

Form A
Bidder Proposal Point of Contact
Request for Proposal Number 6264 Z1

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

Preparation of Response Contact Information	
Bidder Name:	AT&T Corp.
Bidder Address:	One AT&T Way, Bedminster, NJ 07921-0752
Contact Person & Title:	Justin Vaughn, Applications Sales Executive
E-mail Address:	Jv6080@att.com
Telephone Number (Office):	816-808-7264
Telephone Number (Cellular):	816-808-7264
Fax Number:	N/A

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:	AT&T Corp.
Bidder Address:	612 East Walnut Street Belton, MO 64012
Contact Person & Title:	Justin Vaughn, Applications Sales Executive
E-mail Address:	Jv6080@att.com
Telephone Number (Office):	816-808-7264
Telephone Number (Cellular):	816-808-7264
Fax Number:	N/A



AT&T Response to State of Nebraska's RFP 6264 Z1 for ESInet and Core Services (Option C)





612 E. Walnut Street
Belton, MO 64012
www.att.com

Phone: (816) 808-7264
jv6080@att.com

June 3, 2020

Annette Walton and Nancy Storant
State Purchasing Bureau
1526 K Street, Suite 130
Lincoln, NE 68508

Dear Ms. Walton and Ms. Storant:

AT&T would like to thank the State of Nebraska (State) for providing AT&T an opportunity to respond to your Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) RFP. As you evaluate our responses, it is important to consider details beyond your minimum requirements. The AT&T team of technical and applications experts has designed a solution that exceeds your immediate requirements and offers the State exceptional value now and in years to come. The AT&T solution provides these benefits:

- **AT&T's ESInet is Proven and Pre-Built.** AT&T has a proven track record of delivering statewide and local ESInet solutions, including the States of North Carolina, Kansas and Indiana. AT&T's national ESInet, Next Gen Core Services, Network and Security Operations Centers are pre-built to help the ISP accelerate timely rollout of a statewide NG911 Network to comply with IL State law.
- **AT&T's ESInet is i3 compliant.** AT&T's ESInet solution provides the Public Safety community with an i3 architecture built from the ground up. Our commitment to NENA i3 is based on years of contributions to NENA standards committees and understanding the evolving needs and requirements of the Public Safety community.
- **AT&T is Financially Stable and Reliable.** AT&T is a global communications provider with the infrastructure, talent, experience, financial resources, and management track record to be a stable, long-term partner with the State as it looks to procure ESInet service.

In this proposal, we further describe the benefits of our solution. We look forward to continuing our relationship and working with the State to make this project a success. I am the AT&T person to be contacted for any clarifications, so please let me know if I can be of further assistance.

Sincerely,

A handwritten signature in black ink that reads "Justin Vaughn".

Justin Vaughn
Application Sales Executive



Connecting Your World

AT&T Response to State of Nebraska's RFP 6264 Z1 for ESInet and Core Services (Option C)

June 3, 2020

Justin Vaughn
Applications Sales Executive
AT&T
612 East Walnut Street
Belton, MO 64012
Office: 816-275-9840
Mobile: 816-808-7264
jv6080@att.com



AT&T submits this RFP response subject to the specific exceptions and additional information provided in the Response. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State of Nebraska to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer. AT&T is confident that, if awarded the opportunity, AT&T and the State of Nebraska will be able to negotiate a mutually agreeable contract.

Proposal Validity Period—The information and pricing contained in this proposal is valid for a period of ninety (90) days from the date written on the proposal cover page unless rescinded or extended in writing by AT&T Corp. **Proposal Pricing**—Pricing proposed herein is based upon the specific product/service mix and locations outlined in this proposal, and is subject to the proposed terms and conditions of AT&T Corp.'s unless otherwise stated herein. Any changes or variations in AT&T Corp.'s proposed terms and conditions and the products, length of term, services, locations, and/or design described herein may result in different pricing. **Providers of Service**—Subsidiaries and affiliates of AT&T Inc. provide products and services under the AT&T brand. AT&T's Corp., an AT&T company, is the proposer for this opportunity. **Copyright Notice and Statement of Confidentiality**—© 2020 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo, and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The contents of this document are unpublished, proprietary, and confidential and may not be copied, disclosed, or used, in whole or in part, without the express written permission of AT&T Intellectual Property or affiliated companies, except to the extent required by law and insofar as is reasonably necessary in order to review and evaluate the information contained herein.



Table of Contents

Contractual Services Form 1

Executive Summary..... 1

Corporate Overview..... 7

Technical Approach..... 21

 Understanding of the Project Requirements..... 21

 Proposed Development Approach..... 21

 Attachment C (Option C: ESInet and NGCS) 24

 Proposed High-Level Project Plan..... 288

 Schedule for the Lifecycle of this Project 291

 Cost Proposal 291

II. Terms and Conditions 292

 A. General 293

 B. Notification 294

 C. Buyer’s Representative 294

 D. Governing Law (Statutory) 294

 E. Beginning of Work..... 295

 F. Amendment 295

 G. Change Orders or Substitutions 295

 H. Vendor Performance Report(s) 296

 I. Notice of Potential Contractor Breach..... 297

 J Breach 297

 K. Non-Waiver of Breach..... 300

 L. Severability 300

 M. Indemnification..... 300

 1. General..... 301

 2. Intellectual Property (Optional)..... 301





3. Personnel 302

4. Self-Insurance..... 302

N. Attorney’s Fees..... 302

O. Performance Bond 303

P. Assignment, Sale, or Merger..... 303

Q. Contracting with other Nebraska Political Sub-Divisions of the State or Another State 304

R. Force Majeure..... 304

S. Confidentiality..... 305

T. Early Termination..... 306

U. Contract Closeout..... 307

III. Contractor Duties..... 309

A. Independent Contractor / Obligations 309

B. Employee Work Eligibility Status 311

C. Compliance with Civil Rights Laws and Equal Opportunity Employment / Nondiscrimination (Statutory) 312

D. Cooperation with Other Contractors 312

E. Permits, Regulations, Laws 312

F. Ownership of Information and Data / Deliverables..... 313

G. Insurance Requirements 314

H. Antitrust..... 318

I. Conflict of Interest 319

J. State Property..... 320

K. Site Rules and Regulations..... 321

L. Advertising..... 321

M. Nebraska Technology Access Standards (Statutory)..... 322

N. Disaster Recovery/Back Up Plan 322

O. Drug Policy..... 322

P. Warranty 323





IV. Payment 324

- A. Prohibition Against Advance Payment (Statutory)..... 324
- B. Taxes (Statutory)..... 324
- C. Invoices 324
- D. Inspection and Approval..... 325
- E. Payment (Statutory)..... 325
- F. Late Payment (Statutory) 326
- G. Subject to Funding / Funding out Clause for Loss of Appropriations (Statutory) .. 326
- H. Right to Audit (First Paragraph is Statutory) 326

V. Project Description and Scope of Work..... 328

- A. Background and Project Scope 328
- B. Composition of the Request for Proposal 329
- C. Bidder Requirements: 331
- D. General Requirements – Technical 331





Contractual Services Form

AT&T has provided a signed Contractual Services Form on the following page. Please note that the original DocuSign PDF of the Contractual Services Form has been included as a separate attachment.

Please note, that AT&T takes Exception to the portion of this provision that implies that bidder's mere execution and submission of a proposal acts as an acceptance of the terms and conditions in the RFP.

AT&T does not intend that the information described in the Proposal is to be the final expression between the parties. AT&T's proposal is submitted subject to the provisions of its Response; and AT&T reserves the right to negotiate the terms and conditions of the final contract.

For clarification, AT&T will provide the products and services proposed hereunder pursuant to the terms and conditions contained in the definitive Contract Documents to be signed between the parties in the event of an award to AT&T under this RFP. The information contained in this Proposal, or any part thereof, shall only be made a part of any resulting written contract between AT&T and the State of Nebraska to the extent agreed to by both parties.

Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State of Nebraska to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it. AT&T is prepared to negotiate a contract in good faith with the State of Nebraska that includes certain of the State of Nebraska's terms and conditions which are mutually agreed between the parties.



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.

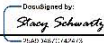
Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

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:	AT&T Corp.
COMPLETE ADDRESS:	3033 Chain Bridge Road, Oakton, VA 22124
TELEPHONE NUMBER:	571-205-6730
FAX NUMBER:	N/A
DATE:	June 3, 2020
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	Stacy Schwartz, VP-Global Public Sector



Executive Summary

AT&T has thoroughly reviewed the State of Nebraska’s Request for Proposal (RFP) for a Next Generation 911 Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS). The extensive requirements listed within the RFP need an experienced solution provider that can address many complex functions that go well beyond just providing an IP Selective Router. The chosen solution provider must have the intimate knowledge and staff to migrate legacy carrier traffic to the NG911 platform. They must also know how to operationalize this infrastructure, coordinate with other service providers and have the ability to provide day two support once that solution has been implemented. AT&T understands how to perform these functions and has a long-established track record in the Public Safety segment as an established 9-1-1 Service Provider. AT&T is very familiar with the Public Safety requirements for NG911 and how they will benefit the State of Nebraska, the PSAP community and the residents of Nebraska.

To meet the State’s RFP requirements, AT&T proposes its flagship AT&T Next-Generation Emergency Services IP Network—AT&T ESInet™. AT&T ESInet combines AT&T’s powerful network capabilities with technology from Intrado Life & Safety, Inc. (Intrado). The AT&T ESInet solution will facilitate an efficient transition from legacy 9-1-1 networks to networks capable of supporting the growing demands of a mobile society. With AT&T ESInet, the State can take advantage of AT&T’s investment in a pre-built, cloud-based solution that delivers next-generation functionality. As part of our RFP response, AT&T is providing our industry-leading AT&T VPN MPLS network for primary access to all PSAPs as well as secondary diverse access to the top 15 PSAPs.

The table below details how AT&T’s solution meets the State’s objectives.

State of Nebraska Goal	AT&T ESInet Solution
Meets or exceeds industry standards	The AT&T ESInet solution provides an i3 architecture built from the ground up. Our commitment to NENA i3 is based on years of contributions to NENA standards committees and understanding the evolving needs and requirements of the public safety community.
PSAP and Originating Service Provider Connections	AT&T’s national ESInet, Next Gen Core Services, Network and Security Operations Centers are pre-built to help the ISP accelerate timely rollout of a statewide NG911 Network to comply with IL State law. Use of the pre-built infrastructure helps reduce implementation cycle times for OSP migration and PSAP implementation and cutover.
Next-generation features and functions	The AT&T ESInet solution is a combination of our world-class IP network and Next Gen Core Services (NGCS) components including the first i3 PSAP deployments in the States of NC and





State of Nebraska Goal	AT&T ESInet Solution
	<p>SCAT&T ESInet comes complete with a full suite of advanced features, including industry leading SLAs, management services and tools to help ensure we provide the best possible service to you and the citizens that you support.</p>
<p>Security Operations Center</p>	<p>AT&T ESInet's defense-in-depth security is built into the architecture. AT&T's Global IP network is monitored by 8 different Security Operations Center (SOC) facilities located across the world. AT&T uses its security portfolio capabilities to protect our data centers and networks that carry more than 335 petabytes of data traffic on an average business day.</p> <p>As the world's largest IP company, AT&T has experience and success in delivering cybersecurity that is unlikely to be matched by any other respondents.</p>
<p>Next Gen Core Services (NGCS) ESInet Buildout</p>	<p>AT&T ESInet provides six (6) geographically diverse and fully redundant facilities to increase resiliency and survivability in natural and man-made disaster scenarios, with scalable capacity capable of supporting more than twice the 9-1-1 busy hour call for the entire United States.</p> <p>AT&T has documented business continuity and restoration plans, including complex disaster and evacuation contingencies. The 24x7 operations center employs an Incident Handling process modeled on FEMA's Incident Command System, with notifications built into this process.</p>
<p>Network Operations Center</p>	<p>AT&T ESInet is monitored 24x7x365 from a NOC with tier 2 and tier 3 technical resources dedicated to AT&T ESInet. AT&T's 9-1-1 Resolution Center has dedicated public safety resources and have a proven track record for deployments and installed base covering nearly 50 million citizens.</p>
<p>Additional Diversity Capabilities</p>	<p>AT&T has the ability to provide redundant and diverse connections to additional PSAPs beyond the mandatory top 15 PSAPs identified with the RFP. AT&T can provide up to 73 locations with redundant and diverse connections using traditional landline fiber connectivity. We are also able to provide FirstNet as a secondary call delivery path to 100% of the secondary PSAP's. This can offer diversity to those PSAPs where it is currently not possible through existing facilities and avoid expensive construction fees. FirstNet unlike standard LTE connections offers preemption and priority all times to ensure connectivity during times of congestion.</p>
<p>Geospatial Routing and GIS Data</p>	<p>AT&T ESInet provides a flexible routing platform that supports both ESN (tabular) and GIS (spatial) routing on the same Emergency Call Routing Function (ECRF). AT&T ESInet also offers a robust toolset for managing on-going updates to GIS data.</p>
<p>Project management</p>	<p>AT&T will provide project management resources to implement the State new system. The AT&T Project Manager will be ultimately responsible for a successful implementation. The State will also participate in planning and implementation. The Project Manager will also direct the Sr. Technology Manager and ESInet Service Manager.</p>





AT&T ESInet: Purpose-built for the next generation

AT&T's solution supports key NENA i3 capabilities today, while forming the basis of a true Next Generation 9-1-1 platform that will support multimedia emergency services as standards are solidified in the industry. The AT&T ESInet solution integrates our world-class IP network and Next Gen 9-1-1 NENA i3 functional elements. Our AT&T ESInet proposal, delivered as a service, comes complete with a full suite of advanced features, management services, and tools to help ensure we provide the best possible service to your Public Safety Access Points (PSAPs) and 9-1-1 agencies—and ultimately the citizens that you support.

Frost & Sullivan named AT&T as the 2017 Company of the Year for Public Safety Solutions in the U.S.

•AT&T is driving visionary innovation in public safety by providing PSAPs with the capabilities to cater to evolving citizen interactions, lifestyles, and technologies. In particular, AT&T's national ESInet solution equips PSAPs with the tools to support multiple modes of communication including texts, photos and video. Thus, AT&T provides PSAPs the ability to prepare for the future and deliver innovative solutions that will transform the way citizens and public safety entities report, react, and respond to emergency situations.

The AT&T ESInet solution provides the public safety community with an i3 architecture purpose-built to meet emerging standards. Our commitment to NENA i3 is based on years of contributions to NENA standards committees and understanding the evolving needs and requirements of the public safety community. Our solution is not just “i3 like,” or “i3 aligned.” As elements of the i3 standard continue to evolve, AT&T will continue its commitment to i3. AT&T ESInet services will provide the State with everything it needs to deliver the critical foundational components of an industry-standard i3 solution delivered over an advanced IP network.

Advanced features of AT&T ESInet

The AT&T ESInet solution offers the following advanced features:

- End-to-end management and monitoring with full lifecycle management of the application. In addition, a dedicated Service Management along with a fully resourced team for implementation.
- Nationally distributed, geographically diverse, and redundant service architecture with six core sites providing a high availability design (99.999% availability) provides initial call processing capacity more than twice the current U.S. E9-1-1 volume. IPv6 capable global MPLS network for connectivity.
- Pre-deployed NENA i3 compliant ESInet Call Processing Centers in AT&T data centers across U.S. with expandable capacity. Aggregation centers in AT&T Central Offices across the U.S. to easily and augment growth capacity.





- Backed by AT&T's business continuity/disaster recovery organization.
- Other features include interoperability with legacy PSAP gateway at neighboring PSAPs, redundant location database, robust reporting suite, Text to 9-1-1 – national TCC Provider.

Security and resiliency for AT&T ESInet

The proposed solution includes six data centers (Core Sites) located at AT&T facilities throughout the country connected via AT&T Switched Ethernet, a secure MPLS VPN network with no single point of failure. AT&T ESInet provides the core backbone for a robust emergency services IP network that helps assure call delivery. The AT&T solution helps enable call delivery into a legacy PSAP environment, an IP-enabled 9-1-1 PSAP, or to peer ESInets. This environment will provide the State with the flexibility to grow its own IP-enabled 9-1-1 solution and to share it with other systems in and around the nation.

AT&T has deep security and support provisions in place. Our security posture is backed by AT&T's 24/7/365 Resolution Center, and AT&T's world-class project management and service delivery organizations.

AT&T qualifications

AT&T is uniquely qualified to perform the work described in this Request for Proposal. AT&T, a \$147B company, is a recognized leader in National Public Safety. A major part of the AT&T Corporation is our Commercial, Consumer, Enterprise, and Government Leadership. AT&T has a robust Public Safety Solutions practice that serves Public Safety Agencies nationwide with legacy and Next Generation 9-1-1 call routing (ESInet), Call Handling, Location Services, Computer Aided Dispatch (CAD), GIS, Records Management, Jail Management, AVL, Security, Cloud solutions, IP Networks, Wireless solutions, Internet of Things (IoT), Unified Communications and many more applications and services. AT&T is driving the convergence and integration of communication technologies and applying its skill and resources to the public safety sector to more quickly and effectively manage emergency response.

FirstNet and ESInet
<ul style="list-style-type: none">• All 50 U.S. states, five territories and the District of Columbia have opted in to FirstNet – America's only broadband communications platform just for first responders.• With both AT&T ESInet™ and FirstNet, the nation's public safety community will be able to create an efficient flow of communications from the caller to the 9-1-1 dispatcher to the first responder.

AT&T was one of the first carriers to implement the original 9-1-1 service, enhanced 9-1-1 and now Next Generation 9-1-1. Because of this, AT&T has an unparalleled





historical knowledge of 9-1-1 operations and platforms. AT&T has almost 50 years' experience in 9-1-1 call routing as well as installing, maintaining, and hosting 9-1-1 call handling solutions. Today, AT&T provides 911 services to more than 3,800 PSAPs nationwide.

AT&T has been delivering Next Gen 911 ESInet solutions since 2011 and currently is in production or contracted with over 500 PSAPs serving over 50M lives.

In March 2017, AT&T was selected by the First Responder Network Authority (FirstNet) to build and manage the first broadband network dedicated to America's police, firefighters, and emergency medical services (EMS). The FirstNet network will cover all 50 states, 5 U.S. territories and the District of Columbia, including rural communities and tribal lands in those states and territories.

FirstNet and AT&T will innovate and evolve the network to keep the public safety community at the forefront of technology advances. For example, as 5G network capabilities develop in the coming years, FirstNet and AT&T will work together to provide the exponential increases in the speed with which video and data travel across the FirstNet network.

Support from AT&T's experienced Public Safety Solutions Team

Your AT&T Public Safety Teams have extensive experience with a wide portfolio of communication products and services related to public safety. This experience makes us experts at designing and supporting solutions such as our proposal for Next Generation 9-1-1 services provided by AT&T ESInet. Your AT&T Public Safety Service Management, Field Services and Account Teams will continue to provide world class customer service to the State and to the PSAPs within the State of Nebraska.

Table 1: AT&T's Nebraska Public Safety Solutions Team

Name	Title	Phone Number	Email
Justin Vaughn	Application Sales Executive	816-808-7264	jv6080@att.com
Brian Hawthorne	Technical Sales Consultant	817-995-6220	bh6248@att.com
Dustin Alexander	Application Sales Manager	214-991-0049	da5917@att.com

AT&T understands the importance of this significant project and how it will positively impact Public Safety for the residents of Nebraska and those traveling through the State of Nebraska. AT&T is best prepared to assist the State in achieving the milestones listed within the RFP. Our flagship AT&T ESInet offer with pre-deployed infrastructure will allow the most efficient path to achieving the implementation timeline required within the RFP.





Connecting Your World

AT&T is fully committed to the Public Safety segment and First Responders within Nebraska are already starting to utilize the benefits of FirstNet. AT&T is best prepared to deliver on the vision of NG911 with an integration our AT&T ESInet and the FirstNet offers. The inherent functionality within these two applications will ultimately enable a true Call to Car to Crisis response to wherever an emergency may take place by providing more information such as pictures, video and other data to the Call Takers and to the First Responders thus improving Public Safety. AT&T recognizes that we must continually earn the privilege to provide innovative solutions to our Public Safety customers and we strive towards continued improvement every day. We look forward to expanding our relationship with the State as we execute this high visibility, high priority project. Thank you for considering our proposal.





Corporate Overview

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

a. Bidder Identification and Information

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

AT&T Response:

AT&T Corp. was incorporated in the State of New York on March 3, 1885. It is a wholly owned subsidiary of AT&T Inc.—a corporation traded on the New York Stock Exchange. At any given time, AT&T and its affiliates' employ nearly 240,000 employees.

You can obtain company information at the following website:

<http://www.att.com/gen/investor-relations?pid=5711>

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.





AT&T Response:

AT&T Corp. is wholly owned subsidiary of AT&T, Inc. and a member of the AT&T Inc. family of companies. AT&T financial information is consolidated and reported at the AT&T Inc. level.

