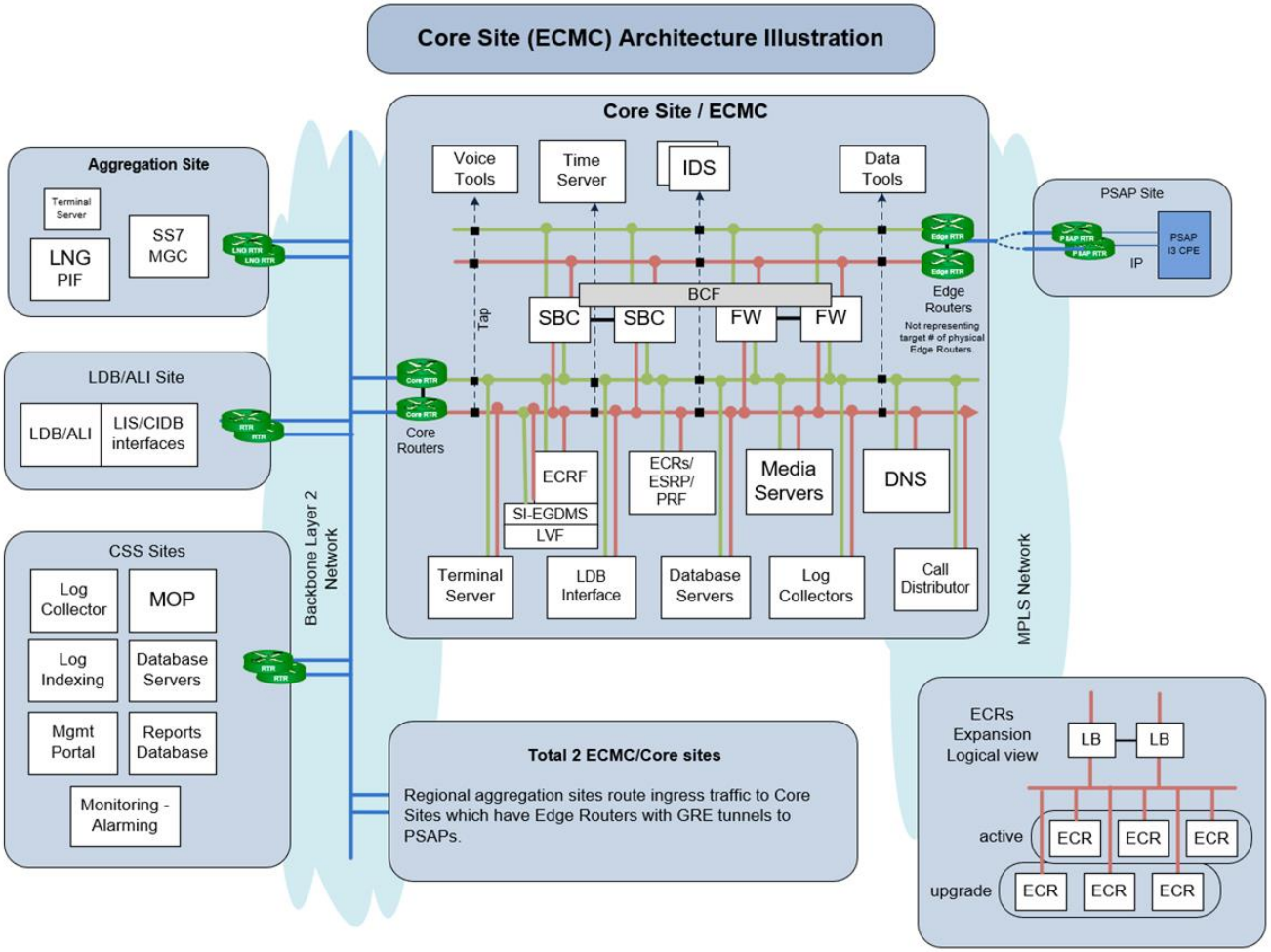

Figure 16: Core Site Architecture with Functional Elements

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

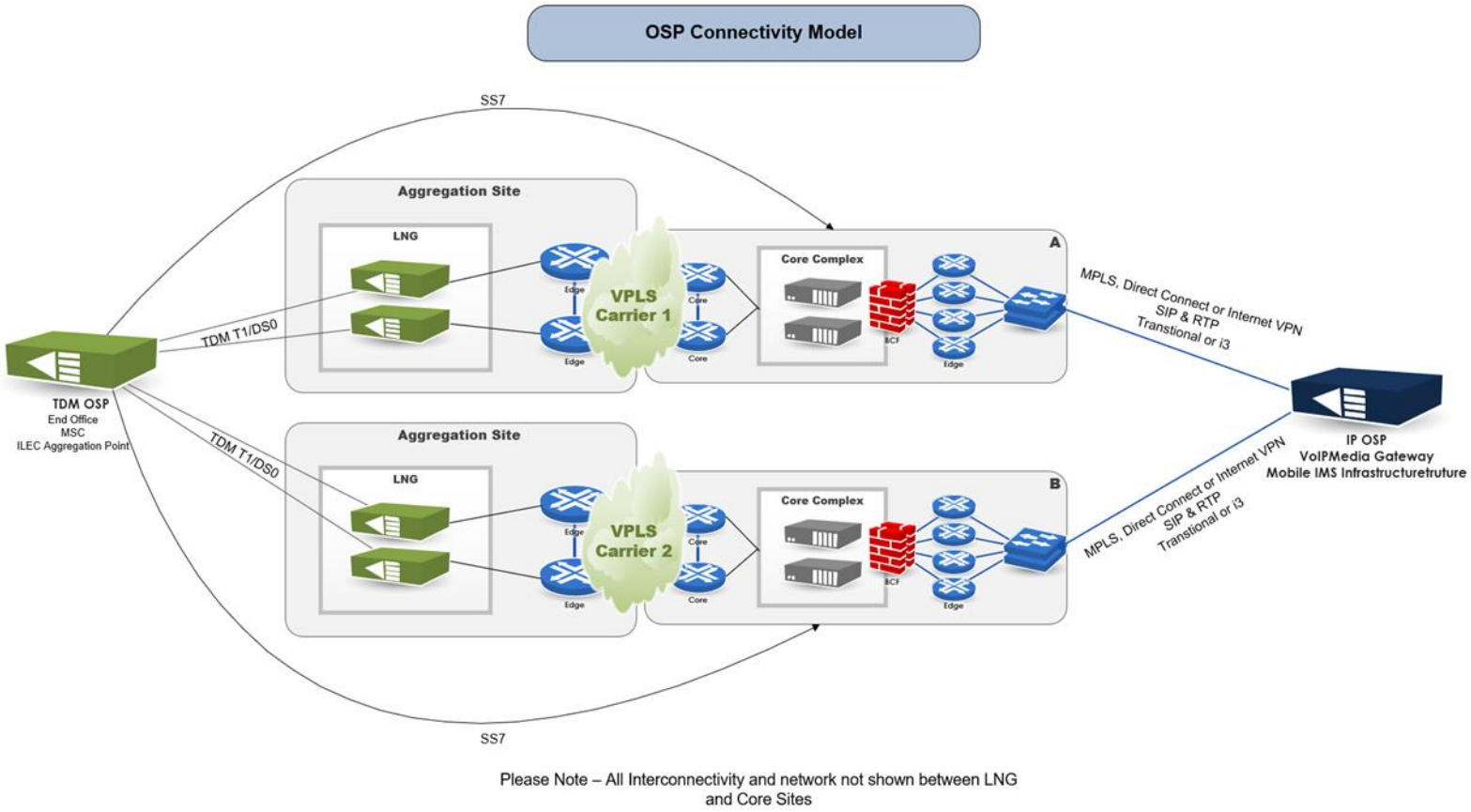

Figure 17: OSP Connectivity Model

Originating Service Provider (OSP) Connectivity
Due Authorization

Intrado is currently an authorized telecommunications provider and will provide a copy of that certification prior to award.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Identification of Service Providers Connected to the Legacy Selective Router Intrado understands and complies with this requirement. Immediately after award, a formal investigation and notification will be completed with all OSPs. As part of the notification, contact information as well as specific interconnectivity options and specifications will be provided to each OSP. The Intrado Technical Project Management team will manage each carrier from initiation through successful deployment. Post deployment, the Intrado Program Manager will responsible for managing additional requirements by OSP, State and PSAP representatives. The Program Manager will track and provide quarterly reports on existing OSP providers serving the State of Nebraska.

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 2	**Next Generation Core Services Elements (NGCS)** **Interconnection and Commercial Agreements, and Trunking** **Originating Service Provider (OSP) Connectivity** Contractor shall be responsible for negotiating interconnection or commercial agreements, and for data and network connection arrangements with each service provider identified in requirement NGCS 1. Interconnection or commercial agreements shall cover subjects including, but not limited to, split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and NGCS, Local Number Portability (LNP), National Number Portability (NNP), and Function of Code R (FoCR). Describe the process and provide timelines for meeting the requirements of this section, as well as the expected process for resolution of disputes.	X			

Bidder Response:

Intrado is a current direct NGCS and ESInet solution provider in many areas across the country. Intrado is a verified CLEC and has created and signed interconnect agreements with both major ILECs that are valid in the state of Nebraska. These agreements detail tandem transfers, split rate center scenarios, and legacy selective router connectivity and interoperation. Additionally, Intrado already has agreements in place with multiple wireless and wireline carriers. For those with whom Intrado does not already have agreements in place, Intrado has a standard process and a dedicated team for negotiation and completion of any/all interconnection and/or interoperability agreements. These include tandem transfers, split rate center scenarios, and legacy selective router connectivity and interoperation.

Intrado currently supports multiple ILEC providers, ALI databases, and fully understands all aspects of LNP, NNP and function of Code R data and processing scenarios. These processes are in place and currently supported by Intrado's LDB/ALI infrastructure. Additionally, steering agreements, and any/all interconnectivity to wireless, VoIP and other mobility solutions are already in place to support the transitional NGCS solution.

Intrado will negotiate interconnection or commercial agreements for data and network connection arrangements with each service provider identified in requirement NGCS 1. Interconnection or commercial agreements shall cover subjects including, but not limited to, split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and NGCS, Local Number Portability (LNP), National Number Portability (NNP), and Function of Code R (FoCR).

The process and timelines for meeting the requirements of this section, as well as the expected process for resolution of disputes are outlined below.

- The Intrado ingress network team is dedicated to onboarding OSPs and provisioning interconnections with other emergency service providers to support PSAP interoperations with external agencies.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• This process begins with analysis of connectivity requirements, project planning, carrier notifications, written and verbal communication of technical information including TDM and IP specification documents and ordering forms, as well as commercial agreements necessary to support the service. • Intrado will work with OSPs to establish any/all processes to submit Service Order Input (SOI) to Intrado's Database Management System (DBMS). Intrado will test and verify that all telephony modifications can take place (Add, Change, Delete, Porting) and that carriers understand the error and statistics files provided after record processing. • Function of Code R is done on an NGCS basis. All processes and procedures for population of foreign databases will occur prior to customer turnup. • OSPs submit circuit orders to connect their end-offices, tandems, or MSCs to at least two geographically diverse POIs on Intrado's network. While OSPs are in the process of direct-connecting their switches to A9-1-1, and in order to migrate PSAPs in the safest and most timely manner, all traffic may be delivered to A9-1-1 from the legacy selective routers (LSRs) via TDM or IP connections for an interim period. This approach supports extensive PSAP testing and implementation soak-time, while not delaying the service transition until the last OSP completes their connectivity to the new system. • As a mature service, TMD connectivity is standard for most carriers. OSPs order and provision emergency service circuits to the Intrado A9-1-1 network by submitting an access service request (ASR) via email form. When an OSP connects its facilities to the POIs, Intrado tests and turns-up the circuits with the carrier to ensure continuity. At each step of testing, the parties conduct troubleshooting until successful results are achieved and documented. Both parties then provision the trunk orders and submit SS7 signaling orders to TNS in parallel. • Intrado's standard interval for TDM trunk orders is 20 business days. On the due date, Intrado contacts the OSP to conduct trunk group testing, whereupon the OSP can cut-over traffic to A9-1-1 and conduct call-through testing to the PSAP to confirm routing, location display, and call quality. This same process supports OSP submission of Moves (maintenance, circuit grooms); Adds (additional circuits or PSAP trunk groups), Changes (augment or decrement trunk groups), or Deletes (Disconnects) as public safety or OSP business needs require. • Many of the TDM connection activities as they pertain to planning, communications, and ordering are applicable to establishing IP ingress to A9-1-1, while OSPs and Intrado execute different technology-specific process steps. For IP ingress, OSPs establish circuit connectivity to 2 geographically diverse POIs. In parallel, Intrado's ingress network team works with each OSP to understand the network configuration the carrier plans to implement based on its switch technology and chosen options for implementing the IP interface specification. Intrado and the OSP

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	provisions the service, tests, and the OSP cuts-over traffic and conducts call-through testing to the PSAP to confirm routing, location display, and call quality. After initial OSP IP connectivity to A9-1-1, Moves, Adds, Changes, and Deletes follow a similar process, but generally require only application table-updates, saving the time and cost of provisioning physical circuits. TDM and IP ingress connectivity are proactively monitored by the Intrado NOC, which also acts as the single point of contact for any PSAP or OSP reported ingress network troubles. Below are the general timeframes for turn-up of a customer. Times can vary based on customers priority • OSP Data Establishment (SOI/ALI/LDB)occurs in 3 months. • OSP Network setup and testing 4-6 months

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 3	**Next Generation Core Services Elements (NGCS)** **Originating Service Provider (OSP) Connectivity** **Management of OSP Connectivity** Contractor shall be responsible for managing moves, adds, changes, and deletions of the connections from the OSPs to the Contractor's systems for the term of the contract. Contractor shall allow for both Time-Division Multiplexing (TDM) and IP ingress to the network, proactively monitor these connections, and work with the respective service providers to resolve problems as they arise. Describe the process and provide timelines for meeting these requirements.	X			

Bidder Response:

Intrado will manage moves, adds, changes, and deletions of the connections from the OSPs to the A9-1-1 systems for the term of the contract.

Intrado will support both Time-Division Multiplexing (TDM) and IP ingress to the network, proactively monitor these connections, and work with the respective service providers to resolve problems as they arise.

A9-1-1 supports both TDM and IP OSP ingress at geographically distributed POIs. A9-1-1 supports standards-based protocol interfaces to external ESInets for call hand-off and call transfers.

A9-1-1 service supports TDM SS7 calls from Originating Service Providers (OSP) as the standard ingress signaling configuration. Other signaling options such as PRI and CAMA can be supported upon request. The ESInet standard interfaces supported are listed below.

- 9-1-1 Call Signaling Type
- SS7 Wireline/NCAS (10 digits)
- PRI/NI-2 (wireline, NCAS)
- Analog CAMA I+7 (I always = 0)
- DS1 CAMA I+7 (I always = 0)
- DS1 CAMA 7 (No I digit)

A9-1-1 also supports SIP ingress for both transitional (basic) and i3-ready originating service providers. The transitional solution allows for SIP and RTP with the Calling party number. The Calling party number is used to query the Intrado provided LDB, and uses transitional methods to acquire callback number and location information for wireless and VoIP callers.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado has designed and tested i3 solutions internally and with carriers and is prepared to deploy when the carriers are ready. Both the *Originating Service Provider (OSP) Network Interface Specification SIP Basic_v.2.1* and the *OSP SIP NNI i3_v.2* documents are provided with Intrado's response in the *Proprietary Information* file. The process and estimated timelines for meeting these requirements are listed below. • The Intrado ingress network team is dedicated to onboarding OSPs and provisioning interconnections with other emergency service providers to support PSAP interoperations with external agencies. • This process begins with analysis of connectivity requirements, project planning, carrier notifications, written and verbal communication of technical information including TDM and IP specification documents and ordering forms, as well as commercial agreements necessary to support the service. • OSPs then submit circuit orders to connect their end-offices, tandems, or MSCs to at least (2) geographically diverse POIs on Intrado's network. While OSPs are in the process of direct-connecting their switches to A9-1-1, and in order to migrate PSAPs in the safest and most timely manner, all traffic may be delivered to A9-1-1 from the legacy selective routers (LSRs) via TDM or IP connections for an interim period. This approach supports extensive PSAP testing and implementation soak-time, while not delaying the service transition until the last OSP completes their connectivity to the new system. • As a mature service, TMD connectivity is standard for most carriers. OSPs order and provision emergency service circuits to the Intrado A9-1-1 network by submitting an access service request (ASR) via email form. When an OSP connects its facilities to the POIs, Intrado tests and turns-up the circuits with the carrier to ensure continuity. At each step of testing, the parties conduct troubleshooting until successful results are achieved and documented. Both parties then provision the trunk orders and submit SS7 signaling orders to TNS in parallel. • Intrado's standard interval for TDM trunk orders is 20 business days. On the due date, Intrado contacts the OSP to conduct trunk group testing, whereupon the OSP can cut-over traffic to A9-1-1 and conduct call-through testing to the PSAP to confirm routing, location display, and call quality. This same process supports OSP submission of Moves (maintenance, circuit grooms); Adds (additional circuits or PSAP trunk groups), Changes (augment or decrement trunk groups), or Deletes (Disconnects) as public safety or OSP business needs require. • Many of the TDM connection activities as they pertain to planning, communications, and ordering are applicable to establishing IP ingress to A9-1-1, while OSPs and Intrado execute different technology-specific process steps. For

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	IP ingress, OSPs establish circuit connectivity to 2 geographically diverse POIs. In parallel, Intrado's ingress network team works with each OSP to understand the network configuration the carrier plans to implement based on its switch technology and chosen options for implementing the IP interface specification. Intrado and the OSP provisions the service, tests, and the OSP cuts-over traffic and conducts call-through testing to the PSAP to confirm routing, location display, and call quality. After initial OSP IP connectivity to A9-1-1, Moves, Adds, Changes, and Deletes follow a similar process, but generally require only application table-updates, saving the time and cost of provisioning physical circuits. TDM and IP ingress connectivity are proactively monitored by the Intrado NOC, which also acts as the single point of contact for any PSAP or OSP reported ingress network troubles.

Any additional documentation can be inserted here

NGCS 4	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **LNG Description** The LNG is a signaling and media interconnection point between callers in legacy call-originating networks, i.e., Enhanced 911 (E911), and the NENA NG911 i3 architecture. The LNG shall log all calls it receives and processes and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (TDM) and the IP side of the LNG shall be logged. The LNG shall have Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) functionality to detect and mitigate Distributed Denial of Services (DDoS) attacks from both the TDM side and the IP side. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The Intrado LNG is a fully NENA-compliant signaling and media interconnection point between callers in legacy call-originating networks, i.e., Enhanced 9-1-1 (E9-1-1), and the NENA NG9-1-1 i3 architecture. The Intrado LNG collects full detail on all calls received on TDM interfaces and transmitted to upstream IP resources. LNG call detail records are transmitted in real-time to the A9-1-1 management systems for reporting and analysis. The system readily supports ad hoc access to log files for troubleshooting and incident response. All call activity on both the legacy side (TDM) and the IP side of the LNG is logged. The A9-1-1 system has intrusion detection system (IDS)/intrusion prevention system (IPS) functionality to detect and mitigate telephony denial of service (TDoS) attacks.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 5	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** Contractor shall provide redundant, resilient LNGs with legacy selective router gateway (LSRG) functionality to allow the legacy selective routers to transfer calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to deployed NGCS and vice versa. Legacy functionality and components shall be in place and operational during the NG911 transitional phase until all 911 authorities and PSAPs served by the legacy selective router have completed the transition. Describe the steps bidder will take to meet the transition timelines and minimize overlapping network costs.	X			

Bidder Response:

Legacy Network Gateway (LNG)

Intrado's A9-1-1 service provides redundant, resilient LNGs with legacy selective router gateway (LSRG) functionality that allows the legacy selective routers to transfer calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to deployed NGCS and vice versa. Legacy functionality and components will be in place and operational during the NG9-1-1 transitional phase until all 9-1-1 authorities and PSAPs served by the legacy selective router complete the transition.

The A9-1-1 Legacy Network Gateways (LNG) perform the following functions.

- The LNG provides a bridge between existing 9-1-1 call origination networks and the ESInet.
- The LNG provides a legacy selective router type interface towards the origination network (such as ISUP or CAMA), and provides a SIP interface towards the ESInet.
- The LNG performs TDM to IP protocol conversion which is an excellent security layer. MPLS is leveraged to segregate IP networks (VRFs) from the TDM ingress sites to the Core call processing sites. Virtual routing and forwarding links (VRFs) VRFs from the LNG to the Core are trusted and can communicate directly with the call processing functions. The LNG LIF will query through a firewall if supporting an external ALI for location queries.
- The LNG supports i3 routing. Location is retrieved for each call which then use the polygon boundaries in the ECRF and the routing policies in the PRF for final PSAP determination.
- The LNG supports location retrieval and uses the HELD interface for Location by-Reference queries by the i3 functional elements.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	The LNG is a standard component of the A9-1-1 solution as long as legacy origination networks are deployed and require TDM access. The LSRG is a signaling and media interconnection point between callers in the legacy originating networks and the NG A9-1-1 service. The LSRG converts calls from TDM to SIP and SIP to TDM signaling for ingress and egress to A9-1-1. The LSRG provides an interface between a 9-1-1 selective router and the ESInet, enabling calls to be routed and/or transferred and/or handed-off between legacy and A9-1-1. A call hand-off may be required when A9-1-1 receives a call that should be rerouted to a legacy foreign selective router. Externally facing TDM connections inherently mitigate TDOS impact to the core ESInet and NGCSs. A9-1-1 interconnects to Legacy Selective Routers to transfer and/or receive calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information through the LSRG. Interconnections will also allow legacy PSAPs served by legacy selective routers to serve as the abandonment route for A9-1-1 PSAPs served by the A9-1-1 solution. This configuration is enabled with the approval of the PSAP. Upon contract award, Intrado will work to ensure that both timelines are met and that overlapping network costs are minimized. Immediately after award, Intrado will begin ordering the necessary connectivity and equipment for the Nebraska regional LNG's. In parallel, the Intrado project management team will notify the carriers and begin reach out and education on the interconnectivity methodology and options. This dual approach will allow Intrado and the state to deploy quickly, while migrating the carriers simultaneously. This allows the State to go-live independent of OSP status, with the understanding that the providers will have multiple options and the support of an experienced management team as to how to proceed with the migration. With a Next Generation solution comes many opportunities. Intrado will work with the IP capable carriers to help them understand that with IP/SIP comes opportunity to not only provide a more reliable, redundant, and diverse solution but also cost-saving options which allow them to reduce TDM trunking and management costs. Over the last 20 years, Intrado has performed thousands of PSAP, OSP, and core 9-1-1 migrations. The two-phased approach allows the PSAPs to benefit from the advantages of Next Gen applications and network immediately. Since the OSP methods, costs, and management are not under the control of the State or Intrado, Intrado will provide the means for the carrier to connect in a legacy fashion as well as educate them on how transitioning to an IP infrastructure can not only help the OSPs provide a better and more reliable 9-1-1 system, but also save them time, effort and cost in the future.

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 6	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Previous Work on Similar Solutions** 1. Explain how bidder has worked with legacy OSPs with similar solutions on similar projects. 2. Submit specific plans for working with established legacy 911 service providers in Nebraska..	X			

Bidder Response:

1. Intrado's proposal provides the State with a comprehensive solution for an Emergency Services IP Network (ESInet) with NENA i3 core functional elements, interoperability with neighboring regional ESInets, and interoperability with legacy selective routers. The proposed solution provides standards-based network interfaces that interoperate with other ESInets via secure and highly reliable facilities. Intrado participates and monitors standards activities to ensure that the solution evolves with national industry standards.

2. Recognizing the imperative for PSAP operations to continue uninterrupted during the system implementation process, Intrado's project methodology outlines in detail the communication and activities necessary to ensure a safe and timely migration of services while special attention is given to identifying and implementing the network arrangements necessary to support all aspects of ongoing PSAP interoperations with the legacy 9-1-1 service provider.

Prior to implementation Intrado will work with OSPs to arrange inter-tandem trunking that is intended to initially deliver all 9-1-1 calls from the legacy selective routers to the ESInet on a rolling basis as PSAPs transition to the new system.

During the implementation process, the inter-tandem trunks will be used to

- Deliver all 9-1-1 calls intended for the PSAP transitioning to the ESInet
- Interoperate with the legacy selective routers to support E9-1-1 call transfers and hand-offs for PSAPs that are not yet migrated to the new system
- Ensure delivery of calls originating from split rate centers to the correct PSAP

The inter-tandem capacity will remain in-service until the majority of OSP traffic has been re-homed directly to the ESInet so that some proportion of the inter-tandem trunks can be disconnected or re-used for subsequent PSAP migrations.

Major activities and milestones achieved in the course of arranging legacy 9-1-1 service provider interconnectivity with the ESInet include all steps executed for other OSPs described above, plus the following:

- Determine PSAP interoperations requiring E9-1-1 transfers and hand-offs
- Conduct legacy 9-1-1 service provider planning calls

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Create legacy 9-1-1 service provider interconnection architecture • Order circuits create and exchange legacy 9-1-1 service provider trunk orders • Test and turn-up legacy 9-1-1 service provider connectivity • Conduct non-live PSAP interoperations testing • Create and execute legacy 9-1-1 service provider cut-over plan During the coordination phase, the joint Intrado and Customer team members verify legacy and existing service installations to include in the system migration. Implementation requirements are documented and refined and updated in the overall solution architecture Working closely with stakeholder groups, the project team designs provisioning plans specific for each PSAP and OSP including incoming trunk route plans, bridge lists, and dialing plans. Additionally, the documentation team and training developers customize the user and process documents and various training courseware, to specifically meet the needs of the customer.

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 7	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Traffic Engineering Process** Describe the process that will be utilized to analyze the current trunk engineering for 911 traffic, and to validate any applicable trunk rebalancing for public-safety grade service.	X			
	Bidder Response: Intrado has developed multiple technologies and solutions sets that allow the carriers to connect to the core infrastructure. Intrado will manage this process and the associated options with the carriers directly. That being said, the choice on how and what bandwidth the carrier will use to connect to Intrado is their decision. Typically, the decision is made based on recommended NENA guidelines (1 DS0 per 10K wireline records) or population/call volume served by a particular cell tower geographic area. The connectivity to the regional LNGs will far exceed the needs of Nebraska, as it currently accommodates 1000 simultaneous calls. Intrado will recommend that all carriers support the appropriate TDM bandwidth to each LNG for legacy TDM traffic or MPLS connectivity to the Intrado core infrastructure for transitional and/or i3 traffic. Additionally, the guideline to connect to geodiverse and redundant POI locations will be highly recommended. Intrado will work with the carriers to examine current configurations and bandwidth and will assist with recommendations on how to augment these configurations if necessary. Our recommendations include estimates and calculations derived from over 15 years of supporting NGCS, wireless, and VoIP voice solutions, including estimates based on current PSAP position capacity, legacy CAMA capacity, and estimated busy hour statistics. Additionally, Intrado will provide a “real world” approach in that it is understood that there is a limitation to what the PSAP infrastructure can truly handle and whether or not it makes sense to over-engineer the incoming trunks with that limitation. Intrado prefers that all default and alternate routing is handled by the NGCS solution, understanding the multiple options that the Intrado system has for routing calls. With these important aspects to keep in mind, Intrado will be available to the OSPs to walk them through the benefits and drawbacks of each scenario - understanding that the OSPs themselves are responsible for the final solution. Intrado will continue to work with the carriers through the term of the service to assist in adjusting configurations when call traffic needs rebalancing. Testing will occur prior to any deployment of a carrier solution to verify all connectivity paths are up and available, alternate paths are available, and proper failover is configured.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 8	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Location Information** The LNG shall obtain location information to define, create, populate and send the correct Presence Information Data Format Location Object (PIDF-LO) parameter to the correct ESRP or terminating PSAP, as described within NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The LNG obtains location information to define, create, populate and send the correct Presence Information Data Format Location Object (PIDF-LO) parameter to the correct ESRP or terminating PSAP, as described within NENA-STA-010.2-2016. The ESRP processes ingress calls received using Session Initiation Protocol (SIP) signaling with location embedded in the PIDF-LO from i3 compliant carrier networks, from legacy carriers, or selective routers via the LNG/LSRG or from an upstream i3-compliant ESInet. For calls from legacy carriers, or legacy selective routers that ingress via the LNG , the location interwork function is used to retrieve location from an Intrado location database. We are able to retrieve both location by-value and location by-reference. We also support foreign location databases such as an ALI service by another provider. The Intrado system creates the PIDF-LO and inserts the location. Our method for location retrieval is NENA-compliant. We support the HELD interface The PIDF-LO is be delivered to the PSAP within the SIP messaging. The HELD interface is also supported from the PSAP CPE to provide location updates for wireless and other call types.				

Any additional documentation can be inserted here:

	-				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 10	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Protocol Conversion** **External Interfaces** The LNG external interfaces shall comply with NENA-STA-010.2-2016, requirements SLA 1-23, and other applicable standards and requirements. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: A9-1-1 service supports TDM SS7 calls from Originating Service Providers (OSP) as the standard ingress signaling configuration. Other signaling options such as PRI and CAMA can be supported upon request. The ESInet interface options are listed below. • 9-1-1 Call Signaling Type • SS7 Wireline/NCAS (10 digits) • PRI/NI-2 (wireline, NCAS) • Analog CAMA I+7 (I always = 0) • DS1 CAMA I+7 (I always = 0) • DS1 CAMA 7 (No I digit) The A9-1-1 LNG complies with all applicable requirements outlined in SLA 1 through 23.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 11	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Baudot Code Transcoding** The bidder's BCF solution shall support transcoding of Baudot tones to real-time text (RTT), as described in IETF RFC 4103. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Intrado understands and complies with this requirement. The Intrado Border Control Function supports the Baudot to TTY transcoding as described in RFC 4103. TTY calls will be transcoded via the SBC component of the BCF. Interaction between the citizen caller and the PSAP is supported for the duration of the call.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 12	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Callback Number** The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the Contractor to obtain the callback number from the wireless or VoIP provider and may include additional recurring and non-recurring costs that are independent of this RFP. The Contractor shall be responsible for all recurring and non-recurring costs associated with this requirement. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 LNG supports obtaining the callback number associated with any pseudo ANI data that does not include the callback number. A9-1-1 retrieves the callback number via an ADR-HELD query to a location database. Queries to the wireless or VoIP providers are provided at no additional charge to the State of Nebraska. In some cases, the query to the Wireless carrier will be a null result. Prior to the carrier's transition to i3, Intrado will continue to manage the location data retrieval on behalf of the OSP per the NENA standard. The Intrado solution leverages the existing VoIP and Wireless legacy location and additional data solutions during the transitional period while those carriers work towards i3 readiness. Prior to i3 readiness, the provider will continue to send the pseudo ANI with the originating call to the A9-1-1 LNG. Once received by the LNG, the A9-1-1 solution will perform the proper NIF, LIF, and PIF functions to query the Intrado-managed LDB and steer queries to the external OSP location database to acquire the callback number and location information. This solution is in production with multiple live Intrado-managed i3 PSAPs.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 13	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Event Logging** The LNG shall facilitate logging of all significant events and 911 calls received and processed. Each call log shall contain all relevant parameters defined in Section 5.13.3 of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The LNG facilitates logging of all significant events and 9-1-1 calls received and processed. Each call log shall contain all relevant parameters as defined in NENA STA-010.2-2016. A9-1-1 provides an i3 logging capability per the NENA STA-010.2 specification. The system supports near real-time log delivery and web service interfaces for log retrieval from authorized clients. The A9-1-1 solution logs hundreds of data points for each call that traverses the system to assist in tracking and troubleshooting calls. Logged events include ingress and egress to the system, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. Detailed call traces are available on demand and are available within 20 seconds of a call initiating. The Customer Management Portal provides participating PSAPs and approved personnel 24x7 access to call detail records through a secure, web-based portal. The call detail records provide the user with all of the pertinent information for each call. Users have a predetermined PSAP or set of PSAPs for which they are able to view statistics. For example, some users will only be able to view their own PSAP's statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping. Event data is time stamped upon ingress of payload entry through the LNG or BCF and at the time of answer and disconnect at the PSAP. Event data also tracks the time for each functional element to perform routing and PSAP assignment, by tracking the time it takes to traverse from the BCF through the ESRP to the PSAP. This event data tracking by functional element allows for call diagnostics.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 14	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Extraction of Log Files** All LNG log files shall be capable of being extracted in near real-time and shall be in a format suitable for importing into a spreadsheet or word-processing program. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: LNG log files are capable of being extracted in near real-time and are available in a format suitable for importing into a spreadsheet or word processing program.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 15	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **High-Availability Design** The LNG solution shall be deployed in a high-availability design to meet public safety-grade resiliency and redundancy requirements, Section V.D.1.b. (General Requirements – Technical – Public Safety Grade). Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: All network infrastructure components are designed and deployed in an N+1 model. N+1 redundancy provides a minimum of one additional unit, module, path, or system in addition to the minimum required to satisfy the base connectivity, ensuring that a failure of any single component at a given diverse site, such as an LNG, will not render the location inoperative. All network connectivity is established via dynamic routing protocols. The use of dynamic routing protocols allows the routers to automatically discover each connected network and adapt to changes in the network topology.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 16	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Legacy Selective Router Gateway (LSRG) Functionality** The LSRG functionality shall support selective transfer, commonly referred to as “star code” transfers, made by legacy PSAPs for calls destined for the NextGen911 PSAPs or to neighboring legacy PSAPs outside of the ESInet. Describe how bidder’s LNG solution provides for LSRG functionality.	X			
	Bidder Response: The LSRG provides an interface between a 9-1-1 selective router and the ESInet, enabling calls to be routed and/or transferred and/or handed-off between legacy and the next generation emergency networks. A call hand-off may be required when the ESInet receives a call that it deems should be rerouted to a legacy foreign selective router. Two or three-digit star codes are supported for ESN-based routing with A9-1-1 IP Selective Routing. A9-1-1 supports star code transfers made by legacy PSAPs for calls destined for PSAPs on the ESInet or to neighboring legacy PSAPs outside of the ESInet. A call taker can use a single button on the call taker’s display to complete either a transfer or three-way conference. They can transfer an incoming 9-1-1 call to another agency by pressing a button labeled with the type of agency; for example, "Fire"-on the PSAP premises equipment. These transfers use pre-provisioned codes on a per-PSAP basis.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 17	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Proposed LNG Locations** Provide the proposed locations for hosting the primary LNGs for the NextGen911 system, including the data center tier level for the host sites.	X			
	Bidder Response: The proposed locations for hosting the A9-1-1 LNGs are below. Both are classified as Tier 3 facilities. 1623 Data Center 1623 Farnam St Omaha, NE 68108 Sharp Data Center 206 S 13th Street Lincoln, NE 68508				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 18	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Charges for Dual Service** The bidder shall be responsible for meeting the timelines outlined above in requirement NGCS 2 and 3. If the transition from the legacy selective routers to NGCS exceeds the committed timeline, and is attributable to the acts or omissions of the Contractor, the Contractor will accept responsibility for financial support of the legacy network until such time as the full transition is complete. Describe how bidder's solution meets this requirement.	X			
	Bidder Response: Intrado understand and complies with the above requirement. If Intrado does not have the necessary equipment, two redundant and diverse POIs, network, processes, and procedures set up in order to accept incoming TDM or SIP traffic from OSPs, Intrado will accept responsibility for financial support of the legacy network.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 19	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Description** The BCF shall provide logical network security functions between external networks and the ESInet, and between the ESInet and PSAP networks. The BCF is responsible for numerous functions, including the following: a. Border firewall; b. VPN; c. IDS/IPS; d. Session Border Control (SBC); e. Opening and closing of pinholes; f. Limiting access to critical components through the use of VLANs; g. Call admission control; h. Media transcoding; i. Signaling protocol normalization and interworking; j. Network Address Translation (NAT); k. Codec negotiation; l. Support for QoS and priority markings; and, m. Media proxy. Provide details, including drawings, describing how the proposed BCF meets or exceeds all functions listed above and the requirements described in NENA-STA-010.2-2016, as well as additional firewall requirements described in NENA 04-503, NENA-INF-015.1-2016, and NENA 75-001, or the next subsequent version of the NENA documents listed that are publicly available at the proposal release date.	X			
	Bidder Response: As part of the A9-1-1 solution, we provide a Border Control Function (BCF) to interface with any non-trusted network components. The BCF provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification. The BCF inspects, modifies and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect, and where the ESInet connects with service provider networks. The BCF mitigates security threats, resolves interoperability problems, and ensures reliable SIP-based communications. It is designed to protect and control real-time voice, video, and text sessions as they traverse networks between callers and Public Safety Answering Points (PSAPs). The core functionality provided by the A9-1-1 BCF under this proposed solution is in alignment with the requirements of the NENA i3 document STA-010.2-2016. Highlights of the key functions provided are:				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- **Border Firewall** – the BCF provides border firewall functionality in accordance with NENA STA-010.2-2016.
- **VPN** – the BCF's SBC supports encryption for calls that are not protected using SSL/TLS or IPSEC VPN.
- **IDS/IPS** - each core emergency call processing site includes security functions such as intrusion detection systems, and intrusion protection systems. Security management personnel specialize in managing and operating these assets and validate their operation.
- **Session Border Control (SBC)** - the SBC supports SIP over Transmission Control Protocol (TCP) primarily User Datagram Protocol (UDP) upon request, and Transport Layer Security over TCP (TLS-over-TCP), As required, the SBC populates Layer 3 headers in order to facilitate priority routing of packets and enables interworking between networks using IPv4 and IPv6.
- **Opening and closing of pinholes** - A9-1-1 BCFs are set to deny by default all traffic. Rules are built into the BCF/firewall such that pinholes between the firewalls will allow trusted/known traffic. Allowances go through rigorous scrutiny before being approved by the NOC/SOC. Once approved, changes are made on a regular basis following standard procedures to ensure no other pinholes are opened. The A9-1-1 NOC/SOC also does on-going traffic studies on the firewalls. If a pinhole is opened but not used, the NOC/SOC will close the pinhole if necessary.
- **Limiting access to critical components through the use of VLANs** – A9-1-1 is a Quality of Service (QoS)-managed private IP network which can prioritize any type of IP traffic; voice, data, and multi-media. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic.
- **Call admission control** – Call admission control (CAC) is used when establishing connectivity to internal and external IP resources.
- **Media transcoding** and **Signaling protocol normalization and interworking** - Below is a detailed list of the various VoIP protocols and established multimedia sessions supported by the Intrado A9-1-1 solution. As designed, the Intrado A9-1-1 solution is evolutionary and will be able to support future i3 specifications. The A9-1-1 infrastructure is created to not only support an IPSR environment, but to support i3 NENA protocols, features, and functions.

  <u>Media Parameters</u>

  - Codecs
    - G.711 – telephony equivalency

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• The Intrado A9-1-1 system performs codec negotiation and upgrades all calls to a codec of G.711
	• Have tested and ready to deploy on demand
	  • G.729
	  • G.723
	  • AMR-WB
	
	• Voice Quality
	  • Adaptive Jitter Buffers
	  • Automatic Gain Control
	  • Echo Cancellation
	  • RCTP-XR
	  • No degradation of MOS score from input to output
	  • Existing deployments have run at > 4.0 MOS score
	
	• MSRP for text
	
	• **Network Address Translation (NAT)** - A9-1-1 uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. The rules are applied when the SBC receives a message, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message.
	
	• **Codec negotiation** - The Intrado A9-1-1 system performs codec negotiation and upgrades all calls to a codec of G.711.
	
	• **Support for QoS and priority markings** - uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic.
	
	• **Media proxy** - The Intrado A9-1-1 solution will perform this function.
	
	In summary the A9-1-1 security architecture employs defenses that include, but are not limited to, stateful packet inspection firewalls, IDS/IPS, multi-factor authentication, strong encryption, anti-virus/anti-malware, and vulnerability/patch

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	management solutions. All inter-zone traffic is restricted to only the necessary protocols/destinations, for both ingress and egress. The network is capable of processing all traffic, but administratively denies protocols identified as a threat, or that otherwise fall outside of pre-defined parameters. This is partially managed via routing tables and/or Access Control Lists (ACLs). Intrado continually investigates and upgrades with new advances in protective technology with tools such as Intrusion Detection System (IDS). The solution incorporates physical, network, and application security principals. Traffic between Core emergency call processing sites and distributed sites (e.g., ingress call traffic, PSAPs, management capabilities) is route- and protocol-secure. A combination of route paths, IP address recognition, limited protocols, VPNs, session border controllers, and firewalls secures the various communication elements of the proposed solution. The following diagram depicts how the A9-1-1 BCF is deployed.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

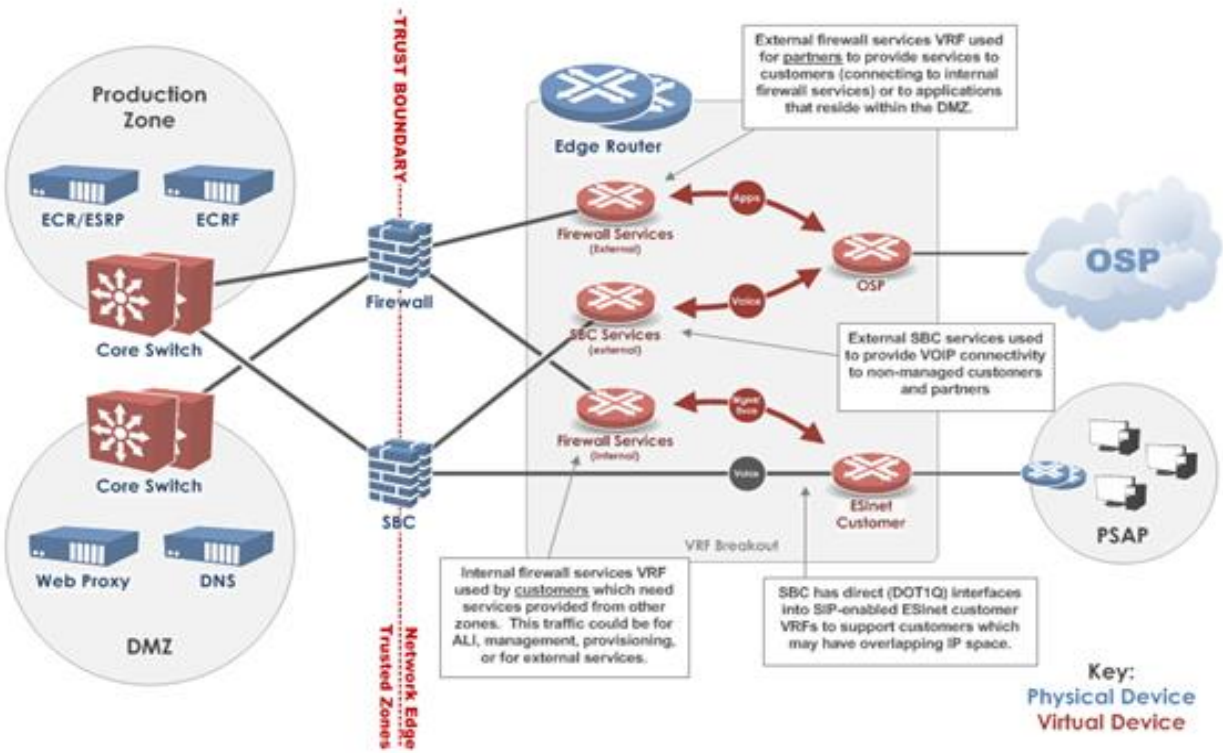

Figure 18: A9-1-1 ESInet Border Control Function

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 20	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **High-Availability Design** The BCF solution shall be deployed in a manner to achieve 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The BCF function is deployed at each of the two geographically-diverse core call processing centers. The redundant n+1 BCF design supports availability of 99.999%.				

Any additional documentation can be inserted here

NGCS 21	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Auditing of System Log Files** Management of the BCF shall include continuous auditing of the system log files for anomalies, and processes for responding to and managing security incidents. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: We monitor and audit all aspects of the A9-1-1 network for threats from a variety of sources. Net flow statistics and packet level capture and forensics are continuously performed. This capability assists in troubleshooting and anomaly resolution as well as providing assurance of reliable performance.				

Any additional documentation can be inserted here

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 22	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Silence Suppression Detection** The BCF shall be capable of detecting when silence suppression is present in the 911 call and of disabling silence suppression if it is detected in the call. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 SBCs are capable of detecting when silence suppression is present in the 9-1-1 call and disabling silence suppression if it is detected in the call. Typically for 9-1-1 calls, an industry best practice is to preserve as much call detail as possible. Techniques such as voice activity detection (VAD) may not be sensitive enough to activate during low audio activity, and important background sounds may be missed. Additionally, some voice detection algorithms may not react in an expedient manner and may cut off the beginning of a word. The following comment is from NENA TID 08-501 in reference to silence suppression: “However, these techniques may not be appropriate for emergency calls in which "background noise" can be an important part of the call (both for the call taker and for logging recording purposes).” To that end A9-1-1 does not enable silence suppression for any calls that use the A9-1-1 service. Currently, when A9-1-1 receives an emergency call with silence suppression requested, the ingress BCF answers with silence suppression disabled. Since we don’t know if silence suppression was active or inactive for the upstream links, disabling silence suppression on the link into the A9-1-1 solution prevents us from potentially being the only link with silence suppression active and dropping potentially important low-level background sounds.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 23	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Call Mediation** The BCF shall mediate all incoming 911 calls from VoIP providers to Session Initiation Protocol (SIP) calls and should be done in accordance with NENA-STA-010.2-2016. Any specific variations or non-compliance with this requirement shall be identified and documented below. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 BCF mediates all incoming 9-1-1 calls from VoIP providers to SIP calls in accordance with NENA STA-010.2-2016 and the ATIS 0700015 standard. The A9-1-1 ingress specifications that support these standards are: • *Originating Service Provider (OSP) Network Interface Specification SIP Basic v.2.1* • *OSP NNI i3 v.2* The specification documents listed above are provided with this response in the *Proprietary Information* file. The A9-1-1 specifications are not only compliant with the NENA and ATIS standards, but also support a transitional approach to accommodate the period until OSPs conform to the prerequisites identified in these standards. This transitional option is referred to as SIP Basic and it emulates a SS7 TDM (gateway) Interface Calls from i3-compliant OSP networks interact with the ESRP and are processed in conformance with the i3 specification. Ingress SIP calls that are not i3-compliant, but instead only include the ANI or pANI (ESRK or ESQK), are also supported via Intrado's SIP Basic interface. This provides maximum flexibility for ingressing calls via IP. The OSP Network SIP Interconnection option accept emergency ingress calls to the ESInet via the BCF using SIP and then processes the call according to the routing logic determined by the 9-1-1 Public Safety Authority. Calls are routed				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	either in conformance with the i3 specification or by equivalent legacy Selective Router logic.				

Any additional documentation can be inserted here:

NGCS 24	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Event Logging** The BCF shall provide the functionality to maintain logs of all 911 sessions and all additional BCF logging and recording requirements, as specified in NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The BCF maintains logs of all 9-1-1 sessions and all additional BCF logging and recording requirements, as specified in NENA STA-010.2-2016. A customer management portal is available for PSAP administrators to view end-to-end CDRs in real time. CDRs include the start time of the call as it enters the ESInet, answer time, end time, digits for ANI and any errors encountered. Additionally, i3 logs from all ESInet i3 components will be available per the NENA STA-010.2 specification. Intrado supports near real-time log delivery and web service interfaces for log retrieval from authorized clients.				

Any additional documentation can be inserted here:

NGCS 25	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **NAT/NAPT Detection and Mediation** Provide details on how the proposed Session Border Control (SBC) will recognize that a Network Address Translation (NAT) or Network Address and Port Translation (NAPT) has been performed on Open Systems Interconnection (OSI) Layer 3, but not above, and correct the signaling message for SIP.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: A9-1-1 uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. When the SBC receives a message the rules are applied, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 26	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **IPv4/IPv6 Interworking** Provide details on how the proposed SBC shall enable interworking between networks utilizing IPv4 and IPv6 through the use of dual stacks, selectable for each SBC interface, based on NENA-STA-010.2-2016. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values.	X			
	Bidder Response: A9-1-1 will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards. All network equipment has the capability to utilize IPv4 and IPv6 addresses and is configurable to support dual stack operation. Whereas some components of internal systems only support IPv4; this will not be a limitation for this solution. When an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet Core strips down the IPv6 packet, removes the IPv6 header and adds the IPv4 header and passes it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. The IPv4 network and IPv6 interfaces are continuously monitored for availability and performance. This is accomplished with the use of a back-to-back user agent session border controller, rather than Network Address Translations (NATs). All devices within the network shall be assigned static addresses.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

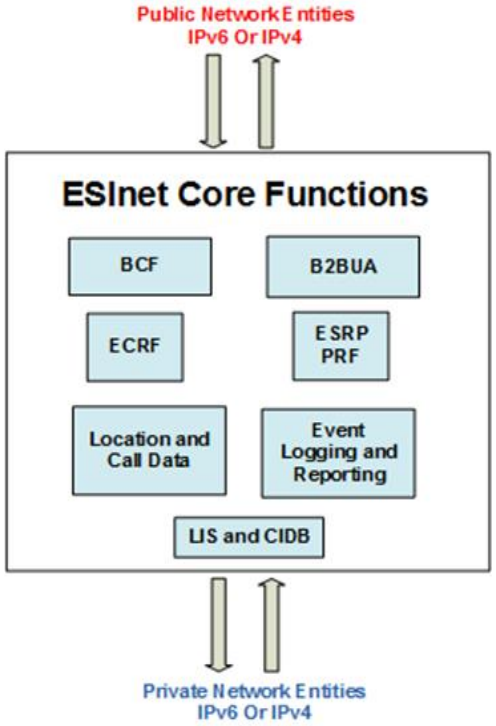

Figure 19: IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 27	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Support Over Multiple Protocols** Provide details on how the proposed SBC shall support SIP over the following protocols: 1. Transmission Control Protocol (TCP), 2. User Datagram Protocol (UDP), 3. Transport Layer Security over TCP (TLS-over-TCP), and 4. Stream Control Transmission Protocol (SCTP). Protocols supported shall be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems.	X			
	Bidder Response: **1. Transmission Control Protocol (TCP)** – The solution uses Transmission Control Protocol (TCP). Intrado highly recommends that PSAP call handling solutions support TCP. If the size of the SIP INVITE is within 200 bytes of the maximum transmission unit (MTU) of an Ethernet frame, fragmentation is likely to occur. Fragmentation may have impacts ranging from call setup delays of unknown duration and quantity, to blocked or abandoned calls. In some instances, fragmentation has no discernible impact to the call. Packet fragmentation is not unexpected, and it can be handled appropriately with the use of Transmission Control Protocol (TCP). **2. User Datagram Protocol (UDP)** – UDP is commonly used in VoIP implementations. This protocol's mechanisms for handling packet fragmentation are weaker. Intrado supports this protocol upon request. While A9-1-1 can support both UDP and TCP, we recommend that TCP be used. This recommendation is based upon the packet size experienced within the A9-1-1 solution, the anticipated growth of such packet sizes with forward-looking NG9-1-1 message sets, and applicable standards including the NENA i3 specification and IETF RFC 3261. **3. Transport Layer Security over TCP (TLS-over-TCP)** – Transport Layer Security over TCP (TLS-over-TCP) is supported. The SBC supports mutual-authentication within a TLS profile. The SBC supports the following TLS Exchange and Authentication models: • Basic—The client authenticates the SBC certificate by using the CA public key, and checks expiration, common name, and ciphers supported. Basic provides confidentiality and integrity through encryption, but does not establish the identity of the endpoint. Credential cracking is still possible, and the move to TLS (based on TCP) may make port exhaustion DoS a bit easier for an attacker. • Mutual—A step is added in which the client certificate is sent to the SBC for verification. You can use single or individual client certificates. Mutual provides the same characteristics of the basic model with the advantage of				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	verifying that the client is likely trusted because an issued certificate is present. If a single certificate is used for all clients then theft or compromise of an endpoint may allow access to an attacker. Individual certificates are more secure, but require more administrative effort to issue and manage. • Mutual with certificate revocation—Certificate revocation for individual clients is possible, which guarantees only expired or revoked clients are refused access. An external Online Certificate Status Protocol (OCSP) server is required to check against the Certificate Revocation List Because TLS is based on TCP, TCP DoS protections can be configured to limit the number of connections per source IP and per SIP interface. At the transport layer, when a request needs to be sent out the SBC first tries to send it over TCP. If that attempt fails then the SBC falls back to UDP and tries the request again. **4. SCTP Stream Control Transmission Protocol (SCTP)** – SCTP is supported upon request. Protocols supported are selectable for each SBC interface to external systems.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 28	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Packet Prioritization Based on Session Type** Provide details on how the proposed SBC shall be capable of populating the Layer 3 headers, based on call/session type (e.g., 911 calls) in order to facilitate priority routing of the packets.	X			
	Bidder Response: Details on how the A9-1-1 SBC populates the Layer 3 headers, based on call/session type (e.g., 9-1-1 calls) in order to facilitate priority routing of the packets is outlined in the following specification documents. • *Originating Service Provider (OSP) Network Interface Specification SIP Basic v.2.1* • *OSP NNI i3 v.2* The specification documents listed above are located in the *Proprietary Information* file provided with this response.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 29	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Encryption of Unencrypted Calls** Provide details on how the proposed SBC supports encryption for calls that are not protected entering the ESInet, based on NENA-STA-010.2-2016.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: A9-1-1'sBorder Control Function supports encryption for calls that ingress from any non-trusted network components. The A9-1-1 solution employs encryption-in-transit on networks under Intrado management. We encrypt-in-transit with networks not under our management where possible. Encryption is achieved using either SSL/TLS or IPSEC VPN.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 30	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Elements** 1. Provide details, including drawings, describing the different BCF elements that the proposed solution comprises. 2. As part of the details, identify all of the elements and/or interfaces to be provided by the Commission and/or PSAPs to the bidder.	X			

Bidder Response:

1. The A9-1-1 Border Control Function provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification.

The BCF inspects, modifies, and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect and where the ESInet connects with service provider networks. The BCF mitigates security threats, resolves interoperability problems and ensures reliable SIP-based communications. It is designed to protect and control real-time voice, video, and text sessions as they traverse IP networks between callers and Public Safety Answering Points (PSAPs).

Each of the A9-1-1 Core sites have redundant BCFs. The redundant BCF components are market-leading products that provide high reliability and high availability. The redundant BCF design and redundant core architecture of the A9-1-1 solution allows for availability to meet or exceed 99.999%.

Each of the A9-1-1 Core sites have redundant BCFs. The redundant BCF components are market-leading products that provide high reliability and high availability. The redundant BCF design and redundant core architecture of the A9-1-1 solution allows for availability to meet or exceed 99.999%.

Components of the BCF include:

- Border Firewall – the BCF provides border firewall functionality in accordance with NENA STA-010.2-2016.
- Opening and closing of pinholes - A9-1-1 BCFs are set to deny by default all traffic. Rules are built into the BCF/firewall such that pinholes between the firewalls will allow trusted/known traffic. Allowances go through rigorous scrutiny before being approved by the NOC/SOC. Once approved, changes are made on a regular basis following standard procedures to ensure no other pinholes are opened. The A9-1-1 NOC/SOC also does on-going traffic studies on the firewalls. If a pinhole is opened but not used, the NOC/SOC will close the pinhole if necessary.
- VPN – the BCF's SBC supports encryption for calls that are not protected using SSL/TLS or IPSEC VPN.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- IDS/IPS - Each core emergency call processing site includes security functions such as intrusion detection systems, and intrusion protection systems. Security management personnel specialize in managing and operating these assets and validate their operation.
- Session Border Control (SBC) - the SBC supports SIP over Transmission Control Protocol (TCP) primarily User Datagram Protocol (UDP) upon request, and Transport Layer Security over TCP (TLS-over-TCP), As required, the SBC populates Layer 3 headers in order to facilitate priority routing of packets and enables interworking between networks using IPv4 and IPv6.
- Call admission control – Call admission control (CAC) is used when establishing connectivity to internal and external IP resources.
- QoS and Limiting access to critical components through the use of VLANs - A9-1-1 is a Quality of Service (QoS)-managed private IP network which prioritizes any type of IP traffic; voice, data, and multi-media. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic.
- Media transcoding and Signaling protocol normalization and interworking - Below is a detailed list of the various VoIP protocols and established multimedia sessions supported by the Intrado A9-1-1 solution. As designed, the Intrado A9-1-1 solution is evolutionary and will be able to support future i3 specifications. Media Parameters

  Codecs

  - G.711 – telephony equivalency
  - The Intrado A9-1-1 system performs codec negotiation and upgrades all calls to a codec of G.711.
  - Have tested and ready to deploy upon demand
    - G.729
    - G.723
    - AMR-WB
- Network Address Translation (NAT) - A9-1-1 uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. The rules are applied when the SBC receives a message, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message.