Please refer to the attached document for AT&T's most recent Annual Report.



complete-2019-annual-report.pdf

Regarding litigation, the question is overbroad and impossible to respond to accurately in any practical fashion. At any point in time, AT&T and its affiliates are involved in thousands of projects around the globe at any point in time and are involved in a significant number of constantly changing litigation matters, arbitrations, and disputes, which could range from material litigation to the most minor of billing disputes. This same level of activity has been in place over the last 10 years and is to be expected of companies with our size, scope and industry position.

To compile the requested information and accurately respond to this request is impractical and quite burdensome due to our size and the largely unbounded breadth of the request. In addition, it is likely that a non-insignificant portion of the requested information may be proprietary in nature. AT&T is recognized as an industry leader in telecommunications with service levels and customer service second to none. To our knowledge, no current litigation, arbitration, investigation, dispute or any other proceeding would prevent AT&T from providing the products and services in compliance with our response to this RFP.

The most recent Form 10-Q for AT&T, filed with the Securities and Exchange Commission, addresses pending litigation in the Other Business Matters section.

The 10-Q is found in the investor relations section of our website at:

<https://investors.att.com/financial-reports/quarterly-earnings/2019>

Click on "SEC Filings" then the 10-Q link.

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.

AT&T Response:

AT&T does not anticipate any change in ownership within the 12 months following the submission of the RFP response. If any change of ownership should occur, AT&T will notify the State at the appropriate time.

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.

AT&T Response:

The AT&T office that will have primary management of this project will be located at:

612 East Walnut Street
Belton, MO 64012

e. Relationship 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.

AT&T Response:

AT&T has invested in our Nebraska communications networks, our people and local communities for 124 years.

These investments include:

- **Environmental Impact.** 23 energy efficiency projects in Nebraska resulting in annualized savings of more than 350,000 kilowatt hours and the equivalent of removing 75 cars from the road annually.
- **Jobs and Economic Support.**
 - Approximately 155 AT&T employees working in Nebraska as of Mar. 31, 2020.
 - 246 AT&T retirees living in Nebraska as of Mar. 31, 2020.





- 58 retail locations in Nebraska, including our company-owned retail stores, authorized dealerships and national retail stores as of Mar. 31, 2020.
- More than \$20 million generated in local and state taxes by AT&T operations in Nebraska in 2018.
- **Building for Tomorrow.**
 - 192 wireless upgrades made in Nebraska in 2019 including 77 new cell sites.
 - 207 wireless upgrades made in Nebraska in 2017-2019 including 81 new cell sites.
 - 95 wireless upgrades made in Nebraska in 2020 including 85 new cell sites.
- **Community Impact.**
 - Approximately 420 hours of personal time given by AT&T employees in Nebraska to community outreach activities in 2018 – worth more than \$10,300.
 - Approximately \$840,000 contributed by AT&T, the AT&T Foundation and our employees from 2016 - 2018 through giving programs in Nebraska.

In addition, AT&T’s subcontractor Intrado has the following contracts with the State:

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

f. Bidder’s Employee Relations to the 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.





AT&T Response:

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 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.

AT&T Response:

AT&T is a worldwide multibillion-dollar company. AT&T and its affiliates process millions of transactions daily across the world; therefore, our ability to provide details around this request, with the specificity requested, within the time allowed to respond to this RFP is so broad when applied to a company of AT&T's scope and scale as to be unmanageable in any practical fashion.

Given the scope and scale of AT&T's operations, governmental contracts are being terminated as a result of term expiration, non-appropriation, or other causes on an ongoing basis.

Past projects that were not completed (for whatever reason) would have no material impact on our ability to perform hereunder.

For more than 135 years, AT&T has made it our goal to provide the best communications services at the best value for all of our customers using the highest ethical and legal standards.





h. Summary of Bidder's Corporate Experience

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

The bidder should address the following:

- i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this solicitation. Provide the number of ESInet and NGCS solutions implemented by the bidder that are in production today and lessons learned throughout the project that will be applied to the deployment of the Nebraska ESInet and NGCS solution. These descriptions should include:
 - a) The time period of the project;
 - b) The scheduled and actual completion dates;
 - c) The bidder's responsibilities;
 - d) For reference purposes, contracting entity name, contact name, contact title, contact email address, and contact telephone number. The Commission may request that references authorize a site visit and the opportunity to review event logs.); and
 - e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.
- 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.

AT&T Response:

In response to this section provide the following information for three similar customers are provided below.





State of Kansas

Description of services: Statewide hosted call handling, ESInet, Rapid Deploy RadiusPlus Tactical Mapping

Overall design/construction cost of project, including initial contract value and change orders including reasons for change orders

We have a contract for 911 as a service, did not purchase anything. As such we pay the following annual fees for service: Call Handling - \$5.3M ESInet - \$3.25M RadiusPlus - \$2.1M Organizational structure of service delivery under the contract. AT&T had an assigned Project Manager for the initial installation period and an assigned Program Manager and Service Manager for the duration of the contract.

Subcontracts (service) used in the performance of the contract Subcontracts are all with AT&T and the subs – Kansas is all through AT&T. Intrado was the only subcontractor.

Schedule history. Contract signed February 2015 Data Centers Stood up – August 2015 First PSAP on hosted system – August 2015 End of year, 2015 – 11 PSAPs on system End of year, 2016 – 47 PSAPs on system End of year, 2017 – 76 PSAPs on system November 2017 – Text-to-911 implemented for all PSAPs on system – Others coming on after this time went live with text-to-911 April 2018 – First Statewide System PSAP in the nation went live on AT&T Nationwide ESInet in RFAI configuration May 2019 – All PSAPs on system live on AT&T Nationwide ESInet in FRAI configuration – others coming on after this time went live on ESInet August 2019 – First PSAP in the nation went live on AT&T Nationwide ESInet in i3 configuration December 2019 - 97 PSAPs on system including 4 backup centers February 2020 – Began implementation of i3 ESInet configuration for all PSAPs on system February 2020 – Began rollout of RadiusPlus Tactical mapping replacement.

Continuing (on-going) services and associated costs of continuing services identified as a system as a service, ongoing costs remain the same as indicated above. All current implementations are expected to be complete by July 2020. Will begin upgrade of RadiusPlus to full Nimbus cloud-based CAD, which maintains all the features of RadiusPlus and provides data sharing capabilities between all Kansas PSAPs in the June to July timeframe.

Contact: Scott Ekberg, 785-438-8440, scott.ekberg@kansas911.org





State of North Carolina

Description of services. ESINet private 911 network. Providing hosted call handling services on multiple platforms (Viper & Vesta). Currently five in-production sites (5) are ESINet only and twenty-seven (27) utilize hosted call handling services. 7-year contract with option for 3 additional.

Overall design/construction cost of project, including initial contract value and change orders including reasons for change orders • We have a contract for 911 as a service, did not purchase anything. Sharing of contract costs for recurring services is prohibited.

Organizational structure of service delivery under the contract. AT&T had an assigned Project Manager for the initial installation period and an assigned Program Manager and Service Manager for the duration of the contract.

Subcontracts (service) used in the performance of the contract Subcontracts are all with AT&T. Intrado was the only subcontractor.

Schedule history. Contract began August 2017. Currently operational at 32 sites with an additional 95 to become operational by EOY 2021. Continuing (on-going) services and associated costs of continuing services. The system, as a service, ongoing costs remain the same throughout contract.

Contact: Gerry Means, Network Engineer 919-754-6781 Gerry.means@nc.gov

City of Alphretta, GA

Description of services. Overall design/construction cost of project, including initial contract value and change orders including reasons for change orders.

We have a contract for 911 as a service, did not purchase anything. Sharing of contract costs for recurring services is prohibited.

Organizational structure of service delivery under the contract. AT&T had an assigned Project Manager for the initial installation period and an assigned Program Manager and Service Manager for the duration of the contract.

Subcontracts (service) used in the performance of the contract. Subcontracts are all with AT&T. Intrado was the only subcontractor.





Schedule history. AT&T ESInet installation and cut-live 10/9/19. Continuing (on-going) services and associated costs of continuing services. The system, as a service, ongoing costs remain the same throughout contract.

Contact: Carl Hall, Division Chief of Technology at Alpharetta 911 Operations. 678-297-6275 chall@alpharetta.ga.us

i. Summary of Bidder's Proposed Personnel/Management Approach

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

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

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

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

AT&T Response:

AT&T shall employ and make available an adequate number of appropriately qualified and trained personnel, familiar with the State's operations and use of telecommunications services, to provide and support the State's use of the Services in accordance with the terms of AT&T's response to this RFP. The identities and titles of specific resources and their availability to provide and support the State's needs will be separately established by authorized representatives of AT&T upon award.

If key AT&T personnel are reassigned or leave the employment of AT&T during the term of this agreement, AT&T shall use all reasonable efforts to ensure a smooth transition of personnel. This will include cooperation between the replaced and the newly assigned





personnel to ensure a smooth transition with minimal impact to the State. AT&T shall augment the personnel assigned to the State from time to time as required to carry out special projects that may come up during the course of the overall project. The AT&T ESInet staff and support teams currently consist of more than 500 personnel from the combined core and edge organizations. These organizations and functions are described below.

Project Management

Within the AT&T Project Management office will be a host of Subject Matter Expert project managers. AT&T Project Management will be responsible for AT&T Customer PSAP implementation on AT&T ESInet. Project managers are associated with each of the following ESInet functional components: OSP, Call Routing, Security, Network, ALI DB, GIS and PSAP.

The AT&T Project Manager will oversee and manage all aspects of the project that enable a PSAP to transition to the AT&T ESInet platform. This will include many of the following activities

- Create PSAP Migration Timeline and manage/escalate any issue that may block an on-time deployment
- Maintain an Issues Log for review and resolution
- Ensure that all PSAP call flow and routing information has been provided and provisioned within the AT&T ESInet
- Schedule AT&T Field Technicians for site visits, network equipment installation, and the test and turn up of the new network.
- Manage CAMA to SIP conversion projects
- Change Event Coordinators

AT&T Project Manager will dedicate as much time as is needed for a successful PSAP migration onto the AT&T ESInet. AT&T OSP Project Manager will serve as a single point of contact for Originating Service Providers to place orders and test and turn up their network for 911 call delivery to the AT&T ESInet.

Please see the attached document for an example of a Sr. Project Management.



Sr Technical Project
Manager.pdf





9-1-1 Service Management

AT&T 9-1-1 Service Management will be responsible for AT&T Customer ongoing support for the service. AT&T 9-1-1 Service Management will collaborate with all parties to manage the customer relationship and basic routing changes as part of ongoing lifecycle management. The Service Manager is the single point of contact for escalation requests and performs the following tasks on a regular basis:

- Lead monthly operations meetings
- Provide upgrade and maintenance event notifications
- Distribute software release notes, test cases, and test case results
- Coordinate software release lab testing
- Escalations
- RCA reporting
- Coordinate data center and Aggregation Site access for technical resources
- Coordinate new user access to operational support tools e.g., customer web portal
- Serve as Change Event Coordinators
- Outage communications
- Manage and monitor trouble ticket analysis and correlation

Technical Planning & Engineering

AT&T Technology Planning and Engineering (TP&E) will participate in architectural design planning, transport procurement and installation, OSP interconnection coordination, and on-going capacity planning.

Local Field Technicians

The AT&T Field Technicians will install the AT&T Customer PSAP network edge equipment and provide ongoing on-site maintenance support at the PSAPs. AT&T has a significant amount of AT&T Field Technicians that are geographically located throughout the State to assist with this project.





Data Center/Legacy Network Gateway (LNG) Technicians

The AT&T Data Center/LNG Technicians will deploy, test, install and maintain core equipment located at AT&T aggregation centers and Tier IV data centers.

Labs

AT&T Labs is responsible for testing the AT&T ESInet and interfaces within the public safety ecosystem. In addition to ongoing software upgrades and release testing, AT&T Labs also supports forward looking initiatives such as new standards development. Test engineers will collaborate with all relevant parties in the creation, review, and execution of test cases as part of the implementation process.

- **Application Testing.** Each application is individually tested to ensure its stability and lack of critical defects.
- **Integration Testing.** After each application is tested individually integration testing is performed. This helps ensure that each version of our applications work well together.
- **Hardware/Software Validation.** Products are constantly validated against new hardware and software, including operating systems, service packs and updates.
- **Load Testing.** Load testing is performed to ensure that the system stays stable and consistent even under peak demand. Specialized software allows us to generate any number of simultaneous calls. Performance is benchmarked both with statistics as well as having end user testing of the application interface and answer calls while under load. This assures that not only are the statistical values acceptable, but perhaps more importantly, the user experiences no negative behavior.

9-1-1 Resolution Center

AT&T will provide support 24x7x365.

The AT&T 9-1-1 Resolution Center is responsible for accepting incoming trouble reports. This group is the first line of support for PSAPs and OSPs. AT&T maintains two 9-1-1 Resolution Centers located in Chicago and Atlanta. Each center serves as a backup for each other in terms of disaster recovery.

AT&T 9-1-1 Resolution Center Responsibilities:

- SPOC for PSAP customer trouble reporting and support





- Coordination with all teams in support of resolving an issue or question
- Customer PSAP abandonment requests and test calls
- Emergency Customer PSAP re-route requests
- Coordination of field dispatch for PSAP Network Edge Equipment
- Outage response and reporting
- Application, Platform and IP Network Monitoring
- Trouble reporting, Incident Management and follow-up
- Voice quality troubleshooting support
- CDR assistance
- Tier 1-4 technical support

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.

AT&T Response:

Below is the information for the requirement above.

- i. Intrado Life & Safety, Inc.
1601 Dry Creek Drive
Longmont, CO 80503
720-494-5800
- ii. Intrado will perform or provide assistance and support to AT&T for the following tasks:
 - Implementation Services
 - Installation Support Services
 - Project Management
 - NGCS Core Services
 - NOC Support
 - Software Development and Day Two Support
 - Customer Edge Equipment (routers, LPGs)
 - Security
 - Monitoring





- Automatic Location Identification Services, SLA Reporting
 - Lifecycle Management, Maintenance Services
 - Capacity Management
- iii. TBD
- iv. TBD





Technical Approach

Understanding of the Project Requirements

As part of the Nebraska Public Service Commission, State 911 Department (The Commission) effort to protect and service it's residents, the Commission is seeking implement a statewide ESInet and NGCS to help advance Next Generation 911 (NG911) across the state.

This solution will take the 68 local PSAPs that manage and maintain independent relationships with 911 service and network providers and give the ability for the Commission to establish and support a statewide ESInet and NGCS to provide 911 service to the regions throughout the state.

There are two elements to this procurement. One is Emergency Services Internet Protocol [IP] Network (ESInet) and the other a Next Generation Core Services (NGCS). AT&T has provided a solution for both elements

Proposed Development Approach

The AT&T ESInet™, a nation-wide next generation emergency network designed to meet the industry standards, is specifically built for emergency services communications. The AT&T ESInet emergency call delivery application and next generation core functional processes are deployed on a highly redundant IP transport infrastructure. This hardened mature solution can withstand the failure of individual components or the failure of core call processing sites and continue to successfully complete 9-1-1 calls 24x7x365.

The AT&T ESInet solution is built on an open standards-based platform. The system complies with SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), NENA 08-003 and STA-010.2, IETF ECRIT best practices, and ANSI standards.

The AT&T ESInet provides multiple legacy network gateways (LNGs), direct SIP NNI and Points of Interface (POIs) for the wireline, wireless, and VoIP originating service providers (OSPs) to send their 9-1-1 call traffic destined for your PSAPs. In the interest of redundancy and diversity, AT&T requires the OSPs to connect to at least two LNGs. Each LNG is built with redundant equipment and power for added solution stability. The LNGs convert the 9-1-1 call traffic from TDM to IP and then route the calls to one of AT&T's six core routing sites. These core routing elements determine the appropriate destination based on pre-provisioned routing tables. The platform includes all i3 routing elements





such as the Border Control Function (BCF), Emergency Services Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Location Information Server (LIS), Additional Data Repository (ADR), and Location Validation Function (LVF). AT&T will migrate the PSAPs to a geospatial i3 routing solution as the PSAPs are prepared to make the migration from ESN-based routing.

The AT&T ESInet supports local, regional, state, federal, and national interconnections to other networks and ESInets. Seamless interworking between the AT&T ESInet and neighboring ESInets that serve their clients with either IPSR and/or i3 routing is accomplished by adhering to NENA standards. It can support independent application platforms and other core functional processes necessary for providing NG9-1-1 services. And, as a shared tenant solution, the AT&T ESInet interconnects at local, regional, state, federal, and national levels to form an IP-based internetwork (network of networks).

IP packets are routable between any two points on the ESInet. The solution is deployed over IP-based Layer 3 VPN services that are used to provide connectivity between endpoint sites (LNGs and PSAPs) and core call processing sites. This provides a scalable point-to-multipoint WAN configuration. Any endpoint attached to a given IP VPN instance can be configured to reach any other endpoint due to the use of dynamic routing protocols that allow precise policy control over routing. Typically, individual endpoint sites use at least two IP instances for redundant connectivity to the six Core sites. Specific attributes of the AT&T ESInet IP routing structure and associated operational processes include:

Intermediate System-to-Intermediate System (IS-IS) is used as an interior gateway protocol (IGP) within the AT&T ESInet (see NENA ESIND section 3.3.2.3). Border Gateway Protocol (BGP) is used within the ESInet to facilitate multi-protocol label switching (MPLS) and as an exterior gateway protocol (EGP) for use in interfacing with external networks.

Dynamic routing protocols are configured to quickly re-converge around network failures. Path failure re-convergence between AT&T ESInet data centers occurs in under one second.

The AT&T ESInet provides automatic rerouting and failover to alternate routes, supporting '99.999' service availability.

QoS is implemented within the ESInet to ensure that routing protocol traffic is prioritized. Routing protocol traffic which exceeds pre-defined queues will not preempt 9-1-1 application traffic.

All IP-enabled elements within the ESInet are statically addressed. The IP address schema allows for sub-netting and is deployed in a hierarchical manner. All subnets are





reachable end-to-end. Note, network reachability between security zones is contingent upon configured firewall policies.

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 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.

The AT&T ESInet is built with significantly more capacity than necessary to allow for component failures and/or maintenance that will not impact customer call processing. According to NENA 9-1-1 Statistics approximately 240 million 9-1-1 calls occur annually in the United States which equate to approximately 7.4 emergency calls originating every second. A “busy hour” call rate can be estimated at ten times the average call rate or approximately 74 calls per second.

The AT&T ESInet can successfully process all of State of Nebraska’s 9-1-1 calls even under severe loads that may occur during unusual events such as natural or man-made disasters or extreme weather events.





Attachment C (Option C: ESInet and NGCS)

This subsection contains AT&T's response to Option C: ESInet and NGCS Technical Requirements.