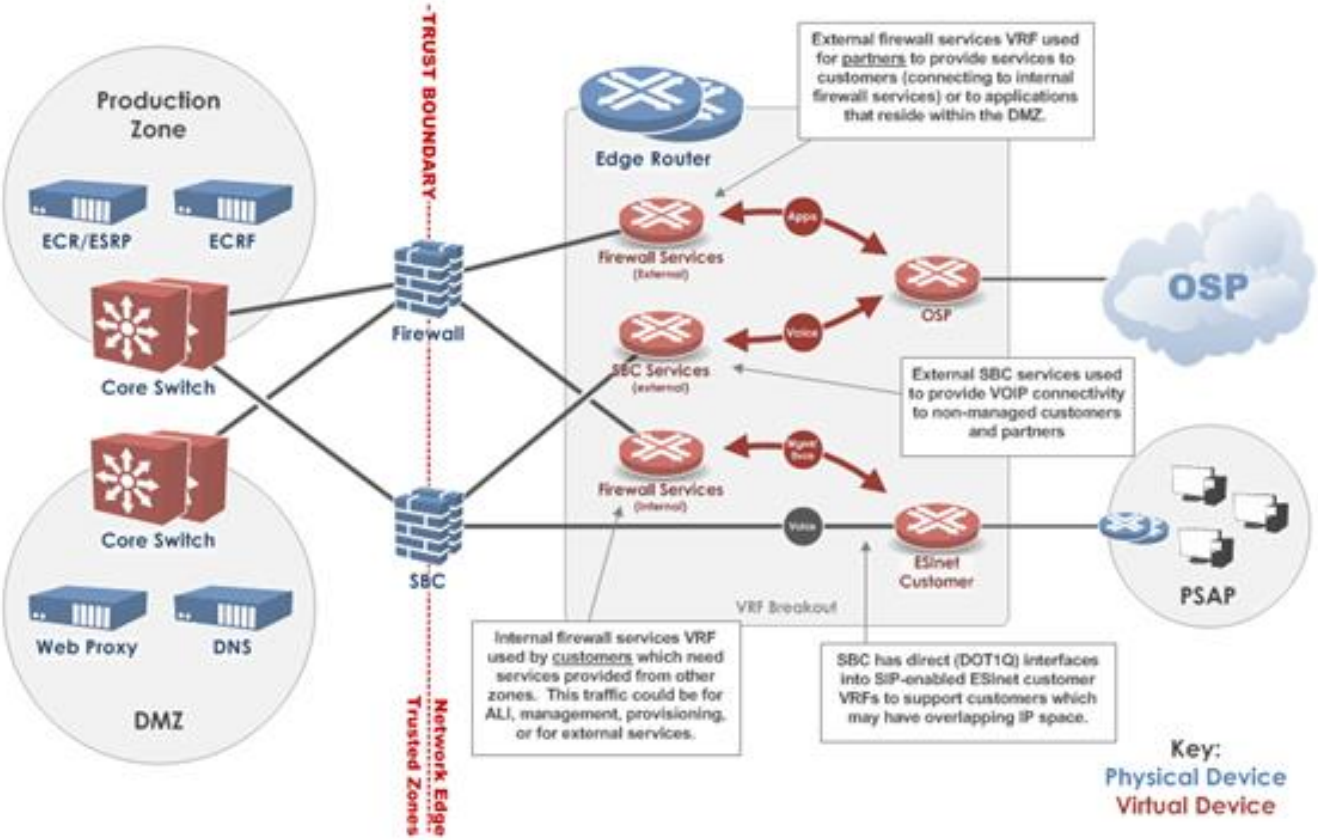

Figure 20: A9-1-1 ESInet Border Control Function

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	2. Intrado's BCF assumes that anything outside the ESInet/NGCS should be treated as untrusted. Therefore, only known traffic is permitted (whitelisted) to be allowed into the solution. Intrado connectivity to the PSAP's CPE assumes the use of BGP as a routing protocol for a multimode setup such as the setup currently implemented in the State of Nebraska. Customers may use their own public ASN if they have one or Intrado can assign an ASN for those that do not have one. Additionally, Intrado supports and recommends the use of BGP passwords. Intrado can generate passwords for those PSAPs not wanting to provide their own. NENA i3 standards strongly encourage the PSAP to have a security device providing a border between the ESInet and the local call taking equipment. Additionally, the ESInet routers installed at the PSAP will only be used for predefined traffic and not used as a default gateway. Using the ESInet provider as a default gateway prevents the call-taking equipment from being able to reach any other local resource, such as email, internet, or other individual applications. Intrado also allows users to access the Intrado ESInet Portal for access to the A9-1-1 Customer Management Portal and additional reporting via secure internet connections using dual factor authentication. Intrado will provide the users with a username/password credentials and associated Entrust token to securely access the Intrado A9-1-1 Portal. Users do not have to supply their own tokens, and setup is included in the cost of the Intrado A9-1-1 solution.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 31	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **ESRP Description** The ESRP routes a call to the next hop. It also evaluates the originating policy rules set for the queue the call arrives on, extracts the location of the caller from the SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next-hop route, evaluates the route based on policy rules and queue states of the downstream entity queues, and then forwards the call to the resulting next hop. Bidder's proposed ESRP must meet or exceed NENA-STA-010.2-2016. Describe how the proposed solution meets or exceeds the standards.	X			
	Bidder Response: The A9-1-1 Emergency Service Routing Proxy (ESRP) supports i3 compliant routing functionality including full integration with geographically determined routing, carrier grade voice quality, and demonstrated reliability. The A9-1-1 solution provides the ability to interoperate with NG9-1-1 systems in various configurations including the hierarchical network-of-networks model. The 9-1-1 technical architecture accommodates interacting ESRPs and ECRFs via the associated SIP and LoST protocols, respectively. Within the ESInet, the ESRP is interconnected with the LIS and ECRF functions. Interconnection with the PSAPs is via the Border Control Function. The diagram below illustrates the ESRP/PRF functional components and the interfaces with other A9-1-1 i3 solution elements.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

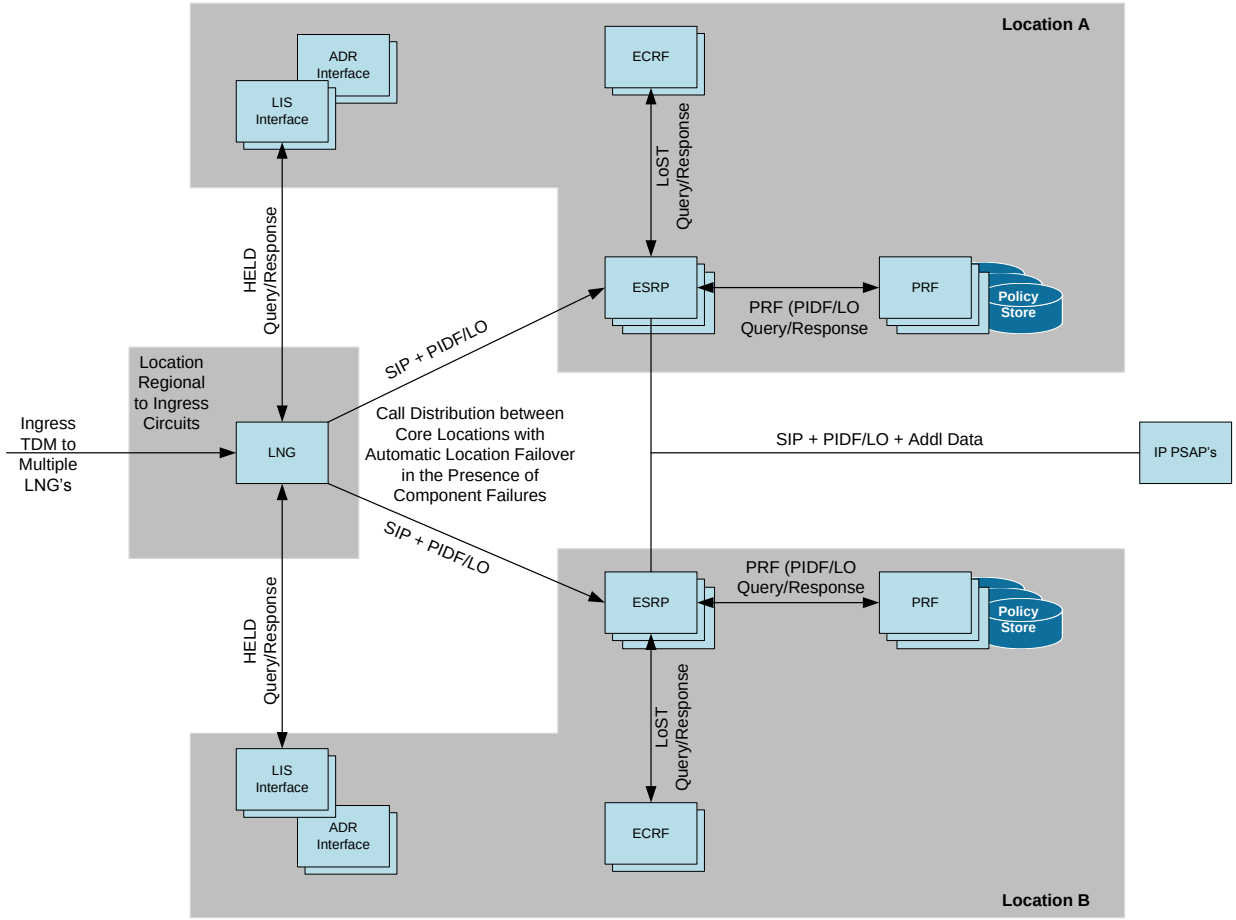

Figure 21: ESRP/PRF Diagram

The ESRP provides PSAPs with peace of mind by supporting multiple default routing fallback options until carriers transition to full i3-compliant call delivery. Fallback to legacy ESN or No Record Found routing is supported to ensure every call is routed as accurately as possible even if VoIP or wireless carriers do not deliver or pre-provision routable location values or if carrier-provisioned records are error treated. If the ESRP has to utilize the fallback ESN or NRF

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	routing scheme, it will continue to deliver the call and location information. This innovative solution provides extreme reliability for the routing of calls. The ESRP supports an option to configure PSAP routing by call type, supporting areas where wireless calls are routed to a different PSAP than would be otherwise determined by PSAP geographical boundaries, such as the State Patrol. Intrado is committed to compliance with the NENA STA-010.2 standards for all external interfaces included in the A9-1-1 Routing service that require interoperability with other vendor's systems. Intrado works directly with various vendors, and participates in NENA Industry Collaboration (ICE) Events and other similar i3 lab programs for the purpose of developing and demonstrating such compliance. Intrado also adheres to the various required interoperability protocols specified for use in the NENA i3 standards, such as HELD, LoST, Additional Data, MSRP, and others. While most internal interfaces are also NENA i3 v2 compliant, certain internal functions are not, for the sake of safety, efficiency, and that they're not currently intended to be exposed as external interfaces. A relatively small number of the NENA i3 v2 requirements are on the A9-1-1 Routing roadmap, waiting for market demand. NENA standards compliance is an ongoing commitment and Intrado actively participates on NENA standards development committees and other Industry Forums (i.e. ATIS) to help define the industry direction. As standards are ratified and there is a market demand for new capabilities, Intrado will work with industry providers to develop and test functionality to the new standards. Policy route determination includes evaluation of the PSAP-configured routing policy, the time of day, the caller's location (for geospatially determined alternate routing policies), the PSAP operational state, and the ring-no-answer timer configuration. The i3 SIP INVITE delivered to the PSAP (terminating ESRP) includes both geodetic/civic location, as available, and additional data conveyed by value and/or reference from the LIS and ADR interface responses. In addition to call delivery to i3-compliant PSAPs, the ESRP supports call delivery to legacy PSAPs. A sub-set of i3 routing policies can be provisioned for legacy PSAPs along with a 10-digit telephone number for delivery. When the ESRP receives an ingress call, it evaluates the SIP INVITE geolocation header within the PIDF-LO. If the geolocation header contains location by reference, the ESRP queries the location database via the HELD interface to dereference the location and obtain a routable location provided as a geodetic and/or civic location value. The ESRP then queries the ECRF via the LoST protocol with the caller's geodetic or civic address location to identify the destination URI for the call.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Using the location-determined URI retrieved from the ECRF via the LoST protocol, the ESRP interacts with the Policy Routing Function to determine call routing. The ESRP supports N-way bridging and call transfers using i3 SIP REFER and subscribe/notify messaging. i3 PSAPs can transfer calls to both i3 and non-i3 PSAPs. Subscribe/notify messaging allows the PSAP or secondary PSAP to take control over the call bridge once the call has been transferred.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 32	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Transition to Geospatial Routing** Bidder understands that all PSAPs and regions may not be ready for geospatial routing on day one of operations and shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. In bidder's separate cost proposal response, indicate the pricing difference between tabular and geospatial routing. Describe the process for transitioning each PSAP or region from tabular routing to geospatial routing as PSAP's becomes ready and the manner in which the solution provides for routing by both means simultaneously.	X			
	Bidder Response: Intrado understands that all PSAPs and regions may not be ready for geospatial routing on day one of operations and will provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. Intrado understands that some PSAPs may be ready to deploy i3 before others. To make the solution advantageous to the State of Nebraska, Intrado has included the i3 services in the tabular cost model. Therefore, there is no price difference between the tabular and the geospatial cost model. The A9-1-1 Routing system is completely integrated for both tabular and geospatial routing providing maximum flexibility for a PSAPs migration to i3 The A9-1-1 service simultaneously supports IPSR and i3 PSAPs and routing logic. As the call is processing, routing logic is dynamically applied based on the profile of the PSAP. This happens seamlessly. The A9-1-1 solution supports both legacy IPSR and i3 routing and call delivery from ingress to egress. For example, a call can ingress in an i3 format (with PIDF-LO). The A9-1-1 system transforms the call during call processing to deliver it to an IPSR-supported PSAP. The i3 LPG is employed to cache the location and present to the IPSR via a standard ALI bid. The process for transitioning each PSAP or region from tabular routing to geospatial routing as PSAPs become ready is outlined below. The majority of the work for the transition from IPSR routing to i3/geospatial routing occurs on the PSAP/regional side. Moving to i3 NG9-1-1 begins with a data assessment of the PSAP's GIS data. Intrado will work with the 9-1-1 Authority to establish a strategy to move from legacy ESN-based call processing to the NENA i3 call processing model. The structure of that transition will affect how to evolve existing data. Intrado has a robust GIS portfolio of services with deep expertise in i3 GIS data sets. Intrado has an *A9-1-1 GIS Data Provisioning Roles and Expectations v.3* document, attached below, which outlines steps that if followed, will enable a smooth transition. This documentation includes guidelines on how to prepare the data for i3				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	functional element consumption. Additionally, training will be provided on how to properly use the GIS Spatial Interface (SI) to upload and manage ongoing spatial information. Intrado will have staff available to assist with the initial implementation and ongoing day-to-day support of GIS data maintenance. The GIS Authority and MSAG coordinator will need to create processes and procedures (if not already completed) to maintain consistency between the MSAG/ALI/Location Database and the Street centerline and address points within the GIS data. Until OSPs are fully i3 and using the LVF for validation of address records, the legacy SOI processes and address validations will need to remain in place. This can be a complicated process. Intrado will provide guidance on processes that have worked well in past i3 implementations. Intrado offers additional services outside of what is requested within this RFP to assist and streamline the ongoing management and validation of the legacy and GIS data. From a NGCS perspective, very few modifications need to be completed for the transition from IPSR to i3 routing. Incoming traffic will need to be re-designated as GIS routable. PSAP i3 configurations within the ESRP will need to be created, and tested through to the CHE prior to deployment. A test plan is run to validate the i3 protocols are handled in the proper way and that calls can be transferred from i3 PSAPs to non- i3 PSAPs internal and external to the Intrado A9-1-1 solution. Fallback to ESN routing with i3 call delivery is also validated during the testing process. The NGCS processes listed above are not theory, they have been and continue to be deployed in Intrado A9-1-1 areas across the country.

Any additional documentation can be inserted here:

Intrado A9-1-1 GIS Data Roles and Expe

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 33	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Policy Routing Function (PRF) Description** The PRF is a required function of the ESRP. The ESRP interacts with the PRF to determine the next hop of a call or event. Before the ESRP sends the call to the next hop, it first queries the PRF to check the status of the next hop to determine if a unique routing rule or policy is in place that would direct the call to another location. The destination of the next hop is typically a queue. The PRF monitors the downstream queues of ESRPs for active understanding of the entity's queue status. Describe how the solution meets or exceeds the standards.	X			

Bidder Response:

Using the location-determined URI retrieved from the ECRF via the LoST protocol, the ESRP interacts with the Policy Routing Function to determine what if any policies are in place that will impact call routing.

The PRF accounts for the operational status of any downstream ESRP in the evaluation of any policy. This ensures that an ESRP is in an operational state before any message is sent to that ESRP.

The A9-1-1 i3 policy routing will provide the State's PSAPs with extensive flexibility to define and update standard and alternate routing polices. PSAPs can modify routing policies, set priorities, and modify their operational state. Routing policies can be defined as recurring or one-time. The rules-based routing proxy includes the following elements:

- A repository of PSAP-defined routing policies. The following types of routing policies are supported:
  - Abandonment/Night Service Routing – The abandonment policy is engaged whenever the terminating ESRP (PSAP) operational state is defined as 'Abandoned'. The PSAP operational state may be modified by contacting the Intrado NOC, triggered via a device installed at the PSAP, or modified online.
  - Overflow Routing – The overflow routing policy is applied during overflow scenarios when a PSAP is receiving more calls than its occupied work stations can accommodate. Upon reaching the designated call capacity for the call type, cumulative calls, or if the target is unreachable, the ESRP engages the primary PSAP's overflow routing policy. Similarly, the alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout.
  - Diversion Routing – The diversion routing policy is applied whenever the PSAP opts to engage alternate diversion routing rules. The PSAP operational state may be modified to engage the diversion routing policy by contacting the Intrado NOC or online.
  - Special Event Routing – Special event routing is a special type of diversion routing policy that is applied during a scheduled time window. If a PSAP jurisdiction contains venues that host events that may warrant dedicated

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	call handling (mobile command center or dedicated resources at the PSAP), special event polygons can be pre-provisioned. Intrado provides a feature-rich management portal for the State and/or PSAPs to view their policies. Policies have attributes such as active/inactive, one-time or recurring time window, priority, or a set of destination(s) to send the call to, and call distribution method as examples. Abandonment, Overflow, and Diversion policies can be configured to use any of the following policy attributes. • Geographically – The system can be configured to send abandonment calls to different alternate PSAPs based on the geographic location of the calling party within the primary PSAP's jurisdiction. Geographic abandonment or alternate routing polygons can be pre-provisioned via the SI or submitted dynamically. • Hierarchically – The system can be configured to cascade a call to up to nine consecutive, alternate PSAPs. • Load-balanced – The system can be configured to distribute calls between PSAPs. All policies loaded by the State are held in a test state (non-active) until the State confirms that all test calls using the policies perform as expected.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 34	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **PRF Policy Store and User Interface** The PRF shall allow defining of policy rules for distributing a wide range of calls in an efficient manner. 1. Describe the solution's Policy Store and the PSAP's ability to effect changes to the PRF. 2. Describe the user interface, role-based authentication, the ability of each PSAP or region to manage PSAP's own policy rules, and the types of policy rules available at the time of proposal submission, as well as those on the product roadmap. Roadmap items must include an estimated time of feature availability.	X			

Bidder Response:

1. A9-1-1 i3 policy store routing provides the PSAPs with extensive flexibility to define and update standard and alternate routing polices. PSAPs can modify routing policies, set priorities, and modify their operational state through a web-based management portal. Routing policies can be defined as recurring or one-time.

Using the location-determined URI retrieved from the ECRF via the LoST protocol, the ESRP interacts with the Policy Routing Function to determine the policy that should be employed to deliver the call.

2. PSAPs can modify routing policies, set priorities, and modify their operational state through a web-based management portal. Routing policies can be defined as recurring or one-time.

Multi-factor authentication and role-based access control are used to restrict user access to the A9-1-1 management portal. User access via the public Internet requires two-factor authentication, where one factor is provided through user name and password and the second factor is provided through a dynamic, randomly changing secure access code from a security token. Users are configured in the Intrado identity management system, linked to a specific security token, and configured for access to a defined list of applications.

The policy store includes the following elements:

- A repository of PSAP-defined routing policies.
- A9-1-1 Customer Management Portal – A feature-rich web tool that allows PSAPs to view routing configurations, edit their routing policies, and modify their status (normal, abandoned, diverted). The feature-rich management portal is a user-friendly tool that can be used by jurisdiction(s) and/or PSAPs to view, enable, and maintain their policies. Policies have attributes such as active/inactive, one-time or recurring time window, priority, or a set of the destination(s) to send the call to as examples. Routing destinations can be pre-provisioned and then enabled in real time to handle incidents.

The following types of routing policies are supported and can be managed by the user via the portal.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- **Abandonment/Night Service Routing.** The abandonment policy is engaged whenever the terminating ESRP (PSAP) operational state is defined as 'abandoned. The PSAP operational state may be modified by contacting the A9-1-1NOC, triggered via a device installed at the PSAP, or modified online.
- **Overflow Routing** – The overflow routing policy is applied during overflow scenarios when a PSAP is receiving more calls than its occupied work stations can accommodate. Upon reaching the designated call capacity for the call type, cumulative calls, or if the target is unreachable, the ESRP engages the primary PSAP's overflow routing policy. Similarly, the alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout.
- **Diversion Routing** – The diversion routing policy is applied whenever the PSAP opts to engage alternate diversion routing rules. The PSAP operational state may be modified to engage the diversion routing policy by contacting the Intrado NOC or online.
- **Alternate Routing.** The alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout. The user can prioritize an alternate destination via the management portal and enable a PSTN back-up route on-the-fly.
- **Special Event Routing.** Special event routing is a special type of diversion routing that is applied during a scheduled time window. If a PSAP jurisdiction contains venues that host events that may warrant dedicated call handling (mobile command center or dedicated resources at the PSAP), special event polygons can be pre-provisioned.

Additionally, abandonment, overflow, and diversion policies can be configured to use any of the following policies.

- **Geographically.** The system can be configured to send abandonment calls to different alternate PSAPs based on the geographic location of the calling party within the primary PSAP's jurisdiction.
- **Hierarchically.** The system can be configured to cascade a call to up to nine consecutive, alternate PSAPs.
- **Load Balanced.** The system can be configured to distribute calls between PSAPs.

All policies loaded are held in a test state (non-active) until the jurisdiction(s) confirms that all test calls using the policies perform as expected.

Additional short-term roadmap items include the support of additional responder boundaries and policies (See *Proprietary Information* file for roadmap date). Intrado looks forward to developing an ongoing relationship with the State of Nebraska.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	This relationship will allow the State and Intrado to fully understand the ongoing and dynamic State-specific requirements within the 9-1-1 environment. The end goal is to establish a partnership, in which future capabilities will be developed and supported together with the end goal of making the Next Generation solution a key part of saving more lives by creating and maintaining innovative, reliable, and available solutions.

Any additional documentation can be inserted here:

NGCS 35	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Next-Hop Queues** A next-hop queue may be a Uniform Resource Identifier (URI) that routes the call to an interactive multimedia response system (as described in IETF RFC 4240) that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via Dual-Tone Multi-Frequency (DTMF) signaling or other interaction protocols. Describe how the bidder's solution implements next-hop queueing.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: A next-hop queue that is a uniform resource identifier (URI) that routes a call to an interactive multimedia response system that plays a voice announcement and accepts responses via Dual-Tone Multi-Frequency (DTMF). DTMF signaling is supported. The PRF accounts for the operational status of any downstream ESRP in the evaluation of any policy. This ensures that an ESRP is in an operational state before any message is sent to that ESRP's queue. Intrado is happy to work with the State of Nebraska to assess and support use cases for when an announcement is negotiated by the caller to be played in a media format other than voice.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 36	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **High-Availability Design** The ESRP/PRF solution shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The redundant ESRP/PRF design and the overall two-core architecture of the A9-1-1 solution allows for availability to meet or exceed 99.999%. ESRP/RFP high availability is achieved through an application processing complex consisting of multiple application servers, each of which operates independently of the others so that a single application processor failure does not disrupt the processing of the complex. There are two application processing complexes that operate independently of each other and are geographically distributed. Each component at an application processing complex has redundancy and high availability within its own domain. The ESRP application is highly redundant within each of the geographically separate sites. There are multiple computers running the ESRP/PRF application and the failure of any one or two of those computers does not affect calls in progress. Failure of a data center results in all future calls being processed by the other geographically diverse data center and will still provide the total required call processing capacity requirement.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 37	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Keep-Alive Signaling Between Elements** Provide an explanation of how the proposed ESRPs use the SIP “options” transactions for maintaining “keep -alive” signaling between ESRPs, LNGs, Legacy PSAP Gateways (LPGs) and session recording services.	X			
	Bidder Response: Option messages are used in the A9-1-1 solution to ensure path and element availability. If an option response is not received, the solution will identify an alternate and/or resource to complete the transaction while maintaining 99.999% availability. SIP monitoring via SIP “Options” messages exists between the core site call control application and each ingress (OSP) and PSAP endpoint. To detect failure of DS0 channels, continuity tests (COT), loopback, and tone check tests are performed between the LNGs and OSP switching equipment before a circuit is established.*				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 38	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF** **TCP/TLS Implementation** The upstream interface on the proposed non-originating ESRPs shall implement Transmission Control Protocol/Transmission Layer Security (TCP/TLS), but shall be capable of fallback to UDP, as described in NENA-STA-010.2-2016. Stream Control Transmission Protocol (SCTP) support is optional. The ESRP shall maintain persistent TCP and TLS connections to the downstream ESRPs or User Agents (UA) that it serves. Provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.	X			
	Bidder Response: A9-1-1 uses Transmission Control Protocol (TCP) within the ESInet and highly recommends that both ingress and egress partners support TCP as well. The A9-1-1 SBC also supports SIP over Transport Layer Security over TCP (TLS over-TCP). Protocols are selectable for each SBC interface to external systems. This transport layer protocol is generated and terminated at each interface to external systems.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 39	**Next Generation Core Services Elements (NGCS)** **NENA Compliance Chart** Provide a description of how the proposed ESRPs meet or exceed all functional requirements below as defined in NENA-STA-010.2-2016, which are listed below.	X			

Bidder Response:

Overview Section 5.2.1.1 – Comply. Intrado supports the Emergency Service Routing Proxy (ESRP) as the base routing function for emergency calls for i3.

The Intrado ESRP manages routing per the Nena standard and supports the hierarchy of originating, intermediate and terminating ESRPs. It receive calls from upstream routing proxies, such as a carrier routing proxy. It accepts SIP messages and outputs SIP messages that can contain rewritten Route headers and additional manipulation of the SIP messages. It interfaces to the ECRF for location-based routing information, as well as the Policy Routing Function (PRF).

For typical 9-1-1 calls with a Request URI starting with “urn:service:sos” received, the Intrado ESRP will:

1. Evaluate an origination policy “rule set”;
2. Query the location-based routing function (ECRF) with the location included with the call (including any steps to dereference location included by reference) to determine the “normal” next hop (smaller political or network subdivision, PSAP or call taker group) URI
3. Evaluate a termination policy rule set for that URI using other inputs available to it such as headers in the SIP message, time of day, PSAP state, etc.

The result of the policy rule evaluation is a URI. The ESRP forwards the call to the URI.

The ESRP also handles calls to “administrative lines,” meaning calls directed to, for example, a 10-digit number listed for a particular PSAP.

For calls forwarded by a PSAP to a responder with a Request URI of “urn:nena:service:responder.*” and a Route header containing the responder URI, the ESRP uses the domain of the Route header to choose an origination policy and evaluates it per 1-3 above.

The ESRP is the “outgoing proxy server” for calls originated by the PSAP. The ESRP will route calls within the ESInet, and will route calls to destinations outside the ESInet through an appropriate gateway or SIP trunk to a PSTN or other carrier connection. Transfers to another PSAP or agency is an example of such outgoing calls to external destinations.

Call Queueing Section 5.2.1.2 – Partially Comply; full compliance road mapped for (see *Proprietary Information* file).

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Queue State Event Package Section 5.2.1.3 – Comply with Future Capability (see *Proprietary Information* file). **De-queue Registration Event Package Section 5.2.1** - Comply with Future Capability (see *Proprietary Information* file). **Policy Routing Function Section 5.2.1.5** – Comply. Policy Routing refers to the determination of the next hop a call or event is forwarded to by an ESRP. The PRF evaluates policy rule sets such as the ingress path the call arrives on, and the other is determined by the result of an ECRF query with the location of the caller. The PRF accepts calls directed to a specific URI. From that URI, it extracts its own “OriginationPolicy” from its Policy Store for that URI and executes the rule set. The rules normally include at least one condition LoSTServiceURN(<urn>) where <urn> is a service URN (either urn:service: or urn:nena:service:). Upon encountering the LoSTServiceURN condition, the PRF queries its (configured) ECRF with the location received with the call using the <urn> parameter in the action. The resulting URI is a variable called “Normal-NextHop”. The PRF extracts a “TerminationPolicy” from its Policy Store associated with the domain of Normal-NextHop and executes the rule set associated with that policy. The rules normally include the action “Route”. The PRF forwards the call to the route. Rules have a priority. If more than one rule yields a value for NextHop, the rule with the highest priority prevails. **ESRP Notify Event Package Section 5.2.1.6** – Comply with Future Capability (see *Proprietary Information* file). **INVITE Transaction Processing Section 5.2.1.7** – Comply. When the ESRP receives an INVITE transaction it first evaluates the Origination rule set. If a LoSTServiceURN condition is encountered it looks for the presence of a Geolocation header. If present, the ESRP evaluates the header and extracts the location in the Geolocation header. Each ESRP is capable of receiving location as a value or a reference, and is provisioned with credentials suitable to present to all LISs in its service area to be able to dereference a location reference using either SIP or HELD. The ESRP handles calls with problems in location. This can occur if the call is originated by an element outside the ESInet, the call is to an emergency service URN, and there is no Geolocation header. This also occurs if the location contents are malformed, the LIS cannot be contacted, the LIS refuses to dereference, the LIS returns a malformed location value or the ESRP encounters another error that results in no location. In all such cases the ESRP makes a best effort to determine a suitable default location to use to route the call. The call source, IP address of the caller or other information from the INVITE may be used to determine the best possible default location. The ESRP then queries its local (provisioned) ECRF with the location, using the service URN specified and the value of the RequestURI in the LoSTServiceURN condition parameter. The ECRF returns a URI for that service.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	The ESRP retrieves the terminating policy rule set for the URI. The PRF evaluates the rule set using the facts available to it such as PSAP state, time of day, queue state, information extracted from the INVITE, etc. **BYE Transaction Processing Section 5.2.1.8** – Comply. Intrado's ESRP processes BYEs per RFC 3261. **CANCEL Transaction Processing Section 5.2.1.9** – Comply. Intrado's ESRP processes CANCELs per RFC 3261. **OPTIONS Transaction Processing Section 5.2.1.10** – Comply with Future Capability. (see *Proprietary Information* file) **Upstream Call Interface Section 5.2.2.1** – Comply with Future Capability. (see *Proprietary Information* file). **Downstream Call Interface Section 5.2.2.2** – Comply with Future Capability. (see *Proprietary Information* file). **ECRF Interface Section 5.2.2.3** – Comply with Future Capability. (see *Proprietary Information* file). **Location Information Server (LIS) Dereference Interface Section 5.2.2.4** – Comply. The ESRP implements both SIP Presence Event Package and HELD dereferencing interfaces. When the ESRP receives a location URI (in a Geolocation header on the upstream SIP interface) it uses the LIS dereferencing interface to obtain a location value to use in its ECRF query. The ESRP uses its PCA issued credentials to authenticate to an external LIS. The ESRP will use TCP/TLS for the LIS Dereferencing interface, with fallback to TCP (without TLS) on failure to establish a TLS connection. The ESRP will maintain persistent TCP and TLS connections to LISs that it has frequent transactions with. **Additional Data Interfaces Section 5.2.2.5** – Comply**.** The ESRP supports mechanisms for retrieving Additional Data These services are invoked when the ESRP receives a call with a CallInfo header field having a "purpose" starting with "EmergencyCallData", or from a PIDF-LO with an appropriate <provided-by> element and when directed to do so by the invoked rule set. The resulting data structure is an input to the Policy Routing Function (PRF). The ESRP accommodates multiple additional data services and structures for the same call. Additional Data, when passed by reference, is retrieved by dereferencing each provided URI against its associated Additional Data Repository (ADR). Additional Data is accessed via the following mechanisms: • Through dereferencing URI(s), added to the Call-Info header field by the device, originating network or service provider handling the call. Each Additional Data URI is dereferenced against its respective target ADR to return the stored caller data.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- By querying an “Identity Searchable Additional Data Repository” (IS-ADR) with the identity obtained from Caller’s From or P-Asserted-Identity headers to retrieve an XML document containing any available Additional Data.

Additional Data may also be retrieved by the ESRP through a location-based query executed against the ECRF. This query returns a URI for Additional Data associated with that location. This URI may be dereferenced by the ESRP on an ADR to drive PRF rules. Any returned Additional Data URI may be added in a Call-Info header field such that it can be referenced by downstream systems. The location used for this query may specify an area that encompasses more than one location that has Additional Data

ESRP, PSAP, Call-Taker State Notification and Subscriptions Section 5.2.2.6 – Comply with Future Capability. (see *Proprietary Information* file).

Time Interface Section 5.2.2.7 – Comply**.** The ESRP maintains reliable time synchronization. The time of day information is an input to the Policy Routing Function as well as the logging interface.

Logging Interface Section 5.2.2.8 – Comply**.** The ESRP supports a logging interface. The ESRP logs every transaction and every message received and sent on its call interfaces, every query to the ECRF and every state change it receives or sends. It is capable of logging the rule set it consulted, the rules found to be relevant to the route, and the route decision it made.

Data Structures Section 5.2.3 – Comply with Future Capability. (see *Proprietary Information* file).

Policy Elements Section 5.2.4 – Comply with Future Capability. (see *Proprietary Information* file).

Provisioning Section 5.2.5 – Partially Comply; full compliance road mapped for (see *Proprietary Information* file). The ESRP is currently provisioned with:

- The default locations it uses, including (potentially) one for each origination domain, and an overall default location
- The ECRF it uses
- The Logging service it uses;
- Mappings from 10-digit PSAP telephone numbers to URIs (if the ESRP handles 10 digit calls on behalf of PSAPs)
- The URI of a default route PSAP that takes calls when a route cannot be determined

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Please note that Intrado has assigned two compliance levels to sections 5.2.1.2 and 5.2.5, below, as we currently partially comply and will be fully compliant as of the roadmap dates.

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Overview Section 5.2.1.1	X			
Call Queueing Section 5.2.1.2		X	X	
Queue State Event Package Section 5.2.1.3			X	
De-queue Registration Event Package Section 5.2.1.			X	
Policy Routing Function Section 5.2.1.5	X			
ESRP Notify Event Package Section 5.2.1.6			X	
INVITE Transaction Processing Section 5.2.1.7	X			
BYE Transaction Processing Section 5.2.1.8	X			
CANCEL Transaction Processing Section 5.2.1.9	X			
OPTIONS Transaction Processing Section 5.2.1.10			X	
Upstream Call Interface Section 5.2.2.1			X	
Downstream Call Interface Section 5.2.2.2			X	
ECRF Interface Section 5.2.2.3			X	
Location Information Server (LIS) Dereference Interface Section 5.2.2.4	X			
Additional Data Interfaces Section 5.2.2.5	X			
ESRP, PSAP, Call-Taker State Notification and Subscriptions Section 5.2.2.6			X	
Time Interface Section 5.2.2.7	X			
Logging Interface Section 5.2.2.8	X			
Data Structures Section 5.2.3			X	
Policy Elements Section 5.2.4			X	
Provisioning Section 5.2.5		X	X	

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 40	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** Describe how the ECRF interfaces with other ECRF solutions which may interface with the bidder's solution. Awarded Contractor shall coordinate with other ECRF solution providers to ensure interoperability between the respective solutions.	X			
	Bidder Response: Interactions with external ECRFs or the PSAP CPE will utilize digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA), once available. Until that time, Intrado will manage credentialing and the issuance of digital certificates to ensure protection and security. This mechanism will also be utilized for PSAP access to systems within the A9-1-1 solution, including access to the LIS interface, ADR interface and ECRF. Interactions between the ECRF and the ESRP are secured within the ESInet. If the ECRF receives a request for a location outside its coverage area, it will send a recursive (parent ECRF) or iterative (National Forest Guide) query to a parent/state ECRF or the National Forest Guide, once available. Absent a parent ECRF or the National Forest Guide, the ECRF can store coverage areas for other ECRFs.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 41	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **ECRF Description** The ECRF shall be designed according to NENA-STA-010.2-2016 and be implemented using diverse, reliable and secure IP connections. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 solution provides geo-redundant emergency call routing functions (ECRF) that use geographic location information to route emergency calls to the appropriate PSAP. The A9-1-1 ECRFs support i3 standards and contain geographic boundaries provided by the customer for 9-1-1 call routing and responder determination. The ECRF LoST protocol interface meets RFC 5222 and NENA STA-010.2 requirements. The A9-1-1 ECRF provides full i3 compliance. Where applicable, the ECRF also meets NENA 01- 014 and NENA 01-010, though there are transitional considerations and conflicts between these documents, NENA STA-010.2, and the draft NG9-1-1 GIS Data Model. The redundant ECRF design and the overall redundant architecture of the A9-1-1 solution allows for availability to meet or exceed 99.999%. The ECRFs exist within a highly available and geographically distributed application processing environment. A single hardware component failure at one of the application processing complexes will not interrupt processing of the ECRF. A single geographic site failure (either the communication to the site or elimination of the site itself) will not prevent further call processing from occurring. High availability is achieved through highly reliable, secure and diverse IP connections as well as high-availability software design, redundant ECRF instances, and transactions using dynamic client/server connections with ECRF serving entities. The ECRF(s) will only allow queries from trusted resources. When implementing the T-ESRP (CPE) onto the system, required configurations and procedures will be established within the various resources to allow for the appropriate amount of LoST traffic for ECRF queries. Standard operating procedures will be verified during interoperability (pre-live) testing. The geographically diverse ECRFs use redundant data stores to support high availability. These systems are monitored 24x7x365 by the Network Operating Center (NOC) and supported through the Incident Command System. All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. With the ECRF architecture including two separate servers at each geographically diverse location, upgrades and other maintenance can be performed one server at a time so that at no time will the system be one-sided.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	As are of all the NGCS elements, the ECRF is architected to be secure, reliable, resilient, and robust. All applications and network in the 9-1-1 call path are designed to achieve 99.999% system availability using a number of techniques to improve resiliency such as geo-diverse redundancy, fail-over techniques, virtualization, high availability, etc. The ECRF supports logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required.

Any additional documentation can be inserted here:

NGCS 42	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **High-Availability Design** Bidder shall supply an ECRF function that meets a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements**.**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The redundant ECRF design and the overall redundant architecture of the A9-1-1 solution allows for availability to meet or exceed 99.999%. The ECRFs exist within a highly available and geographically distributed application processing environment. A single hardware component failure at one of the application processing complexes will not interrupt processing of the ECRF. A single geographic site failure (either the communication to the site or elimination of the site itself) will not prevent further call processing from occurring. High availability is achieved through highly reliable, secure and diverse IP connections as well as high-availability software design, redundant ECRF instances, and transactions using dynamic client/server connections with ECRF serving entities. The ECRF(s) will only allow queries from trusted resources. When implementing the T-ESRP (CPE) onto the system, required configurations and procedures will be established within the various resources to allow for the appropriate amount of LoST traffic for ECRF queries. Standard operating procedures will be verified during interoperability (pre-live) testing. The geographically diverse ECRFs utilize redundant data stores to support high availability. These systems are monitored 24x7x365 by the Network Operating Center (NOC) and supported through the Incident Command System. All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. With the ECRF architecture including two separate servers at each geographically diverse location, upgrades and other maintenance can be performed one server at a time so that at no time will the system be one-sided.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 43	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility by Outside Functional Elements** Contractors providing an ECRF shall ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, an LNG, an ESRP in a next-generation emergency services network, or by some combination of these functions. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Interactions between the ECRF and the ESRP are secured within the ESInet. Interactions with external ECRFs or the PSAP CPE will use digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA), once available. Until that time, Intrado will manage credentialing and the issuance of digital certificates to help ensure protection and security. If the ECRF receives a request for a location outside its coverage area, it will send a recursive (parent ECRF) or iterative (National Forest Guide) query to a parent/state ECRF or the National Forest Guide, once available. Absent a parent ECRF or the National Forest Guide, the ECRF can coverage areas for other ECRFs. When a request for a location that falls outside of its own coverage area is received, the ECRF will check to see if the location falls within another known coverage area and send a recursive query to that ECRF and per RFC 5222, pass that response along to the requesting system. Interactions between the A9-1-1 ECRF and ECRFs outside the A9-1-1 System also require credentialing/authentication.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 44	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility Inside the ESInet** Contractor shall provide an ECRF accessible inside an ESInet, which shall permit querying from any PSAP (or future entity authorized to connect to the ESInet) inside the ESInet. ECRFs provided by other entities may have their own policies regarding who may query them. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Any system secured within the A9-1-1 solution is considered safe, so the ECRF does allow LoST queries from any entity inside the ESInet. As a matter of best practice, the A9-1-1 ECRF will only be provisioned with coverage area for external ECRFs for which interoperability agreements and associated digital certificates for authentication have been provisioned for access into the different systems. Once the PSAP Credentialing Agency (PCA) has been established, there will no longer be a need for Intrado to manage the digital certificates.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 45	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Origination Network ECRF** An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Describe the functionality of such an ECRF equivalent and document where this functional element resides within the proposed solution.	X			
	Bidder Response: The origination network ECRF would typically reside within its own network, as noted. Intrado can optionally provide an “external” ECRF available for LoST queries by authorized origination network providers to be used to determine emergency call routing to the correct ESInet. This function is dependent on Nebraska’s ability to negotiate receipt of the authoritative boundaries for any non-A9-1-1 networks within the State.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 46	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Routing Query Interface** The ECRF shall support a routing query interface that can be used by an endpoint, ESRP or PSAP to request location-based routing information from the ECRF. Additionally, it shall support both iterative and recursive queries to external ECRF sources. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The ECRF supports a routing query interface that can be used by an endpoint, ESRP or PSAP to request location-based routing information from the ECRF. Additionally, the ECRF supports both iterative and recursive queries to other LoST servers, such as an external ECRF or National Forest Guide, once available. Note the National Forest Guide, per NENA-INF-009.1-2014, only supports iterative queries.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 47	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **LoST Protocol Support** The ECRF shall interface with the Location-to-Service Translation (LoST) protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CHE, or any other permitted IP host. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: In compliance with NENA i3 specifications, the ECRF supports the LoST protocol as defined in RFC 5222, with receipt of civic addresses, geo-coordinates, or both location elements as input. All queries from outside the A9-1-1 system must be authenticated.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 48	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Query Rate-Limiting** The proposed ECRF shall allow for rate-limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. Additionally, transaction and error information is available to the authorized parties through the Customer Management Portal. The ECRF has been designed to handle extreme query loads. The ECRF tested to support a minimum of 100 queries per second for five (5) minutes, even if one node is down and can easily support this rate in all up conditions. Rate limiting of queries from sources other than the proposed ESRP(s) is a supported function.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **Supported Functions** The ECRF shall support each of the following items. Describe how the solution meets or exceeds each of the requirements below:				
NGCS 49	Bidder Response: The ECRF provides full i3 compliancy and contains the geographic boundaries provided by the jurisdiction(s) for 9-1-1 call routing and responder determination. The ECRF LoST protocol interface meets RFC 5222 and NENA 08-003v1 requirements. The A9-1-1 ECRF has been supporting production Next Generation 9-1-1 call routing solutions since 2009. The A9-1-1 ECRF LoST interface was tested during the NENA Industry Collaboration Event (ICE 4), where it passed all scenarios tested. In addition, the ECRF meets the following requirements. **Logging of all connections, connection attempts, data updates, ECRF query results and LoST transactions:** All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. **Location error identification:** The A9-1-1 Spatial Interface has the ability to perform GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any erroneous data from being provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data changes. The SI validation engine refers errors back to the originating 9-1-1 Authority in comprehensive reports that are retrieved in the Enterprise Geospatial Database Management System (9-1-1EGDMS) portal. Validation errors must be corrected by the 9-1-1 Authority within their own GIS database and resubmitted to the Spatial Interface. Ongoing 9-1-1EGDMS	X			

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	validations include road centerline, address point, and polygons for each data upload. Critical errors will not be loaded into the A9-1-1 systems. All critical errors should be resolved prior to switching to geospatial call routing. **Critical Errors Management:** Following are examples of features with critical errors that will not be provisioned. These errors must be corrected and resubmitted to load to production ECRF and LVF resources. • Unique ID Duplicate: The feature's Unique ID is duplicated within the agency's layer • Geometry Error: A record exists in the attribute table that is not associated with a geographic feature or the geometry of a feature is in error. • Attribute Duplicate: The feature's attributes are duplicated in multiple features, but each feature has a unique location • Address Range Overlap: An overlap exists in one or both sides of the address ranges between two connected and identically named road centerline segments. • Field Constraint: An attribute value is incompatible with the EGDMS database schema and cannot be loaded into the database. • Outside Authoritative Boundary: All or part of the feature falls outside the Authoritative Boundary. • Boundary - Neighbor – Gap: A gap exists between the boundary polygon and an adjacent data source's boundary polygon. • Boundary - Internal – Gap: A gap exists between the boundary polygon and another boundary polygon within the database. • Boundary - Neighbor – Overlap: The boundary polygon feature overlaps an adjacent data source's boundary polygon.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Boundary - Internal – Overlap: The boundary polygon feature overlaps another boundary polygon within the database. • Routing URI: The routing Uniform Resource Identifier (URI) is either missing or invalid within the service response boundary polygon. **Updates from the SI in near real-time with no degradation of LoST services:** When time is critical, it is recommended that boundary updates are submitted independently of Site Structure/Address Point and Road Centerline updates as the validation process on these can take longer, depending on the number of changes that have been made since the previous data update. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, alarm notifications will be sent to the NOC and relevant operations teams. If this occurs the previously active map layer will remain active. ECRF prescribed functions that are not directly related to call-time activities (e.g., gap/overlap detection) are performed on separate servers to prevent any “administrative” oriented ECRF functions from interfering with the call-time functions. Timing of updates is dependent on the data being updated. As is requested in another bullet point in this section (Validation of GIS updates before they are provisioned into the ECRF), validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF system is near real-time. It is always recommended that “urgent” updates to one or more polygon layers be provisioned without the Site Structure Address Points (SSAPs) or Road Centerlines (RCLs) as validation and provisioning of the SSAPs and RCLs can take a few or many minutes, depending on the size of the feature set being loaded. It is possible to				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	reduce the number of validations performed on the data updates to decrease provisioning speed, but that is balanced by the increased risks of not performing all available validations. **Routing of calls based on geographic coordinates, geodetic shapes and civic addresses:** For expediency during call processing, the geodetic location, if available, is used by the ESRP for routing determination by using a point-in-polygon lookup. Latitude and longitude (XY) circle, sphere, and ellipsoid are the geodetic shapes currently supported. Other geodetic shapes will be added in future releases as required by the market. Routing and other services can also be determined with civic address when geodetic locations are not available. **Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire/rescue and emergency medical services (EMS):** The GIS data layer(s) that are used to identify the PSAP, emergency, and additional service types are configured on a per-service basis, e.g., urn:service:sos. When there is only a civic location element available in the PIDF-LO, the ECRF will follow the LoST protocol to locate a matching address point feature or, if one cannot be determined from the address point layer, the ECRF will attempt to locate a matching Road Centerline feature. If either is located, the ECRF will return the URI associated with the URN also specified in the LoST request. The ECRF supports provisioning of separate boundary layers for first responder service types for police, fire, and emergency medical services, as long as the polygon datasets are provided with the GIS data. The ECRF is not limited to these minimum data sets and will support additional boundary layers, each identified with a unique URN. The ECRF client may query the ECRF for additional service URNs associated with the location. **Permitting of LoST queries for find service request association with each layer:** The ECRF supports LoST query types. It also supports queries to retrieve Additional Data Repository (ADR) URIs that may be associated with a particular location. Hosting of the Location ADRs themselves is not the responsibility of the ECRF provider.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Compliance with NENA 02-010 and NENA 02-014: NENA 02-014 addresses GIS data collection and maintenance standards. While certain layer collection does apply, any requirements in this document would be superseded by STA-010.2 and the [draft] NG9-1-1 GIS data model. Similarly, NENA 02-010 conflicts with STA-010.2 and the [draft] NG9-1-1 GIS data model. The A9-1-1 ECRF complies with these documents, except where they conflict with STA-010.2 and the [draft] NG9-1-1 GIS data model, in which case the more recent standards are followed. **Dynamic updates to GIS without disruption of the ECRF:** Updates provisioned via the SI are applied with no degradation of LoST services. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. As well, the ECRF and LVF are implemented independently even though they provide similar functions, due to the provisioning nature of the LVF function and the real-time call processing nature of the ECRF. This architecture ensures that the Location Validation Function does not interfere with the critical call routing functions provided by the ECRF. **Validation of GIS updates before they are provisioned into the ECRF:** Any updates to the GIS data within the ECRF, whether to correct errors within the current data set or enhance it for any other reason, will be uploaded through the A9-1-1 Spatial Interface. The GIS updates are provisioned through the Spatial Interface which has the additional ability to perform GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	prevent any unwanted data being provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities.				

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions	X			
Location error identification.	X			
Updates from the SI in near real-time with no degradation of LoST services	X			
Routing of calls based on geographic coordinates, geodetic shapes, and civic addresses	X			
Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS).	X			
Permitting of LoST queries for find service request association with each layer.	X			
Compliance with NENA 02-010 and NENA 02-014.	X			
Dynamic updates to GIS without disruption of the ECRF.	X			
Validation of GIS updates before they are provisioned into the ECRF.	X			

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 50	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **User Interface and Provisioning** Define bidder's method for: 1. provisioning the ECRF; 2. updating the ECRF (including the frequency of updates); 3. validating data provisioning; 4. performing error logging; 5. performing gap and overlap analysis; and 6. supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet. 7. Provide a clear description of the functionality of the ECRF; list features and capabilities; 8. describe the error handling, default mechanisms, and logging; and 9. provide an overview of deployment recommendations to achieve 99.999 percent reliability.	X			

Bidder Response:

1. Provisioning the ECRF

The Spatial Interface (SI) provisions updated GIS layers to ECRF via a fully automated process. Immediately upon successful completion of QA/QC processing, the SI provisions a .zip file containing the updated files to the ECRF system. The ECRF update process checks for updated files every minute, and when an update is available, the files are processed immediately. Once the update process has occurred, a results file containing information about the success / failure of the update is sent to the SI. If the update is successful, the updated data is applied immediately. Any update failure will be investigated and corrected, however the data in production prior to the failed update will remain in place

2. Updating the ECRF (including the frequency of updates)

When time is critical, it is recommended that boundary updates are submitted independently of Site Structure/Address Point and Road Centerline updates as the validation process on these can take longer, depending on the number of changes that have been made since the previous data update.

Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory.

Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, alarm notifications will be sent to the NOC and relevant operations teams. If this occurs the previously active map layer will remain active.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	ECRF prescribed functions that are not directly related to call-time activities (e.g., gap/overlap detection) are performed on separate servers to prevent any “administrative” oriented ECRF functions from interfering with the call-time functions. Timing of updates is dependent on the data being updated. As is requested in another bullet point in this section (Validation of GIS updates before they are provisioned into the ECRF), validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF system is near real-time. It is always recommended that “urgent” updates to one or more polygon layers be provisioned without the Site Structure Address Points (SSAPs) or Road Centerlines (RCLs) as validation and provisioning of the SSAPs and RCLs can take a few or many minutes, depending on the size of the feature set being loaded. It is possible to reduce the number of validations performed on the data updates to decrease provisioning speed, but that is balanced by the increased risks of not performing all available validations. Updates are processed upon receipt from the PSAP. **3. Validating data provisioning** Updates provisioned via the SI are applied with no degradation of LoST services. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. **4. Performing error logging** All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. **5. Performing gap and overlap analysis** The EGDMS/Spatial Interface (SI) provisions updated GIS layers to ECRF via a fully automated process. Immediately upon successful completion of QA/QC processing, the SI provisions a .zip file containing the updated files to the ECRF system. The ECRF update process checks for updated files every minute, and when an update is available, the files are processed immediately. Once the update process has occurred, a results file containing information about the success / failure of the update is sent to the SI. If the update is successful, the updated data is applied immediately. Any update

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	failure will be investigated and corrected, however the data in production prior to the failed update will remain in place. Data validations include Gap/Overlap detection, reporting and error logging The A9-1-1 Spatial Interface (SI) has configurable thresholds for triggering gap and overlap alarms/reports The Spatial Interface performs GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted data being provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. The Spatial Interface performs logging of uploads and any associated errors and provisioning status (succeeded/failed). The following are examples of gap and overlap assessments performed. Address Range Overlap: An overlap exists in one or both sides of the address ranges between two connected and identically named road centerline segments. Outside Authoritative Boundary: All or part of the feature falls outside the Authoritative Boundary. • Boundary - Neighbor – Gap: A gap exists between the boundary polygon and an adjacent data source's boundary polygon. • Boundary - Internal – Gap: A gap exists between the boundary polygon and another boundary polygon within the database. • Boundary - Neighbor – Overlap: The boundary polygon feature overlaps an adjacent data source's boundary polygon. • Boundary - Internal – Overlap: The boundary polygon feature overlaps another boundary polygon within the database. **6. Supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet** • LoST queries from ESRPs, the PSAP CPE, and other authorized hosts within the ESInet are supported. • The ECRF supports <findService>, <listServices> and <listServicesByLocation> LoST query types.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- The ECRF supports provisioning of separate boundary layers for first responder service types for police, fire, and emergency medical services, as long as the polygon datasets are provided with the GIS data. The PSAP may query the ECRF for additional service URNs associated with the location.
- The PSAP may also query the ECRF for the URI associated with an Additional Data Repository (ADR), specific to the civic location provided in the LoST request. If that information is provisioned with the jurisdiction(s) Address Point data, the ADR URI will be returned.
- Additionally, if the ECRF receives a request for a location outside its coverage area, it will send an iterative query to the National Forest Guide, once available. Absent the National Forest Guide, the ECRF can store coverage areas for other ECRFs. When a request for a location that falls outside of its own coverage area is received, the ECRF will check to see if the location falls within another known coverage area and send a recursive query to that ECRF and per RFC 5222, pass that response along to the requesting system.
- The ECRF also has the optional capability to provide National Forest Guide functions, in lieu of a National Forest Guide. Rate limiting of queries from sources other than the proposed ESRP(s) is a supported function. For obvious reasons, rate querying any “call path” requests will not be allowed.
- The ECRF supports both iterative and recursive queries to other LoST servers, such as an external ECRF or National Forest Guide, once available.
- Support for both Geodetic Location elements and Civic Location elements.
- Support for multiple service layers beyond PSAP, Police, Fire and EMS.
- RFC 5222 compliance, including LoST error responses to LoST clients.

7. Provide a clear description of the functionality of the ECRF; list features and capabilities;

The ECRF provides full i3 compliancy and contains the geographic boundaries provided by the jurisdiction(s) for 9-1-1 call routing and responder determination. The ECRF LoST protocol interface meets RFC 5222 and NENA 08-003v1 requirements. The A9-1-1 ECRF has been supporting production Next Generation 9-1-1 call routing solutions since 2009,

The A9-1-1 ECRF LoST interface was tested during the NENA Industry Collaboration Event (ICE 4), where it passed all scenarios tested.

In addition, the ECRF meets the following requirements.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Logging of all connections, connection attempts, data updates, ECRF query results and LoST transactions: All transactions are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. Location error identification: The A9-1-1 Spatial Interface has the ability to perform GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any erroneous data to be provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data changes. The SI validation engine refers errors back to the originating 9-1-1 Authority in comprehensive reports that are retrieved in the Enterprise Geospatial Database Management System (9-1-1EGDMS) portal. Validation errors must be corrected by the 9-1-1 Authority within their own GIS database and resubmitted to the Spatial Interface. Ongoing 9-1-1 EGDMS validations include road centerline, address point, and polygons for each data upload. Critical errors will not be loaded into the A9-1-1 systems. All critical errors should be resolved prior to switching to geospatial call routing. Critical Error Management: Following are examples of features with critical errors that will not be provisioned. These errors must be corrected and resubmitted to load to production ECRF and LVF resources. . • Unique ID Duplicate: The feature's Unique ID is duplicated within the agency's layer • Geometry Error: A record exists in the attribute table that is not associated with a geographic feature or the geometry of a feature is in error. • Attribute Duplicate: The feature's attributes are duplicated in multiple features, but each feature has a unique location • Address Range Overlap: An overlap exists in one or both sides of the address ranges between two connected and identically named road centerline segments. • Field Constraint: An attribute value is incompatible with the EGDMS database schema and cannot be loaded into the database. • Outside Authoritative Boundary: All or part of the feature falls outside the Authoritative Boundary.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Boundary - Neighbor – Gap: A gap exists between the boundary polygon and an adjacent data source's boundary polygon. • Boundary - Internal – Gap: A gap exists between the boundary polygon and another boundary polygon within the database. • Boundary - Neighbor – Overlap: The boundary polygon feature overlaps an adjacent data source's boundary polygon. • Boundary - Internal – Overlap: The boundary polygon feature overlaps another boundary polygon within the database. • Routing URI: The routing Uniform Resource Identifier (URI) is either missing or invalid within the service response boundary polygon. **Updates from the SI in near real-time with no degradation of LoST services**: When time is critical, it is recommended that boundary updates are submitted independently of Site Structure/Address Point and Road Centerline updates as the validation process on these can take longer, depending on the number of changes that have been made since the previous data update. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, alarm notifications will be sent to the NOC and relevant operations teams. If this occurs the previously active map layer will remain active. ECRF prescribed functions that are not directly related to call-time activities (e.g., gap/overlap detection) are performed on separate servers to prevent any “administrative” oriented ECRF functions from interfering with the call-time functions. Timing of updates is dependent on the data being updated. As is requested in another bullet point in this section (Validation of GIS updates before they are provisioned into the ECRF), validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF system is near real-time. It is always recommended that “urgent” updates to one or more polygon layers be provisioned without the Site Structure Address Points (SSAPs) or Road Centerlines (RCLs) as validation and provisioning of the SSAPs and RCLs can take a few or many minutes, depending on

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	the size of the feature set being loaded. It is possible to reduce the number of validations performed on the data updates to decrease provisioning speed, but that is balanced by the increased risks of not performing all available validations. **Routing of calls based on geographic coordinates, geodetic shapes and civic addresses:** For expediency during call processing, the geodetic location, if available, is used by the ESRP for routing determination by using a point-in-polygon lookup. Latitude and longitude (XY) circle, sphere, and ellipsoid are the geodetic shapes currently supported. Other geodetic shapes will be added in future releases as required by the market. Routing and other services can also be determined with civic address when geodetic locations are not available. **Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire/rescue and emergency medical services (EMS):** The GIS data layer(s) that are used to identify the PSAP, emergency, and additional service types are configured on a per-service basis, e.g., urn:service:sos. When there is only a civic location element available in the PIDF-LO, the ECRF will follow the LoST protocol to locate a matching address point feature or, if one cannot be determined from the address point layer, the ECRF will attempt to locate a matching Road Centerline feature. If either is located, the ECRF will return the URI associated with the URN also specified in the LoST request. The ECRF supports provisioning of separate boundary layers for first responder service types for police, fire, and emergency medical services, as long as the polygon datasets are provided with the GIS data. The ECRF is not limited to these minimum data sets and will support additional boundary layers, each identified with a unique URN. The ECRF client may query the ECRF for additional service URNs associated with the location. **Permitting of LoST queries for find service request association with each layer:** The ECRF supports LoST query types. It also supports queries to retrieve Additional Data Repository (ADR) URIs that may be associated with a particular location. Hosting of the Location ADRs themselves is not the responsibility of the ECRF provider. **Compliance with NENA 02-010 and NENA 02-014:** NENA 02-014 addresses GIS data collection and maintenance standards. While certain layer collection does apply, any requirements in this document would be superseded by STA-010.2 and the [draft] NG9-1-1 GIS data model. Similarly, NENA 02-010 conflicts with STA-010.2 and the [draft] NG9-1-1 GIS data model. The A9-1-1 ECRF complies with these documents, except where they conflict with STA-010.2 and the [draft] NG9-1-1 GIS data model, in which case the more recent standards are followed. **Dynamic updates to GIS without disruption of the ECRF**: Updates provisioned via the SI are applied with no degradation of LoST services. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. As well, the ECRF and LVF are implemented independently even though they provide similar functions, due to the provisioning nature of the LVF function and the real-time call processing nature of the ECRF. This architecture ensures that the Location Validation Function does not interfere with the critical call routing functions provided by the ECRF. In compliance with NENA i3 specifications, the ECRF supports the LoST protocol as defined in RFC 5222, with receipt of civic addresses, geo-coordinates, or both location elements as input. **8. Describe the error handling, default mechanisms, and logging;** Any updates to the GIS data within the ECRF, whether to correct errors within the current data set or enhance it for any other reason, will be uploaded through the A9-1-1 Spatial Interface. The GIS updates are provisioned through the Spatial Interface which has the additional ability to perform GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted data being provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. **9. Provide an overview of deployment recommendations to achieve 99.999 percent reliability** The A9-1-1 ECRFs exist within a highly available and geographically distributed application processing environment. A single hardware component failure at one of the application processing complexes will not interrupt processing of the ECRF. A single geographic site failure (either the communication to the site or elimination of the site itself) will not prevent further call processing from occurring. With the dual ESInet cores, multiple geographic site failures could occur without interrupting the ECRF from performing its critical functions. High availability is achieved through high availability software design, redundant ECRF instances, and transactions using dynamic client/server connections with multiple ECRF serving entities. The geographically diverse ECRFs use redundant data stores to support high availability. These systems are monitored 24x7x365 by the Network Operating Center (NOC) and supported through our Incident Command System. All transactions

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	are logged. Errors are logged for reporting and analysis and directed to the NOC when immediate action is required. Additionally, transaction and error information is available to the customer through the management and reporting suite.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 51	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Hierarchical Integration with Other ECRFs** The ESInet will be part of an overall hierarchical plan that includes interconnectivity to other regions and ECRFs. Provide details regarding bidder's vision for how this interconnection will include replicas of ECRF/LVF at different levels of the hierarchy, as well as access/origination networks.	X			

Bidder Response:

At the State's discretion, the A9-1-1 ECRFs and LVFs can operate in various deployment models. There are two deployment models described in the current draft of NENA STA-005, NENA Standards for the Provisioning and Maintenance of GIS data to ECRFs and LVFs:

- Coordinated, Intergovernmental Approach: Planned and coordinated deployments of NG9-1-1 capabilities that are governed by statewide 9-1-1 Authorities, regional Authorities, or informal mechanisms that enable a cooperative deployment.
- Independent, Unilateral Approach: Decentralized deployments of NG9-1-1 capabilities by local jurisdictions through independent initiatives.