**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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

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

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

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

1. Complies: Bidder's proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, generally available, and successfully deployed. Responding with “Complies” or “Complies with Future Capability” shall mean the bidder's solution meets or exceeds the requirement regardless of any comments included as additional information.
2. Complies Partially: Bidder's proposal addresses the RFP requirements through another method that currently is developed and available for implementation (i.e., shall be generally available), or the solution complies with some, but not all of the requirements. Bidder is responsible for clearly explaining how the proposed solution does not fully comply.
3. Complies with Future Capability: The RFP requirements will be met with a capability delivered at a future date. This response shall include a calendar quarter and year in which the requirement will be met with a generally available product or service at no additional cost.
4. Does Not Comply: Bidder's proposal does not/cannot meet the specific RFP requirement.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Req Identifier	Requirement Description																															
GEN-1	<p>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).</p> <p>Bidder Response:</p> <p>AT&T's vision is to provide the premier NG911 solution in the market. AT&T does this by working this industry leader Intrado to develop a comprehensive solution that can deliver the only end-to-end solution on the market.</p> <p>AT&T meets or exceeds all currently applicable NENA standards and is committed to providing best-in-class Next Generation 9-1-1 (NG9-1-1). Our solutions adhere to NENA i3 models and offer customers transition strategies from current operating models to NG9-1-1 end state visions. As new NENA i3 standards are released, AT&T/Intrado products will comply with the aforementioned standards in a timely manner. As standards are ratified and there is a market demand and capability, we will work diligently with providers to develop, test and if available, certify to the new standards.</p> <p>AT&T is an active member of the Public Safety Community and the products and services we provide and maintain conform to NENA i3 standards. We participate at the highest level on industry boards and development forums ensuring our offers are in step with the industry we are associated with. Our experience delivering the AT&T ESInet and NGCS highlights our capability to deploy the talent, investment and technology necessary to manage the complex infrastructures our public safety clients require. AT&T has a proven track record of innovation, leadership and commitment to public safety. We continue to play a key role in developing emerging technologies and defining new standards in support of public safety as evidenced in our partnerships with NENA, NENA Industry Collaboration Events (ICE), Next Generation Partner Program (NGPP), APCO, ATIS and FCC CSCIC working groups.</p> <p>Currently, AT&T has members on the following NENA committees and work groups.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Committees</th> <th colspan="2" style="text-align: center;">Work Groups</th> </tr> </thead> <tbody> <tr> <td>Agency Systems</td> <td>ESInet-PSBN Interconnection</td> <td>RTT</td> </tr> <tr> <td>Data Management</td> <td>ASC NG9-1-1 Call Processing Metrics</td> <td>i3 Architecture</td> </tr> <tr> <td>PSAP Logistics</td> <td>EIDO-JSON</td> <td>EIDD-IDX Concerns</td> </tr> <tr> <td>911 Core Services</td> <td>Monitoring and Managing NG9-1-1</td> <td>Security for NG9-1-1</td> </tr> <tr> <td>Systems Security & Resiliency</td> <td>NG9-1-1 PSAP Systems</td> <td>Communication Modalities</td> </tr> <tr> <td>ICE Steering</td> <td>Provisioning & Maintenance of GIS Data to ECRF-LVF</td> <td>Emergency Notification for Persons with Disabilities</td> </tr> <tr> <td>Accessibility</td> <td>NG9-1-1 Impacts on the PSAP</td> <td>IOT/APPS</td> </tr> <tr> <td></td> <td>RFP</td> <td></td> </tr> </tbody> </table>	Committees	Work Groups		Agency Systems	ESInet-PSBN Interconnection	RTT	Data Management	ASC NG9-1-1 Call Processing Metrics	i3 Architecture	PSAP Logistics	EIDO-JSON	EIDD-IDX Concerns	911 Core Services	Monitoring and Managing NG9-1-1	Security for NG9-1-1	Systems Security & Resiliency	NG9-1-1 PSAP Systems	Communication Modalities	ICE Steering	Provisioning & Maintenance of GIS Data to ECRF-LVF	Emergency Notification for Persons with Disabilities	Accessibility	NG9-1-1 Impacts on the PSAP	IOT/APPS		RFP		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		Committees	Work Groups																													
Agency Systems	ESInet-PSBN Interconnection	RTT																														
Data Management	ASC NG9-1-1 Call Processing Metrics	i3 Architecture																														
PSAP Logistics	EIDO-JSON	EIDD-IDX Concerns																														
911 Core Services	Monitoring and Managing NG9-1-1	Security for NG9-1-1																														
Systems Security & Resiliency	NG9-1-1 PSAP Systems	Communication Modalities																														
ICE Steering	Provisioning & Maintenance of GIS Data to ECRF-LVF	Emergency Notification for Persons with Disabilities																														
Accessibility	NG9-1-1 Impacts on the PSAP	IOT/APPS																														
	RFP																															
		X																														

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

NENA Industry Collaboration Events (ICE)

AT&T's partner, 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.

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 include 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.

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.

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.

Most recently at ICE 7, Intrado tested its Additional Data Repository (ADR) and Location (LIS) server products.

Intrado continues to embrace its responsibility to collaborate with NENA and the public safety industry to help solve i3 interoperability issues in a multi-vendor next-generation 9-1-1 environment. As such Intrado will continue to participate in the upcoming ICE events. NENA ICE events 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. Intrado is also involved with the ICE Planning Committee and the Steering Committee.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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: AT&T provided responses to requirements 1 and 2 below: 1. AT&T does not employ any proprietary standards, interfaces, or protocols in our network design. All standards, interfaces, and protocols used are industry standard. 2. Proposer will represent that it has all intellectual property rights to provide the offered solution. There are no technical limitations based on patents or other intellectual property rights.				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	System and Network Architecture	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-3	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>The AT&T ESInet solution utilizes a private, self-healing, Public Safety grade network. Every PSAP has connectivity to the entire AT&T ESInet infrastructure consisting of six geographically diverse ECMCs and diverse aggregation centers. Network connectivity is provided by AT&T’s global MPLS network service AVPN. The AT&T ESInet employs 5 POPs Nebraska and when coupled with diverse access to the PSAP, traffic will route around network problems allowing for ultimate reliability for PSAP call delivery.</p> <p>The AT&T ESInet core call routing centers are capable of processing more than twice the estimated busy hour rate for all 9-1-1 calls across the nation. The AT&T ESInet can successfully process 9-1-1 calls in Nebraska even under severe loads that may result from unplanned events such as natural or man-made disasters.</p> <p>Reliability</p> <p>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</p> <ul style="list-style-type: none"> • 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 <p>AT&T ESInet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. All i3 functions necessary for call processing are deployed in a highly available configuration. Each i3 element has multiple instances within a single core to provide redundancy for that core. The same redundant configuration is replicated at each of the six geographically diverse core sites. The nine Aggregation sites use the same design approach of redundancy within each individual site mirrored at the other sites. 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 AT&T ESInet components are designed and configured for continuous operation. AT&T ESInet availability is calculated from the time the outage begins that impacts call processing ability, until such time that the AT&T ESInet call processing ability is restored. This includes all AT&T ESInet downtime for the end-to-end service.</p> <p>Regular maintenance and full load testing with no scheduled downtime is required at each site to maintain reliability in our public safety grade network. We schedule planned events for routine maintenance in ways that 9-1-1 operations are not impacted. A notification of the upcoming event</p>				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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.

Availability

The AT&T ESInet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. 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 AT&T ESInet components are designed and configured for continuous operation. AT&T ESInet availability is calculated from the time an outage begins that impacts call processing ability, until such time that the AT&T ESInet call processing ability is restored.

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 AT&T ESInet 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 an alternate geographically diverse core site—giving the solution multiple levels of redundancy. 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 the AT&T ESInet to process 9-1-1 calls, assuming telecommunication transport services for the impacted region are operable.

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 six core processing centers. The end result is an infrastructure that is public safety grade with respect to capacity, reliability, scalability, and redundancy.

The AT&T ESInet 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:

- Six core call processing sites located across the U.S.
- 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 ESInet to the Public Safety Answering Point (PSAP) for delivery 9-1-1 calls.
- Redundant Common Support Services (CSS) for management, monitoring, and reporting with a web-based Customer Management Portal that delivers real-time CDRs, call trace and solution testing.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Core Sites work in an active-active mode; calls are distributed across all core sites. The six-core site architecture is more than capable of processing all the 9-1-1 calls in the United States; therefore, there is no need for NGCS capacity supplementation as PSAPs on-board to the AT&T ESInet service.

AT&T 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. AT&T event team personnel will keep the customer informed of event progress. AT&T 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. AT&T will include the required back-out time within the scheduled maintenance time frame.

Based on our public safety experience, AT&T has found that measuring Service Availability from a call processing perspective is more applicable and relevant to 9-1-1 service versus traditional methods of calculating availability through Mean time between failure (MTBF) and Mean time to repair (MTTR) measures. Therefore, AT&T ESInet Service Availability SLA measures the system wide availability for Call Processing that encompasses network availability (Service Availability). Call Processing is the ability of the Service to deliver calls from the inbound Service demarcation point into the Core Call Processing Nodes and from the Service demarcation point to a Valid Destination (for example a PSAP). The Service Availability is calculated from the time an issue is reported that impacts Call Processing ability, until such time that the Service Call Processing ability is restored.

Security

Secure communications are retained through the following measures, as recommended in NENA-INF-015.1-2016, Section 3.2:

NENA-INF-015.1-2016 Security Measures	AT&T Response
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.	<p>Intrado will manage credentialing and issuing digital certificates to help ensure protection and security as defined within section 6 of NENA-STA-010.2-2016.</p> <p>Intrado verifies credentialed devices or that carriers are authorized access in the following manner:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		administrative functions based on section 6.5 of the NENA-STA-010.2-2016.
c) Advanced Encryption Standard (AES)-based encryption to provide confidentiality		AT&T employs AES 256 encryption-in-transit on our own networks and on networks not under direct AT&T control. Encryption is achieved either using SSL/TLS or IPSEC VPN. VPN tunnels offer a stateful connection across the MPLS cores, so that both ends can quickly identify black holes or other network impairment. Each router at a remote site has two tunnels built from that router via its attached MPLS network to the mGRE hub interfaces at each core site.
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.
<p>Network Traffic Restrictions</p> <p>All data traversing the AT&T ESInet and access to that data is restricted to public safety use as required in NENA-STA-010.2-2016. Commercial and non-public safety data and access is prohibited from sharing bandwidth for ESInet use.</p>		

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	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
GEN-4	<p>Bidder Response:</p> <p>The AT&T ESInet is built with significantly more capacity than necessary to allow for component failures and/or maintenance that will not impact customer call processing. According to NENA 9-1-1 Statistics (http://www.nena.org/?page=911Statistics) approximately 290 million 9-1-1 calls occur annually in the United States, which equate to approximately 7.7 emergency calls originating every second. A “busy hour” call rate can be estimated at ten times the average call rate or approximately 77 calls per second.</p> <p>The AT&T ESInet can successfully process all State of Nebraska 9-1-1 calls even under severe loads that may occur during unusual events such as extreme weather.</p> <p>AT&T ESInet is capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. As a recognized Gartner leader in Global IP Networking, AT&T has demonstrated significant expertise in IP Network delivery. AT&T can easily scale IP capacities through simple provisioning processes, eliminating the need for additional network buildouts, and enabling customers to increase capacities within a few weeks vs. months. AT&T 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.</p> <p>AT&T takes into consideration all current and potential core functions and applications in planning for network capacity expansion needs. The AT&T ESInet IP network is continually monitored for capacity trends that indicate the need for proactive growth and processes have been established to upgrade such capacity of the ESInet. IP network transport used by the AT&T ESInet will initially be sized to comply with specified network bandwidth requirements. 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.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Capacity - Scalable Deployment As the Commission migrates toward a fully compliant NG911 environment, additional PSAP functions will transition to the systems and network. The bidder's systems and network solution shall be designed and deployed in a way that is easily scalable, with the capability to grow in both capacity and coverage without disruption in service. Describe in detail how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-5	<p>Bidder Response:</p> <p>The AT&T ESInet solution is the most redundant, reliable, and available full-service solution offered in today's marketplace. It is designed and built to process all 9-1-1 calls 24x7x365. The AT&T ESInet can withstand the failure of individual components or the failure of core call processing sites and continue to successfully deliver 9-1-1 calls to the appropriate destination. The AT&T ESInet is built with significantly more capacity than necessary to allow for component failures and/or maintenance that will not impact customer call processing. According to NENA 9-1-1 Statistics (http://www.nena.org/?page=911Statistics) approximately 290 million 9-1-1 calls occur annually in the United States which equate to approximately 7.7 emergency calls originating every second. A "busy hour" call rate can be estimated at ten times the average call rate or approximately 77 calls per second.</p> <p>The AT&T ESInet can successfully process all 9-1-1 calls in the State of Nebraska even under severe loads that may occur during unusual events such as extreme weather. The AT&T ESInet is not only able to meet the expected and future call volume in the State of Nebraska, it is also designed to handle more than twice the national 9-1-1 call volume. Each AT&T ESInet Core can exceed a call arrival rate of 30 calls per second and handle thousands of simultaneous calls. The AT&T ESInet Core ESRP and ECRF configurations distribute transactions across a set of processors in an active/active configuration and any Core can handle and process any given call. Maintenance, logging and alarm management functions are all incorporated into our capacity management process.</p> <p>AT&T ESInet™ Is scalable to support growth by 50 percent</p> <p>The current proposed AT&T ESInet™ design for the State of Nebraska accounts for a 50 percent growth of bandwidth required to serve the total number of simultaneous calls that traverse the network. For example, the North Central Region Host Location requires 10 call paths and will be provisioned with two MPLS circuits that can support up to 50 simultaneous call paths, which exceeds the Commission's requirement to allow for 50 percent traffic and usage growth. Should one access facility fail, the second one continues to provide the full call capacity required. Ingress and egress capacity is not oversubscribed.</p> <p>The AT&T ESInet™ calculation of bandwidth takes into account a N+1 design, a 100kps per call standard, and a 200% capacity capability at each element. Our backbone network has the scalability to adjust bandwidth by 50 percent or more. It scales to changing needs easily, quickly, and with minimal operational impact.</p>	X			

The AT&T ESInet™ core call processing centers are capable of handling more than twice the estimated national busy hour rate for 9-1-1.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 1	<p>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.</p>				
	<p>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.</p> <p>Describe how the solution meets or exceeds the above requirements.</p> <p>Bidder Response:</p> <p>AT&T complies with applicable standards listed in Section V.D.1., Table 1 of the RFP.</p> <p>AT&T's ESInet cyber security policies, standards, and guidelines are consistent with industry best practices as defined by the International Organization for Standardization (ISO) and Control Objectives for Information and related Technology (COBIT). Due to the complexity of the AT&T ESInet solution and the challenges of continuously tracking compliance across numerous and constantly changing compliance frameworks, we adhere to AT&T security requirements and the NENA Security for Next-Generation 91-1 Standard (NG-SEC). In addition, our overall information security program is based upon the requirements of the ISO/IEC 27001 international standard. 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.</p> <p>AT&T ESInet™ is a highly secure, privately managed IP network providing IP based call routing services for next generation 9-1-1 call delivery. All inbound and outbound traffic interactions are with pre-authorized entities, utilize agreed upon protocols and traverse controlled access points. Call processing and real-time data delivery are protected through both physical and logical. The solution incorporates physical, network, and application security principles. Traffic between core processing sites and PSAPs 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. AT&T ESInet complies with the NG-SEC standard (75-001).</p> <p>AT&T provides the necessary security requirements across data centers, Network Housing Structures, Regeneration Sites, PSAPs, dispatch centers, ESInet and NGCS elements.</p> <p>Data Centers / Network Housing Structures / Regeneration Sites</p> <p>The AT&T ESInet™ architecture takes advantage of geographically diverse, hardened and secure AT&T central offices and data centers strategically located across the country. Our AT&T central offices are used to aggregate and collect inbound 9-1-1 TDM calls. These calls are converted to IP and</p>	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

interconnect over AT&T’s Switched Ethernet (ASE) WAN to geographically diverse, distributed ESInet core call routing complexes residing within our Data Centers. Both AT&T Data Centers and Central Offices are secured through a defense in depth security strategy.

AT&T uses multi-tiered security measures to restrict access to our data centers. AT&T restricts access to only those authorized personnel contained within an access list. All additions to this list must be submitted in advance and in writing. Access is limited to areas designated in the access list.

Information regarding the security status of AT&T’s infrastructure and services is managed and communicated on a need-to-know basis. Results of security health checks with audit and vulnerability testing are tracked and reported compliance management.

Security measures within data centers include continuous closed-circuit video monitoring, 24-hour on-premises live security, electronic key card access, individual, personal access codes, and biometric scans. We further protect our operations and equipment by using controlled entrance and exit doors, security breach alarms, secured cage and cabinet environment, automatic man-traps, and discrete buildings (no signage).

AT&T ESInet™ Customer Portal Access

AT&T incorporates a robust strategy for identity management for access to the AT&T ESInet™ customer management portal for reporting. User access is protected through an identity management system. New users must complete a registration process prior to gaining access. Multi-factor authentication and role-based access control are used to restrict user access to AT&T’s trusted resources.

User access via the public Internet requires two-factor authentication, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from an AT&T-provided security token. Users are configured in the AT&T identity management system and linked to a specific security token and configured for access to a defined list of applications.

AT&T ESInet™ implements a highly secure, private IP managed network built to withstand sophisticated attacks. All inbound and outbound traffic interactions are with pre-vetted entities, using IPSEC key exchange between controlled access points. Call processing and real-time data delivery are implemented through specialized subnets. AT&T 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), Access Control Lists (ACLs), Role-based Access control, multi-factor authentication, strong encryption, and anti-virus. Furthermore, AT&T protects its systems with build standards, patch management, and regular vulnerability scans.

AT&T ESInet™ 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.

NGCS Elements

Sensitive data is housed in data centers with logical and physical access controls. All NGCS elements deployed in a production environment go through stringent release management processes that incorporate thorough testing and scans. Development environments are separate from production. 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 AT&T custody) pass through applications or communication channels with encryption to safeguard confidentiality and integrity.

AT&T ESInet™ implements a multi-zoned strategy to achieve appropriate separation and risk management between NGCS elements. These Zones/Domains are managed according to characteristics of trusted or untrusted traffic. Trusted domains include areas of the network where AT&T

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

has control or influence of traffic and access mechanisms, to minimize and mitigate the risk of unwanted activities. Typical security zones or security domains in the Next Generation ESInet deployments include four (4) main domains and can be defined as:

- Call routing or core domain (ESInet)
- Call handling or host domain
- PSAPs/dispatch center domain (customer)
- Other ESInet core domain (such as another carrier connecting to the core ESInet).

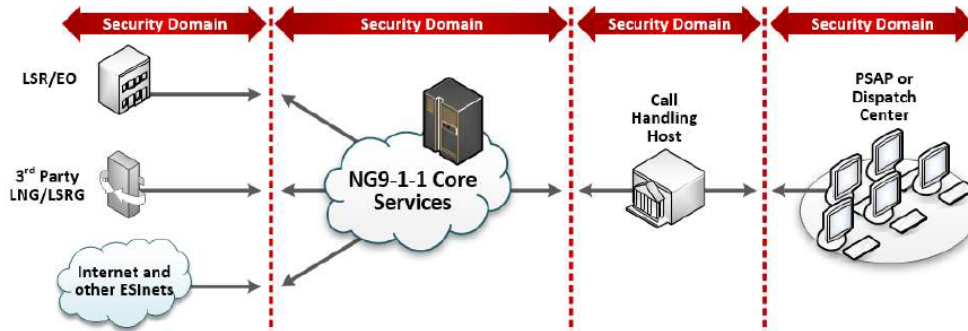


Figure 1: Event Management Framework

In addition to the different zones/domains that are protected by firewalls AT&T also separates data types to efficiently pass data between zones and NGCS elements. Information is categorized as voice or data as it leaves NGCS elements. Voice traffic (SIP/RTP) is routed through session border controllers (SBCs). Data traffic traverses and is controlled by data border elements such as firewalls and routers. IP traffic is only accepted from known and pre-authenticated entities.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Security Plan A comprehensive security plan is a critical component of the Nebraska's NG911 network solution. Describe the security plan, including the 1. mitigation; 2. monitoring; 3. alerting and incident-response processes; and 4. provide information on specific hardware components and software systems incorporated in the proposed security plan. The proposed solution's security plan is required to utilize the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) and Task Force on Optimal PSAP Architecture (TFOPA) best practices .	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 2	<p>Bidder Response:</p> <p>AT&T has policies and procedures that 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.</p> <p>Policies that govern ESInet establishment and operation include but are 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 created and maintained.</p> <p>AT&T'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 AT&T ESInet infrastructure is built to withstand sophisticated attacks. AT&T ESInet 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. AT&T 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, (RBAC) 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.</p> <p>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 and production environments are physically separate. This eliminates the potential to compromise the integrity of the production system. Similarly, development and test data is never used in production environments. Inter-zone traffic is restricted to only the necessary protocols/destination and data that transits un-trusted networks (leaves AT&T custody) pass through applications or communication channels with encryption to safeguard confidentiality and integrity.</p> <p>AT&T ESInet 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</p>	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

address recognition, limited protocols, VPNs, session border controllers, and firewalls secure the various communication elements of the proposed solution.

Logging and Monitoring

AT&T will provide 24x7x365 logging and monitoring of the network supporting the State. For security purposes, AT&T does not allow outside vendor/customer access to monitoring equipment. AT&T will provide real-time reporting capabilities as well as access to the NOC for real-time updates on network and equipment health. AT&T provides 24x7x3657 monitoring and Denial of Service mitigation tools.

AT&T monitors the core network for traffic anomalies and shared resource consumption thresholds to protect the core network and preserve the performance of other customers.

AT&T monitors and audits all aspects of the network for threats from a variety of sources. NetFlow 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 AT&T ESInet™ environment. 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, AT&T immediately engages the AT&T ESInet™ 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 AT&T 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.

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.

AT&T 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.

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 System (IDS).

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

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.

AT&T ESInet 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 to help ensure 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.

Please see Exhibit 1: ESInet Security Strategy for a thorough description of the security aspects of the ESInet's critical information assets such as encryption, firewalls, anti-virus protection, and access. Also see Exhibit 2: AT&T Information & Network Security for additional information,

Any additional documentation can be inserted here:



Exhibit 1_ESInet



Exhibit 2_AT&T

Security Strategy.pdf Information & Netwo

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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

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

Bidder Detailed Response:

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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

InfoSec establishes 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
- 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

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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.

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

With respect to incident reporting, Intrado:

- Utilizes 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
- 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:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- 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:

- 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

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- 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
- 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

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

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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.”