A9-1-1 ECRFs and LVFs can be deployed to support both approaches.

Using the coordinated, intergovernmental approach, coverage areas for any other ECRFs or LVFs would be provisioned into the A9-1-1 ECRF and LVF, and the A9-1-1 ECRF and LVF coverage areas would be provisioned into other ECRFs and/or LVFs in the area. This allows the local ECRF to recursively query other known ECRFs when a location falls within the neighboring ECRF or LVF's region. Access to a National Forest Guide, when available, is not necessary using this approach unless the location falls outside of all the ECRF/LVF known regions.

Using the Independent, unilateral approach, utilization of the National Forest Guide or a parent ECRF (statewide or multi-state) would be required to discover the correct ECRF or LVF to query for a response. The A9-1-1 ECRF and LVF can potentially be utilized as a statewide or multi-state parent system to support this task.

It is up to the access/origination networks to know how to direct 9-1-1 calls across a given region. As an optional service, Intrado can work with the Commission to explore the feasibility of providing an ECRF to direct access/origination network providers to the correct ESInet, assuming there may be multiple serving a multi-state region. Intrado looks forward to working with the Commission to develop a complete set of requirements and scope of work necessary for ESInet interconnection with regional and state level ECRFs. Pricing and lead time for implementation is to be determined pending future completion of engineering requirements discovery.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 52	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Forest Guide** Provide explanations of any tradeoffs between aggregations of data at higher-level ECRFs versus the use of Forest Guides (as defined in NENA-INF-009.1-2014) to refer requests between ECRFs that possess different levels of data. As part of that explanation, provide details on how the appropriate ECRF/LVF data will be managed and provisioned for use in overload and backup routing scenarios in the current environment, and any dependencies that might impact provisioning.	X			
	Bidder Response: NENA's general vision for ECRF hierarchy includes local ECRF implementations that have parent "state level" ECRFs, which know coverage areas for all local ECRFs within the state. Each state ECRF would use iterative requests to the National Forest Guide to find the URI for an ECRF serving the location provided in the request. There may be more or less hierarchical levels depending on a given state's implementation. Per the draft NENA document describing provisioning of GIS data to ECRF/LVFs, there is also a more cooperative approach that would allow ECRFs to share coverage regions with other ECRFs. If a request to an ECRF falls outside its coverage region, but it knows which ECRF has the data to respond to the request, the ECRF can send a recursive query to the secondary ECRF and pass the response along to the original LoST client without having to interface with the National Forest Guide. Either scenario is acceptable and meets the NENA guidelines and is supported by RFC 5222. The A9-1-1 ECRF can provide functionality to support either scenario in that it is capable of being provisioned with coverage areas for other ECRF systems as well as acting as a pseudo National Forest Guide until one has been established. The ECRF can be loaded with any number of polygon layers for multiple purposes. Polygon sets can be created, validated and provisioned for anticipated overload, backup routing, abandonment, special event and other routing scenarios as desired. Each would be provisioned with a unique URN. Using optional advanced PRF functions, when the ECRF returns a PSAP URI for routing, the PRF will evaluate it for special policy routing rules. The PSAP policy can direct the ESRP to query the ECRF again with the URN prescribed within the policy (e.g. geospatially distributed abandonment polygons which spread the abandonment load to multiple PSAPs depending on call location). Using the caller's location and the prescribed URN, the ESRP will query the ECRF, which will return the URI associated with the new URN and the location provided in the query.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 53	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** An LVF is a LoST protocol server where civic location information for every call originating endpoint is validated against the SI-provisioned GIS data Describe how the LVF solution interfaces with other LVF solutions which may interface with bidder's solution. Contractor shall coordinate with other LVF solution providers to ensure interoperability between the respective solutions.	X			
	Bidder Response: The A9-1-1 LVF will be a public-facing LVF provisioned for use by service providers outside the ESInet. The PSAP CPE can be pointed to the public-facing LVF or optionally, the ESInet ECRF, which can be configured to respond to LVF queries as well as ECRF. This choice will be left to the State. The A9-1-1 LVF fully supports the NENA standard and will be able to interoperate with external LVFs that also follow the standard.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 54	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **LVF Description** The SI is responsible for provisioning and updating the information used for location validation in the LVF, which shall contain a standardized interface to the SI. Describe how the LVF solution meets the above requirements**.**	X			
	Bidder Response: The LVF is functionally almost identical to the ECRF, but implemented 100% independently from the ECRF as to not interfere with the critical call path functions of the ECRF. Functionally, the address elements that are presented in the LoST request are validated against the GIS data provisioned to the LVF. The LVF can be configured to look at the Address Point layer followed by the Road Centerline layer to locate a match *OR* to only look at the Address Points. The A9-1-1 LVF is secure. In lieu of the NENA PSAP Credentialing Agency (PCA), which does not exist at this time, Intrado will issue digital certificates to LVF clients for authenticated access to the LVF. Provisioning of the LVF is identical to the ECRF provisioning. It is simply another provisioning target of the Spatial Interface. As such, it always contains the same GIS data as the ECRF.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 55	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **Location Validation** The LVF shall be available to validate civic locations at the time a wireline device is ordered— e.g., Service Order Interface (SOI) validation—when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB shall be allowed to periodically revalidate the civic location information against the GIS data contained within the LVF. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 LVF is available to validate civic locations at the time a wireline device is ordered, when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB is allowed to periodically revalidate the civic location information against the GIS data contained within the LVF.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 56	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **High-Availability Design** The LVF shall support all functionality as defined in NENA-STA-010.2-2016, shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability, and shall be provisioned with the same data as the ECRF. Describe how the solution meets or exceeds the above requirements.		X		
	Bidder Response: The A9-1-1 LVF used for service provider validation of their subscriber records is provided in a 99.9% redundant environment. It is implemented in the same manner as the ECRF and is available from two geodetically diverse locations, each with redundant processing elements. The LVF is not part of the call processing function. It is an administrative resource for address validation done outside of call processing. Provisioning of the LVF is identical to the ECRF provisioning. It is simply another provisioning target of the Spatial Interface. As such, it will always contain the same GIS data as the ECRF.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 57	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **Public-Facing LVF** Outline options for a public-facing LVF provisioned for use by service providers outside the ESInet.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The A9-1-1 LVF is a public-facing LVF and is configured for use by service providers outside the ESInet. The PSAP CPE can be pointed to the public-facing LVF or optionally, to the ESInet ECRF, which can be configured to respond to LVF queries as well as ECRF queries. This choice will be left to the State.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 58	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **User Interface and Security** Describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined in NENA-STA-010.2-2016, with particular attention to: 1. the arrangement of the proposed components; 2. user interface and features; 3. and security aspects.	X			

Bidder Response:

As part of the A9-1-1 i3 solution, the Location Validation Function (LVF) is available to OSPs via the LoST protocol (RFC 5222), allowing them to pre-validate customer and device records against the GIS data to ensure that the civic addresses are 9-1-1 valid and will route and plot properly.

1. Below is the arrangement of the proposed LVF solution components.

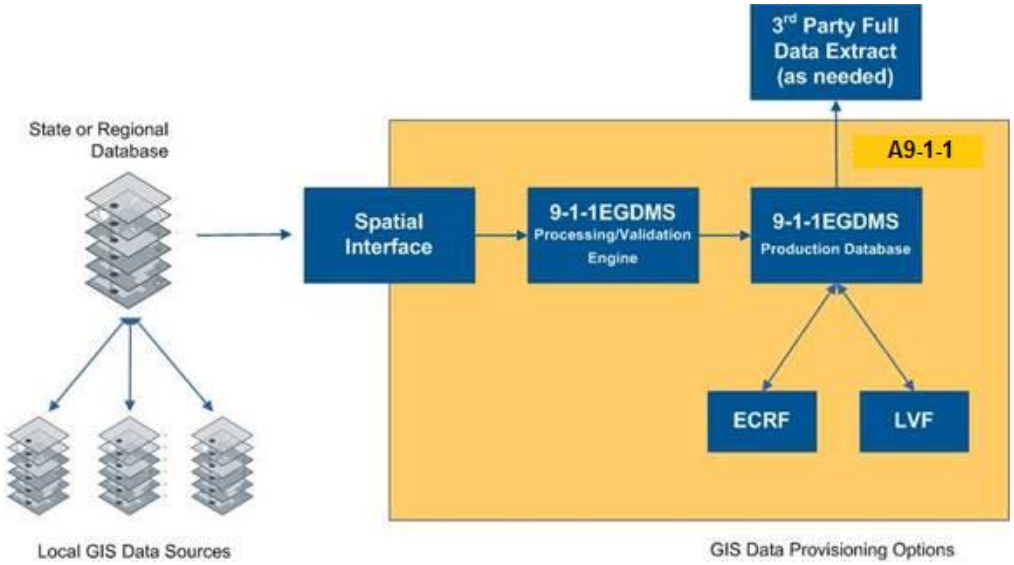

Figure 22: Spatial Interface, ECRF, and LVF

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	2. Functionally, the address elements that are presented in the LoST request are validated against the GIS data provisioned to the LVF. The LVF can be configured to look at the Address Point layer followed by the Road Centerline layer to locate a match OR to only look at the Address Points. The LoST findService transaction with validateLocation set to “true” only supports civic location validation, as there is no concept of validating geodetic locations per NENA STA-010.2. The LVF fully meets the requirements defined in RFC 5222. To assist carriers in their transition Intrado has developed a LoST interworking specification which identifies the specifics of the A9-1-1 implementation along with LoST Request and Response examples to aid the carriers with their LVF client implementations. Note that the User Interface required to interact with the LVF will be the responsibility of the service provider making the LVF LoST requests. The queries between the OSP’s LIS and the LVF is anticipated to be machine-to-machine. Intrado does provide a user interface for single address validations. This tool is named GIS Director. **3.** The A9-1-1 LVF is secure. In lieu of the NENA PSAP Credentialing Agency (PCA), which is just now being rolled out, Intrado will issue digital certificates to LVF clients for authenticated access to the LVF. Intrado will fully support the NENA PCA once it is in place. Provisioning of the LVF is also identical to the ECRF provisioning. It is simply another provisioning target of the SI. As such, it will always contain the same GIS data as the ECRF.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 59	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **SI Description** The SI is responsible for provisioning and updating authoritative GIS data to the ECRF, the LVF, the map viewer, the PSAP tactical map display, CAD systems, and similar applications that consume GIS data. GIS data provisioned by the SI shall undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

The A9-1-1 solution provides the NENA Spatial Interface (SI) as a function of the 9-1-1 Enterprise Geospatial Database Management System (9-1-1EGDMS). The SI is a fully-hosted, managed service that encompasses all necessary processes to receive GIS data from a single source. Data can be submitted in a GIS database managed by a vendor or by the state itself. The SI provides data validation, error reporting, and provisioning to the Emergency Services Network (ESInet) functional elements including Emergency Call Routing Function (ECRF) and Location Validation Function (LVF). The SI provides:

- NG9-1-1 GIS data compliancy checks
- Ongoing GIS data accuracy validation (QA/QC)
- GIS data error reporting
- Provisioning to i3 systems (ECRF/LVF)

The SI performs data quality and data integrity checks that ensures that the data complies with all applicable requirements of NENA 02-010, NENA 02-014 and Attachment B of NENA 08-003. Where these requirements conflict with STA-010.2 and the NG9-1-1 GIS Data Model (draft), the newer requirements documents will be used.

There are currently no NENA guidelines describing any protocols for the SI updates to external systems. The original 08-003 defined use of a Web Feature Service (WFS) to do such, but it has been removed in the current version of the specification (STA-010.2).

Section 4.6 of STA-010.2 states the following:

“Note: OGC 10-069r2 is an OGC Public Engineering Report, not a standard. OGC 10- 069r2 is not believed to be definitive enough to enable multiple interoperable implementations. A future OGC specification or a future revision of this document is needed to describe the protocol definitively. As with any standardized interface in this document; implementations may

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

provide alternatives to the SI interface in addition to the standard interface defined in this section. A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future revision of this document."

While the SI provides a consistent means to update Intrado's ECRF, LVF, and map-based tools at the PSAP, a means to update other vendors' systems must be collaboratively decided upon (e.g., furnish the third-party systems with full data extracts) until such time that the NENA requirements have been created to describe these provisioning functions.

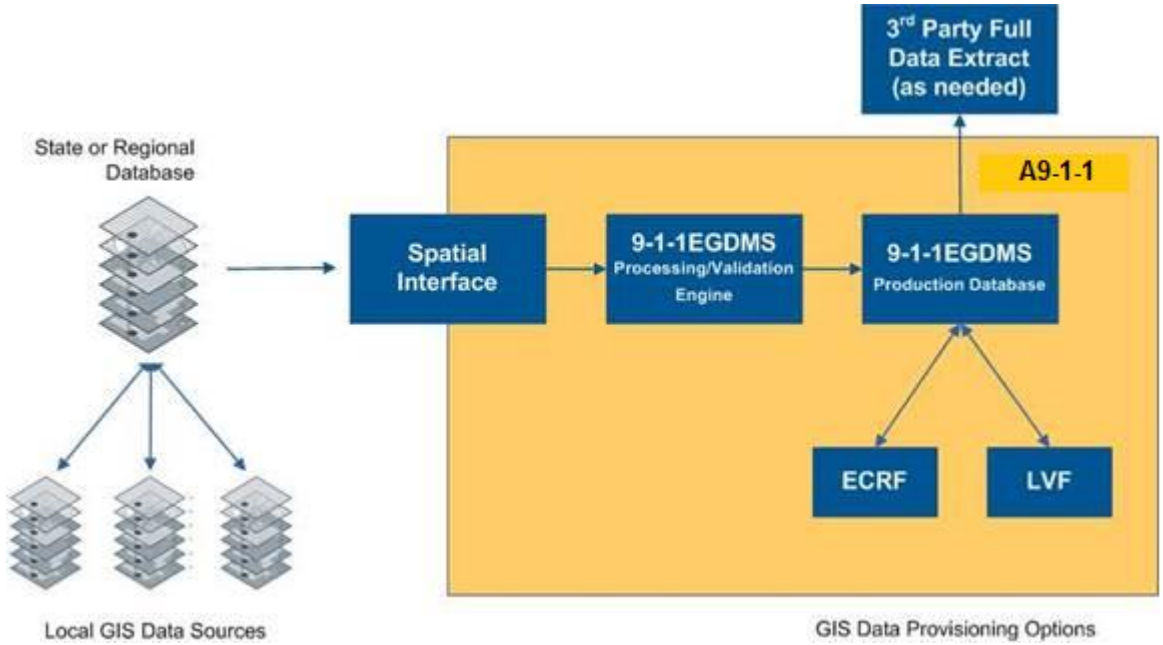

Figure 23: Spatial Interface

GIS updates are provisioned through the Spatial Interface which performs GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system is established to monitor and manage data discrepancies and to track data change requirements.

Validated GIS updates are normalized, re-projected if necessary to WGS84, and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. Each

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. It is recommended that new updates not be sent until the notification has been received from the Spatial Interface that the previous update has finished processing. This timing can vary greatly depending on the feature sets updated and the number of changes within the feature sets. Currently the 9-1-1 EGDMS Data Upload application supports file upload in the following formats: • File geodatabase • Shape file All GIS layers must be in the same coordinate system/projection.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 60	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Web Feature Service and Updates** The SI shall convert the GIS data into the format (data structure and projection) used by the ECRF and LVF, in real-time or near real-time, using a web feature service. The SI shall be able to provision and perform incremental updates, in near real-time, to the ECRF, LVF, the map viewer service, the PSAP tactical map display and similar applications that consume GIS data. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

The SI will normalize the GIS data, converting it into a consistent format, which will meet the ECRF/LVF Lost protocol requirements.

There are currently no NENA guidelines describing any protocols for the SI updates to external systems. The original 08-003 defined use of a Web Feature Service (WFS) did such, but it has been removed in the current version of the specification (STA-010.2). Section 4.6 of STA-010.2 states the following:

“Note: OGC 10-069r2 is an OGC Public Engineering Report, not a standard. OGC 10- 069r2 is not believed to be definitive enough to enable multiple interoperable implementations. A future OGC specification or a future revision of this document is needed to describe the protocol definitively. As with any standardized interface in this document; implementations may provide alternatives to the SI interface in addition to the standard interface defined in this section. A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future revision of this document.”

While the SI provides a consistent means to update the ECRF and LVF, a means to update other vendor’s systems must either be collaboratively decided upon (e.g. furnish the third-party systems with full data extracts) until such time that the NENA requirements have been created to describe these provisioning functions. Intrado is fully supportive of pursuing a collaborative effort to use a common GIS data set for all i3 routing and PSAP tools.

Timing of updates is dependent on the data being updated. Validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF system is near real-time. It is always recommended that “urgent” updates to one or more polygon layers be provisioned without the Site Structure Address Points (SSAPs) or Road Centerlines (RCLs) as validation and provisioning of the SSAPs and RCLs can take a few or many minutes, depending on the size of the feature set being loaded. It is possible to reduce the number of validations performed on the data updates to decrease provisioning speed, but that is balanced by the increased risks of not performing all available validations.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

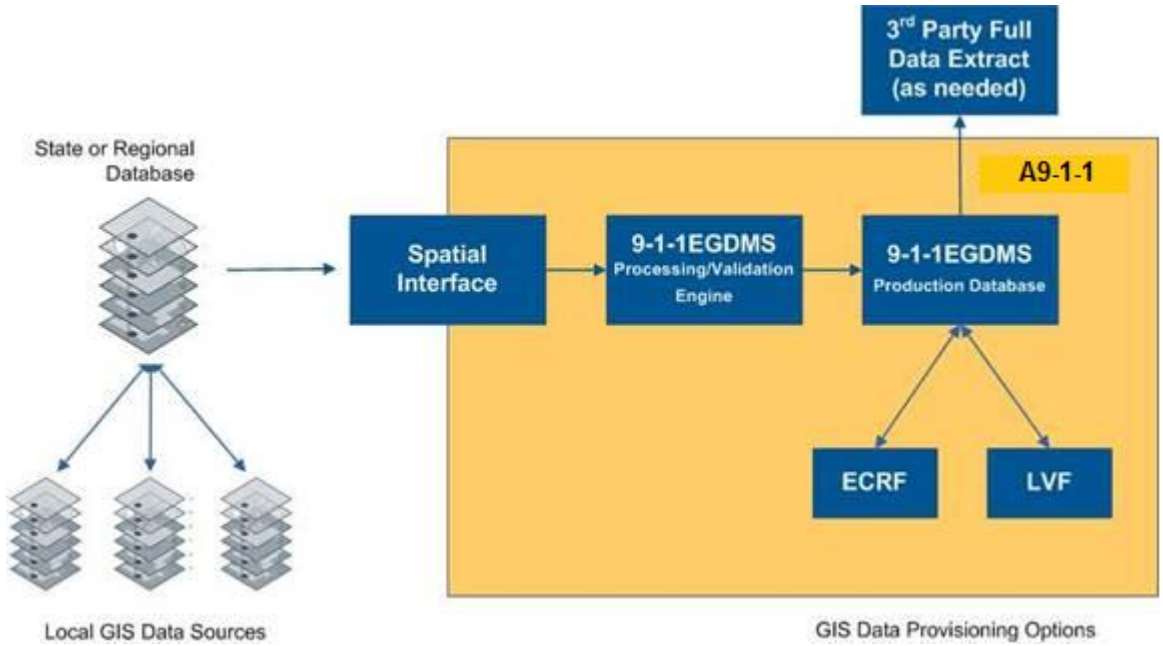

Figure 24: Spatial Interface

GIS updates are provisioned through the Spatial Interface which performs GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system is established to monitor and manage data discrepancies and to track data change requirements.

Validated GIS updates are normalized, re-projected if necessary, to WGS84 and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. It is recommended that new updates not be sent until the notification has been received from the Spatial

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Interface that the previous update has finished processing. This timing can vary greatly depending on the feature sets updated and the number of changes within the feature sets.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 61	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Data Provisioning and Validation** Describe the functionality of the proposed SI solution in sufficient detail to explain the validation of GIS data and data updates prior to provisioning into the ECRF and LVF, along with the means of real-time or near real-time provisioning of incremental updates to the GIS data provisioned to the ECRF and LVF.	X			

Bidder Response:

The GIS updates are provisioned through the Spatial Interface (SI) which performs GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted data being provisioned in the ECRF that may introduce ambiguity in the data that would prevent the ECRF from being able to make a definitive response to certain requests. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one.

New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements (two per geographically diverse location), the ECRF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the Spatial Interface which will send out alarm notifications. If this occurs the previously active map layer will remain active. It is recommended that new updates not be sent until the notification has been received from the Spatial Interface that the previous update has finished processing. This timing can vary greatly depending on the feature sets updated and the number of changes within the feature sets

The SI validation engine refers errors back to the originating 9-1-1 Authority in comprehensive reports that are retrieved in the 9-1-1EGDMS portal. Validation errors must be corrected by the 9-1-1 Authority within their own GIS database. Updates are submitted and processed on an on-going basis. Ongoing 9-1-1EGDMS validations include road centerline, address point, and polygon for each data upload.

Features with critical errors cannot be loaded into the A9-1-1 systems due to incompatibility or addressing errors that would result in inaccurate call routing. All critical errors should be resolved prior to switching to geospatial call routing.

Critical Error Description

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Any features with critical errors will not be provisioned. Errors must be corrected and resubmitted to load to production ECRF and LVF and avoid default routes or failed validation. • Unique ID Duplicate: The feature's Unique ID is duplicated within the agency's layer • Geometry Error: A record exists in the attribute table that is not associated with a geographic feature or the geometry of a feature is in error. • Attribute Duplicate: The feature's attributes are duplicated in multiple features, but each feature has a unique location • Address Range Overlap: An overlap exists in one or both sides of the address ranges between two connected and identically named road centerline segments. • Field Constraint: An attribute value is incompatible with the EGDMS database schema and cannot be loaded into the database. • Outside Authoritative Boundary: All or part of the feature falls outside the Authoritative Boundary. • Boundary - Neighbor – Gap: A gap exists between the boundary polygon and an adjacent data source's boundary polygon. • Boundary - Internal – Gap: A gap exists between the boundary polygon and another boundary polygon within the database. • Boundary - Neighbor – Overlap: The boundary polygon feature overlaps an adjacent data source's boundary polygon. • Boundary - Internal – Overlap: The boundary polygon feature overlaps another boundary polygon within the database. • Routing URI: The routing Uniform Resource Identifier (URI) is either missing or invalid within the service response boundary polygon. Timing of updates is dependent on the data being updated. Validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF system is near real-time. It is always recommended that “urgent” updates to one or more polygon layers be provisioned without the Site Structure Address Points (SSAPs) or Road Centerlines (RCLs) as

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	validation and provisioning of the SSAPs and RCLs can take a few or many minutes, depending on the size of the feature set being loaded. It is possible to reduce the number of validations performed on the data updates to decrease provisioning speed, but that is balanced by the increased risks of not performing all available validations.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 62	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Use of the Commission's GIS Data Model** 1. Describe how the bidder's solution will use the Commission's GIS data model (Attachment B) without modification to the schema. 2. Define bidder's processes and methods to receive and incorporate the updated SI datasets. 3. Describe bidder's proposed workflow for receiving GIS updates from regions to allow for a smooth transition. 4. Describe all security and monitoring aspects, and any additional features supported by the proposed SI.	X			
	Bidder Response: **1.** GIS updates are provisioned through the SI. The SI provides a field mapping service which allows the Commission's data model to be mapped to the corresponding fields in the ESInet GIS data model, without any adjustment to customer's data model. Unless the local data model changes, this is a one-time operation. **2.** Data can be loaded by full feature set or can optionally be updated via delta updates. Shapefile and File Geodatabase are the current supported formats. **3.** The A9-1-1 solution provides the NENA Spatial Interface (SI) as a function of the 9-1-1 Enterprise Geospatial Database Management System (9-1-1EGDMS). The SI is a fully-hosted, managed service that encompasses all necessary processes to receive GIS data from single or multiple data sources. Data can be submitted in a GIS database managed by a vendor or by the state itself. Updates are made via a secured portal that requires two-factor authentication for access. **4.** The SI provides data validation, error reporting, and provisioning to the Emergency Services Network (ESInet) functional elements including Emergency Call Routing Function (ECRF) and Location Validation Function (LVF). The SI provides: • NG9-1-1 GIS data compliancy checks • Ongoing GIS data accuracy validation (QA/QC) • GIS data error reporting • Provisioning to i3 systems (ECRF/LVF) The SI performs GIS validations, including validations to ensure routing integrity. The QA/QC processes provided during validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. A change control model is implemented to track changes between the GIS provisioning platform and the production ECRF instances. The GIS layers supported include: • Street Centerlines - Street centerline data for your agency's jurisdiction. • Fire Response Boundary - Fire response boundary polygons for your agency's jurisdiction. • Site/Structure Address Point - Site/structure address points for your agency's jurisdiction. • Law Response Boundary - Law response boundary polygons for your agency's jurisdiction. • PSAP Area Boundary - Public Safety Answering Point boundary polygons for your agency's jurisdiction. • EMS Response Boundary - EMS/medical response boundary polygons for your agency's jurisdiction. • Emergency Service Zone - Service response boundary (ESN boundary) polygons that include Fire, Law, and EMS response agencies in your jurisdiction. • Municipal Boundary - Municipal boundary polygon(s) for your agency's jurisdiction. • Authoritative Boundary - Authoritative boundary polygon that covers the geographic region for which your agency has jurisdiction.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 63	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** Describe how the solution interfaces with other LDB solutions which may participate in or interface with bidder's solution. Contractor shall coordinate with other LDB solution providers to ensure interoperability between the respective solutions. Also explain how the proposed solution would deal with multiple ALI/MSAG databases and the locations where ALI steering may be in place.	X			

Bidder Response:

Intrado strongly encourages all carriers to move to the i3 specified standards. With the i3 model, carriers will maintain their own LIS/ADR in which they provide customer location information by reference or value at the time of the call. Intrado understands that for some carriers this option is not yet available. During the time of transition to i3 Intrado's preferred methodology, in order to maintain reliability and dependability of location data, is for carriers to utilize the already available and deployed centralized LDB/ALI database managed by Intrado. The Intrado A9-1-1 LDB/ALI database is a transitional system which allows for:

- Established OSP's service order address input, processes, and error management to be maintained
- Established interaction and error resolution with MSAG coordinators to remain in place
- Translating the Intrado validated location data, real time, into i3 compliant protocols to use for PSAP in any state of readiness for Next Gen Services.

If the carrier has a strong preference to utilize a non-i3 LDB provided by themselves or a third party, the Intrado A9-1-1 system can support that solution. Additional resources, processes and procedures will need to be established in order to create a reliable, redundant, and dependable solution for the state of Nebraska. Intrado will be available to complete interoperability with other LDB solution providers including setting up connectivity, having a highly reliable and redundant solution, network monitoring and alarming, as well as interoperability testing in a pre-production environment. These solutions would need to be examined on a case-by-case basis.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 64	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** **LDB Description** A LDB serves as both a legacy ALI database and as a LIS in an i3-compliant NG911 environment. The LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can utilize the new protocols required in an NG911 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or Gateway Mobile Location Center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols. Describe the functionality of the proposed LDB, including additional features and capabilities, error handling, FoCR capabilities, logging and deployment recommendations in detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface, and features, and security aspects.	Comply X	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: Intrado's Location Database Services provides a suite of feature-rich services that allows for the eventual replacement of legacy ALI services, while continuing to support all legacy ALI services in the interim. Intrado Location Database Services, in conjunction with Intrado's A9-1-1 Services, provides all the necessary services to eliminate any need for a fully featured i3 end point to interface with a legacy ALI database. The Intrado transitional LIS solution supports HELD queries in conformance with RFC 5985 as well as Additional Data queries in conformance with RFC 7852. It leverages the legacy ALI database, which also functions as the LDB by providing the location information to the LIS Interface, which formats the HELD response to the LNG or PSAP CPE. Connectivity for E9-1-1 PSAPs remains unchanged. The LIS Interface receives and responds per the HELD protocol for i3-compliant CPE, allowing simultaneous support for both NG9-1-1/i3 and legacy standards for PSAPs throughout the migration timeline. The LIS interface provides all of the i3 logs for HELD per NENA-STA-010.2-2016. While the Intrado ALI/LDB previously supported NENA 04-005 which defines ALI Query Service (AQS), that service has been retired due to lack of market demand and increased demand for support of the i3 protocols. The Intrado LDB also supports all data retrieval protocols required to obtain information for wireless calls by querying the MPC, GMLC or VPC and returning the information retrieved in the format required by the PSAP CPE. Regardless of the legacy data source, the LIS Interface follows Appendix A of NENA STA-010.2-2016 describing the mapping of data elements between legacy and NG9-1-1 when forming a HELD response for delivery to i3 compliant CPE.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Currently, the LDBs used for the Intrado A9-1-1 Service are located outside of the ESInet – they are the legacy ALI systems managed by Intrado Life & Safety, and they do not need any further deployment work to be utilized.

The LIS interfaces within the ESInet, which communicate with the LDB, do reside in the ESInet: they have already been deployed and tested as part of the Intrado A9-1-1 platform buildout and acceptance.