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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

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
- 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:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	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
SEC 4	Bidder Response	X			
	<p>The AT&T solution provides predictive analysis and modeling to combat security threats as described below.</p> <p>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 AT&T ESInet 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.</p> <p>We deploy heuristic analysis, a method used 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 a particular threat/risk using various decision rules or weighing methods.</p> <p>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.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 5	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>Interactions between the ECRF and the ESRP are secured within the ESInet. Interactions with external ECRFs or the PSAP CPE will utilize digital certificate-based authentication as defined by NENA and when available managed by the PSAP Credentialing Agency (PCA). Until that time, AT&T will manage credentialing and issue digital certificates to help ensure protection and security. This mechanism will also be utilized for PSAP access to systems within the AT&T ESInet, including access to the LIS interface, ADR interface and ECRF. At no time will ECRFs used for call routing or PSAP determination provide un-credentialed access. This is due to the potential for Denial of Service (DoS) attacks impacting their critical functions.</p> <p>Following are devices and/or protocols used to restrict access.</p> <ul style="list-style-type: none"> • AT&T ESInet 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. <p>AT&T verifies credentialed devices or carriers are authorized access in the following manner:</p> <ul style="list-style-type: none"> • Client certificates are issued by a trusted Certificate Authority (CA) are required in order to access I3 services such as LIS, ADR and ECRF. • The trusted Certificate Authority is currently provided by Intrado, once available, the NENA designated PCA vendor will be utilized. • The IP address of any far end SIP endpoint must be provisioned in the SBC. <ul style="list-style-type: none"> ○ 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 authorized OSP's and/or data sources. ○ Connectivity the ESInet is only by signed and approved agreement with data encapsulated by IPSEC MPLS VPN. 				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	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
SEC 6	<p>Bidder Response:</p> <p>AT&T undergoes security audits internally and by third-party vendors on a regular (yearly) basis. Audits specifically requested and initiated by the State of Nebraska shall be added to this schedule upon request</p> <p>AT&T in cooperation with the State will allow the State to conduct a security assessment of the ESInet solution given the following requirements:</p> <ul style="list-style-type: none"> • Whitelisted, credentialed scanning must be performed by an AT&T approved third party. We will work with the State to develop a mutually agreeable Statement of Work (under separate SOW). • All testing will occur during a mutually agreed upon schedule. • All testing will require a mutually agreeable test plan. • All test results provided to the State will be subject to a confidentially agreement. • AT&T will allow monthly vulnerability scans to be performed as long as they are coordinated at a mutually agreeable date and time. 	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Physical Security All structures outside the Commission's control that will house components of the ESInet and NGCS shall have security and access-control systems that ensure that only duly authorized individuals can access the areas housing the Commission's systems and network equipment. Any workstations or other equipment connected to, or capable of accessing, the ESInet and NGCS systems shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the Commission's systems similarly shall be protected. Identify any elements that are not under the direct control of the bidder, and a description of the building's security and access-control systems shall be provided.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SEC 7	<p>Bidder Response:</p> <p>Physical access controls are based on the principle of "Least Privilege" that strives to restrict or limit all access to only areas necessary to perform authorized functions. AT&T operates in secured environments where physical access to staff office space, switching centers, global network and service management centers and other network facilities are controlled through an enterprise-wide physical security standard that applies to AT&T companies, affiliates and contractors. Physical access to AT&T facilities is controlled with the use of an AT&T-issued Photo ID Card and one or more devices including an access card, code and biometric reader. All access devices are approved and validated by an authorizing manager.</p> <p>Critical facilities are controlled through alarming and monitoring based on physical security standard criteria and periodic audits are performed to confirm adherence to the requirements of this standard.</p> <p>AT&T uses various procedures to help ensure physical security in our data centers and supporting infrastructure, including controlling, monitoring, and recording physical access to facilities where application 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.</p> <p>Our physical security controls include:</p> <ul style="list-style-type: none"> • Access policies and procedures • Access control system, including secure-card key access, biometrics scanners, mantrap, and alarmed doors • Logged Access procedures including employee, contractor, vendor, and visitor access • Closed circuit TV cameras and recorders • Global Client Support Center (GCSC) security • 24x7 physical security officer presence • Multi-factor authentication for data center access • Closed circuit TV monitoring • Access logs • Monthly review of access list <p>Local and remote monitored Power and Environmental controls (built at least to an N+1 methodology) include:</p> <ul style="list-style-type: none"> • HVAC • Sophisticated fire detection and suppression systems 				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Diverse commercial power feeds
 - Standby generator systems
 - Uninterruptible Power Supply (UPS)
 - Grounding architecture
 - Commercial power contingency arrangements

Our automated access control system uses electronic badge readers, biometric scanners, and PIN keypads to control and monitor access to AT&T 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 compromised or not immediately closed.

We limit access to the data centers, aggregation sites and Global 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.

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.

For Intrado locations, AT&T requires that Intrado

1. Ensures all information resources intended for use by multiple users are located in secure physical facilities with access restricted to authorized individuals only.
2. Monitors and records, access to the physical facilities containing information i.e., sources intended for use by multiple users in connection with supplier's performance of in-scope Work.
3. Physically secures any area where in-scope information is accessible to prevent access by unauthorized persons. In addition, supplier shall monitor and record the physical access to any facilities where in-scope information is accessible to prevent access by unauthorized persons.

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	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 <ol style="list-style-type: none"> 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 As an industry-leading provider of 9-1-1 and public safety services for more than 30 years, AT&T has successfully implemented mature, proven processes and operational procedures for supporting a NOC/SOC that can rapidly triage calls. The AT&T ESInet Network Operations Center (NOC) is staffed 24x7x365 days a year to actively monitor and manage the AT&T ESInet associated services and connectivity. The NOC is located in Longmont, CO. AT&T's MPLS core network is supported from eight security operations centers (SOCs) in North America, Latin America, Europe and Asia Pacific to ensure a high-level of visibility, monitoring and response capabilities. 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. NOC/SOC Interoperability AT&T has extensive experience in the operating with other vendor NOCs. As an industry-leading provider of 9-1-1 and public safety services for more than 30 years, AT&T has experience with communicating, troubleshooting in coordination with other NOCs including PSAPs, OSPs, and other 9-1-1				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

System Service Providers (SSP). The AT&T 9-1-1 Resolution Center is available 24x7x365 and is responsible for accepting incoming trouble reports, performing initial triage, implementing call routing changes, and is the first line of support for PSAPs, OSPs, and vendors.

The AT&T Resolution Center has established procedures to cover both communication and troubleshooting to all the PSAPs and OSPs in their current 21-state footprint for the legacy Selective Router and ALI services. In addition, as part of the ESInet deployment AT&T works with each of the legacy SSPs, OSPs, and PSAPs to establish set procedures for communication should an issue be encountered. AT&T establishes an Interconnect Agreement with each of the OSPs and SSPs before any connections are established and uses this to create processes for NOC-to-NOC communication. AT&T also has worked with other NG providers to establish communication and troubleshooting processes for areas where two different providers border each other. AT&T currently works with INdigital in the State of Indiana as calls are handed off between INdigital and AT&T for termination at various PSAPs throughout the State. AT&T also has established communication and troubleshooting procedures with Intrado for their A9-1-1 platform. AT&T is currently ebonded with Intrado's NOC to provide ticket status. AT&T will work with the State of Nebraska and other vendor NOCs to establish processes and procedures. Ebonding between NOCs could require additional costs as specific information would be needed from the vendor's NOC to scope the level of effort and any changes to the AT&T Resolution Center's systems.

Currently, AT&T uses a web-based application for communication. The web-based application used for notification by the AT&T 9-1-1 Resolution utilizes a pre-populated template and distribution list per customer, to communicate potential or actual FCC significant events to the PSAP communities. The notification can be sent to multiple PSAPs, Districts, or State personnel depending on the requirements/needs of the State of Nebraska.

NOC/SOC Operations Model

AT&T has provided responses to requirements 1-6 below.

1. NOC/SOC Operations Model

As an industry-leading provider of 9-1-1 and public safety services for more than 30 years, AT&T has successfully implemented mature, proven processes and operational procedures for supporting a NOC/SOC that can rapidly triage calls.

The AT&T ESInet Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage the AT&T ESInet associated services and connectivity. The NOC is located in Longmont, CO. AT&T's MPLS core network is supported from eight security operations centers (SOCs) in North America, Latin America, Europe and Asia Pacific to ensure a high-level of visibility, monitoring and response capabilities. 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.

Multiple network management components monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Active application monitoring and alerting complement traditional network management. The AT&T ESInet application elements also report network failures as detected by their application messaging activity, some of which is specific to managing the availability and integrity of the solution.

All network elements are monitored at the NOC in Longmont CO. This includes LNGs, ESRPs, ECRFs, BCFs, and PSAP site equipment.

The NOC monitors and tracks net flow statistics and performs packet level capture and forensics at the AT&T ESInet™ core sites. There are currently two varieties of monitoring systems in use at the NOC. One provides a “single pane of glass” for network and system status. This provides SNMP trap

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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.

AT&T's MPLS core network is supported from eight security operations centers (SOCs) in North America, Latin America, Europe, and Asia Pacific. AT&T also brings deep security expertise and methodologies across several disciplines to customer engagements, with a support team of more than 9,000 AT&T badged sales personnel who are trained in security as well as 1,500+ dedicated security experts. AT&T's security portfolio capabilities are used to protect our data centers and networks that carry more than 206.4 petabytes of data traffic on an average business day. The SOC team also performs vulnerability assessments on our network to continually assess our systems' security posture.

2. Continuity of Operations Plan (COOP)

The AT&T ESInet solution is backed by AT&T's business continuity/disaster recovery organization. AT&T and Intrado have 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, 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

Network Disaster Recovery

AT&T has established defined and reasonable business continuity and restoration plans including complex disaster and evacuation contingencies and conducts annual reviews to confirm adequacy of the plans. Adequate hardware spares are on hand to enable attainment of reliability and mean time between failure objectives. Geographically diverse engineering and redundancy provide ability to survive disaster scenarios. Power infrastructure and environmental systems are deployed so that a commercial power failure does not result in an interruption of service.

AT&T has developed its disaster recovery plans and processes to achieve the key objectives of maintaining the highest industry availability of the 9-1-1 infrastructure and the ability to recreate the core of North America's 9-1-1 systems in a minimal amount of time in the event of a major network and system incident. Our security infrastructure and processes also play a key role in ensuring maximum uptime of the AT&T ESInet™ systems.

AT&T's solutions are highly fault tolerant with automated failover capabilities to minimize down time and the need for user intervention in the event of a catastrophic failure. All vital system components are protected through the use of redundant modules to eliminate any single point of failure.

AT&T 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. AT&T'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.

Network Service Restoration

In the event of an outage AT&T applies immediate and sustained effort, 7x24, until a final resolution is in place. AT&T & Intrado use all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. If a temporary workaround solution is provided, AT&T & Intrado provide an action plan to be mutually agreed upon for the final resolution. AT&T & Intrado continue resolution activity until

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

full service is restored. The primary objective of an incident is to mitigate impact. The Incident Commander and Incident Administrator are able to call upon whatever resources are required to identify and restore functionality.

Network Outage Mitigation

Some of the steps AT&T has taken to prevent or circumvent outages in the AT&T ESInet systems and services include the following.

- The ESInet design supports the ability to automatically reroute traffic to alternate routes in order to bypass network outages and system failures.
- AT&T's essential processes, systems, and networks supporting 9-1-1 traffic are designed and deployed with diversity to accommodate possible disruptions and disasters to any given element or data center and support 24x7x365 continuous operation.
- Core sites are geographically distributed to prevent a geographic disaster from causing a service outage.
- Each of the Core sites is equipped with multiple battery backups, as well as generators permanently located at each site. Each facility is required to have priority fuel contracts in place, guaranteeing constant fuel supplies during extended outages. Regular maintenance and full load testing is required at each site to provide reliability.
- 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.

In the event of an outage AT&T applies immediate and sustained effort, 7x24, until a final resolution is in place. AT&T and Intrado use all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. If a temporary workaround solution is provided, AT&T and Intrado provide an action plan to be mutually agreed upon for the final resolution. AT&T and Intrado continue resolution activity until full service is restored. The primary objective of an incident is to mitigate impact. The Incident Commander and Incident Administrator are able to call upon whatever resources are required to identify and restore functionality.

Business Continuity

AT&T 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. AT&T'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

- Risk Assessment
 - The AT&T 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.
- Service Continuity Strategy
 - AT&T is strongly committed to providing essential business processes, systems, and networks on a 24x7x365 basis and is well prepared for possible disruptions and disasters. AT&T has a robust business and service continuity program designed to prevent or mitigate

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	<p>service disruptions and support rapid response to loss or impairment of crucial business functions or infrastructure. To address potential risks, AT&T utilizes:</p> <ul style="list-style-type: none"> ▪ Redundant, Geographically Diverse Systems – The six-core site AT&T ESInet architecture is located in geographically diverse and redundant data centers throughout. <ul style="list-style-type: none"> • Incident Management <ul style="list-style-type: none"> ○ 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, AT&T 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. • Business and Service Continuity, Disaster Recovery, and Emergency Procedures <ul style="list-style-type: none"> ○ AT&T has established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to our facilities or systems, including: <ul style="list-style-type: none"> ▪ 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 ▪ Inclement weather ▪ Building disasters • Implementing Risk Reduction and Recovery Measures <ul style="list-style-type: none"> ○ AT&T’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 AT&T 9-1-1 systems to continue operating while Incident Management processes are engaged to identify and resolve issues so that redundancy is fully restored. • Developing Plans and Procedures <ul style="list-style-type: none"> ○ 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. AT&T 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. AT&T 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: <ul style="list-style-type: none"> ▪ Essential functions and personnel ▪ Employee emergency contact information ▪ Building emergency procedures
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- 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
 - AT&T implements and tests its Incident Management Plan on a regular basis and conducts audits and reviews based on industry best practices 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
 - AT&T conducts an annual maintenance review of its continuity plans. This review is coordinated by business continuity management team, the interdependent plan owners identify, validate, implement, and document changes to the plan components.

3. Problem and Change Management

The AT&T Change Management system and processes described below will provide the State's program manager with the ability to review proposed change requests, coordination and communications with other vendors, and the client approval process.

AT&T will maintain historical information for the term of the contract, provide copies of the data to the State on request and at the end of the contract, and provide monthly reports detailing change tickets opened, pending, resolved, and closed. AT&T's Service Manager will provide change management reports.

Change Management System/Tools

AT&T's utilizes both Incident/Problem Management and the Change Management module of ServiceNow providing the required interface to enable correlation of information.

AT&T utilizes these tools in conjunction with 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. Our tool suite and built-in ITIL best practices enable us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.

AT&T will conduct major and minor planned and critical unplanned changes for all AT&T ESInet system maintenance or upgrades that may impact customers. AT&T 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. AT&T 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. AT&T will include the required back-out time within the scheduled maintenance time frame.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Change Management / Maintenance Plan

AT&T broadly classifies Change Management into two categories

- Global Change Management Process for AT&T ESInet™ (Change Management)
 - How AT&T operates, administers and maintains our national call routing service e.g., Changes to network, hardware and software components affecting all users of the service
- Local Change Management via Move, Add, Change and Disconnect (MACD)
 - How customers operate, administer and maintain their own PSAP specific information e.g., Provisioning data (Speed dial lists, Route changes, contact information etc.)

Global Change Management Process for AT&T ESInet (Change Management)

Change Management process governs the planning, coordinating, monitoring, reviewing, approving, auditing and communicating of change in the interest of maintaining service at target performance and availability levels for the AT&T ESInet. AT&T 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. Our tool suite and built-in ITIL best practices enables us to understand and minimize risk while making Global changes, as well as allowing the environment to be stable, reliable, and predictable.

This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.

The Change Management process ensures that all organizations impacting 9-1-1 will:

- Implement changes as scheduled and approved
- Perform deconfliction to reduce the number of concurrent changes that can be scheduled without impairing service
- Communicate planned change activity in a timely manner to allow accurate impact assessment and approvals
- Proactively eliminate or reduce incidents and outages caused by change
- Protect the production AT&T ESInet™ service
- Provide high availability for applications, network, services and infrastructure

The Change Management process cares for platform wide changes in the AT&T ESInet Core Routing platform. AT&T tracks scheduled changes to all components of the AT&T ESInet, which include Aggregation Sites, Core Call Routing Complexes, AT&T ESInet PSAP network edge equipment as well as the interconnections to each.

Most maintenance activities on the AT&T ESInet™ solution are completed with no scheduled downtime for the customer. AT&T follows the notification policies in the Change Event Definitions and Notifications Matrix below.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Change Event Definitions and Notifications Matrix

Event Type	Definition	Notification
Normal	<ul style="list-style-type: none"> • Pre-planned maintenance events or upgrades • Normal changes are categorized according to risk and impact 	<ul style="list-style-type: none"> • AT&T shall notify customers in advance when there are potential impacts identified to the service
Emergency	<ul style="list-style-type: none"> • Typically, unplanned events • Issues that have a potential for an immediate threat to the production environment or 9-1-1 service. 	<ul style="list-style-type: none"> • AT&T shall notify customers as soon as the need for emergency maintenance is identified and every effort is made to provide as much advanced notice as possible for any issues anticipated to result in a service disruption

Change Management Steps

The AT&T Change Management process includes the following steps to ensure successful planning, governance and execution of implementing changes to help eliminate / minimize service impact.

Planning

AT&T Labs will thoroughly test all software updates and service packs as they are released by our suppliers and prior to releasing them into the live customer environment. This includes an Approval for Use (AFU) process which certifies new software releases. These upgrade and testing processes help ensure that our solution will work in a real-world environment and not just in test labs.

The standard AT&T ESInet™ maintenance window is 12 a.m.-6 a.m. 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 12 a.m.-6 a.m. Central.

MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

Review

AT&T utilizes a 9-1-1 Change Governance process to support 9-1-1 Change Management. Changes impacting 9-1-1 are submitted to a centralized 9-1-1 Governance Review Board for deconfliction and pre-approval. Planned events are scheduled in a manner that 9-1-1 operations are not impacted.

All change requests submitted to the 9-1-1 Governance Review Board for pre-approval must include the following before being considered for scheduling:

- A Risk Assessed MOP that includes a step-by-step guide of the changes being made
- Clear definition of scope
- Clearly stated impacts, if any

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Detailed validation and back-out plan(s) to rollback changes and revert to the previous production configuration
- All event resources are clearly listed (includes escalation lists)

Approval

This 9-1-1 governance process includes reviewing service availability, capacity, configurations and hardware/software release levels prior to approving any changes in the Service.

Once pre-approved, Change Requests with a potential large impact or any actual customer impact are submitted to our centralized 9-1-1 Governance Approval Board for executive review and approval. The 9-1-1 Governance Approval Board is a committee that consists of executive stakeholders and their representatives who review change requests and makes decisions regarding whether the change submitted should be implemented or not. The 9-1-1 Governance Approval Board meets weekly but is also engaged on an ad-hoc basis for emergency approvals should they be required.

Notification

AT&T's Service Management Organization will provide advanced notice of maintenance events, when there is possible customer impact identified. For questions during the maintenance window, the customer should contact the AT&T 9-1-1 Resolution Center.

Execution

The AT&T ESInet™ team conducts major and minor planned and critical un-planned events for all AT&T ESInet™ system maintenance or upgrades. Events are fully staffed and managed with a trained event management team, facilitating the change implementation and monitoring through the length of the event. For events that have potential for customer impact, additional steps are in place to ensure the co-ordination of the event via internal conference bridges and chat rooms.

Post Execution

The result of each change is tracked in AT&T's change management system and available for future reference in the system whether it was successful or unsuccessful. All unsuccessful events that result in a service impairment are tracked in AT&T's incident management system as incidents and follow our Incident Management Process where sustained effort is provided until service is restored.

AT&T ESInet Hardware/Software Maintenance Plan

The AT&T ESInet™ is designed and implemented as a fully managed service that eliminates the customer's need to constantly maintain, upgrade, and administer a complex hardware and software solution and it maximizes the customer's ability to focus on public safety.

Key components within the AT&T ESInet are periodically renewed to enable PSAPs to operate on the most modern communications technology during the life of the contract. AT&T maintains and monitors all equipment and software within the solution, and it is AT&T's goal to replace End of Support (EOS) equipment prior to the EOS vendor published date.

AT&T 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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Local Change Management Process (MACD)

MACD is an acronym used for PSAP Move, Add, Change, & Disconnect activities and is used to describe the processes and actions that take place on the existing live service.

MACDs are typically customer-initiated changes that allow and enable customers to operate, administer and maintain PSAP specific provisioned data such as speed dial lists, route changes and contact information.

Depending on complexity, MACD activities can be implemented either in a coordinated or non-coordinated manner.

- Coordinated MACDs include changes to call routing which may impact 911 call delivery. For coordinated MACDs there will be ongoing communication between AT&T and the customer regarding implementation, including timelines. Depending on the change requested, customers may be asked to participate in a conference bridge for immediate testing, which allows for unsuccessful changes to be promptly rolled back.
- Non-coordinated MACDs are limited to those that do not impact 911 call delivery. For non-coordinated MACDs, AT&T provides a completion notification to the customer once implemented.