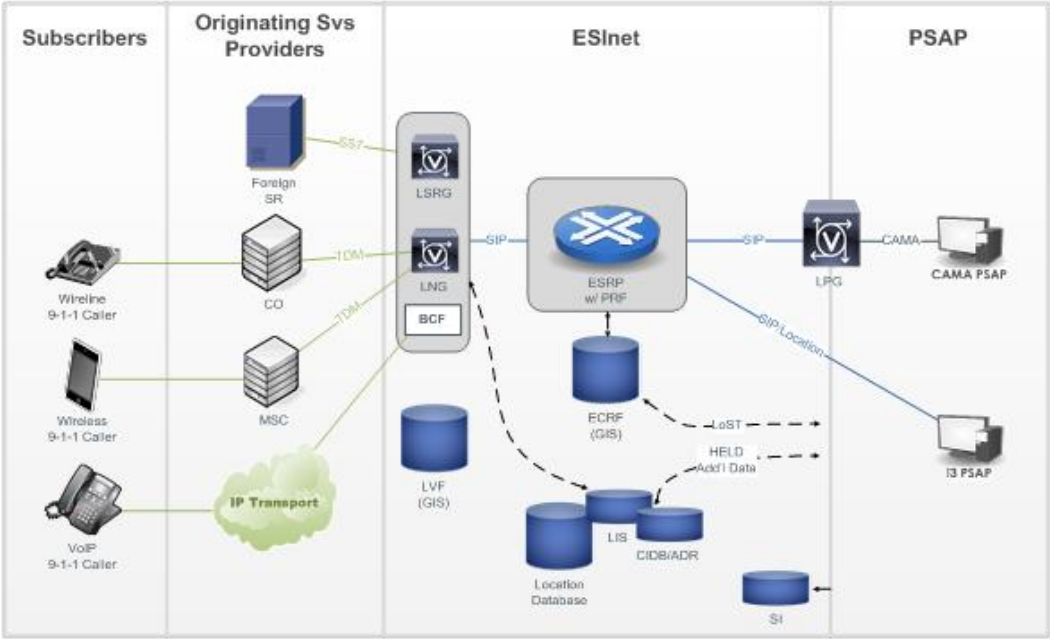

Figure 25: Transitional State with Location Database Components

Support for LIS Functionality and NENA i3 Interfaces

Intrado's A9-1-1 Service uses a Legacy Network Gateway (LNG) that provides a mechanism to obtain the caller's location at the time of the call by using the Location Interwork Function (LIF) to query the caller's appropriate Location Information Server (LIS) database.

Interactions between the LIS interface (transitional) and the LNG are secured within the ESInet. Interactions with external LIS systems will utilize digital certificate-based authentication as defined by NENA and managed by the PSAP

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Credentialing Agency (PCA), once available. Until that time, Intrado will manage credentialing and the issuance of digital certificates to help ensure protection and security. This mechanism will also be utilized for PSAP access to systems within the Intrado ESInet, including access to the LIS interface, ADR interface, and ECRF. During carrier transition to NENA i3 compliance, Intrado will maintain the HELD interface into the ALI platform to simultaneously support legacy PSAPs and i3 PSAPs. The HELD interface into the Intrado Location Database is leveraged by the LNG to retrieve PIDF-LO, by value and/or reference, to be delivered to the PSAP within the SIP messaging. The HELD interface is also presented to the PSAP CPE to provide dereferencing services and/or provide location updates for wireless calls. Note that not all ALI fields map to PIDF-LO, for example, Class of Service and Customer Name. As such, Intrado will also provide an ADR interface to retrieve this information to be included in the SIP signaling. For these fields, the LNG supports the Additional Data protocol (draft-ietf-ecrit-additional-data-28) to provide these data fields via the Call Additional Data Repository (ADR), formerly known as the Call Information Database (CIDB). The Additional Data specification was recently finalized as RFC 7852. The differences between draft 28 and the final RFC are minor and updates will be placed on the roadmap, as it is critical that the implementations are coordinated with the different i3 functional elements (ADR, LNG, Terminating ESRP) that leverage this protocol. Carriers providing their own LIS services must continue to send their SOI records to Intrado to be validated and provisioned to the Intrado ALI system until all PSAPs in the State are served by i3-compliant OSPs. Once compliant, all calls originating from their network will leverage their LIS to provide location information server functions, including dereferencing of locations provided by reference to the LNG or PSAP. At this time, the ALI database will no longer be needed and carriers providing their own LIS will no longer have to send SOI to Intrado for ALI provisioning, though they will be required to utilize the ESInet LVF for location validation before provisioning records to their LIS. Carriers who still do not have a LIS will continue to send SOI records for validation and provisioning into the ALI database. A carrier LIS is considered outside of the ESInet, while the jurisdiction's ALI and its associated LIS interface is located inside the ESInet within the secured zone protected by firewalls and authentication. **Support for Legacy Interfaces** The Intrado ALI database systems are deployed in a redundant, geographically diverse configuration to ensure the highest reliability and survivability. All critical system components are redundant, and the application employs application level monitoring and automated failover to recover from system failures without impact to 9-1-1 call processing.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

The Intrado ALI database systems meet or exceed legacy interface standards including relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI DBMS and NENA standards (J-036, E2, E2+, NCAS, CAS).

The Intrado ALI database systems include the following features:

- Query response verification messaging between ALI systems and heart beating/application monitoring systems are employed to ensure high availability. Dynamic ALI updates retrieved from selective routers and wireless/VoIP Mobile Positioning Center (MPC)/ VoIP Positioning Center (VPC) systems are shared between ALI systems to help prevent network and system outages.
- Retrieval of wireless and Voice over Internet Protocol(VOIP) location updates via the E2 or PAM (PSAP to ALI Message specification) interfaces.
- Steering to retrieve location information for Wireline calls from multiple external database systems. ALI steering is highly configurable and supports Function of Code R (FOC-R) steering, trunk steering, Telephone Number (TN) range steering, and No Record Found (NRF) steering.
- A highly configurable ALI format editor and services to support customized ALI formats.

Intrado will provide a feature-rich, highly configurable web-based data management system that allows PSAPs to fully self-manage their private MSAG and ALI DB records and to resolve any error fallout. 9-1-1 NET functionality includes MSAG Query and MSAG Change Requests (CRs) allowing users to make changes to the MSAG for their jurisdiction/region. 9-1-1 NET also allows users to manage ALI discrepancy requests including No Record Found (NRF), incorrect address, and other discrepancies associated to an entry that is loaded in the LDB. The enterprise service is accessed via a web-based portal following secure sign-on.

Synchronization of GIS and LDB

The Intrado A9-1-1 solution utilizes a database management system that performs validation of Carrier SOI records before records can be placed in the LDB/ALI. In this model, there is no need for revalidation of records in the LDB using the LVF, as advanced validation mechanisms are utilized in the database management system that surpass the current capabilities of the LVF.

For Carriers who are providing their own LIS, the LVF is available for validations and subsequent revalidations. Authentication of any server accessing the LVF will be required.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Intrado also offers optional Transitional Data Management Services that will allow GIS data to serve as the authoritative source for 9-1-1 address validation. With this service, Intrado will replace the jurisdiction's legacy tabular MSAG with a GIS-derived validation to ensure continuous synchronization of carrier subscriber records submitted for SOI validation against the jurisdiction's GIS data. This approach ensures continuous ongoing synchronization with GIS updates submitted by the jurisdiction through Intrado's Spatial Interface and simultaneous support for NG9-1-1 GIS and legacy address standards. Intrado's NG9-1-1 Transitional Data Management provides the following benefits: • Operational efficiency – 9-1-1 address management using GIS data • Highest NG9-1-1 data accuracy - continuous GIS to ALI synchronization • No changes required for carriers - support of legacy OSP provisioning and ALI • Full i3 readiness – Streamlines deployment to Intrado A9-1-1 Services This service includes a map-based web tool (GIS Director) that allows customers to review their 9-1-1 data through a map interface, request changes to resolve errors and discrepancies, and GIS validate addresses against the Intrado LVF.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

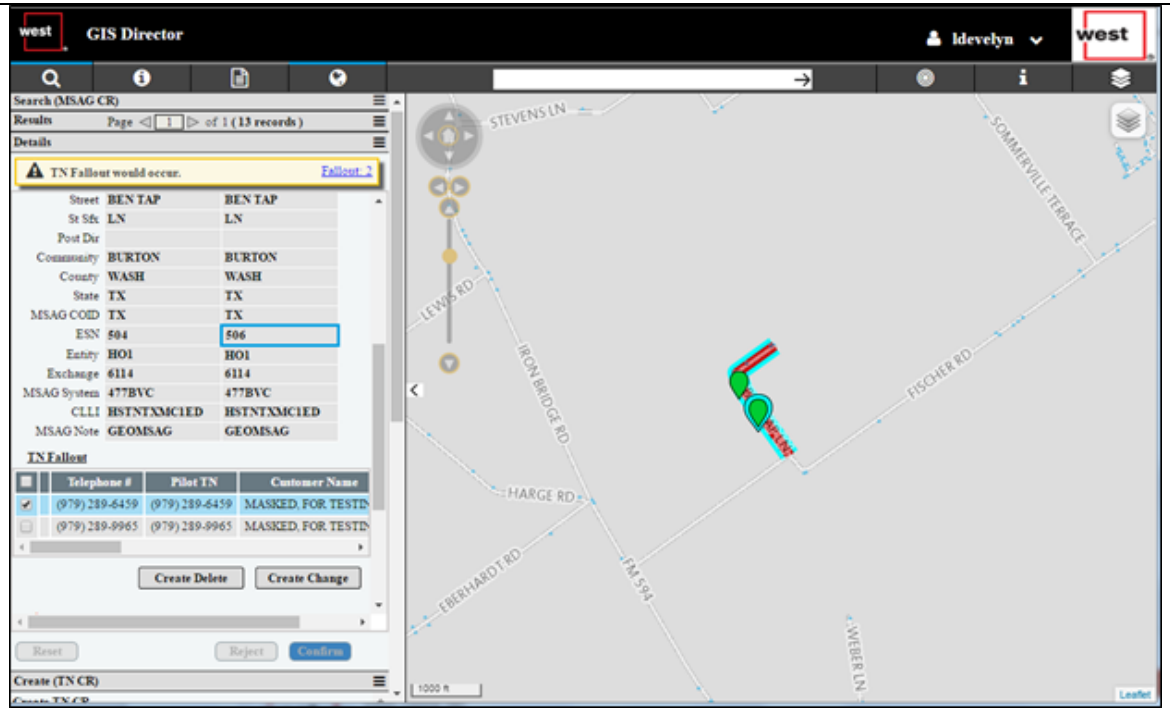

Figure 26: geoMSAG Error Resolution

Any additional documentation can be inserted here:

The LDB shall meet the following requirements:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI Database Management System (DBMS).	X			
Shall be capable of assuming the role of a location DBMS as defined in NENA-INF-008.2-2013, NENA NG9 1-1 Transition Plan Considerations.	X			

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Shall support NENA standards J-036, E2, E2+, non-call-associated signaling (NCAS) and call-associated signaling (CAS).	X			
Shall be able to provide LIS functionality and interfaces as defined in NENA-STA-010.2-2016	X			
Shall be able to seamlessly interact with a NENA i3-compliant ECRF, as described in NENA-STA-010.2-2016.	X			
Shall be able to dereference a location by reference, as defined in NENA-STA-010.2-2016.	x			
Shall be able to dereference requests for additional information, as defined in NENA-STA-010.2-2016.	X			
Shall be able to interface simultaneously with multiple wireless callers.	X			
Shall be able to interface simultaneously with multiple remote ALI databases.	x			
Shall automatically detect, import and validate customer records (SOI records).	X			
Shall have the ability to be used simultaneously by both NG911-capable and E911 capable PSAPs.	X			
Shall allow different PSAPs to use different ALI formats based on individual needs.	X			
Shall utilize LVFs to validate civic addresses.	X			
Shall support PIDF-LO location data formatting as defined in NENA-STA-010.2-2016.	X			
Shall periodically reevaluate the location information using LVF functions within the system.	X			
Shall be able to communicate with NG911 functional elements using the SIP and HELD protocols.	X			
Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response.	X			
Shall be able to dereference additional data requests.	X			
Shall consistently respond to all requests within 400 milliseconds (ms).	X			

NGCS 65	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** **Integration of Multi-Line Telephone System Data** The LDB shall support the Integration of Multi-Line Telephone System (MLTS) databases. As part of this migration, Contractor shall be responsible for migrating records from the current MLTS databases to the LDB. Provide details on the database migration process and the user interface for management of these MLTS data records.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	As the State is currently utilizing Intrado ALI databases, no migration of MLTS records would be required. Intrado offers enterprise services that allow records to be submitted with a detailed location description for each end user behind a PBX or Call Server. Both batch record submission and a web-based tool for managing and submitting individual location detail updates are offered for a fee to our customers. Additionally, enterprise customers can utilize a web-based application to manage records in the DMBS, as the application allows view of records and manual manipulation limited to user's access. Use of the web-based application for enterprise record management does require the end-user customer acquire a NENA ID in order to identify with their records and limit change access.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 66	**Next Generation Core Services Elements (NGCS)** **Discrepancy Reporting** 1. Provide details regarding the proposed solution's report functions for notifying PSAPs any time a discrepancy is detected concerning the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, explain how a report will be sent for the purpose of reporting the discrepancy to multiple responding PSAPs, as determined by the Commission. Discrepancy reporting is outlined in Section 4.7 of NENA-STA-010.2-2016. 2. Describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.	X			
	Bidder Response: Intrado has a full-featured solution for Discrepancy Reporting for legacy and Next Generation PSAPs. Once the NENA requirements are hardened we will add to our roadmap/release schedule. Full i3-compliant discrepancy reporting is a future development. Until such time, A9-1-1 supports equivalent discrepancy reporting using a combination of 9-1-1 NET for the reporting of ALI Discrepancies (DRs) and MSAG Change Requests (CRs) and EGDMS for the reporting of GIS-related validation errors. Misroutes, Policy Routing discrepancies, incomplete/incorrect PIDF-LO, and incomplete/incorrect Additional Data are reported via ALI DRs. Because of the integrated nature of the BCF, ESRP, and PRF, discrepancies are identified in logs and the logs are actively monitored. Alarms are programmatically set to identify specific discrepancies and automatically provide notifications when the specified events occur. Further, the A9-1-1 ESRP and PRF provide safeguards around how routing policies are entered to help ensure that only valid policies are configured to prevent discrepancies. Policies and rules are tested prior to enabling in production. Fall-back routing (e.g., default trunk group routing) due to inaccurate location or subscriber data, such as no record found, is reported via a 9-1-1 NET ALI DR for research and correction. ECRF, LVF, and SI discrepancies are handled via data validation reports each time GIS data is provisioned via the SI. Routing discrepancies are reported via an ALI DR using 9-1-1 NET. Any misroutes are individually investigated as the cause may be in one of several places. Access to 9-1-1 NET requires two factor authentication for all users. The following list, as provided in STA-010.2, lists the types of discrepancies that will be addressed with a full i3 solution. Note that almost all discrepancies begin with a human; very few can be automatically generated. The list also includes how the discrepancies would be initiated using current applications as noted above.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• The LIS needs to file a Discrepancy Report on the LVF.
	  ○ Customers with ALI Location Data Management services would create a MSAG CR through 9-1-1 NET.
	• The ECRF/LVF may be receiving data from another ECRF/LVF and thus will file a DR on its upstream provider.
	  ○ When talking about receiving coverage area data, that would allow one ECRF to recurse to another ECRF; that coverage area would be provisioned through the SI, which will generate any reports regarding discrepancies in the data.
	• The ECRF/LVF needs to file a DR on the GIS.
	  ○ At the time of provisioning via the SI, error reporting would identify these discrepancies.
	• The ESRP needs to file a DR on the owner of a routing policy (PSAP, ESRP) that has a problem.
	  ○ The A9-1-1 ESRP and PRF are integrated and safeguards exist on how routing policies are entered to help ensure only valid policies can be configured.
	• The PSAP needs to file a DR on an ESRP if a call is misrouted.
	  ○ ALI Location Data Management customers would create an ALI DR through 9-1-1 NET to be investigated by an analyst. As with any misroute, the cause of the misroute could be in multiple places.
	• Any client of an ECRF needs to file a DR on the routing data.
	  ○ ALI Location Data Management customers would create an ALI DR through 9-1-1 NET to be investigated by an analyst. As with any misroute, the cause of the misroute could be in multiple places.
	• A PSAP or ESRP needs to file a DR on a LIS.
	  ○ Customers with Intrado ALI Location Data Management services would create an ALI DR through 9-1-1 NET.
	• A PSAP or ESRP needs to file a DR on an ADR/IS-ADR.
	  ○ Customers with Intrado ALI Location Data Management services would create an ALI DR through 9-1-1 NET.
	• A BCF, ESRP, or PSAP needs to file a DR on an originating network sending it a malformed call.
	  ○ Complies with Future Capability. (see *Proprietary Information* file)

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Any client may need to file a DR on the ESInet operator.
	  ○ This requirement will require further explanation in a future release of NENA STA-010.
	• One PSAP needs to file a DR on another PSAP that transferred a call to it.
	  ○ Not applicable for the services requested in this RFP.
	• A data user may need to file a DR on a data owner due to rights management issues.
	  ○ This requirement will require further explanation in a future release of NENA STA-010.
	• A log client (logging entry or query) may need to file a DR on the Logging Service.
	  ○ Complies with Future Capability. (see *Proprietary Information* file)
	• Any entity may have to file a DR on another entity due to authentication issues.
	  ○ These discrepancies would currently be reported by opening a trouble ticket.
	• An ESRP or PSAP may need to file a DR on a Border Control Function.
	  ○ This requirement will require further explanation in a future release of NENA STA-010. Interactions between the ESRP and BCF would be logged and alarmed upon if discrepancies cause interoperability issues. A PSAP may file a suspected DR using a trouble ticket.
	• Any Policy Enforcement Point may need to file a DR on a Policy owner due to formatting, syntax, or other errors in the policy.
	  ○ This requirement will require further explanation in a future release of NENA STA-010. Depending on where an error takes place, it would typically be via an ALI DR in 9-1-1 NET or a trouble ticket.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

NGCS 67	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** PSAPs may have a variety of logging recorders capable of recording SIP traffic and associated media. PSAPs will use the Emergency Call Tracking System (ECaTS) for call logging and capture event details. The Commission will gather statistical data from PSAPs through ECaTS. Describe how the solution interfaces with logging recorders and ECaTS.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado will provide ECaTS with a near real-time feed of NGCS elements from the Intrado -managed i3 logger for the State of Nebraska. The interconnection between the NGCS platform and ECaTS data servers is in place and in operation. i3 element data follows NENA defined specifications. Dedicated redundant and diverse connectivity between the Intrado A9-1-1 NGCS i3 logger and the ECaTS server architecture is established and actively monitored.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 68	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Event Logging Description** Extensive logging of NG911related events, transactions, media, and operations is required. All log entries shall be accurately time-stamped. Logging must include all elements in the call flow including logging of NG911related events within ESInets, the NGCS, the PSAP, and related operations, and is a standardized function used throughout ESInets, NG911 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress, and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The A9-1-1 solution logs hundreds of data points for each call that traverses the system to assist in tracking and troubleshooting calls. Events are logged 24x7x365 and include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. Only authorized processes have write access. The A9-1-1 Customer Management Portal (CMP) provides participating PSAPs and approved personnel 24x7 access to call detail records through a secure, web-based portal. The call detail records provide the user with all of the pertinent information for each call. A drop-down in the CMP allows the user to choose the time zone for the timestamps. Users have a predetermined PSAP or set of PSAPs for which they are able to view statistics. For example, some users will only be able to view their own PSAP's statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping. Event data is time stamped upon ingress of payload entry through the LNG or BCF and at the time of answer and disconnect at the PSAP. Event data also tracks the time for each functional element to perform routing and PSAP assignment, by tracking the time it takes to traverse from the selective router to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics. Event data is archived for seven years. A9-1-1's standard reporting suite provides the following reports through a web-based interface. • Event Count Reports per Hour– provides metrics for total calls by hour for a day, week or month. • Event Count by Routing Reason and Destination – Provides metrics for total calls in which the Customer PSAP participated as the Primary versus Alternate route per route type, broken out by hour for day, week, or month. • Event Count by Type – Provides metrics for total calls by call type (wireless, wireline, VoIP) broken out by hour for day, week, or month.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Event Count by Incoming Trunk Group – Provides metrics for total calls by trunk group with an hourly breakout. • Bridge Call Summary – Provides metrics for calls bridged in or out by bridge type (fixed, selective, manual). Call detail is available for each bridged call. • Routing Database Processing – provides a breakout of initial calls where the Customer PSAP was Primary by selectively routed versus default routed with a No Record Found (NRF) breakout. • Event Setup Time – provides statistics on the time to route and deliver calls where the Customer PSAP is Primary, including the minimum, maximum, median and average times. • Event Count Reports per Hour– provides metrics for total calls in which Customer's PSAP participated by hour for a day, week or month.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 69	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Integration with Call-Handling Equipment** 1. Describe how bidder's event-logging solution may integrate with the each PSAP's call-handling equipment, to provide a complete, end-to-end view of a call. 2. Describe how the Commission can gain access to information in the event-logging solution. 3. Describe the requirements of the PSAP's call-handling equipment, software license agreements, and interfaces required to support integration with the bidder's event-logging solution.	X			

Bidder Response:

1. A9-1-1 provides an i3 logging capability per the NENA STA-010.2 specification. Intrado supports near real-time log delivery and web service interfaces for log retrieval from authorized clients. Intrado will provide ECaTS with a near real-time feed of i3 NGCS element data for the State of Nebraska. The interconnection between the NGCS platform and ECaTS data servers is in place and in operation. i3 element data follows NENA-defined specifications.

2. In addition to the ECaTS solution already contracted to the State directly, and the new reports that ECaTS will provide with the availability of the i3 information made available from Intrado, the Intrado A9-1-1Customer Management Portal (CMP) provides participating PSAPs and approved personnel 24x7x365 access to a reporting suite including call detail records through a secure, web-based portal. Call detail records provide the user with all of the pertinent information for each call.

The CMP web-based reporting suite is a business intelligence reporting tool for metrics reporting supplies authorized users with A9-1-1 Routing and Location Data Management reports. Access is available to authorized users via two-factor verification.

CMP provides access to the following information:

- Operation State of PSAP(s)
  - Current status
  - History of changes in status including who made the change and when
  - Resource Counts (available TDM trunks or IP Contacts)
  - Operation State color-coded with indications for In Service/Out of Service
- PSAP Route Lists
  - Primary
  - Alternative

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• Abandonment • Backup • Fixed Transfer/Bridge List • Statewide PSAP Directory • Call Detail Records • Call Detail Records provide PSAPs information including alternately routed calls, i3 to ESN fallback, and transferred calls Users can view summary data for a "big picture" view, and in many cases, drill down to the detail for a more "granular" view. Users can also download a report as a comma-delimited file, which can be imported into Excel or another database application. The A9-1-1 tool gives users the ability to drill down and capture additional contextual information that can be used to more efficiently manage ongoing 9-1-1 operations. A secure web portal in a standardized HTML format, customized to each authorized user's profile, access level, and preferences, provides access to more than 270 compliance reports and other existing reports. Users can create customized reports and perform real-time data and trend analysis, including graphing, based on daily data updates. The web-based tool gives 9-1-1 officials the ability to convert static data into actionable information anywhere and at any time. As shown in the following sample screenshots of the reporting tool, hyperlinks allow the user to easily drill down to further levels of detail. For example, clicking on the Company A link in the second example below, allows the user to see further detail on Service Order processing. The results are typically returned within one second.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Monthly ALI Retrieval Report

July 2025

Region: Region Total

Back one page | Report Description | Export to Excel | Printer-friendly version

Hourly Distribution

Hour	ALI Retrievals	Base Retrievals	Manual Retrievals
0:00	56,512	41,618	4,521
1:00	48,061	35,249	4,124
2:00	40,780	29,552	3,446
3:00	32,989	23,837	2,610
4:00	26,876	19,404	2,294
5:00	27,863	20,286	2,315
6:00	38,166	27,542	3,229
7:00	52,753	38,625	5,135
8:00	66,718	49,335	6,549
9:00	76,106	56,769	7,811
10:00	84,985	62,815	8,409
11:00	91,946	67,658	8,580
12:00	97,949	71,091	8,818
13:00	102,265	74,747	9,006
14:00	108,013	78,901	9,897
15:00	116,440	84,929	10,443
16:00	120,959	87,466	10,438
17:00	122,115	87,798	9,425
18:00	116,916	83,752	9,645
19:00	103,451	74,832	8,316
20:00	94,838	68,992	7,855
21:00	84,514	62,147	7,582
22:00	74,020	54,573	6,100
23:00	61,190	44,983	5,366
Total	**1,846,425**	**1,346,901**	**161,914**

Special Case Retrievals

Description	ALI Retrievals	% ALI Retrievals	Base Retrievals	% Base Retrievals
Anonymous Calls 911-0000	50,255	2.72%	n/a	n/a
Seizure with no ANI 000-0000	14,240	0.77%	n/a	n/a
ESCO Calls 911-0XXX	9,909	0.54%	n/a	n/a
Single Link Retrievals	50,092	2.71%	30,794	2.29%
No Records Found	125,095	6.77%	110,696	8.22%
Selectively Routed	1,674,243	90.67%	1,233,608	91.59%
Correctly Routed	1,653,401	89.55%	1,212,766	90.04%
Misrouted	20,842	1.13%	20,842	1.13%
Non-selectively Routed	172,182	9.33%	113,293	8.41%

Class of Service Breakout

Class	Description	ALI Retrievals	% ALI Retrievals	Base Retrievals	% Base Retrievals
0	Business with off premise ext	4,922	0.27%	3,104	0.23%
1	Residence	488,681	26.47%	378,492	28.10%
2	Business	236,833	12.83%	181,247	13.46%
3	Residence PBX	1,079	0.06%	830	0.06%
4	Business PBX	104,021	5.63%	57,733	4.29%
5	Centrex	43,003	2.33%	35,592	2.64%
6	Coin (out-going only)	14,890	0.81%	10,684	0.79%
7	Coin (two way)	45,693	2.47%	32,842	2.44%
8	Wireless/Mobile	203,111	11.00%	107,616	7.99%
9	Residence with off premise ext	1,166	0.06%	1,005	0.07%
W	Wireless	120,487	6.53%	100,198	7.44%
X	Wireless	44,145	2.39%	37,889	2.81%
G	Wireless Phase I	288,784	15.64%	247,467	18.37%
H	Wireless Phase II	108,292	5.86%	41,506	3.08%
	NRF	125,095	6.77%	110,696	8.22%
	Other	16,223	0.88%	0	0.00%
	Total	**1,846,425**		**1,346,901**	

ODPM User Home Page | Reports Page | ODPM Help | Email Metrics Support

Site Map | Privacy | Legal | Copyright

Figure 27: Sample ALI Retrieval Report

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

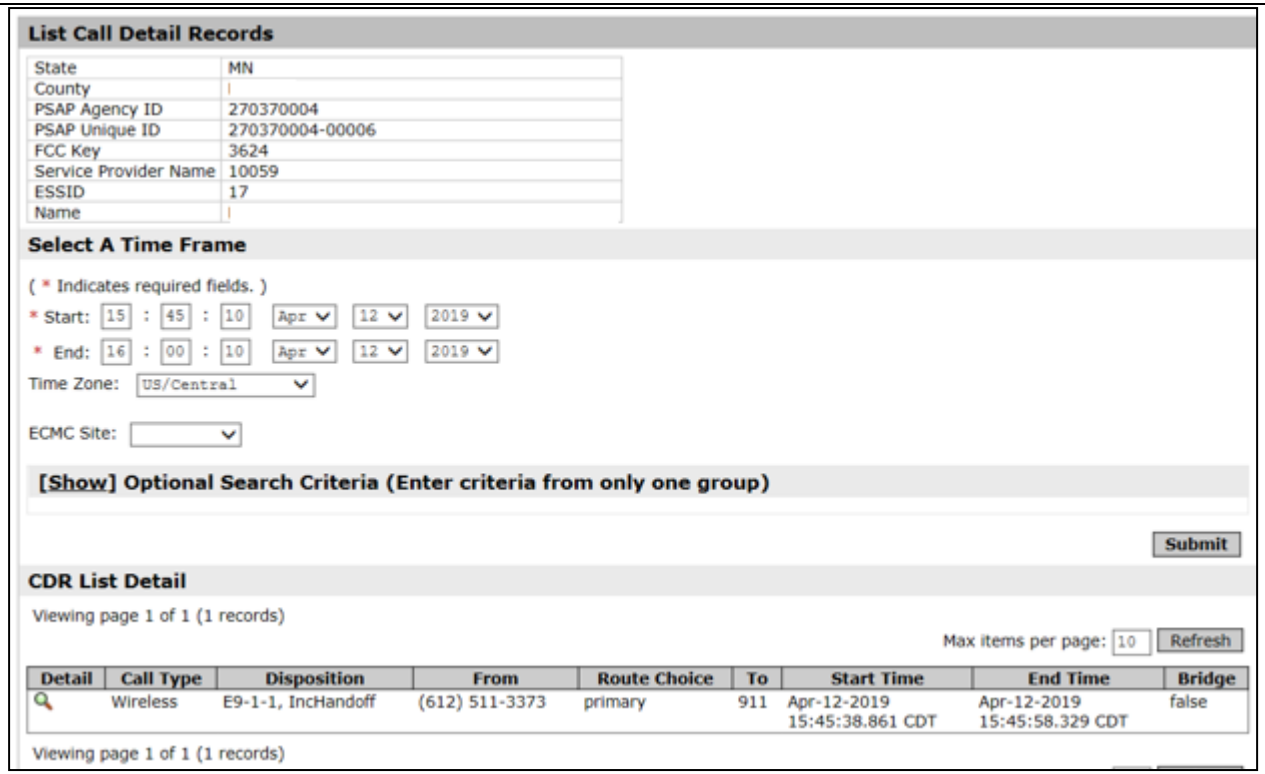

Figure 28: Sample CDR Report

At every level of each report the user can:

- Click on the “Export to Excel” hyperlink to produce an Excel version of the data displayed on the screen.
- Click on the “Printer-friendly version” hyperlink to produce an HTML version of the data as displayed on the screen without headers and footers for printing simplicity.

3. The ECaTS solution, which will have the interaction with the local CHE equipment for MIS purposes, will handle the individual licensing and software agreements with the State of Nebraska. The interconnection and data spills provided to the ECaTS platform are included as part of the A-9-1-1 solution. The standard reporting and CMP capabilities listed

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	previously in the response will be made available to any/all parties that the State grants permission. No additional licensing and or interconnection interfaces are required by the NGCS provider.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 70	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Access to Event Logging Data** 1. Describe how the PSAPs and the Commission will gain access via role-based authentication to the event-logging solution data and run statistical and other MIS reports. The PSAP is the custodian of such data for purposes of the Nebraska Public Records Statutes, Neb. Rev. Stat. §§ 84-712 to 84 712.09. The PSAP is responsible for maintaining such data pursuant to the PSAP record-retention schedule applicable to such data as provided in the Nebraska Public Record Statutes, Neb. Rev. Stat. §§ 84 1201 to 84 1229. The state is implementing the ECaTS MIS solution statewide. Upon deployment, the Contractor shall coordinate with ECaTS, the state, and the PSAPs to deliver event logging data to the ECaTS solution. An existing data-sharing agreement (DSA) between the state and the PSAPs governs what data the state may access along with notifications of records requests. This DSA will govern data collected by the NGCS and ESInet provider whether that data is delivered to ECaTS or directly to the state or PSAPs. 2. Describe the reports, MIS tools, and performance metrics made available to each PSAP, the user interface for retrieving or receiving reports, role-based authentication to limit access to data and reports, and the ability to customize reports based on individual PSAP needs. These reports may be used as a basis for changes to bandwidth and capacity. The required reports and metrics will include, but is not limited to: a. Timing b. Call-delivery time c. Call-processing time between elements d. Volumes e. Call volumes by call type f. Alternate-routed calls g. Text-to-911 h. All NGCS element usage volumes i. Bandwidth/trunk utilization j. Calls per trunk k. Trunk utilization l. Circuit utilization	X			
	Bidder Response: **1.** The PSAPs and Commission can gain access to event logging data through the web-based A9-1-1 Customer Management Portal (CMP) available via role-based, two-factor authentication. Users have a predetermined PSAP or set of PSAPs for which they are able to view statistics. For example, some users will only be able to view their own PSAP's				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping.

Intrado will coordinate with ECaTS, the State, and the PSAPs to deliver event logging data to the ECaTS solution.

2. The A9-1-1 service provides an i3 logging capability per the NENA STA-010.2 specification. Intrado supports near real-time log delivery and web service interfaces for log retrieval from authorized clients. The A9-1-1 solution logs hundreds of data points for each call that traverses the system to assist in tracking and troubleshooting calls. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

The Customer Management Portal provides participating PSAPs and approved personnel 24x7 access to call detail records and very detailed call trace records through a secure, web-based portal. The call detail records provide the user with all of the pertinent information for each call.

Users have a predetermined PSAP or set of PSAPs for which they are able to view statistics. For example, some users will only be able to view their own PSAP's statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping.

Event data is time stamped upon ingress of payload entry through the LNG or BCF and at the time of answer and disconnect at the PSAP. Event data also tracks the time for each functional element to perform routing and PSAP assignment, by tracking the time it takes to traverse from the selective router to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics.

Reporting

The A9-1-1 standard reporting suite provides the following reports through a web-based interface.

- **Event Count Reports per Hour.** Provides metrics for total calls by hour for a day, week or month.
- **Event Count by Routing Reason and Destination.** Provides metrics for total calls in which the Customer PSAP participated as the Primary versus Alternate route per route type, broken out by hour for day, week, or month.
- **Event Count by Type.** Provides metrics for total calls by call type (wireless, wireline, VoIP) broken out by hour for day, week, or month.
- **Event Count by Incoming Trunk Group.** Provides metrics for total calls by trunk group with an hourly breakout.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

- **Bridge Call Summary**. Provides metrics for calls bridged in or out by bridge type (fixed, selective, manual). Call detail is available for each bridged call.
- **Routing Database Processing.** Provides a breakout of initial calls where the Customer PSAP was Primary by selectively routed versus default routed with a No Record Found (NRF) breakout.
- **Event Setup Time.** Provides statistics on the time to route and deliver calls where the Customer PSAP is Primary, including the minimum, maximum, median and average times
- **Event Count Reports per Hour.** Provides metrics for total calls in which Customer's PSAP participated by hour for a day, week or month

The A9-1-1 tool gives users the ability to drill down and capture additional contextual information that can be used to more efficiently manage ongoing 9-1-1 operations. A secure web portal in a standardized HTML format, customized to each authorized user's profile, access level, and preferences, provides access to more than 270 compliance and other existing reports.

For ALI management, users can create customized reports and perform real-time data and trend analysis, including graphing, based on daily data updates. The A9-1-1 solution gives 9-1-1 officials the ability to convert static data into actionable information anywhere and at any time.

Hyperlinks allow the user to easily drill down to further levels of detail. For example, clicking on the Company A link in the example below, allows the user to see further detail on Service Order processing. The results are typically returned within one second.

Users can create customized reports and perform real-time data and trend analysis, including graphing, based on daily data updates. A9-1-1 gives 9-1-1 officials the ability to convert static data into actionable information anywhere and at any time.

At every level of each report the user can:

- Click on the "Export to Excel" hyperlink to produce an Excel version of the data displayed on the screen.
- Click on the "Printer-friendly version" hyperlink to produce an HTML version of the data as displayed on the screen without headers and footers for printing simplicity.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

In summary, the following metrics are available with the A9-1-1 Customer Management Portal.

- Timing via CDRs and Call Trace
- Call-delivery time via CDRs, Call Trace and reports
- Call-processing time between elements via CDRs
- Volumes via Reports
- Call volumes by call type via CDRs
- Alternate-routed calls via CDRs and Reports
- Text-to-911 via CDRs
- Bandwidth/trunk utilization
- Calls per trunk via Reports
- Trunk utilization via Reports and real time stats through the CMP

Transactional volume by each functional element is available via ad-hoc report requests.

Below are example screen shots for how statistics will be displayed to the State of Nebraska.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Circuit utilization (PSAP Resource)

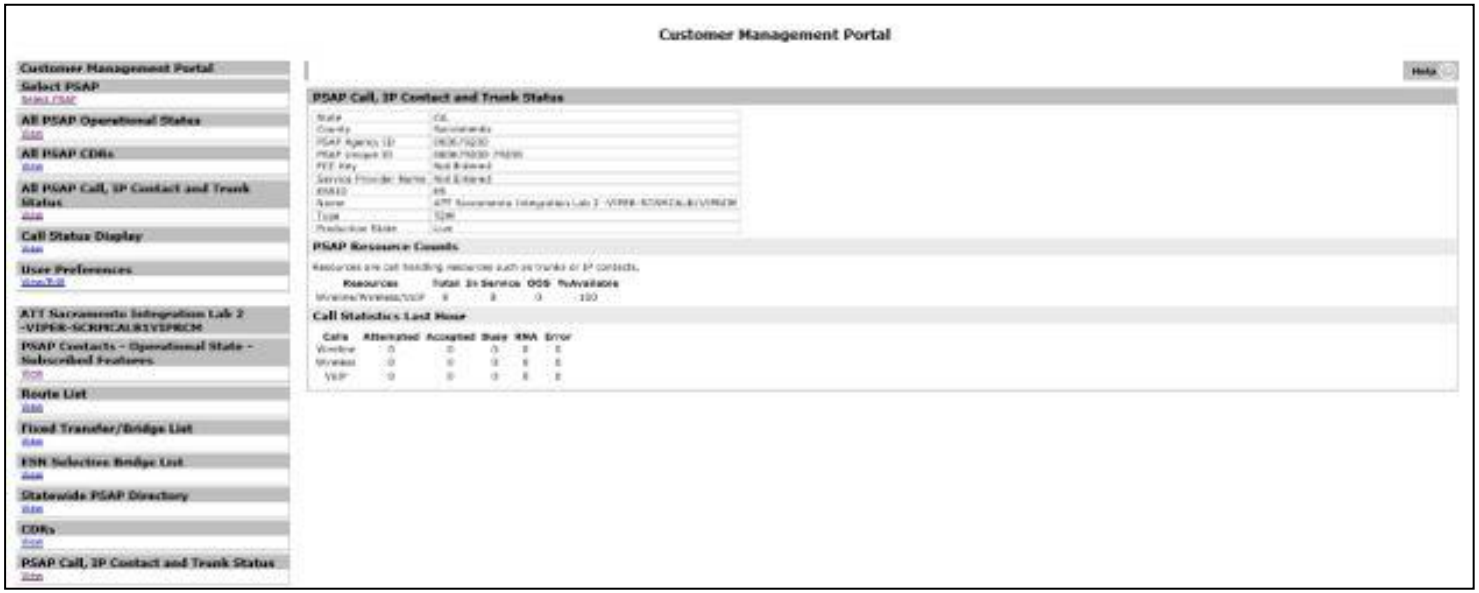

Figure 29: PSAP Resource Availability and Statistics

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Operational State

Figure 30: PSAP Operation State and Subscribed Features

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 71	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **NENA Standards Compliance** The bidder's proposed logging solution shall meet the requirements set forth in NENA-STA-010.2-2016. **Third-Party Certification Fees** Bidder is responsible for any third-party certification fees. Describe how the solution meets or exceeds these above requirements.	X			
	Bidder Response: **NENA Standards Compliance** The A9-1-1 service provides an i3 logging capability per the NENA STA-010.2 specification. Additionally, i3 logs from ESInet i3 components will be available per the NENA STA-010.2 specification. **Third-Party Certification Fees** The A9-1-1 service includes third-party certification fees.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 72	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** Bidder's solution shall sync with existing time sources to maintain consistent time stamps across the network and systems. Describe how bidder's solution complies with this requirement.	X			
	Bidder Response: The A9-1-1 solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the NTP time services interface, accurate to 1 millisecond. Intrado will work with the Commission and PSAPs to assess how to support interoperability with the Intrado A9-1-1 integrated time source.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 73	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Master Clock Description** The bidder shall provide redundant, resilient network-attached Stratum 2 time sources ("master clocks") capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: A9-1-1 processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the A9-1-1 sphere. Time stamps are included in logs, system traces, and user reports.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 74	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Accessibility by PSAP Equipment** The master clock time source(s) shall be accessible to the PSAPs for synchronizing call-handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the NTP for maintaining system clock accuracy. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: A9-1-1 processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the A9-1-1 realm. PSAPs will be offered use of the NTP service to synchronize the clocks on their 9-1-1 CPE, workstations, etc. The A9-1-1 solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the NTP time services interface, accurate to 1 millisecond.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 75	**Next Generation Core Services Elements (NGCS)** **NG911 Application Integration** Bidder shall describe other NG911 applications, additional data integrations, and personal safety applications that may be integrated with the NGCS solution. The bidder's system must be capable of integration with Additional Data Repositories (ADR), Identity-Searchable Additional Data Repositories (IS-ADR) or commercial third-party LIS, as described in NENA STA-010.2-2016, within two years of the deployment of the first PSAP. Describe how the solution will accomplish integration, information storage, and use/transmission of data to PSAP CHE.	X			

Bidder Response:

Intrado and its partners have experience integrating multiple "non-traditional" systems into the NGCS infrastructure. These include, but are not limited to, Telematics, VoIP Services, Text, Multimedia, and Gunshot detection. We are currently capable of supporting queries to external i3 resources such as ADRs, IS-ADR, and LIS. We have completed interoperability with third parties to query their i3 location and additional data resources.

If the data applications are delivered via either legacy TDM/ALI or i3 standard protocols, the integration would be seamless, and the call flow should be identical to that of a typical legacy and/or i3 call. If for some reason, the additional data provider is unable to provide the voice and location information in an industry-standard format, additional resources would need to be expended to design, test, and implement a non-standard solution.

Intrado can work through engineering requirements discovery with the State to develop a mutually agreed upon scope of work that would be priced separately upon completion of functional requirements analysis.

The Intrado A9-1-1 service will interwork seamlessly with external application providers by supporting and adhering to NENA and ATIS standards.

For native end-to-end i3 calls, the Carrier (OSP) is responsible for formatting the 9-1-1 call in an i3-compliant manner. For location, the call will include either location by value or location by reference when passed to the NG Service Provider (Intrado). If a location by reference is provided, the Intrado A9-1-1 service will query for location using the HELD protocol as required. The Intrado A9-1-1 service will pass the ADR URI to the PSAP so that they can query the ADR resource for additional data. The PSAP will use the ADR protocol to do so.

There are two types of solutions listed within the requirement above. Typical integration will be discussed for each of the solutions.

- LIS/ADR – Carrier-provided

  Carrier Provided LIS/ADR is location information approved by the OSP (originating Service Provider). This information is used for providing real time data when a call first enters the 911 infrastructure and/or subsequent 911

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

location updates. This location data is used for routing of a 911 call. When an OSP is ready to deploy this technology using an OSP approved and verified LIS/ADR, Intrado resources will immediately engage with that provider to enable a network path to the designated LIS/ADR. The i3 standards suggest that this path be a dedicated IP path via MPLS. This network path will support the i3 industry standard protocols to support location delivery. The steps for integration include planning, design, implementation, testing and turn-up.

- LIS/ADR – Third-party (not a Carrier)

  This technology is used for providing real time data after a call has reached the PSAP. Various third-party providers are offering this service which allows the PSAP to gather additional information outside of the OSP already approved and deployed 9-1-1 LIS/ADR. When a PSAP would like to enable this service, specific design of the network will need to take place. Assuming the PSAP would like to use the Intrado ESInet as the path to the third-party providers LIS/ADR, some other requirements will need to be determined. Those requirements include the network path from the Intrado A9-1-1 core infrastructure to the third-party LIS/ADR. Choices include MPLS, dedicated path, or Internet connectivity. This network path will support the i3 industry standard protocols to support additional data. The steps for integration include planning, design, implementation, testing, and turn-up.

Information Storage

The carrier-approved LIS/ADR is used as the primary source of routable and displayable 9-1-1 location information. All information provided by the OSP used for routing by the Intrado core call processing elements and transmitted to the PSAP is stored and available via the Intrado A9-1-1 CMP.

Leveraging the redundancy, reliability, and security in the ESInet, Intrado has created a service which allows the PSAP to query third-party LIS/ADR providers. This service includes connectivity to the third-party LIS/ADR, however, since that information is not used for routing and is encrypted in transit, the Intrado system does not capture the elements of those direct third-party to PSAP LIS/ADR messages. Intrado will, of course, continue to monitor the network path over which the LIS/ADR queries and responses travel. The responsibility for information storage for these transactions is held at the third-party LIS/ADR provider as well as the PSAP call handling logging and reporting application.

Use/Transmission to PSAP CPE

The Intrado ESInet solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including queries to and responses from additional data repositories (ADR), including queries to ADRs hosted by commercial providers. The *ESRP – Terminating ESRP Interface for ESInet Specification v1.4.1* document included with this response contains a

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	detailed description of the functionality of the PSAP interfaces for ADR resources, specifically including the user interface, additional features, and security aspects. Please reference the following interface specifications for additional detail. • *ECRF-LoST Interface Specification v1.4.2* • *LIS-Held Interface Specification v1.4* • *ADR-Additional Data Interface Specification v1.3.1* Please refer to the *Proprietary Information* file submitted with the Intrado response for copies of the above documents.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 76	**Next Generation Core Services Elements (NGCS)** **Message Session Relay Protocol Text (MSRP) Integration** The PSAPs have deployed short messaging service (SMS)-to-911 service. 1. Describe the ability to integrate existing web-based and MSRP-integrated SMS-to-911 and Real-Time Text (RTT) services into the solution. 2. Explain whether the solution supports location-by-reference and/or location-by-value. This requirement is for the integration of text messaging with MSRP and not a requirement for procuring text services.	X			

Bidder Response:

1. A9-1-1 supports TCC interfaces to deliver "SMS to 9-1-1" services to Nebraska PSAPs. The three industry-defined methods of SMS delivery to PSAPs are supported. Existing PSAP TCC services can co-exist with the A9-1-1 implementation and can use the ESInet IP transport and/or NGCS services as individual PSAPs are deployed on the ESInet. As a PSAP's CPE provides support, PSAPs can have their "SMS to 9-1-1" SIP signaling, or call control messaging, pass through the A9-1-1 ESRP functions and benefit from a common and centrally controlled set of PSAP routing policies, such as PSAP Abandonment/Evacuation routing.

The Intrado-managed TCC has interconnections to all current TCC providers and their respective customers. Carrier initiated emergency text messages can be aggregated at the Intrado-managed TCC and integrated with ESInet transport and NGCS. At that time, any ancillary transport provided to PSAP CPE demarcation sites just for the purpose of "SMS to 9-1-1" service delivery can be retired in lieu of using ESInet transport.

"SMS to 9-1-1" industry defined service delivery mechanisms are:

- TTY calls are sent into the A9-1-1 system and handed off to the PSAP CPE from the Legacy PSAP Gateway (LPG). The PSAP CPE needs to support TTY in order to have a text conversation through this method.
- Web Browser – The Web Browser provides a GUI interface which allows the end PSAP user to communicate with the text initiator over the public internet. Since this workstation is connected to the public internet, it is typically a standalone workstation and uses the "swivel chair" approach.
- MSRP – Intrado has established redundant connections between the Intrado-managed TCC and A9-1-1. When a text is initiated, the text will traverse the ESInet infrastructure. The ESRP/PRF is used to determine and route MSRP traffic. All PRF rules will be applied when routing to the PSAP. The message will traverse the established ESInet redundant paths and be handed off to the Terminating ESRP/CPE. It will be the PSAP's responsibility to procure a solution with their CPE vendor. Protocol specifications can be provided upon request.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	Regarding MSRP, redundant connections exist between the Intrado-managed TCC and the A9-1-1. When a text is initiated, the text will traverse the ESInet infrastructure. The ESRP/PRF will be used to determine and route any MSRP traffic for calls that ingress in an i3 compliant format. All PRF rules will be applied when routing to the PSAP. The message will traverse the established ESInet redundant paths and be handed off to the terminating ESRP/CPE. Support for Real Time Text (RTT) is road-mapped for (see *Proprietary Information* file). Native RTT calls will be supported at ingress to the Intrado NG Routing service. IP ingress from the OSP is required. RTT calls will be delivered to RTT-capable PSAPs and PSAPs that support TTY. Intrado will transcode the RTT call to TTY as required. The service includes (or will include) the following elements. • Redundant, secure IP connectivity between the end user PSAP and A9-1-1 • The ability to transfer a text session to another PSAP on the network is roadmapped for 1H 2021 • SIP-based communication protocol compliant to existing standards, NENA i3 and ATIS J-STD-110 MSRP protocol • Log retention of text dialogues **Sample Message Flow** 1. An RI sends a text message to 9-1-1. 2. The text request is routed through the wireless carrier's network to the TCC. 3. TCC determines location of the RI via a Mobile Location Protocol (MLP). 4. TCC determines the ESInet by using the cell sector or caller's latitude and longitude and sends the call to A9-1-1 or the PSAP Web Browser interface. 5. If using a TTY or MSRP, A9-1-1 determines the PSAP by querying the ECRF. A9-1-1 sends the call to the PSAP where tones are recognized and converted into displayable characters. **2.** For location, a call can include either location by-value or location by-reference when passed to the NG service provider (Intrado). If a location by-reference is provided, A9-1-1 will pass the location and ADR URI to the PSAP so that they can query the resources for additional data.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	If location by-value is provided, that value will be passed to the PSAP.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 77	**Next Generation Core Services Elements (NGCS)** **1. Make-Busy Functionality** Some PSAPs have a physical make-busy switch that can be activated in the event of an emergency evacuation. Bidder's solution shall support this functionality to all PSAPS.	X			
	2. Ringdown Functionality Bidders' solution shall support ringdown functionality, either through the call-handling system or through the NGCS.	X			
	3. Near-Simultaneous Transfer The solution shall support near-simultaneous conference and transfer capability, with up to at least 12 parties in the conference. This feature shall allow transfer or conference buttons to be programmed to automatically establish a conference with multiple parties. For instance, one button at a police department might establish a conference between the police, fire, and EMS PSAPs and the original caller, without having to add each additional party individually. Describe how bidder's solution meets or exceeds these requirements.	X			

Bidder Response:

1. Make Busy Functionality

Intrado supports make-busy functionality with a variety of solutions.

- A call to the Intrado NOC .
- The web-based Customer Management Portal provides authorized PSAP representative(s) with the real-time ability to invoke abandonment themselves for a specific PSAP via internet access.
- Physical equipment can be provided at the host and/or remote PSAP location at an additional cost.

Since the third option requires specific equipment and secured and sometimes independent network support (for remote PSAP locations), the recommended path is for PSAPs to use the included web portal or Intrado NOC to activate the "make busy" functionality.

2. Ringdown Functionality

The A9-1-1 Solution supports ring down functionality with the appropriate call handling system. Understanding that there may be various technical solutions to support this legacy functionality, Intrado looks forward to discussing which solution best fits the State of Nebraska's needs.

3. Near Simultaneous Transfer

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	The Intrado A-9-1-1 solution supports 12-way bridging and call transfers using i3 SIP REFER and subscribe/notify messaging. i3 PSAPs can transfer and conference calls to both i3 and non-i3 PSAPs.

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 78	**Next Generation Core Services Elements (NGCS)** **PSAP Interfaces and Backroom Equipment Requirements** **Support of PSAP Interfaces** Bidder's solution shall have the ability to support PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the following:				
	a. SIP calls	X			
	b. NGCS call delivery	X			
	c. Web services	X			
	d. All baseline media and multimedia (as described in NENA STA-010.2-2016, Section 4)			X	
	e. NTP time services interface, accurate to 1 ms	X			
	f. Transport layer security	X			
	g. Discrepancy reporting			X	
	Describe the functionality of the PSAP interfaces in detail to address the requirements outlined above, with particular attention to the user interface, additional features, and security aspects.				

Bidder Response:

The A9-1-1 solution supports the above PSAP interfaces specified in NENA STA-010.2-2016, Section 4.1, as follows:

a. SIP calls – Comply. Please see Intrado's ESRP to T-ESRP interface specification for a detailed explanation of the user interface, features. and security aspect.

b. NGCS Call delivery – Comply. Please see Intrado's ESRP to T-ESRP interface specification for a detailed explanation of the user interface, features, and security aspect.

c. Web services – Comply. Intrado web services will typically use 1149 Representational State Transfer (REST) moving forward in anticipation of the NENA i3 Standard v3.

d. All baseline media and multimedia (as described in NENA STA-010.2-2016, Section 4) – Complies with Future Capability. Intrado currently supports voice and MSRP. RTT is roadmapped for (see *Proprietary Information* file). Multi-media and video are roadmapped for (see *Proprietary Information* file).

e. NTP time services interface, accurate to 1 millisecond – Comply. A9-1-1 processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the A9-1-1

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	realm. PSAPs will be offered use of the NTP service to synchronize the clocks on their 9-1-1 CPE, workstations, etc. The A9-1-1 solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the NTP time services interface, accurate to 1 millisecond. **f. Transport layer security** – Comply. The SBC supports mutual-authentication within a TLS profile. The SBC supports the following TLS Exchange and Authentication models: • Basic—The client authenticates the SBC certificate by using the CA public key, and checks expiration, common name, and ciphers supported. Basic provides confidentiality and integrity through encryption, but does not establish the identity of the endpoint. Credential cracking is still possible, and the move to TLS (based on TCP) may make port exhaustion DoS a bit easier for an attacker. • Mutual—A step is added in which the client certificate is sent to the SBC for verification. You can use single or individual client certificates. Mutual provides the same characteristics of the basic model with the advantage of verifying that the client is likely trusted because an issued certificate is present. If a single certificate is used for all clients, then theft or compromise of an endpoint may allow access to an attacker. Individual certificates are more secure, but require more administrative effort to issue and manage. • Mutual with certificate revocation—Certificate revocation for individual clients is possible, which guarantees only expired or revoked clients are refused access. An external Online Certificate Status Protocol (OCSP) server is required to check against the Certificate Revocation List Because TLS is based on TCP, TCP DoS protections can be configured to limit the number of connections per source IP and per sip-interface. At the transport layer, When a request needs to be sent out the SBC first tries to send it over TCP. If that attempt fails then the SBC falls back to UDP and tries the request again. **g. Discrepancy reporting** – Complies with Future Capability. Reports are available via the A9-1-1 Routing Customer Management Portal. i3-specific formats are roadmapped for (see *Proprietary Information* file). The *ESRP-Terminating ESRP Interface for ESInet Specification v1.4.1* document, referenced above, contains a detailed description of the functionality of the PSAP interfaces, specifically including the user interface, additional features, and security aspects. This document together with the three specification documents listed below can be found in the *Proprietary Information* file included with Intrado's response. Please see the following additional documents for the above interfaces.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	• ECRF-LoST Interface Specification v1.4.2 • *LIS-Held Interface Specification v1.4* • *ADR-Additional Data Interface Specification v1.3.1* • *Intrado 9-1-1 EGDMS User Guide v3.4,* attached below

Any additional documentation can be inserted here:

Intrado 9-1-1EGDMS_3.4.pdf

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 79	**Next Generation Core Services Elements (NGCS)** **PSAP Interfaces and Backroom Equipment Requirements** **Support of Call Handling Equipment (CHE) Platforms** 1. Provide a list of CHE platforms for which bidder has successfully implemented the interfaces listed above in a live production environment, noting any interfaces that have not yet been tested with each CHE vendor/model. 2. Where interfaces with CHE vendors/models have yet to be deployed and/or tested, please describe the integration testing process that the bidder will perform prior to acceptance testing of the solution. 3. Describe the physical interface handoff required at the PSAP CHE demarcation point.	X			

Bidder Response:

1. The CHE vendors we have supported using CAMA, RFAI and i3 interfaces as appropriate are:

- Intrado VIPER
- Zetron
- Baker
- CML
- Motorola / Airbus
- Motorola / Comm Works
- Solacom
- Comtech
- Central Square

West Tel and Tri Tech will be used in an upcoming deployment in Colorado.

2. Intrado supports field testing at PSAP sites with CPE vendors using interfaces they have not yet deployed with Intrado. In this case, the CPE vendor would create a non-live profile on the customer CPE, or stand up a new non-live version of their CPE, enabling the full suite of pre-migration testing to be performed within the customer environment using the exact production configuration and equipment that will eventually be deployed. Upon request and contract, a CPE vendor may connect their CPE lab to an Intrado environment prior to field deployment in order to perform interoperability testing of i3 or RFAI. This interop testing may incur a charge to the CPE vendor. Connectivity for this method of testing uses internet VPN and follows a suite of suggested test cases within a defined testing window. Intrado would assist with

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

	provisioning, enabling call tests, and confirming messaging in our logs, but does not certify interoperability. Intrado's role is to provide a method for the CPE vendor to pre-validate that their equipment is ready to deploy in the field. **3.** Descriptions of the physical interface handoffs expected at the PSAP call-handling demarcation points follow. • In the Legacy CAMA interface, the demarcation point between A9-1-1 and the PSAP environment is the ingress side of the CPE 66 block for CAMA trunks. • In the i3 or RFAI IP interface the A9-1-1 demarcation point is a LAN port on the A9-1-1 network edge routers. Intrado can also provide a *PSAP Installation Overview* document after contract award that details the physical interface handoff and PSAP equipment requirements. This document covers PSAP data collection, site survey information, PSAP Network Edge Equipment requirements and also includes General Facility requirements and Equipment Room requirements. These documents describe in detail the physical requirements needed to support the installation of the PSAP routers and the connectivity between the A9-1-1 ESInet and the PSAP's Call Handling Equipment. All interface specification documentation below is located in the *Proprietary Information* file included with Intrado's RFP response. • *ECRF-LoST Interface Specification v1.4.2* • *LIS-Held Interface Specification v1.4* • *ADR-Additional Data Interface Specification v1.3.1*

Any additional documentation can be inserted here:

NGCS 80	**Next Generation Core Services Elements (NGCS)** **Transfer to 7/10-Digit Numbers** The bidder's solution shall be capable of transferring 911 calls to 7 or 10-digit numbers with the Calling Party Number (CPN). Describe how the solution meets or exceeds this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The A9-1-1 solution allows for the transfer of 9-1-1 calls to 7- or 10-digit numbers with the CPN using various methods. These transfer methods include fixed transfer, PSAPDN transfer, star code transfer, and PSTN transfer. Additionally, for i3, Intrado will follow the appropriate NENA-STA-010.2-2016 protocols for transfers and is doing so in live i3 environments today.				

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Any additional documentation can be inserted here:

SVAL-1	**Service Validation** Throughout the life of the contract, upon request of the Commission, Bidder shall allow for network testing and validation by a third-party entity, to verify that the service(s) and/or solution(s) are in compliance with the contract's scope.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Intrado will allow for this type of connection and testing/validation. Intrado will work with the Commission to understand and establish scope, timelines, and potential impact. After agreement by all parties, testing/verification will be planned and implemented.				

OPTIONAL SERVICE

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 81	**Next Generation Core Services Elements (NGCS)** **OPTIONAL SERVICES** **NG911 Applications and Alarm Integration** **Alarm Integration Description** NG911 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and associated data. Describe bidder's experience with integrating alarms, sensors, and other non-interactive call types with bidder's NGCS solution and include separate pricing.	X			
	Bidder Response: Intrado and its partners have experience integrating multiple "non-traditional" systems into the NGCS infrastructure. These include, but are not limited to, Telematics, VoIP services, Text, Multimedia, and Gunshot Detection. If the participating technologies can use traditional TDM/ALI protocols or NENA standard i3 protocols to connect and provide address information to the NGCS infrastructure, then the solution and interoperation should be seamless. ASAP is an alarm-based protocol that is tied to the INLETS message switch with INLETS assigned IDs and is how alarm companies route alarm calls to the appropriate PSAP CAD. These IDs are not transferable or usable in/on an ESInet or with NGCS because they are not defined in the NENA specification. Until APCO ratifies the protocol to be used on a common IP transport and uses common NGCS services for routing of calls based on location elements, ASAP cannot be used on an ESInet. That being said, Intrado is working with Alarm and IOT companies to standardize calls for service in an i3 methodology. Intrado anticipates the first Alarm company will be supported in production (3Q 2020). This service will be made available to the State of Nebraska when ready.				