MACD activities are not conducted under the control of the AT&T ESInet™ Change Management process, which is more geared towards global platform maintenance. As MACD activities are directly coordinated between AT&T and the customer, there are no MACD tickets created. MACD changes are noted in the AT&T customer database of record once completed and confirmed successful.

4. Reporting Systems

AT&T's incident management solution provides both a dedicated toll-free number as well as a web-based user portal (AT&T Express Ticketing Portal) for our AT&T ESInet 9-1-1 customers to utilize for reporting and obtaining/providing status on issues/tickets. The AT&T Express Ticketing Portal for creating and checking status on open trouble tickets also provides historical trouble ticket information for 60 days after the ticket is closed.

AT&T Customer Management Portal

The AT&T web-based portal will also provide the State with a comprehensive reporting suite. Users have a predetermined PSAP or set of PSAPs for which they can 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 ESInet entry point to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics.

AT&T's comprehensive 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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- **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, refer). Call detail is available for each bridged call.
- **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.

Reports are created for AT&T ESInet by collecting event data for each call that comes into the AT&T ESInet™ destined for a Public Safety Answering Point (PSAP). Event data is time-stamped for time of answer and disconnect. Event data also identifies the time for each functional element to perform routing and PSAP assignment. Collecting this data also helps facilitate call diagnostics and troubleshooting.

5. Escalation Plan

AT&T has jurisdiction-level escalation processes in place with our subcontractors to be used during incidents that affect service, particularly those that result in critical service outages.

AT&T maintains an escalation list for our subcontractors. The escalation list includes the first, second, third and fourth level contact for an escalation. During a service impacting outage, at a minimum, our subcontractor will provide status to the AT&T 911 Resolution Center via a live bridge until service is restored. Should there be a need for escalation, AT&T will utilize the guidelines listed below when contacting subcontractors.

Initial Contact	After 30 Minutes with No Response	After 1 Hour with No Response	After 2 Hours with No Response
Supervisor	Manager	Director	Vice President

AT&T will maintain and make accessible these procedures on the AT&T Customer Management Portal. The escalation procedures listed above will be included as well as a list of escalation contacts.

AT&T ESInet has been designed with unmatched levels of redundancy and resiliency which greatly reduces the potential for service impacting outages. Severity Level 1 or Severity Level 2 service impacting outages will take precedent over a Severity Level 3 or Severity Level 4 issue. Should there be a service impacting Severity Level 1 or Severity Level 2 outage at a local, regional or statewide level; AT&T has the technical resources, associated tools and human resource capacity to address multiple incidents (local or statewide) at the same time. Listed below are items that aid in the escalation process and the Escalation Matrix for AT&T ESInet.

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

- Customer’s name and telephone number
- Active WFA ticket number(s)
- Trouble Location
- Trouble description (e.g., out of service, service degraded, etc.)

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- The action or resolution requested

AT&T ESInet 9-1-1 Resolution Center Escalation Matrix

Escalation Intervals	Level	Responsibility
First Escalation SEV 1: 2 Hours SEV 2: 4 Hours	Resolution Manager	<ul style="list-style-type: none"> • Review Customer Request and keep customer updated • Escalate as needed to the appropriate partner center
Second Escalation (Customer Discretion)	Lead Resolution Manager	<ul style="list-style-type: none"> • Review customer request and keep customer updated • Escalate as needed to the appropriate partner center
Third Escalation (Customer Discretion)	Area Manager or Delegate	<ul style="list-style-type: none"> • Review status of ticket • Monitor ticket progress • Notify Director - when appropriate
Fourth Escalation (Customer Discretion)	Director	<ul style="list-style-type: none"> • Status Customer • Escalate as needed to partner centers • Monitor ticket Progress/ documentation • Notify AVP when appropriate

AT&T’s escalation procedures are consistent for all issues. If there are discrepancies between the performance of AT&T ESInet and the State of Nebraska service level agreements, the AT&T dedicated 911 Service Manager will work on the behalf of the State of Nebraska to address and resolve the identified issues. Should further escalation be necessary, the dedicated 911 Service Manager will notify the Director of 911 Service Management for assistance.

AT&T’s communication procedures with internal technical personnel, suppliers, customers as well as external agencies (i.e. federal, state and local emergency response agencies) are defined in our Event Management Framework (EMF). AT&T’s EMF provides an incident command structure used to manage planned or unplanned events that impact AT&T business processes, assets, or people. The EMF defines AT&T’s Emergency Management Operations (EMO), the delineation of the different entities within the EMO, and the roles and responsibilities of those entities as well as decision-making authority at the corporate, Business Unit, and local levels.

Event Definition

An Event is AT&T preferred term describing a Product/Service, Technology, and/or Administrative Space disruption. Each Business Unit in AT&T is required to create and maintain Business Continuity Plans that describe how it will respond to an Event. For common communication standards and status reporting purposes, Events are categorized into four levels based on severity:

Disaster Severity Levels

The disaster severity level matrix defines events by the severity of the damage to AT&T technology assets and/or personnel. The table provides examples of the magnitude of damage, as well as examples of the associated impact for each of the four levels. It also identifies the network organization responsible for command and control of a response.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Level 4	Level 3	Level 2	Level 1
Description	Local service disruptions that can be restored by local teams. Teams follow normal, BAU procedures.	Outage exceeds the restoration capacity of local teams.	Regional incident requiring coordination of multiple disciplines/response organizations.	Major event requiring the coordination and deployment of extensive resources.
Examples	Cable cuts, power failures, localized hazardous conditions.	Minor or regional flooding, small tornadoes.	Earthquakes and widespread weather hazards (hurricanes, multiple tornadoes, major flooding).	Cybersecurity attacks, national security attacks, major health incident, severe earthquakes.
Technology Impact	Localized, single-element failures.	Impacts more than one technical group or geographical area.	Multiple, large-scale incidents requiring dedicated teams for 3CP (Command, Control, and Communications).	Impact is so severe that enterprise management required.
Incident Command	Impacted Business Unites, Local Response Center (LRC)	Event Management Technical Reliability Center (EM-TRC) and LRCs	Global Emergency Management Center, Emergency Operations Center (EOC), Global Technology Operations Center (GTOC)	Executive Command Council (ECC)

Disaster Severity Level Matrix

AT&T Event Management Framework approach utilizes the continuous assessment and action refinement methodology shown in the figure below.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

- Level 1**
Senior Officers manage Event
 DHS Escalations, Corporate-wide impact, Significant Cyber attack
- Level 2**
Corporate Teams manage Event
 Major network impacts, Severe Weather, Significant technology impact, Communicable Infectious Disease
- Level 3**
Business Units manage
 Minor network impacts, local situations impacting buildings/facilities
- Level 4**
~ Business As Usual
 Network monitoring, infrastructure impact, Building power outage, Individual technology outage



Figure 2: Event Management Framework

Event Levels

- **Level 4 Business As Usual Event.** Low Impact: Local emergencies or service interruptions that can be resolved with the resources under the jurisdiction of the Business Unit. Teams follow Business As Usual processes.
- **Level 3 Business Unit Event.** Moderate Impacts: A moderate Event level that impacts more than one Business Unit/Organization/Work Group. The Event can be resolved with the resources of the Business Units, using the procedures documented in their business continuity plans. Global EMC notification is mandatory.
- **Level 2 Multiple-Business Unit Event.** High Impacts: A significant Event, requiring deployment of additional assets and coordination of efforts across multiple Business Units. Escalation occurs when the Event's coordination needs exceed the capabilities outlined in the Business Units' continuity plans. Global Emergency Management Center (GEMC) activation is required for overall incident command and control. Executive notification is mandatory.
- **Level 1 Corporate Disaster.** Extreme Impacts: A Major Event requiring deployment of extensive Company assets and coordination of significant efforts across Multiple Business Units. Escalation occurs when the Event's coordination needs exceed the capabilities outlined in the Business Unit's continuity plans and Executive management oversight is required. Executive notification including the Executive Command Council (ECC) and GEMC is mandatory.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Event Escalation Process

As an Event progresses, it may escalate or deescalate in its impact on AT&T operations. Each Business Unit Response Team is responsible for activating their plan and determining if the Event warrants escalation from Level 4 to Level 3.

- If the Business Unit feels it needs assistance or the Event requires a higher level of coordination, the responder escalates to the GEMC for appropriate Command & Control.
- If the Event passes Level 2 requirements for Incident Command, the Global EMC will engage the ECC with a recommendation to activate the GEMC and potentially the ECC.
- If the decision is made to activate the ECC, it will assume Incident Command and the GEMC will provide operational support for the duration of the event.

Furthermore, AT&T has an established operations manual describing policies and procedures for communicating with technical personnel in our supplier organization. AT&T has implemented electronic interfaces (ebonding) to improve speed of communications with our vendor suppliers. The 9-1-1 Resolution Center uses the Everbridge system as a way of providing written and verbal mass notifications to communicate potential ESInet service-affecting or actual FCC significant events to the PSAP communities. We have the capability to provide notification by phone, email, or text as directed by the customer. Notifications can be sent to the State, a PSAP, or other approved contact, depending on the requirements/needs of the customer and their capabilities. These can include customer specific instructions for phone numbers and email distribution lists to meet the needs of the customer.

AT&T ESInet™ service operation is actively supported by a team comprised of Tier 1, Tier 2 and Tier 3 technical staff responsible for identification, isolation, and mitigation in the event of an incident or issues related to hardware, software, security, and operational process functions. Tier 1 support engages Tier 2 and Tier 3 support as required to assist in resolution of high-priority tickets and complex alarms.

AT&T ESInet™ 9-1-1 Resolution Center Escalation Matrix

Escalation Intervals	Level	Responsibility
First Escalation SEV 1: 2 Hours SEV 2: 4 Hours	Resolution Manager	<ul style="list-style-type: none"> • Review Customer Request and keep customer updated • Escalate as needed to the appropriate partner center
Second Escalation (Customer Discretion)	Lead Resolution Manager	<ul style="list-style-type: none"> • Review customer request and keep customer updated • Escalate as needed to the appropriate partner center
Third Escalation (Customer Discretion)	Area Manager Or Delegate	<ul style="list-style-type: none"> • Review status of ticket • Monitor ticket progress • Notify Director - when appropriate
Fourth Escalation (Customer Discretion)	Director	<ul style="list-style-type: none"> • Status Customer • Escalate as needed to partner centers • Monitor ticket Progress/ documentation • Notify AVP when appropriate

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<p>6. Conformance with Best Practices</p> <p>AT&T utilizes both Incident/Problem Management and the Change Management module of ServiceNow in conjunction with 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. Our tool suite and built-in ITIL best practices enable us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

NOC/ SOC 2	<p>NOC/SOC - Remote Connectivity Required</p> <p>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.</p>	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	<p>Bidder Response:</p> <p>The AT&T ESInet solution deploys minimal hardware at the Call Handling Host sites. Should this equipment need troubleshooting, AT&T will attempt to remote in through the existing network used for call and data delivery. In the event AT&T cannot access remotely, an AT&T technician will be deployed to the site and will require access to the routers installed on-site.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 3	<p>NOC/SOC - Network Security Monitoring and Management Security Management Solution</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>The AT&T system adheres to NENA 75-001 (NENA Security for Next-Generation 9-1-1 Standard [NG-SEC]) and NENA 04-503 (PSAP Security), as applicable. Our solution provides for the centralized management of user permissions, rights, and security settings by designated administrators. The system administrators can use the application to manage user roles and privileges, including granular authentication, user profiles, and other security rights.</p> <p>AT&T 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.</p> <p>While AT&T has deployed cloud infrastructure that is CJIS-compliant, the AT&T ESInet solution is not, as it is not intended to house CJJ data.</p>				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
NOC/ SOC 4	<p>Bidder Response:</p> <p>The AT&T ESInet provides a Next Generation 9-1-1 (NG9-1-1) solution that 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, as well as the standards listed in Appendix A. AT&T, and our partner Intrado, are engaged with, and play active roles in, industry associations that develop standards applicable to NG911, including NENA, APCO, ATIS, FCC, PCIA, and TIA.</p> <p>AT&T ESInet solution adheres to AT&T security requirements and the NENA Security for Next-Generation (NG-SEC) 9-1-1 Standard to track compliance across the numerous frameworks.</p> <p>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.</p> <p>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.</p> <p>Additionally, AT&T External & Legislative Affairs (E&LA) staff monitors Local, State and Federal laws and regulations that are applicable to the Products and Services we provide. If there are changes in any laws, regulations or standards, or new ones are introduced, those changes are communicated to the potentially impacted organizations/Business Units. It is the responsibility of the Business Unit to modify or adapt to remain in compliance with the new or changed law, regulation or standard. Using an E&LA Compliance Notification Portal, Business Unit leads must provide E&LA with a certification of Implementation /Certification of Compliance. AT&T has a Chief Compliance Organization that reports directly to the CEO of AT&T and monitors our compliance.</p> <p>Security Reports and Recommendations</p> <p>AT&T will provide security reports on a monthly basis, including incidents and incident response, and updates or changes to security systems and software. A compilation of these reports can be provided to the State of Nebraska in soft form at the end of the contract. AT&T Corporate Real Estate, Asset Protection & Security teams are happy to work with the State of Nebraska on any request related to physical access to facilities that are part of the ESInet solution. In addition, AT&T will proactively contact the State of Nebraska and communicate any relevant security concerns as they are identified.</p>				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	NOC/SOC – Connected Systems Compliance Support for Similar Solutions	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/SOC 5	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			
	<p>Bidder Response:</p> <p>AT&T’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). AT&T’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.</p> <p>The AT&T ESInet infrastructure (illustrated in the figure below) is built to withstand sophisticated attacks (including DDOS) by means of a defense in depth strategy. AT&T 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, AT&T’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.</p>				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

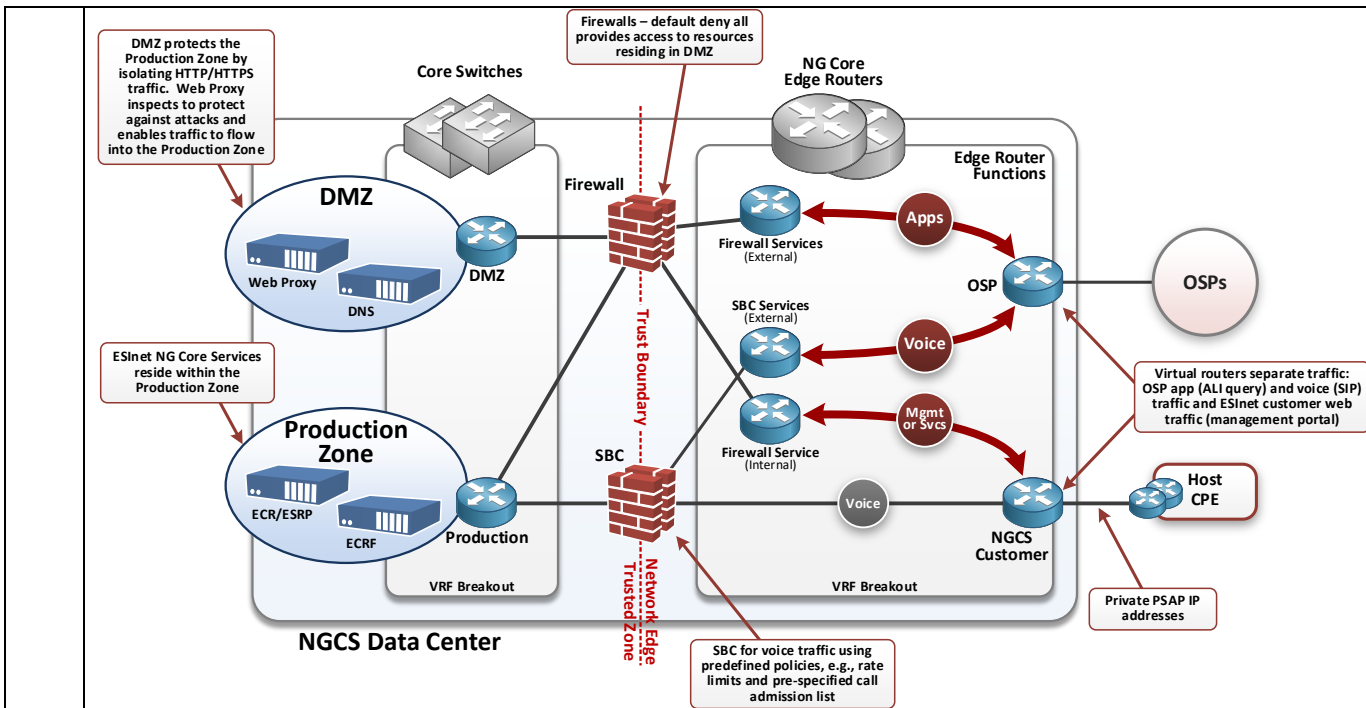


Figure 3: Defense in-depth Security Architecture*

The network can process 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), and through continuous network monitoring traffic analysis. AT&T 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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

AT&T ESInet 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 vulnerability scans.

AT&T employs an Incident Handling process modeled on FEMA's Incident Command System, with notifications built into this process.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	NOC/SOC - Physical Access Monitoring and Management	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 6	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>Physical access controls are based on the principle of "Least Privilege" that strives to restrict or limit all access to only areas necessary to perform authorized functions. AT&T operates in secured environments where physical access to staff office space, switching centers, global network and service management centers and other network facilities are controlled through an enterprise-wide physical security standard that applies to AT&T companies, affiliates and contractors. Physical access to AT&T facilities is controlled with the use of an AT&T-issued Photo ID Card and one or more devices including an access card, code, biometric reader and/or company-issued key. All access devices are approved and validated by an authorizing manager.</p> <p>Critical facilities are controlled through alarming and monitoring based on physical security standard criteria and periodic audits are performed to confirm adherence to the requirements of this standard.</p> <p>AT&T uses various procedures to help ensure physical security in our data centers and supporting infrastructure, including controlling, monitoring, and recording physical access to facilities where application 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.</p> <p>Our physical security controls include:</p> <ul style="list-style-type: none"> • Access policies and procedures • Access control system, including secure-card key access, biometrics scanners, mantrap, and alarmed doors • Logged Access procedures including employee, contractor, vendor, and visitor access • Closed circuit TV cameras and recorders • Global Client Support Center (GCSC) security • 24x7 physical security officer presence • Multi-factor authentication for data center access • Closed circuit TV monitoring • Access logs • Monthly review of access list 				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Our automated access control system uses electronic badge readers, biometric scanners, and PIN keypads to control and monitor access to AT&T 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 and Global 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.

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.

For Intrado locations, AT&T requires that Intrado

1. Ensures all Information Resources intended for use by multiple users are located in secure physical facilities with access restricted to authorized individuals only.
2. 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.
3. Physically secures any area where In-Scope Information is accessible to prevent access by unauthorized persons. In addition, Supplier shall monitor and record the physical access to any facilities where In-Scope Information is accessible to prevent access by unauthorized persons.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 7	<p>NOC/SOC - Incident Management System</p> <p>The bidder's incident management system shall log all support requests, both from users and those automatically generated.</p> <p>1. Provide examples of monthly reports detailing tickets opened, pending, resolved, and closed.</p> <p>2. Provide a matrix outlining Service Impact Levels in a detailed response, to include notification times and response times.</p>	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	<p>Bidder Response:</p> <p>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 AT&T proposed solution.</p> <p>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.</p> <p>AT&T 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.</p> <p>AT&T's incident management solution provides both a dedicated Toll-Free number as well as a web-based user portal (AT&T Express Ticketing Portal) for our AT&T ESInet™ 9-1-1 customers to utilize for reporting and obtaining/providing status on issues/tickets. The AT&T Express Ticketing Portal for creating and checking status on open trouble tickets also provides historical trouble ticket information for 60 days after the ticket is closed.</p> <p>All support requests from users and those automatically generated are logged.</p> <p>See the following for answers to requirements 1 and 2.</p> <ol style="list-style-type: none"> 1. Samples of monthly ticket reports can be found in Exhibit 3: AT&T Monthly Trouble Ticket Sample 2. AT&T ESInet™ Severity, Response and Restoral Matrix 	X			

Severity Code	Description (Examples)	Response/ Notification Time	Restore Time	Status Frequency
Critical (Sev. 1)	<ul style="list-style-type: none"> • Trunk outages • Alternate Routing activation • All calls misrouting • No ANI/ALI • Loss of service • FCC reportable incidents • PSAP unable to perform core functions 	15 minutes	2 hours	1 hour

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none"> • Transfer failures (all calls) • Circuit outage • Ransomware or Malware attack 				
Major (Sev.2)	<ul style="list-style-type: none"> • Intermittent misroutes • Intermittent transfer failures • Intermittent ALL issues no/incorrect data • WAN links bouncing intermittently • Inability of PSAP to support 911 calls due to equipment failures 	30 minutes	4 hours	2 hours	
Minor (Sev.3)	<ul style="list-style-type: none"> • Occasional calls misrouting Occasional transfers to other PSAPs failures • PSAP equipment issues that do not impact call taker response 	1 hour	5 Calendar Days	24 hours	
Intermittent (Sev.4)	<ul style="list-style-type: none"> • Non-critical and informational request • Maintenance Activities 	2 hours	15 Calendar Days	Weekly	

Any additional documentation can be inserted here:



Exhibit 3_AT&T
Monthly Trouble Ticks

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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			
<p>Bidder Response:</p> <p>The AT&T Change Management system and processes described below will provide the State's program manager with the ability to review proposed change requests, coordination and communications with other vendors, and the client approval process.</p> <p>AT&T will maintain historical information for the term of the contract, provide copies of the data to the State on request and at the end of the contract, and provide monthly reports detailing change tickets opened, pending, resolved, and closed. AT&T's Service Manager will provide change management reports.</p> <p>Change Management System/Tools</p> <p>AT&T's utilizes both Incident/Problem Management and the Change Management module of ServiceNow providing the required interface to enable correlation of information.</p> <p>AT&T utilizes these tools in conjunction with 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. Our tool suite and built-in ITIL best practices enable us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.</p> <p>AT&T will conduct major and minor planned and critical unplanned changes for all AT&T ESInet system maintenance or upgrades that may impact customers. AT&T 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. AT&T 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. AT&T will include the required back-out time within the scheduled maintenance time frame.</p> <p>Change Management / Maintenance Plan</p> <p>AT&T broadly classifies Change Management into two categories</p> <ul style="list-style-type: none"> • Global Change Management Process for AT&T ESInet™ (Change Management) <ul style="list-style-type: none"> ○ How AT&T operates, administers and maintains our national call routing service e.g., Changes to network, hardware and software components affecting all users of the service • Local Change Management via Move, Add, Change and Disconnect (MACD) <ul style="list-style-type: none"> ○ How customers operate, administer and maintain their own PSAP specific information e.g., Provisioning data (Speed dial lists, Route changes, contact information etc.) 				