Any additional documentation can be inserted here:

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

d. Proposed high-level project plan

Intrado Response: Comply.

A proposed high-level Project Plan is included in the *Proprietary Information* file submitted with Intrado's response.

e. Schedule for the lifecycle of this project

Intrado Response: Comply.

A proposed schedule is part of the high-level Project Plan included in the *Proprietary Information* file submitted with Intrado's response.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

FORM A: BIDDER PROPOSAL POINT OF CONTACT

Request for Proposal Number 6264 Z1

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

Preparation of Response Contact Information	
Bidder Name:	Intrado Life & Safety, Inc.
Bidder Address:	1601 Dry Creek Drive Longmont, CO 80503
Contact Person & Title:	Elizabeth Lett Proposal Manager
E-mail Address:	elett@intrado.com
Telephone Number (Office):	720-864-5096
Telephone Number (Cellular):	609-598-4667
Fax Number:	720-494-6600

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

Communication with the State Contact Information	
Bidder Name:	Intrado Life & Safety, Inc.
Bidder Address:	1601 Dry Creek Drive Longmont, CO 80503
Contact Person & Title:	Rich Johnston Sr. Sales Engineer.
E-mail Address:	rjohnston@intrado.com
Telephone Number (Office):	720-494-5943
Telephone Number (Cellular):	303-888-5194
Fax Number:	720-494-6600

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Request For Proposal For Contractual Services Form

Please see the REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM on the following page.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

DocuSign Envelope ID: B3E9C296-9B88-4B66-BA8B-541EB0162618

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance

CONTRACTOR MUST COMPLETE THE FOLLOWING

with the procedures stated in this Solicitation, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

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

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

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

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

FORM MUST BE SIGNED USING AN INDELIBLE METHOD OR BY DOCUSIGN

FIRM:	**Intrado Life & Safety, Inc.**
COMPLETE ADDRESS:	**1601 Dry Creek Drive Longmont, CO 8-5-3**
TELEPHONE NUMBER:	**720-494-5800**
FAX NUMBER:	**720-494-6600**
DATE:	May-22-2020
SIGNATURE:	DocuSigned by: Mark R. Scott 29F005CAF2D6473...
TYPED NAME & TITLE OF SIGNER:	**Mark Scott Sr. Vice President/General Manager**

ADDENDUMS FROM THE STATE OF NEBRASKA

Intrado Life & Safety, Inc. acknowledges that we have received Addendums 1 – 8 to RFP 6264 Z1 issued by the State of Nebraska.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

SECTIONS II – IV

II. TERMS AND CONDITIONS

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

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

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:

If only one Party has a particular clause then that clause shall control;
If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;
If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

Intrado Response: Comply.

Intrado's affiliate has recently entered into a separate agreement with the Nebraska Public Service Commission ("NPSC" and "Customer"), and if awarded this Contract, we request mirroring the legal terms from such agreement for these services. A copy of this agreement is included in the NOTES/COMMENTS box below. Specifically under this RFP, Intrado notes the following exceptions further detailed in the specific sections.

- II. Terms and Conditions, Section M.2.
- II. Terms and Conditions, Section T.3.i.
- II. Terms and Conditions, Section U.4. and U.5.

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MM			WSSC.Nebraska Public Service Comm

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Request for Proposal and Addenda;
Amendments to the solicitation;
Questions and Answers;
Bidder's proposal (Solicitation and properly submitted documents);
The executed Contract and Addendum One to Contract, if applicable; and,
Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

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

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

B. NOTIFICATION

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

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

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

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

C. BUYER'S REPRESENTATIVE

The State reserves the right to appoint a Buyer's Representative to manage (or assist the Buyer in managing) the contract on behalf of the State. The Buyer's Representative will be appointed in writing, and the appointment document will specify the extent of the Buyer's Representative authority and responsibilities. If a Buyer's Representative is appointed, the Contractor will be provided a copy of the appointment document, and is required to cooperate accordingly with the Buyer's Representative. The Buyer's Representative has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

D. GOVERNING LAW (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must be brought in the State of Nebraska per state law; (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity,

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

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

E. BEGINNING OF WORK

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

F. AMENDMENT

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

G. CHANGE ORDERS OR SUBSTITUTIONS

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

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

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

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

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

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

H. VENDOR PERFORMANCE REPORT(S)

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

MM			

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

I. NOTICE OF POTENTIAL CONTRACTOR BREACH

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

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

J. BREACH

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

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

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

K. NON-WAIVER OF BREACH

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

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

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

L. SEVERABILITY

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

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

M. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		MM	Intrado requests that Section M.2. be removed from the contract and replaced with the same IP infringement language as in the NPSC agreement: “Intrado will (a) defend or settle any third-party claim against Customer that Services infringe any patent issued as of the Order effective date ("IP Claim"); and (b) pay any final judgment or settlement agreed to by Intrado. These obligations will not apply if a claim arises in whole or in part from (1) Customer's alteration of Services; (2) Customer Materials or Services based on Customer Materials, or information, design, specifications, directions, instruction, software, data, or material not furnished by Intrado; (3) combination of Services with Customer Materials or any materials, products, or services not provided by Intrado; or (4) any third party products or services. If an IP Claim occurs or Intrado believes may occur, Intrado may (1) obtain the right to continue to provide Services; (2) modify Services so they are non-infringing and in compliance with this Agreement: (3) terminate Services without liability other than this indemnity obligation. To the extent permitted by law, this Section describes Customer's exclusive

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

			remedy for any infringement claims.”

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

2. **INTELLECTUAL PROPERTY (Optional)**
The Contractor agrees it will, at its sole cost and expense, defend, indemnify, and hold harmless the indemnified parties from and against any and all claims, to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of any patent, copyright, trade secret, trademark, or confidential information of any third party by the Contractor or its employees, subcontractors, consultants, representatives, and agents; provided, however, the State gives the Contractor prompt notice in writing of the claim. The Contractor may not settle any infringement claim that will affect the State’s use of the Licensed Software without the State’s prior written consent, which consent may be withheld for any reason.

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

3. **PERSONNEL**
The Contractor shall, at its expense, indemnify and hold harmless the indemnified parties from and against any claim with respect to withholding taxes, worker’s compensation, employee benefits, or any other claim, demand, liability, damage, or loss of any nature relating to any of the personnel, including subcontractor’s and their employees, provided by the Contractor.

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

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

N. ATTORNEY'S FEES

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

		Solicitation Response (Initial)	
MM			

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

O. PERFORMANCE BOND

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

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

P. ASSIGNMENT, SALE, OR MERGER

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

Either Party may assign the contract upon mutual written agreement of the other Party. Such agreement shall not be unreasonably withheld.

The Contractor retains the right to enter into a sale, merger, acquisition, internal reorganization, or similar transaction involving Contractor's business. Contractor agrees to cooperate with the State in executing amendments to the contract to allow for the transaction. If a third party or entity is involved in the transaction, the Contractor will remain responsible for performance of the contract until such time as the person or entity involved in the transaction agrees in writing to be contractually bound by this contract and perform all obligations of the contract.

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

MM			

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

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

R. FORCE MAJEURE

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

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

S. CONFIDENTIALITY

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

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

T. EARLY TERMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		MM	Intrado requests that Section T.3.i. be removed from the contract and replaced with "Subject to Funding/Funding out Clause for Loss of Appropriations" with the same Funding Out Clause as in the NPSC agreement: "The State's obligation to pay amounts due on the Agreement for a fiscal year following the current fiscal year Is contingent upon legislative appropriation of funds. Should said funds not be appropriated, the State may terminate the Agreement with respect to those payments for the fiscal year(s) for which such funds are not appropriated . The State will give the Contractor written notice thirty (30) calendar days prior to the effective date of termination. All obligations of the State to make payments after the termination date will cease. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit."

The contract may be terminated as follows:

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

2. The State, in its sole discretion, may terminate the contract for any reason upon thirty (30) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided.

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

f. a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;
g. Contractor intentionally discloses confidential information;
h. Contractor has or announces it will discontinue support of the deliverable; and,
i. In the event funding is no longer available.

U. CONTRACT CLOSEOUT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
		MM	Intrado requests the addition of the word "Reasonably" to Sections Q.4 and Q.5, as in the NPSC agreement: 4. Reasonably cooperate with any successor Contactor, person or entity in the assumption of any or all of the obligations of this Agreement; 5. Reasonably cooperate with any successor Contactor, person or entity with the transfer of information or data related to this Agreement.

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

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

III. CONTRACTOR DUTIES

A. INDEPENDENT CONTRACTOR / OBLIGATIONS

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

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

The Contractor is solely responsible for fulfilling the contract. The Contractor or the Contractor's representative shall be the sole point of contact regarding all contractual matters.

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

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

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

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

1. Any and all pay, benefits, and employment taxes and/or other payroll withholding;
2. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;
3. Damages incurred by Contractor's employees within the scope of their duties under the contract;
4. Maintaining Workers' Compensation and health insurance that complies with state and federal law and submitting any reports on such insurance to the extent required by governing law;
5. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,
6. All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination alleged against the Contractor, its officers, agents, or subcontractors or subcontractor's employees).

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

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

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

B. EMPLOYEE WORK ELIGIBILITY STATUS

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

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

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

1. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html.

2. The completed United States Attestation Form should be submitted with the solicitation response.

3. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

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

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

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

D. COOPERATION WITH OTHER CONTRACTORS

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

MM			

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

E. PERMITS, REGULATIONS, LAWS

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

The contract price shall include the cost of all royalties, licenses, permits, and approvals, whether arising from patents, trademarks, copyrights or otherwise, that are in any way involved in the contract. The Contractor shall obtain and pay for all royalties, licenses, and permits, and approvals necessary for the execution of the contract. The Contractor must guarantee that it has the full legal right to the materials, supplies, equipment, software, and other items used to execute this contract.

F. OWNERSHIP OF INFORMATION AND DATA / DELIVERABLES

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

The State shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or obtained by the Contractor on behalf of the State pursuant to this contract.

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

G. INSURANCE REQUIREMENTS

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

The Contractor shall throughout the term of the contract maintain insurance as specified herein and provide the State a current Certificate of Insurance/Acord Form (COI) verifying the coverage. The Contractor shall not

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

commence work on the contract until the insurance is in place. If Contractor subcontracts any portion of the Contract the Contractor must, throughout the term of the contract, either:

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

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

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

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

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

1. WORKERS' COMPENSATION INSURANCE

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

2. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

REQUIRED INSURANCE COVERAGE	
COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Medical Payments	$10,000 any one person
Damage to Rented Premises (Fire)	$300,000 each occurrence
Contractual	Included
XCU Liability (Explosion, Collapse, and Underground Damage)	Included
Independent Contractors	Included
Abuse & Molestation	Included
If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.	
WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K
Statutory Limits- All States	Statutory - State of Nebraska
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$2,000,000 per occurrence
PROFESSIONAL LIABILITY	
All Other Professional Liability (Errors & Omissions)	$1,000,000 Per Claim / Aggregate
COMMERCIAL CRIME	
Crime/Employee Dishonesty Including 3rd Party Fidelity	$1,000,000
CYBER LIABILITY	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	$10,000,000
MANDATORY COI SUBROGATION WAIVER LANGUAGE	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
MANDATORY COI LIABILITY WAIVER LANGUAGE	
"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory as additionally insured."	

3. EVIDENCE OF COVERAGE

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

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

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

and types of coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

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

4. DEVIATIONS

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

H. ANTITRUST

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

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

I. CONFLICT OF INTEREST

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

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

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

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

J. STATE PROPERTY

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

MM			

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

K. SITE RULES AND REGULATIONS

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

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

L. ADVERTISING

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

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

M. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory)

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2-201.html and ensure that products and/or services provided under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

N. DISASTER RECOVERY/BACK UP PLAN

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

MM			

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

O. DRUG POLICY

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

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

P. WARRANTY

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

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

IV. PAYMENT

A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)

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

B. TAXES (Statutory)

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

C. INVOICES

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

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

D. INSPECTION AND APPROVAL

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

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

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

E. PAYMENT (Statutory)

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

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

F. LATE PAYMENT (Statutory)

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

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

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

H. RIGHT TO AUDIT (First Paragraph is Statutory)

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

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

The Parties shall pay their own costs of the audit unless the audit finds a previously undisclosed overpayment by the State. If a previously undisclosed overpayment exceeds one-half of one percent (.5%) of the total contract billings, or if fraud, material misrepresentations, or non-performance is discovered on the part of the Contractor, the Contractor shall reimburse the State for the total costs of the audit. Overpayments and audit costs owed to the State shall be paid within ninety (90) days of written notice of the claim. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit.

© 2020 Intrado Life & Safety, Inc.
All rights reserved.

Instructions To Bidders

General

- All cells are locked except those allowing input (shaded green).
- **Do not attempt to edit formula cells**. Any attempt to edit a formula may cause bidder's entire response to be rejected.
- Tabs will contain cells for Non-Recurring Costs (NRC) and Monthly Recurring Charges (MRC).
- Follow the instructions for each Tab.
- Save as an Excel file and give it a unique name, using the following format: "**Company XYZ XXXX Z1 Cost Proposal Option C ESInet and NGCS**".
- Print the workbook (not just the worksheets) to verify content of each tab. Also, verify that all data can be seen in each cell.
- Include the saved Excel file when submitting the RFP response package to the Nebraska State Purchasing Bureau.
- If more rows are needed in each region, you can insert additional rows.
- Each sheet is divided into the 7 regions. Enter pricing information for each region based on bidders implementation plan.
- All PSAPs and regions may not be ready for geospatial routing on day one of operations and Bidder shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. Be sure the cost proposal response indicates the pricing difference between tabular and geospatial routing.
- Include pricing for Optional NGCS services on the Optional Svc tab.

NRC Milestones

- Milestone Payments - NRC payments will be made as structured on the NRC Milestones Tab.As each region is completed on each tab, it is calculated into the total milestone. **Bidders should prepare their cost proposal to reflect the timeline submitted with Bidder's Implementation Plan.**

Summary Tab

- As the name implies, this tab contains the totals from the ESInet, **Legacy Network Gateway (LNG)**, **Border Control Function (BCF)**, **Emergency Services Routing Proxy and Policy Routing Function (ESRP & PRF)**, **Emergency Call Routing Function and Location Validation Function (ECRF & LVF)**, **Spatial Interface (SI)**, **Location Database (LDB)** and **Miscellaneous (MISC) tabs.**
- Enter the Bidder name and date in the designated cells. This information automatically populates the other tabs.
- All other cells are locked.

ESInet Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services IP Network services (hardware, software, connectivity, training, maintenance, etc.) for each region. Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly per person amounts in cents**. The monthly amounts are automatically multiplied by the population of the region and by 12 months.

LNG Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Legacy Network Gateway services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the region's population.

BCF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Border Control Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ESRP & PRF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services Routing Proxy and Policy Routing Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ECRF & LVF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Call Routing Function and Location Validation Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

SI Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information for Spatial Interface services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

LDB Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Location Database services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

MISC Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Miscellaneous services that are not part of one of the above functional elements or that may not have been covered in the RFP but are required in order to complete the project. Add rows for each region as needed.

ESInet Milestones	
Milestone 1: **Region 1** regional host connection and testing acceptance	0.00
Milestone 2: **Region 2** regional host connection and testing acceptance	0.00
Milestone 3: **Region 3** regional host connection and testing acceptance	0.00
Milestone 4: **Region 4** regional host connection and testing acceptance	0.00
Milestone 5: **Region 5** regional host connection and testing acceptance	0.00
Milestone 6: **Region 6** regional host connection and testing acceptance	0.00
Milestone 7: **Region 7** regional host connection and testing acceptance	0.00
TOTAL	0.00

NGCS Milestones	
Milestone 1: **Region 1** deployments complete	19,286.00
Milestone 2: **Region 2** deployments complete	19,286.00
Milestone 3: **Region 3** deployments complete	19,286.00
Milestone 4: **Region 4** deployments complete	19,286.00
Milestone 5: **Region 5** deployments complete	19,286.00
Milestone 6: **Region 6** deployments complete	19,286.00
Milestone 7: **Region 7** deployments complete	19,286.00
TOTAL	135002.00

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name															
Date (MM/DD/YYYY):															
Next Generation Core Services	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		YEAR 6	YEAR 7	YEAR 8	YEAR 9	YEAR 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
ESInet	0.00	660,735.70	0.00	660,735.70	0.00	660,735.70	0.00	660,735.70	0.00	660,735.70	660,735.70	660,735.70	660,735.70	660,735.70	660,735.70
LNG	105,000.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BCF	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ESRP & PRF	0.00	1,620,585.12	0.00	1,620,585.12	0.00	1,620,585.12	0.00	1,620,585.12	0.00	1,620,585.12	1,620,585.12	1,620,585.12	1,620,585.12	1,620,585.12	1,620,585.12
ECRF & LVF	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
LDB	0.00	463,024.32	0.00	463,024.32	0.00	463,024.32	0.00	463,024.32	0.00	463,024.32	463,024.32	463,024.32	463,024.32	463,024.32	463,024.32
MISC	30,002.00	180,579.48	0.00	180,579.48	0.00	180,579.48	0.00	180,579.48	0.00	180,579.48	180,579.48	180,579.48	180,579.48	180,579.48	180,579.48
Total	135,002.00	2,924,924.63	0.00	2,924,924.63	0.00	2,924,924.63	0.00	2,924,924.63	0.00	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63

Project Totals	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Yearly Totals (NRC+MRC)	3,059,926.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63	2,924,924.63
Initial Contract (5 Year NRC+MRC)	14,759,625.15									
+ Optional Year 6 (6 Year NRC+MRC)	17,684,549.78									
+ Optional Years 7 (7 Year NRC+MRC)	20,609,474.41									
+ Optional Years 8 (8 Year NRC+MRC)	23,534,399.04									
+ Optional Years 9 (9 Year NRC+MRC)	26,459,323.66									
+ Optional Years 10 (10 Year NRC+MRC)	29,384,248.29									

State Population	
	2019 Estimates
Region One - ~~SE~~ SC	259,183
Region Two - ~~SC~~ SE	512,126
Region Three - Metro	772,006
Region Four - NC	28,227
Region Five - EC	180,423
Region Six - NE	114,203
Region Seven - Metro West	63,100
Total Population	1,929,268

Bidder Name:	0
Date (MM/DD/YYYY):	1/0/1900

Emergency Services IP Network	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 1 TOTAL	0.0000	88,764.9938	0.0000	88,764.9938	0.0000	88,764.9938	0.0000	88,764.9938	0.0000	88,764.9938	88,764.9938	88,764.9938	88,764.9938	88,764.9938	88,764.9938
Region Two Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 2 TOTAL	0.0000	175,392.9125	0.0000	175,392.9125	0.0000	175,392.9125	0.0000	175,392.9125	0.0000	175,392.9125	175,392.9125	175,392.9125	175,392.9125	175,392.9125	175,392.9125
Region Three Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 3 TOTAL	0.0000	264,396.6149	0.0000	264,396.6149	0.0000	264,396.6149	0.0000	264,396.6149	0.0000	264,396.6149	264,396.6149	264,396.6149	264,396.6149	264,396.6149	264,396.6149
Region Four Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 4 TOTAL	0.0000	9,667.1830	0.0000	9,667.1830	0.0000	9,667.1830	0.0000	9,667.1830	0.0000	9,667.1830	9,667.1830	9,667.1830	9,667.1830	9,667.1830	9,667.1830
Region Five Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Bidder Input		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 5 TOTAL	0.0000	61,791.2690	0.0000	61,791.2690	0.0000	61,791.2690	0.0000	61,791.2690	0.0000	61,791.2690	61,791.2690	61,791.2690	61,791.2690	61,791.2690	61,791.2690
Region Six Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 6 TOTAL	0.0000	39,112.2434	0.0000	39,112.2434	0.0000	39,112.2434	0.0000	39,112.2434	0.0000	39,112.2434	39,112.2434	39,112.2434	39,112.2434	39,112.2434	39,112.2434
Region Seven Milestone															
Redundant CHE Connection		0.0207		0.0207		0.0207		0.0207		0.0207	0.0207	0.0207	0.0207	0.0207	0.0207
Gen-1 Req: PSAP Traffic other than Emergency Calls		0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 7 TOTAL	0.0000	21,610.4880	0.0000	21,610.4880	0.0000	21,610.4880	0.0000	21,610.4880	0.0000	21,610.4880	21,610.4880	21,610.4880	21,610.4880	21,610.4880	21,610.4880
ESInet Total	0.0000	660,735.7046	0.0000	660,735.7046	0.0000	660,735.7046	0.0000	660,735.7046	0.0000	660,735.7046	660,735.7046	660,735.7046	660,735.7046	660,735.7046	660,735.7046

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
	INITIAL CONTRACT PERIOD														
Legacy Network Gateway	**YEAR 1**		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
LNG Site Build	15,000.0000	Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per Pop Fee		Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per P	Included in ESRP & PRF Per Pop Fee
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	15,000.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
LNG Total	**105,000.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
	INITIAL CONTRACT PERIOD														
Border Control Function	**YEAR 1**		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
BCF Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
Emergency Services Routing Proxy & Policy Routing Function	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
NGCS Per Pop Fee: Tabular and Geo-Spatial		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	217,713.7200	0.0000	217,713.7200	0.0000	217,713.7200	0.0000	217,713.7200	0.0000	217,713.7200	217,713.7200	217,713.7200	217,713.7200	217,713.7200	217,713.7200
Region Two Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	430,185.8400	0.0000	430,185.8400	0.0000	430,185.8400	0.0000	430,185.8400	0.0000	430,185.8400	430,185.8400	430,185.8400	430,185.8400	430,185.8400	430,185.8400
Region Three Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	648,485.0400	0.0000	648,485.0400	0.0000	648,485.0400	0.0000	648,485.0400	0.0000	648,485.0400	648,485.0400	648,485.0400	648,485.0400	648,485.0400	648,485.0400
Region Four Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	23,710.6800	0.0000	23,710.6800	0.0000	23,710.6800	0.0000	23,710.6800	0.0000	23,710.6800	23,710.6800	23,710.6800	23,710.6800	23,710.6800	23,710.6800
Region Five Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	151,555.3200	0.0000	151,555.3200	0.0000	151,555.3200	0.0000	151,555.3200	0.0000	151,555.3200	151,555.3200	151,555.3200	151,555.3200	151,555.3200	151,555.3200
Region Six Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	95,930.5200	0.0000	95,930.5200	0.0000	95,930.5200	0.0000	95,930.5200	0.0000	95,930.5200	95,930.5200	95,930.5200	95,930.5200	95,930.5200	95,930.5200
Region Seven Milestone															
Bidder Input		0.0700		0.0700		0.0700		0.0700		0.0700	0.0700	0.0700	0.0700	0.0700	0.0700
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	53,004.0000	0.0000	53,004.0000	0.0000	53,004.0000	0.0000	53,004.0000	0.0000	53,004.0000	53,004.0000	53,004.0000	53,004.0000	53,004.0000	53,004.0000
ESRP & PRF Total	**0.0000**	**1,620,585.1200**	**0.0000**	**1,620,585.1200**	**0.0000**	**1,620,585.1200**	**0.0000**	**1,620,585.1200**	**0.0000**	**1,620,585.1200**	**1,620,585.1200**	**1,620,585.1200**	**1,620,585.1200**	**1,620,585.1200**	**1,620,585.1200**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
Emergency Call Routing Function & Location Validation Function	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
ECRF & LVF Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
Spatial Interface	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
Included in ESRP & PRF Per Pop Rate															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
SI Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
Location Database	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	62,203.9200	0.0000	62,203.9200	0.0000	62,203.9200	0.0000	62,203.9200	0.0000	62,203.9200	62,203.9200	62,203.9200	62,203.9200	62,203.9200	62,203.9200
Region Two Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	122,910.2400	0.0000	122,910.2400	0.0000	122,910.2400	0.0000	122,910.2400	0.0000	122,910.2400	122,910.2400	122,910.2400	122,910.2400	122,910.2400	122,910.2400
Region Three Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	185,281.4400	0.0000	185,281.4400	0.0000	185,281.4400	0.0000	185,281.4400	0.0000	185,281.4400	185,281.4400	185,281.4400	185,281.4400	185,281.4400	185,281.4400
Region Four Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	6,774.4800	0.0000	6,774.4800	0.0000	6,774.4800	0.0000	6,774.4800	0.0000	6,774.4800	6,774.4800	6,774.4800	6,774.4800	6,774.4800	6,774.4800
Region Five Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	43,301.5200	0.0000	43,301.5200	0.0000	43,301.5200	0.0000	43,301.5200	0.0000	43,301.5200	43,301.5200	43,301.5200	43,301.5200	43,301.5200	43,301.5200
Region Six Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	27,408.7200	0.0000	27,408.7200	0.0000	27,408.7200	0.0000	27,408.7200	0.0000	27,408.7200	27,408.7200	27,408.7200	27,408.7200	27,408.7200	27,408.7200
Region Seven Milestone															
ALI/Location Database		0.0200		0.0200		0.0200		0.0200		0.0200	0.0200	0.0200	0.0200	0.0200	0.0200
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	15,144.0000	0.0000	15,144.0000	0.0000	15,144.0000	0.0000	15,144.0000	0.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000
LDB Total	**0.0000**	**463,024.3200**	**0.0000**	**463,024.3200**	**0.0000**	**463,024.3200**	**0.0000**	**463,024.3200**	**0.0000**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:	0														
Date (MM/DD/YYYY):	1/0/1900														
Miscellaneous	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	4,286.0000	24,259.5288	0.0000	24,259.5288	0.0000	24,259.5288	0.0000	24,259.5288	0.0000	24,259.5288	24,259.5288	24,259.5288	24,259.5288	24,259.5288	24,259.5288
Region Two Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	4,286.0000	47,934.9936	0.0000	47,934.9936	0.0000	47,934.9936	0.0000	47,934.9936	0.0000	47,934.9936	47,934.9936	47,934.9936	47,934.9936	47,934.9936	47,934.9936
Region Three Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	4,286.0000	72,259.7616	0.0000	72,259.7616	0.0000	72,259.7616	0.0000	72,259.7616	0.0000	72,259.7616	72,259.7616	72,259.7616	72,259.7616	72,259.7616	72,259.7616
Region Four Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	4,286.0000	2,642.0472	0.0000	2,642.0472	0.0000	2,642.0472	0.0000	2,642.0472	0.0000	2,642.0472	2,642.0472	2,642.0472	2,642.0472	2,642.0472	2,642.0472
Region Five Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	4,286.0000	16,887.5928	0.0000	16,887.5928	0.0000	16,887.5928	0.0000	16,887.5928	0.0000	16,887.5928	16,887.5928	16,887.5928	16,887.5928	16,887.5928	16,887.5928
Region Six Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	4,286.0000	10,689.4008	0.0000	10,689.4008	0.0000	10,689.4008	0.0000	10,689.4008	0.0000	10,689.4008	10,689.4008	10,689.4008	10,689.4008	10,689.4008	10,689.4008
Region Seven Milestone															
Executive Dashboard	4,286.0000	0.0078		0.0078		0.0078		0.0078		0.0078	0.0078	0.0078	0.0078	0.0078	0.0078
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	4,286.0000	5,906.1600	0.0000	5,906.1600	0.0000	5,906.1600	0.0000	5,906.1600	0.0000	5,906.1600	5,906.1600	5,906.1600	5,906.1600	5,906.1600	5,906.1600
MISC Total	**30,002.0000**	**180,579.4848**	**0.0000**	**180,579.4848**	**0.0000**	**180,579.4848**	**0.0000**	**180,579.4848**	**0.0000**	**180,579.4848**	**180,579.4848**	**180,579.4848**	**180,579.4848**	**180,579.4848**	**180,579.4848**

Bidder Name:	0
Date (MM/DD/YYYY):	1/0/1900

Optional Svc for NGCS	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	13,100.0000	20,154.0701	0.0000	20,154.0701	0.0000	20,154.0701	0.0000	20,154.0701	0.0000	20,154.0701	20,154.0701	20,154.0701	20,154.0701	20,154.0701	20,154.0701
Region Two Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	13,100.0000	39,822.9178	0.0000	39,822.9178	0.0000	39,822.9178	0.0000	39,822.9178	0.0000	39,822.9178	39,822.9178	39,822.9178	39,822.9178	39,822.9178	39,822.9178
Region Three Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	13,100.0000	60,031.1866	0.0000	60,031.1866	0.0000	60,031.1866	0.0000	60,031.1866	0.0000	60,031.1866	60,031.1866	60,031.1866	60,031.1866	60,031.1866	60,031.1866
Region Four Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	13,100.0000	2,194.9315	0.0000	2,194.9315	0.0000	2,194.9315	0.0000	2,194.9315	0.0000	2,194.9315	2,194.9315	2,194.9315	2,194.9315	2,194.9315	2,194.9315
Region Five Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	13,100.0000	14,029.6925	0.0000	14,029.6925	0.0000	14,029.6925	0.0000	14,029.6925	0.0000	14,029.6925	14,029.6925	14,029.6925	14,029.6925	14,029.6925	14,029.6925
Region Six Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	13,100.0000	8,880.4253	0.0000	8,880.4253	0.0000	8,880.4253	0.0000	8,880.4253	0.0000	8,880.4253	8,880.4253	8,880.4253	8,880.4253	8,880.4253	8,880.4253
Region Seven Milestone															
Transitional Data Management For Geo-Spatial Routing and Location Database Management	13,100.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	13,100.0000	4,906.6560	0.0000	4,906.6560	0.0000	4,906.6560	0.0000	4,906.6560	0.0000	4,906.6560	4,906.6560	4,906.6560	4,906.6560	4,906.6560	4,906.6560
Opt. Svc NGCS Total	**91,700.0000**	**150,019.8797**	**0.0000**	**150,019.8797**	**0.0000**	**150,019.8797**	**0.0000**	**150,019.8797**	**0.0000**	**150,019.8797**	**150,019.8797**	**150,019.8797**	**150,019.8797**	**150,019.8797**	**150,019.8797**