NOC/
SOC
8

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Global Change Management Process for AT&T ESInet™ (Change Management)

Change Management process governs the planning, coordinating, monitoring, reviewing, approving, auditing and communicating of change in the interest of maintaining service at target performance and availability levels for the AT&T ESInet™. AT&T 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. Our tool suite and built-in ITIL best practices enables us to understand and minimize risk while making Global changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.

The Change Management process ensures that all organizations impacting 9-1-1 will:

- Implement changes as scheduled and approved
- Perform deconfliction to reduce the number of concurrent changes that can be scheduled without impairing service
- Communicate planned change activity in a timely manner to allow accurate impact assessment and approvals
- Proactively eliminate or reduce incidents and outages caused by change
- Protect the production AT&T ESInet™ service
- Provide high availability for applications, network, services and infrastructure

The Change Management process cares for platform wide changes in the AT&T ESInet™ Core Routing platform. AT&T tracks scheduled changes to all components of the AT&T ESInet, which include Aggregation Sites, Core Call Routing Complexes, AT&T ESInet™ PSAP network edge equipment as well as the interconnections to each.

Most maintenance activities on the AT&T ESInet™ solution are completed with no scheduled downtime for the customer. AT&T follows the notification policies in the Change Event Definitions and Notifications Matrix below.

Change Event Definitions and Notifications Matrix

Event Type	Definition	Notification
Normal	<ul style="list-style-type: none"> • Pre-planned maintenance events or upgrades • Normal changes are categorized according to risk and impact 	<ul style="list-style-type: none"> • AT&T shall notify customers in advance when there are potential impacts identified to the service
Emergency	<ul style="list-style-type: none"> • Typically, unplanned events • Issues that have a potential for an immediate threat to the production environment or 9-1-1 service. 	<ul style="list-style-type: none"> • AT&T shall notify customers as soon as the need for emergency maintenance is identified and every effort is made to provide as much advanced notice as possible for any issues anticipated to result in a service disruption

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Change Management Steps

The AT&T Change Management process includes the following steps to ensure successful planning, governance and execution of implementing changes to help eliminate / minimize service impact.

Planning

AT&T Labs will thoroughly test all software updates and service packs as they are released by our suppliers and prior to releasing them into the live customer environment. This includes an Approval for Use (AFU) process which certifies new software releases. These upgrade and testing processes help ensure that our solution will work in a real-world environment and not just in test labs.

The standard AT&T ESInet™ maintenance window is 12 a.m.-6 a.m. 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 12 a.m.-6 a.m. Central.

MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

Review

AT&T utilizes a 9-1-1 Change Governance process to support 9-1-1 Change Management. Changes impacting 9-1-1 are submitted to a centralized 9-1-1 Governance Review Board for deconfliction and pre-approval. Planned events are scheduled in a manner that 9-1-1 operations are not impacted.

All change requests submitted to the 9-1-1 Governance Review Board for pre-approval must include the following before being considered for scheduling:

- A Risk Assessed MOP that includes a step-by-step guide of the changes being made
- Clear definition of scope
- Clearly stated impacts, if any
- Detailed validation and back-out plan(s) to rollback changes and revert to the previous production configuration
- All event resources are clearly listed (includes escalation lists)

Approval

This 9-1-1 governance process includes reviewing service availability, capacity, configurations and hardware/software release levels prior to approving any changes in the Service.

Once pre-approved, Change Requests with a potential large impact or any actual customer impact are submitted to our centralized 9-1-1 Governance Approval Board for executive review and approval.

The 9-1-1 Governance Approval Board is a committee that consists of executive stakeholders and their representatives who review change requests and makes decisions regarding whether the change submitted should be implemented or not. The 9-1-1 Governance Approval Board meets weekly but is also engaged on an ad-hoc basis for emergency approvals should they be required.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Notification

AT&T’s Service Management Organization will provide advanced notice of maintenance events, when there is possible customer impact identified. For questions during the maintenance window, the customer should contact the AT&T 9-1-1 Resolution Center.

Execution

The AT&T ESInet team conducts major and minor planned and critical un-planned events for all AT&T ESInet™ system maintenance or upgrades. Events are fully staffed and managed with a trained event management team, facilitating the change implementation and monitoring through the length of the event. For events that have potential for customer impact, additional steps are in place to ensure the co-ordination of the event via internal conference bridges and chat rooms.

Post Execution

The result of each change is tracked in AT&T’s change management system and available for future reference in the system whether it was successful or unsuccessful. All unsuccessful events that result in a service impairment are tracked in AT&T’s incident management system as incidents and follow our Incident Management Process where sustained effort is provided until service is restored.

Local Change Management Process (MACD)

MACD is an acronym used for PSAP Move, Add, Change, & Disconnect activities and is used to describe the processes and actions that take place on the existing live service.

MACDs are typically customer-initiated changes that allow and enable customers to operate, administer and maintain PSAP specific provisioned data such as speed dial lists, route changes and contact information.

Depending on complexity, MACD activities can be implemented either in a coordinated or non-coordinated manner.

- Coordinated MACDs include changes to call routing which may impact 911 call delivery. For coordinated MACDs there will be ongoing communication between AT&T and the customer regarding implementation, including timelines. Depending on the change requested, customers may be asked to participate in a conference bridge for immediate testing, which allows for unsuccessful changes to be promptly rolled back.
- Non-coordinated MACDs are limited to those that do not impact 911 call delivery. For non-coordinated MACDs, AT&T provides a completion notification to the customer once implemented.

MACD activities are not conducted under the control of the AT&T ESInet™ Change Management process, which is more geared towards global platform maintenance. As MACD activities are directly coordinated between AT&T and the customer, there are no MACD tickets created. MACD changes are noted in the AT&T customer database of record once completed and confirmed successful.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: AT&T uses both Incident/Problem Management and the Change Management module of ServiceNow providing the required interface to enable correlation of information. AT&T uses these tools in conjunction with 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. Our tool suite and built-in ITIL best practices enable us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	NOC/SOC – Change Management System Change Testing and Training Environment A non-production ESInet replica, test lab, or similar system shall be established to test, and exercise proposed upgrades, third-party interfaces, and applications prior to release in live production. This system also could be leveraged for training purposes. Provide detailed descriptions of how the solution satisfies this function in the change management process.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 10	<p>Bidder Response:</p> <p>AT&T and its call handling vendors have set up test PSAPs connected to AT&T ESInet for some larger customers. These test PSAPs are used for AT&T and Customer Operational Readiness Testing, exercising, and training purposes. AT&T can work with NGCS and their call handling vendors to build a test environment if so desired. As AT&T ESInet is already fully functional it should be noted that AT&T thoroughly tested the AT&T ESInet platform prior to production release. This included functional/system, failover, load, performance and stability testing of all components in the six core data centers (ECMCs) and Aggregation Sites. Integration testing was performed with Intrado Viper, Motorola Vesta and Solacom Guardian call handling systems and supported voice (CAMA, RFAI and i3) and text-to-911 interfaces. ESInet platform and call handling testing is ongoing as new software and hardware are released and circuits added to the system.</p> <p>In addition, AT&T performs thorough Operational Readiness and cutover testing prior to PSAP migration to AT&T ESInet. AT&T can provide test cases to NGCS for review. AT&T’s ESInet has a dedicated lab that is used for testing upgrades, third party interfaces, and applications prior to the releasing the enhancements to the live ESInet environment. Once tested without errors, these enhancements are implemented in production. This lab environment utilizes the same hardware/software as in the production environment to ensure testing done in the lab environment will validate the components used in production. This non-production environment is also used for training of personnel and administrators of the system.</p> <p>Additionally, AT&T would be happy to coordinate periodic visits to the AT&T Lab.</p> <p>AT&T Labs will be responsible for testing and exercising the AT&T ESInet and interfaces. This includes not only software upgrade and release testing on an on-going basis, but also forward-looking initiatives e.g., new standards development. Test engineers will collaborate with all relevant parties in the creation, review, and execution of test cases as part of the implementation process.</p> <ul style="list-style-type: none"> • Application Testing. Each application is individually tested to ensure its stability and lack of critical defects. • Integration Testing. After each application is tested individually integration testing is performed. This helps ensure that each version of our applications work well together. • Hardware/Software Validation. Products are constantly validated against new hardware and software, including operating systems, service packs and updates. • Load Testing. Load testing is performed to ensure that the system stays stable and consistent even under peak demand. Specialized software allows us to create any number of simultaneous calls. Performance is benchmarked both with statistics as well as having users navigate the application interface and answer calls while under load. This assures that not only are the statistical values acceptable, but perhaps more importantly, the user experiences no negative behavior. <p>AT&T Labs:</p> <ul style="list-style-type: none"> • Develops test plan in conjunction with equipment and software vendors • Maintains identical lab ESInet architecture to production environment 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none">• Schedules and conducts all testing for the introduction of new hardware and/or software releases• Coordinates with vendor to address any problems related with new product or software releases• Oversees the First Office Application of all newly introduced hardware or software releases• Monitors in conjunction with ATS organization after FOA• Provides Approval for Use and certifies new hardware or software release upon successful completion of FOA soak period
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	NOC/SOC – Change Management System Change Management Process 1. Outline bidder’s proposed change management process. The ITIL change management standard methods and procedures are preferred. 2. Include a description of the process for notifying the Commission and affected PSAPs. Notification shall be made no less than ten (10) business days in advance of the change, except in emergency situations, in which case notification shall be provided immediately. 3. Include explanation of solution’s Fault, Configuration, Accounting, Performance, and Security (FCAPS) procedures. 4. Provide a detailed explanation describing how the proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 11	<p>Bidder Response:</p> <p>The following is AT&T’s point-by-point response to requirements 1-4:</p> <ol style="list-style-type: none"> AT&T 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. Our tool suite and built-in ITIL best practices enables us to understand and minimize risk while making Global changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts. <p>The Change Management process ensures that all organizations impacting 9-1-1 will:</p> <ul style="list-style-type: none"> Implement changes as scheduled and approved Perform deconfliction to reduce the number of concurrent changes that can be scheduled without impairing service Communicate planned change activity in a timely manner to allow accurate impact assessment and approvals Proactively eliminate or reduce incidents and outages caused by change Protect the production AT&T ESInet™ service Provide high availability for applications, network, services and infrastructure <p>The Change Management process cares for platform wide changes in the AT&T ESInet™ Core Routing platform. AT&T tracks scheduled changes to all components of the AT&T ESInet, which include Aggregation Sites, Core Call Routing Complexes, AT&T ESInet™ PSAP network edge equipment as well as the interconnections to each.</p> <p>Change Management Tools</p> <p>AT&T utilizes both the Incident / Problem Management module and the Change Management module of ServiceNow in conjunction with our best practices to enable us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable.</p>	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Change Management Steps

The AT&T Change Management process includes the following steps to ensure successful planning, governance and execution of implementing changes to help eliminate / minimize service impact:

- **Planning**

AT&T Labs will thoroughly test all software updates and service packs as they are released by our suppliers and prior to releasing them into the live customer environment. This includes an Approval for Use (AFU) process which certifies new software releases. These upgrade and testing processes help ensure that our solution will work in a real-world environment and not just in test labs.

The standard AT&T ESInet™ 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.

MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

- **Review**

AT&T utilizes a 9-1-1 Change Governance process to support 9-1-1 Change Management. Changes impacting 9-1-1 are submitted to a centralized 9-1-1 Governance Review Board for deconfliction and pre-approval. Planned events are scheduled in a manner that 9-1-1 operations are not impacted.

All change requests submitted to the 9-1-1 Governance Review Board for pre-approval must include the following before being considered for scheduling:

- A Risk Assessed MOP that includes a step-by-step guide of the changes being made
- Clear definition of scope
- Clearly stated impacts, if any
- Detailed validation and back-out plan(s) to rollback changes and revert to the previous production configuration
- All event resources are clearly listed (includes escalation lists)

- **Approval**

This 9-1-1 governance process includes reviewing service availability, capacity, configurations and hardware/software release levels prior to approving any changes in the Service.

Once pre-approved, Change Requests with a potential large impact or any actual customer impact are submitted to our centralized 9-1-1 Governance Approval Board for executive review and approval. The 9-1-1 Governance Approval Board is a committee that consists of executive stakeholders and their representatives who review change requests and makes decisions regarding whether the change submitted should be implemented or not. The 9-1-1 Governance Approval Board meets weekly but is also engaged on an ad-hoc basis for emergency approvals should they be required.

- **Notification**

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

AT&T’s Service Management Organization will provide advanced notice of maintenance events, when there is possible customer impact identified.

For questions during the maintenance window, the customer should contact the AT&T 9-1-1 Resolution Center.

- **Execution**

The AT&T ESInet™ team conducts major and minor planned and critical un-planned events for all AT&T ESInet™ system maintenance or upgrades. Events are fully staffed and managed with a trained event management team, facilitating the change implementation and monitoring through the length of the event. For events that have potential for customer impact, additional steps are in place to ensure the co-ordination of the event via internal conference bridges and chat rooms.

- **Post Execution**

The result of each change is tracked in AT&T’s change management system and available for future reference in the system whether it was successful or unsuccessful. All unsuccessful events that result in a service impairment are tracked in AT&T’s incident management system as incidents and follow our Incident Management Process where sustained effort is provided until service is restored.

2. Most maintenance activities on the AT&T ESInet™ solution are completed with no scheduled downtime for the customer. AT&T follows the notification policies in the Change Event Definitions and Notifications Matrix below:

Change Event Definitions and Notifications Matrix

Event Type	Definition	Notification
Normal	<ul style="list-style-type: none"> • Pre-planned maintenance events or upgrades • Normal changes are categorized according to risk and impact 	<ul style="list-style-type: none"> • AT&T shall notify customers in advance when there are potential impacts identified to the service
Emergency	<ul style="list-style-type: none"> • Typically, unplanned events • Issues that have a potential for an immediate threat to the production environment or 9-1-1 service. 	<ul style="list-style-type: none"> • AT&T shall notify customers as soon as the need for emergency maintenance is identified and every effort is made to provide as much advanced notice as possible for any issues anticipated to result in a service disruption

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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none">• 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. <p>4. Our adherence to Information Technology Infrastructure Library (ITIL) framework and best practices enables us to understand and minimize risk while making changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/SOC - Network Management System and Network Management Software Software packages are widely available for capturing, analyzing, and reporting the network's health based on the Simple Network Management Protocol (SNMP) traffic it receives. Provide the name and description of the management software that will be implemented including all functional modules associated with it (e.g., reporting, backup, and IP address management).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X		
<p>Bidder Response:</p> <p>The AT&T 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 AT&T 9-1-1 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 AT&T 9-1-1 NOC. These systems also provide ICMP and SNMP trending and threshold alarming.</p> <p>The NOC also utilizes the following:</p> <ul style="list-style-type: none"> • 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. <p>The AT&T ESInet 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.</p> <div data-bbox="210 922 957 1201" style="text-align: center;"> </div> <p>Figure 4: ESInet Monitoring</p> <p>BlueCat's Proteus IP Address Management (IPAM) solution is our IP Management tool; it enables us to design, deploy, reconfigure, and maintain the IP address inventory of all company devices in the network, production, and lab environments.</p>				

NOC/
SOC
12

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/SOC – Network Management System NMIS Interworking with Elements and Services Provide a detailed explanation and associated drawings explaining how the proposed solution interworks with all of the various elements and services of the proposed systems and network elements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X			
Bidder Response: AT&T uses multiple tools to track performance and fault management activities. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to HP Openview, which is used to present a single pane of glass to the AT&T 9-1-1 NOC. OpenView utilizes the HP Operations Manager (OM) module, which monitors systems and applications using agents, and the HP Network Node Manager (NNMi) network monitoring software module based on SNMP. Visual alerts are available 24x7x365 to the AT&T 9-1-1 NOC. The AT&T ESInet 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.				
NOC/ SOC 13	<p>The diagram illustrates the network architecture and monitoring mechanisms. It is divided into three main sections: Aggregation Sites, NGCS Data Centers, and PSAP. <ul style="list-style-type: none"> Aggregation Sites: Contains two LNGs (Local Network Gateways) connected to two routers. NGCS Data Centers: Contains a Core Complex with two servers, connected to a stack of four routers. PSAP: Contains PSAP CPE (Customer Premises Equipment) connected to two routers. Below the network diagram, three monitoring mechanisms are shown with arrows indicating their scope: <ul style="list-style-type: none"> WAN Health Checks / Automated Failover: Two arrows, one spanning from the Aggregation Sites to the NGCS Data Centers, and another from the NGCS Data Centers to the PSAP. Packet Capture / Analytics: A single arrow spanning from the NGCS Data Centers to the PSAP. Application Health Checks / Reporting: Two arrows, one spanning from the Aggregation Sites to the PSAP, and another from the NGCS Data Centers to the PSAP. Syslog / SNMP / Agent-based Fault & Performance Management: A single long arrow spanning the entire network from the Aggregation Sites to the PSAP. </p>			
	Figure 5: ESInet Monitoring			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 14	<p>NOC/SOC - Network Event Logging System and Network Event Logging and Reporting</p> <p>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)).</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>Our AT&T Global Technology Operation Center (GTOC) provides complete 24/7 proactive service monitoring and operations support to help ensure optimum network availability and performance. The GTOC performs various maintenance services, including fault detection, isolation, and repair.</p> <p>The GNTC uses Simple Network Management Protocol (SNMP)-based software to monitor the IP network and employs a combination of other tools to monitor non-SNMP equipment and network servers. Displays in each GTOC provide 24/7 reports on network status to our staff, and we log any change in IP network status and use that information to evaluate staff responsiveness and network availability.</p> <p>AT&T has provided a description of our GTOC capabilities below.</p> <p>The AT&T Global Technology Operations Center</p> <p>AT&T's GTOC one of the largest and most technology advanced network operations centers in the industry. From this sophisticated command and control center, AT&T manages a network that services the world's leading businesses, including all the Fortune 1000 companies. Using state-of-the-art diagnostic tools, the network management team proactively monitors and manages the flow of global data, video and voice traffic, helping to ensure the highest level of reliability, performance, and security -24 hours a day.</p>				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



Figure 6: The AT&T GNOC

The AT&T **GNOC-Incident Management Team** (GNOC-IM) continually assesses the condition of AT&T's global network when outages reach GNOC thresholds for tracking & reporting. When an anomaly occurs that threatens or impacts the performance of our network the GNOC-IM team is engaged for those issues meeting threshold. The response is then managed by the GNOC-IM staff through a practiced and proven incident command process called 3CP (Command, Control, and Communications). Real time updates are provided to management based on subscriptions.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESNet
Request for Proposal Number 6264 Z1

GTOC – IM Process Flow

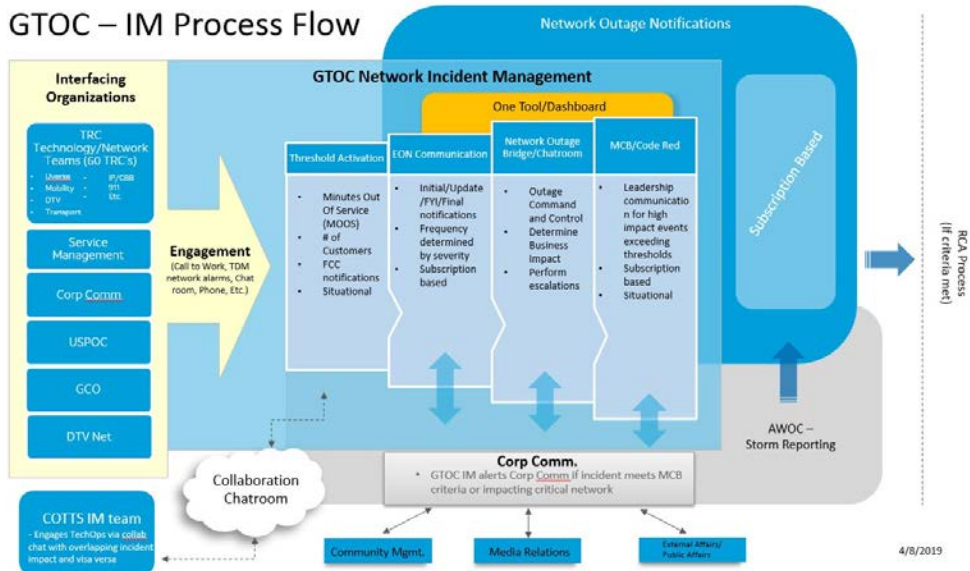


Figure 7: IM Process Flow

The responsibilities of the GNOC-IM team Include:

- Assesses the condition of AT&T's global network when outages reach GTOC thresholds for tracking & reporting 24x7x365.
- Activate appropriate network management traffic controls in the switched circuit (Voice) network.
- Drive restoral of service; escalate as needed.
- Provide technical support for certain technologies such as Transport, Voice or Emerging Services.
- Create and send outage notifications and Executive communications, as well as working level communications.
- Conduct Call Wrap-up process and Outage Accounting for assigned D2 Applications.
- Execute and assign Action Items as required on high profile incidents and service disruptions that require executive summaries.
- Update ticketing systems to track outages via NERS and ONE Tool.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESNet
Request for Proposal Number 6264 Z1

Below are some examples of reports from the GTOC Dashboard allowing them to efficiently manage the network:

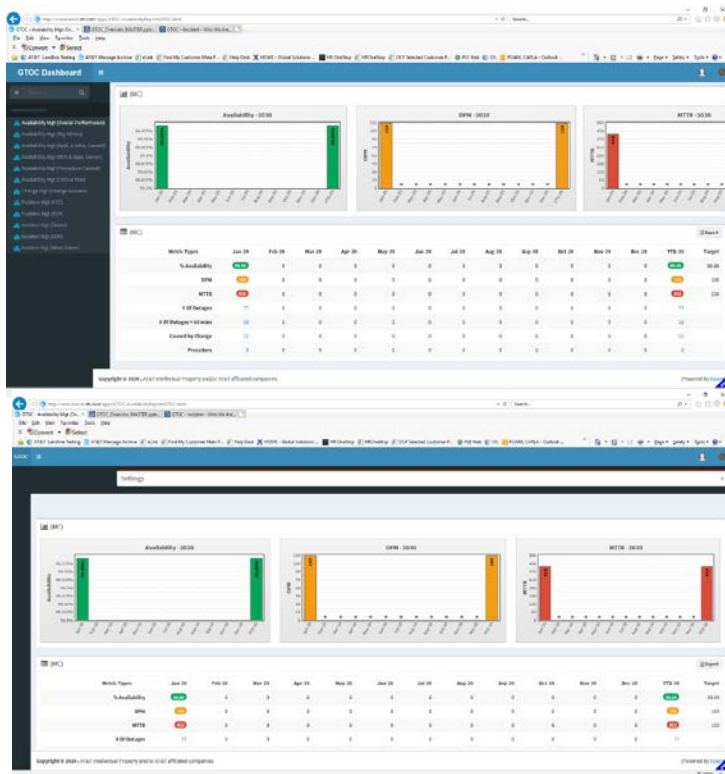


Figure 8: GTOC – Availability Reports

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

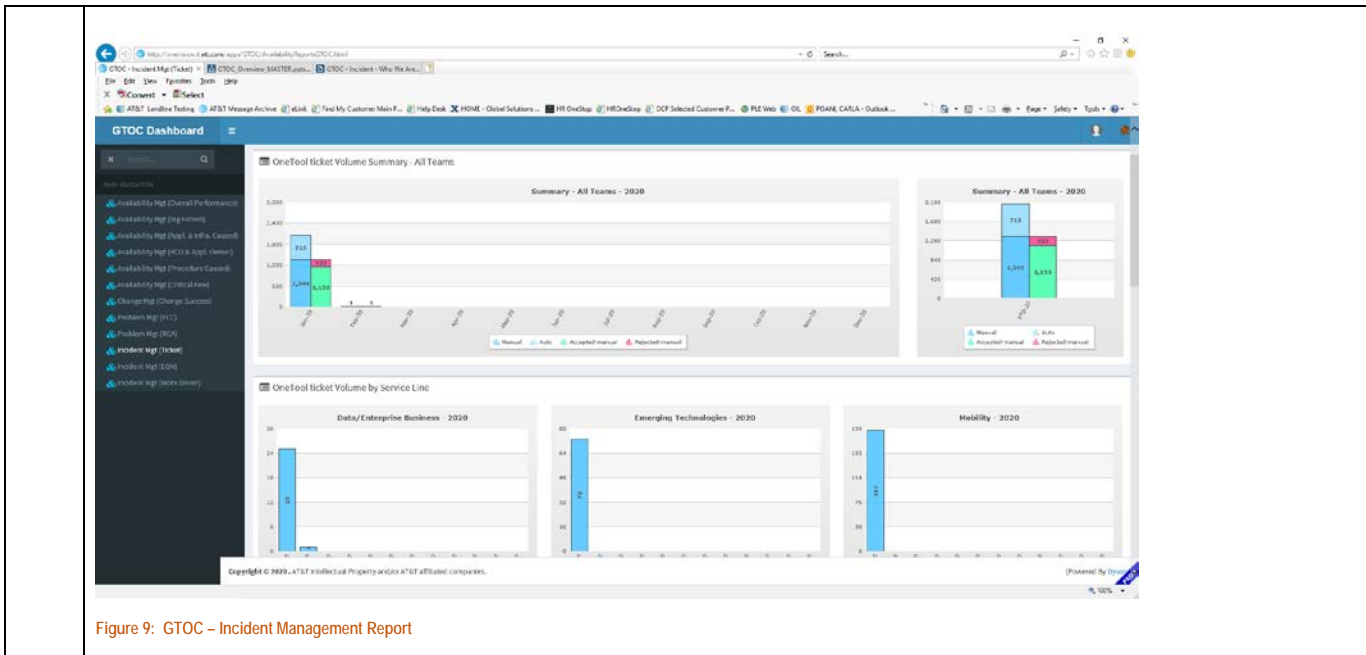


Figure 9: GTOC – Incident Management Report

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

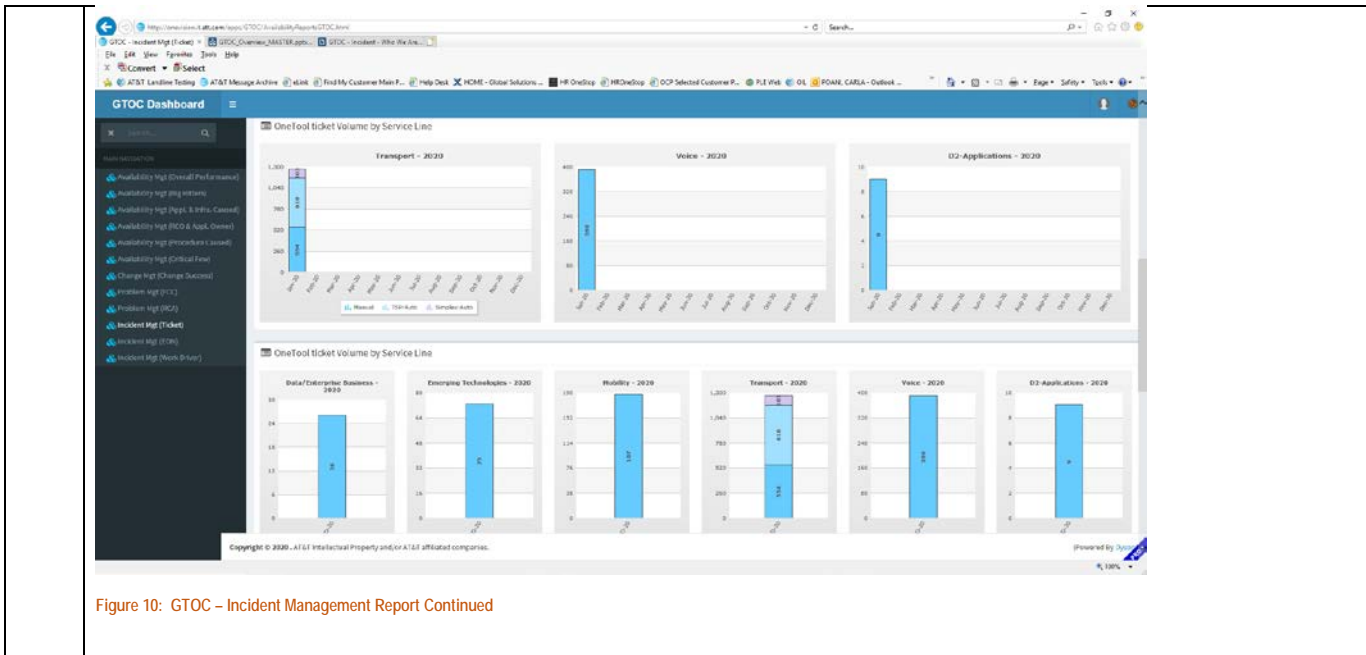


Figure 10: GTOC – Incident Management Report Continued

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

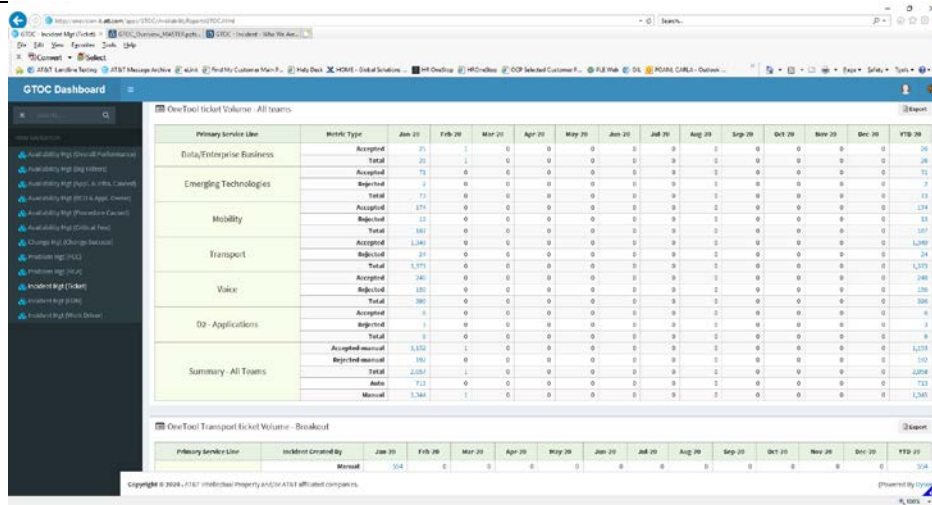


Figure 11: GTOC – Incident Management Summary

i3 Logging Capability

In addition, the AT&T ESInet service provides an i3 logging capability per the NENA STA-010.2 specification. AT&T can support near real-time log delivery and web service interfaces for log retrieval from authorized clients. The AT&T ESInet solution logs hundreds of data points for each call that traverses the system to assist in tracking and troubleshooting calls. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

The Customer Management Portal provides participating PSAPs and approved personnel 24x7 access to call detail records through a secure, web-based portal. The call detail records provide the user with all of the pertinent information for each call.

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Reporting

AT&T'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.
- **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

The AT&T 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. AT&T 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.

AT&T has provided some additional management reports that would be available to the State below.

Attachment "C" Option C Technical Requirements Public Service Commission ESInet Request for Proposal Number 6264 Z1

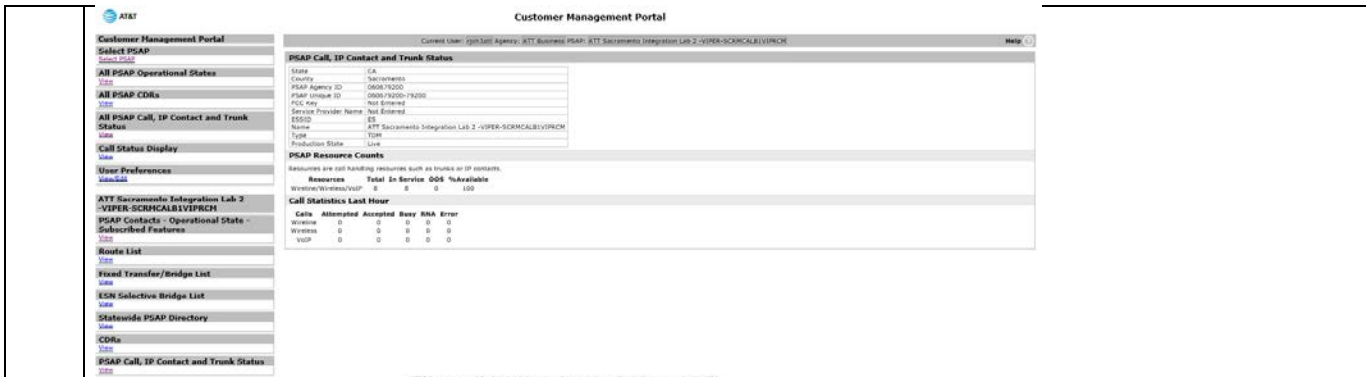


Figure 12: PSAP Resource Availability and Statistics

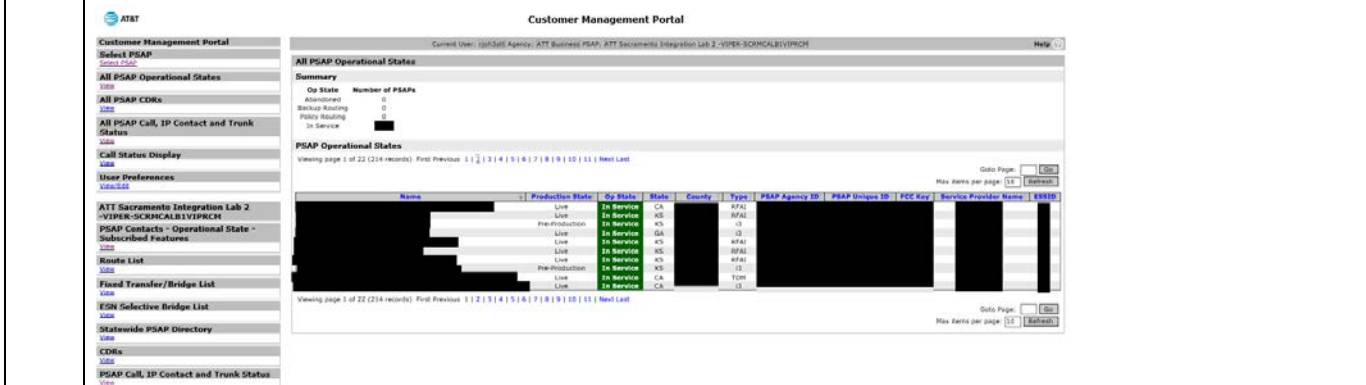


Figure 13: PSAP Operation Status

**Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

The screenshot shows the AT&T Customer Management Portal interface. The main content area displays the following information:

- PSAP Contacts - Operational State - Subscribed Features**
- State: CA
- County: Sacramento
- PSAP Agency ID: 060919200
- PSAP Import ID: 060919200-79200
- PSIC Key: Not Entered
- Service Provider Name: Not Entered
- ESGID: ES
- Name: ATT Sacramento Integration Lab 2 -VIPER-SCRMCALBIVIPRCH
- Type: TDM
- Production State: Live

Additional sections visible include 'Contacts' with details for a contact named 'Anyone' and 'Operational State' showing 'En Service'.

Figure 14: PSAP Operation State 7 Subscribed Features

Any additional documentation can be inserted here:

NOC/ SOC 15	NOC/SOC - Network Event Logging Management System Interface to Incident Management System This system should be part of, or interfaced with, the bidder's incident management system, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract and provide copies of the data to the Commission on request, and at the end of the contract. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Bidder Response: AT&T and its supplier Intrado have integrated eBonding ticketing exchange 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 the data is transferred to archive.	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

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: AT&T and Intrado have implemented processes and procedures for interfacing regarding event logging. The following examples listed below describe process flows for use cases where an event occurs within a) an AT&T aggregation center and b) within the AT&T call routing core complexes.																																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #ADD8E6;"> <th style="text-align: center;">Step #</th> <th style="text-align: center;">Description</th> <th style="text-align: center;">Responsibility</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td>The Intrado 9-1-1 NOC receives an alarm related to the Aggregation Site equipment.</td> <td>Intrado 9-1-1 NOC</td> </tr> <tr> <td style="text-align: center;">2</td> <td>The Intrado 9-1-1 NOC opens an eBonded ticket and/or call the AT&T E9-1-1 Resolution Center specifying that the Intrado Life & Safety investigation is still in progress.</td> <td>Intrado 9-1-1 NOC</td> </tr> <tr> <td style="text-align: center;">3</td> <td>The AT&T E9-1-1 Resolution Center receives the eBonded ticket, if sent.</td> <td>AT&T E9-1-1 Resolution Center</td> </tr> <tr> <td style="text-align: center;">4</td> <td>The Intrado 9-1-1 NOC, either remotely or via on hands support, confirms that the issue is facility related and outside of Intrado Life & Safety control.</td> <td>Intrado 9-1-1 NOC</td> </tr> <tr> <td style="text-align: center;">5</td> <td>Is the issue a Severity 1 issue? If yes, go to the Outage Process. If no, go to step 6.</td> <td>Intrado 9-1-1 NOC</td> </tr> <tr> <td style="text-align: center;">6</td> <td>The Intrado 9-1-1 NOC contacts AT&T to request on-site assistance and updates the eBonded ticket for the AT&T E9-1-1 Resolution Center.</td> <td>Intrado 9-1-1 NOC</td> </tr> <tr> <td style="text-align: center;">7</td> <td>The AT&T Local Operations Center (LOC) coordinates with LOC resources for on-site support and updates the ticket with an ETA.</td> <td>AT&T Local Operations Center</td> </tr> <tr> <td style="text-align: center;">8</td> <td>The AT&T Data Center Tech, upon arrival at the site, contacts the Intrado 9-1-1 NOC via the dedicated toll free number to coordinate remote hands support.</td> <td>AT&T Data Center Tech</td> </tr> <tr> <td style="text-align: center;">9</td> <td>Can the AT&T Data Center Tech resolve the issue? If yes, go to step 16.</td> <td>AT&T Data Center Tech</td> </tr> </tbody> </table>						Step #	Description	Responsibility	1	The Intrado 9-1-1 NOC receives an alarm related to the Aggregation Site equipment.	Intrado 9-1-1 NOC	2	The Intrado 9-1-1 NOC opens an eBonded ticket and/or call the AT&T E9-1-1 Resolution Center specifying that the Intrado Life & Safety investigation is still in progress.	Intrado 9-1-1 NOC	3	The AT&T E9-1-1 Resolution Center receives the eBonded ticket, if sent.	AT&T E9-1-1 Resolution Center	4	The Intrado 9-1-1 NOC, either remotely or via on hands support, confirms that the issue is facility related and outside of Intrado Life & Safety control.	Intrado 9-1-1 NOC	5	Is the issue a Severity 1 issue? If yes, go to the Outage Process. If no, go to step 6.	Intrado 9-1-1 NOC	6	The Intrado 9-1-1 NOC contacts AT&T to request on-site assistance and updates the eBonded ticket for the AT&T E9-1-1 Resolution Center.	Intrado 9-1-1 NOC	7	The AT&T Local Operations Center (LOC) coordinates with LOC resources for on-site support and updates the ticket with an ETA.	AT&T Local Operations Center	8	The AT&T Data Center Tech, upon arrival at the site, contacts the Intrado 9-1-1 NOC via the dedicated toll free number to coordinate remote hands support.	AT&T Data Center Tech	9	Can the AT&T Data Center Tech resolve the issue? If yes, go to step 16.	AT&T Data Center Tech
Step #	Description	Responsibility																																	
1	The Intrado 9-1-1 NOC receives an alarm related to the Aggregation Site equipment.	Intrado 9-1-1 NOC																																	
2	The Intrado 9-1-1 NOC opens an eBonded ticket and/or call the AT&T E9-1-1 Resolution Center specifying that the Intrado Life & Safety investigation is still in progress.	Intrado 9-1-1 NOC																																	
3	The AT&T E9-1-1 Resolution Center receives the eBonded ticket, if sent.	AT&T E9-1-1 Resolution Center																																	
4	The Intrado 9-1-1 NOC, either remotely or via on hands support, confirms that the issue is facility related and outside of Intrado Life & Safety control.	Intrado 9-1-1 NOC																																	
5	Is the issue a Severity 1 issue? If yes, go to the Outage Process. If no, go to step 6.	Intrado 9-1-1 NOC																																	
6	The Intrado 9-1-1 NOC contacts AT&T to request on-site assistance and updates the eBonded ticket for the AT&T E9-1-1 Resolution Center.	Intrado 9-1-1 NOC																																	
7	The AT&T Local Operations Center (LOC) coordinates with LOC resources for on-site support and updates the ticket with an ETA.	AT&T Local Operations Center																																	
8	The AT&T Data Center Tech, upon arrival at the site, contacts the Intrado 9-1-1 NOC via the dedicated toll free number to coordinate remote hands support.	AT&T Data Center Tech																																	
9	Can the AT&T Data Center Tech resolve the issue? If yes, go to step 16.	AT&T Data Center Tech																																	

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	If no, go to step 10.	
10	Is replacement equipment needed? If yes, go to step 11. If no, go to step 18.	AT&T Data Center Tech
11	The Intrado 9-1-1 NOC initiates the shipment of replacement equipment.	Intrado 9-1-1 NOC
12	The Intrado 9-1-1 NOC updates the eBonded ticket with shipment location, ETA, and tracking information.	Intrado 9-1-1 NOC
13	The AT&T Local Operations Center coordinates with the LOC support to schedule on-site work.	AT&T Local Operations Center
14	The AT&T Data Center Tech completes the hardware replacement installation and contacts the Intrado 9-1-1 NOC to validate that the issue has cleared.	AT&T Data Center Tech
15	Is the alarm/issue resolved? If yes, go to step 16. If no, go to step 18	Intrado 9-1-1 NOC
16	The Intrado 9-1-1 NOC validates that the issue is resolved and closes the eBonded ticket.	Intrado 9-1-1 NOC
17	The AT&T E9-1-1 Resolution Center closes their ticket.	AT&T E9-1-1 Resolution Center
18	The Intrado 9-1-1 NOC updated the eBonded ticket and notifies AT&T that additional troubleshooting is necessary.	Intrado 9-1-1 NOC
19	The Intrado 9-1-1 NOC, the AT&T E9-1-1 Resolution Center, the AT&T Local Operations Center, and the AT&T Data Center Tech troubleshoot via a conference bridge session.	Intrado 9-1-1 NOC AT&T E9-1-1 Resolution Center AT&T Local Operations Center AT&T Data Center Tech

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Step #	Description	Responsibility
1	The Intrado 9-1-1 NOC receives an alarm related to the Core Call Routing equipment.	Intrado 9-1-1 NOC
2	The Intrado 9-1-1 NOC opens an eBonded ticket and/or calls the AT&T E9-1-1 Resolution Center specifying that the Intrado Life & Safety investigation is still in progress.	Intrado 9-1-1 NOC
3	The AT&T E9-1-1 Resolution Center receives the eBonded ticket, if sent.	AT&T E9-1-1 Resolution Center
4	The Intrado 9-1-1 NOC, either remotely or via on hands support, confirms that the issue is facility related and outside of Intrado Life & Safety control.	Intrado 9-1-1 NOC
5	Is the issue a Severity 1 issue? If yes, go to the Outage Process. If no, go to step 6.	Intrado 9-1-1 NOC
6	The Intrado 9-1-1 NOC contacts AT&T IT to request on-site assistance and updates the eBonded ticket for the AT&T E9-1-1 Resolution Center.	Intrado 9-1-1 NOC
7	AT&T IT coordinates with Data Center resources for on-site support and updates the ticket with an ETA.	AT&T IT
8	The AT&T Data Center Tech, upon arrival at the site, contacts the Intrado 9-1-1 NOC via the dedicated toll free number to coordinate remote hands support.	AT&T Data Center Tech
9	Can the AT&T Data Center Tech resolve the issue? If yes, go to step 16. If no, go to step 10.	AT&T Data Center Tech
10	Is replacement equipment needed? If yes, go to step 11. If no, go to step 18.	AT&T Data Center Tech
11	The Intrado 9-1-1 NOC initiates the shipment of replacement equipment.	Intrado 9-1-1 NOC
12	The Intrado 9-1-1 NOC updates the eBonded ticket with shipment location, ETA, and tracking information.	Intrado 9-1-1 NOC

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	13	AT&T IT coordinates with Data Center support to schedule on-site work.	AT&T IT
	14	The AT&T Data Center Tech completes the hardware replacement installation and contacts the Intrado 9-1-1 NOC to validate that the issue has cleared.	AT&T Data Center Tech
	15	Is the alarm/issue resolved? If yes, go to step 16. If no, go to step 18	Intrado 9-1-1 NOC
	16	The Intrado 9-1-1 NOC validates that the issue is resolved and closes the eBonded ticket.	Intrado 9-1-1 NOC
	17	The AT&T E9-1-1 Resolution Center closes their ticket.	AT&T E9-1-1 Resolution Center
	18	The Intrado 9-1-1 NOC updated the eBonded ticket and notifies AT&T that additional troubleshooting is necessary.	Intrado 9-1-1 NOC
	19	The Intrado 9-1-1 NOC, the AT&T E9-1-1 Resolution Center, AT&T IT, and the AT&T Data Center Tech troubleshoot via a conference bridge session.	Intrado 9-1-1 NOC AT&T E9-1-1 Resolution Center AT&T IT AT&T Data Center Tech

Any additional documentation can be inserted here:

NOC/ SOC 17	NOC/SOC - Access to Technical Staff	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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.	X			
	Bidder Response: The following are AT&T's response to requirements 1 and 2. 1. The AT&T Resolution Center will communicate with our technical personnel from our participating suppliers and Customer entities through phone calls and ticketing system applications. A dedicated AT&T Toll-Free number has been established for both State of Nebraska and our participating suppliers to utilize for reporting and obtaining/providing status on ESInet issues. Intrado has also established a dedicated Toll-Free number for use by the AT&T Resolution Center for ESInet issues. AT&T provides a web-based ticketing system for use by our customers as well and a ticketing interface tool between AT&T and a participating supplier. 2. AT&T will require technical personnel to have a minimal level of assistance from Subcontractor, Commission, and participating PSAPs.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	NOC/SOC - Notification Specify how the bidder's NOC informs the Commission and the affected PSAPs or their designees of problems with the network, scheduled service and maintenance outages, and upgrades. Include all methods of notification used. Notifications for scheduled maintenance or outages shall be made no less than ten (10) business days in advance, except for emergency situations in which case, notification will be given immediately. Tickets related to the services delivered to subcontractors shall be forwarded automatically. Notification shall be provided via multiple communications means to the Commission and applicable PSAPs. Entities requiring notification may change, depending on the alarm or incident. Provide a detailed explanation explaining how the solution meets or exceeds the above requirements, including the methods of communications used.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 18	<p>Bidder Response:</p> <p>In case of a service interruption and/or outage, we have instituted Incident Management processes and procedures for dealing with various severity levels during the course of an event. Our incident response tools include use of the Incident Command System (ICS modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post- event analysis. We manage incidents and provide customers with up to the minute notification and status of ongoing service affecting issues that may impact the AT&T ESInet solution. Notifications to the affected PSAPs and the State will be provided by the AT&T 9-1-1 Resolution Center using the Everbridge system. This system will provide written and verbal mass notification to PSAPs of outages/issues that may be 9-1-1 service-affecting. AT&T will notify all impacted parties identified by the customer. We provide notification by email and SMS. A PSAP customer would need to notify the AT&T Resolution Center if they chose to be selected or deselected for outage notifications. The web-based application used for notification by the AT&T 9-1-1 Resolution utilizes a pre-populated template and distribution list per customer, to communicate potential or actual FCC significant events to the PSAP communities. The notification can be sent to multiple PSAP's, District's, or State Personnel depending on the requirements/needs of the State of Nebraska.</p> <p>Additionally, the AT&T Service Manager will notify the State of Nebraska of any scheduled maintenance of the AT&T ESInet solution. Scheduled maintenance is done with no scheduled downtime for Life and Mission Critical Services. 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 if applicable. Planned events are fully staffed and managed with a trained event management team, facilitating the change implementation, monitoring, and communication to all impacted parties through the length of the event. The AT&T ESInet 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. AT&T 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 State of Nebraska 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. AT&T has factored in the required back-out time within the scheduled maintenance time frame.</p> <p>Level 3 - Normal</p> <p>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 AT&T support will be reviewed with AT&T prior to the scheduled date. Example: Router replacement, PSAP activation, AT&T ESInet™ 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.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here:

	NOC/SOC - Executive Dashboard Contractor shall provide a web-based executive dashboard or similar tool, providing near real-time visibility of network status displayed geographically with service impact levels color-coded. Open ticket status shall be available to users through this dashboard. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 19	<p>Bidder Response:</p> <p>PSAP customers are able to access incident ticket status information via the AT&T Business Direct portal. Additionally, the CMP (Customer Management Portal) provides information indicating when Alternate (Disaster), Abandonment, or Overflow routing is active. Upon award, AT&T will work with the State of Nebraska to customize and enhance the portal user experience based on additional requirements and discovery to determine pricing (if applicable) and lead time for implementation</p> <p>AT&T's incident management solution provides a web-based user portal (AT&T Express Ticketing Portal) for AT&T ESInet™ 9-1-1 customers to create and check status on open trouble tickets. The AT&T Express Ticketing Portal provides historical trouble ticket information for 60 days after the ticket is closed.</p> <p>AT&T Express Ticketing is an online ticketing system which will allow the State to easily create, check status, add notes and escalate trouble tickets from a mobile phone, tablet or PC.</p> <p>Please see Exhibit 4: AT&T Express Ticketing User Guide for an overview of the tool and capabilities.</p> <p>AT&T's Customer Management Portal (CMP) provides a web-based executive dashboard to participating PSAPs and approved personnel 24x7x365 access to a reporting suite including call detail records and PSAP operational status to provide system and service performance. AT&T ESInet's CMP includes reporting tools for each of the functional elements in the ESInet architecture that produce standard reports of utilization, ad-hoc reports and threshold alarms.</p>	X			

Any additional documentation can be inserted here:



Exhibit 4_AT&T
Express Ticketing User

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 20	NOC/SOC - Escalation Procedures 1. Outline a detailed regional-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. 2. Describe how discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed. These procedures shall be maintained and accessible via an online portal. This escalation notification process shall be integrated with the notification processes described above, based on the problem reported.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply															
		X																		
Bidder Response: AT&T has provided responses to requirements 1 and 2 below. 1. AT&T 9-1-1 Escalation Procedures																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e1f5fe;"> <th style="text-align: left;">Escalation Intervals</th> <th style="text-align: left;">Level</th> <th style="text-align: left;">Responsibility</th> </tr> </thead> <tbody> <tr> <td>First Escalation SEV 1 - 2 Hours SEV 2 - 4 Hours SEV 3 - 6 Hours</td> <td>Resolution Manager</td> <td> <ul style="list-style-type: none"> Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center </td> </tr> <tr> <td>Second Escalation Customer Discretion</td> <td>Area Manager Or Delegate</td> <td> <ul style="list-style-type: none"> Review status of ticket Monitor ticket progress Notify Director - when appropriate </td> </tr> <tr> <td>Third Escalation Customer Discretion</td> <td>Director</td> <td> <ul style="list-style-type: none"> Status Customer Escalate as needed to partner centers Monitor ticket Progress/ documentation Notify AVP when appropriate </td> </tr> <tr> <td>Fourth Escalation</td> <td>AVP</td> <td> <ul style="list-style-type: none"> Ensure adequate resources are available and engaged for prompt resolution Update customer as appropriate Escalate as needed to appropriate levels </td> </tr> </tbody> </table>						Escalation Intervals	Level	Responsibility	First Escalation SEV 1 - 2 Hours SEV 2 - 4 Hours SEV 3 - 6 Hours	Resolution Manager	<ul style="list-style-type: none"> Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center 	Second Escalation Customer Discretion	Area Manager Or Delegate	<ul style="list-style-type: none"> Review status of ticket Monitor ticket progress Notify Director - when appropriate 	Third Escalation Customer Discretion	Director	<ul style="list-style-type: none"> Status Customer Escalate as needed to partner centers Monitor ticket Progress/ documentation Notify AVP when appropriate 	Fourth Escalation	AVP	<ul style="list-style-type: none"> Ensure adequate resources are available and engaged for prompt resolution Update customer as appropriate Escalate as needed to appropriate levels
Escalation Intervals	Level	Responsibility																		
First Escalation SEV 1 - 2 Hours SEV 2 - 4 Hours SEV 3 - 6 Hours	Resolution Manager	<ul style="list-style-type: none"> Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center 																		
Second Escalation Customer Discretion	Area Manager Or Delegate	<ul style="list-style-type: none"> Review status of ticket Monitor ticket progress Notify Director - when appropriate 																		
Third Escalation Customer Discretion	Director	<ul style="list-style-type: none"> Status Customer Escalate as needed to partner centers Monitor ticket Progress/ documentation Notify AVP when appropriate 																		
Fourth Escalation	AVP	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Customer's name and telephone number Active WFA ticket number(s) Trouble Location Trouble description (e.g., out of service, service degraded, etc.) The action or resolution requested 																				
2. Discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed with the assigned AT&T Service Manager. The State will have access to an online portal that will include escalation procedures.																				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 21	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.	X			
	2. Provide with the detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement.				
	<p>Bidder Response:</p> <p>AT&T has provided responses to requirements 1 and 2 below.</p> <ol style="list-style-type: none"> As of June 15, 2011, AT&T has adopted the new Statement on Standards for Attestations Engagements (SSAE 16) in conjunction with the International Standard on Assurance Engagements (ISAE 3402). SSAE 16/ISAE 3402 replaced the Statement on Auditing Standards No. 70 (SAS 70) standard as the professional standard for service organizations to obtain an independent assessment about the effectiveness of internal controls that are relevant to their customer's financial statements. SSAE 16/ISAE 3402 is based heavily on the preceding SAS 70 audit standard. <p>An examination under this standard signifies that a service organization has had its control objectives and control activities, including controls over information technology and related processes, examined by an independent accounting and auditing firm. A formal report containing the auditor's opinion, detailed control descriptions, and test results is issued to the service organization at the conclusion of the examination. This formal report is now referred to as a Service Organization Control (SOC) Report 1 or simply "SOC 1".</p> <p>AT&T sponsors several Type II examinations which are managed by GCSS in the areas of Application Services, Enterprise Hosting Services, Managed Services, and Outsourced Network Management. It also sponsors SOC 1 Type I and Type II reports for Synaptic Compute as a Service and Synaptic Storage as a Service.</p> <ol style="list-style-type: none"> AT&T undergoes security audits internally and by third-party vendors on a regular (yearly) basis. Audits specifically requested and initiated by the State of Nebraska shall be added to this schedule upon request. <p>For certain Services, AT&T retains external auditors for periodic reviews of AT&T's security practices against various standards, such as SSAE18/ISAE3402, SysTrust, and Payment Card Industry (PCI) Data Security Standard (DSS). Additional information about external audits and certifications relevant to the Services is available from Customer's AT&T account team upon request. AT&T will provide Service Organization Control (SOC) audit reports to Customer for any audits of the Services against the SSAE18/ISAE3402 standards that AT&T undertakes as part of its general business operations</p>				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	NOC / SOC - Configuration Backup and Restoration	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 22	<p>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.</p> <p>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.</p> <p>3. Describe bidder's COOP as it applies to the NGCS and delivery of 911 traffic via IP network to the respective host locations.</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>1. AT&T and Intrado have a robust and consistent system to perform and save daily backups of AT&T ESInet network elements using a tool called Riverbed and then, also daily, those backups are copied to a different system where they are saved for at least three months. Every change MOP and following change management requirements will have back-out steps to restore from these backups if/when needed.</p> <p>Any updates/configuration changes are done on the inactive side. Once the changes are validated, the system is flipped such that the inactive side now becomes the active side. There is a soak period of 48 hours during which data changes are replicated between the active and inactive sides such that if there needs to be a return to the old configuration, any interim data changes have been captured. The AT&T ESInet network configuration tools provide version control and "rollback" functionality to all network elements. This allows the restoration of previously "known good" configurations or timely restoration of stored configurations in the event of equipment failure or disaster recovery. T&T can provide reports confirming regularly scheduled daily backup and restoration files archived and provide additional details on backup and restoration activity as required. AT&T can provide copies of all data upon request.</p> <p>2. AT&T can perform on-demand backups and provide reports confirming on-demand backup and restoration files archived and provide additional details on backup and restoration activity as required. AT&T can provide copies of all data upon request.</p> <p>3. The AT&T ESInet solution is backed by AT&T's business continuity/disaster recovery organization. AT&T and Intrado have established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to our facilities or systems, including:</p> <ul style="list-style-type: none"> • 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 				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

AT&T has a 24x7x365 NOC dedicated to 911 call delivery services. The NOC is comprised of Tier 2 and Tier 3 Technicians responsible for identification, isolation, and mitigation in the event of an incident. An escalation matrix is in place to ensure that AT&T utilizes industry standard processes, including adherence to the Information Technology Infrastructure Library (ITIL) and Federal Emergency Management incident management practices (FEMA). Should a disaster occur that prevents NOC staff from inhabiting the corporate facility, a Business Continuity Plan (BCP) is in place. A full BCP exercise is executed at least twice each calendar year by the NOC, Incident Management, and Problem Management.

Multiple network management components monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Active application monitoring and alerting complement traditional network management. The AT&T ESInet application elements also report network failures as detected by their application messaging activity, some of which is specific to managing the availability and integrity of the solution.

All network elements are monitored at the NOC in Longmont CO. This includes LNGs, ESRPs, ECRFs, BCFs, and PSAP site equipment.

The NOC monitors and tracks net flow statistics and performs packet level capture and forensics at the AT&T ESInet™ core sites. There are currently two varieties of monitoring systems in use at the NOC. One provides a “single pane of glass” for network and system status. This provides SNMP trap and syslog receiver capabilities. These systems also provide ICMP and SNMP trending and threshold alarming. The second type of system provides packet capture, display, and troubleshooting capabilities.

4. When it comes to business continuity, proactive planning and a strong execution strategy are essential steps in reducing exposure from “events”, natural or man-made, accidental or intentional, internal or external, with or without warning. AT&T maintains a Business Continuity Management (BCM) Program to help prevent or mitigate service disruptions and aims to rapidly respond to any loss of essential AT&T business processes and restore service as quickly and safely as possible.

The AT&T Business Continuity Management Program is certified to the international business continuity standard ISO 22301:2012. It is also aligned with the Disaster Recovery Institute International (DRII) Professional Practices, Business Continuity Institute Good Practice Guidelines, Department of Homeland Security National Incident Management System and ISO 31000. The Program includes management disciplines, processes, and techniques to support AT&T essential business processes in the event of a significant business disruption.

AT&T is committed to keeping our Customers connected - even in the wake of unpredictable, catastrophic events - by maintaining the reliability of the AT&T global network. The mission of the Network Disaster Recovery (NDR) Team is to recover AT&T voice and data service network elements to an area affected by a disaster. Telecommunications is vital for our business and government Customers following a disaster, both for the impacted area and for the rest of the country. AT&T is the first company nationwide to receive United States Department of Homeland Security's (DHS) Private Sector Preparedness Program (PS-Prep) certification.

The AT&T Network Disaster Recovery plan has three (3) primary goals:

- Route non-involved communications traffic around an affected area.
- Provide the affected area communications access to the rest of the world.
- Recover the communications service to a normal condition as quickly and safely as possible through restoration and repair.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NOC/ SOC 23	<p>NOC/SOC - Third-Party Management</p> <p>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.</p> <p>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.</p> <p>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.</p>				
	<p>Bidder Response:</p> <p>AT&T supports the integration of a third-party NOC/SOCs. Currently the AT&T and Intrado NOCs are connected via e-Bonding that provides integration of alarming and incident notification and trouble ticketing. AT&T ESInet service includes a proven, robust 24x7x365 NOC/SOC support capability. Should the Commission desire to move forward with a 3rd party NOC/SOC function, then AT&T would recommend setting up an engineering design workshop to identify a complete set of functional requirements and agreement on technical interface specification. Based upon the outcome of the workshop, AT&T could provide lead times for availability and potential updates to pricing.</p>				

1. In support of the Commission's consideration of such an option, bidder shall indicate the compliance level of experience in providing access to third-party NOC/SOC overarching support, as related to the requirements identified in the table below.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Change management processes	X			
Coordinating and managing trouble tickets to resolution from bidder and multiple suppliers.	X			
Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly).	X			
Notification processes for bidder and suppliers, and any other entities or people designated by the Commission.	X			
System alarm access in the form of SNMP or syslog data.	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Experience and processes for interworking of multiple public safety data system suppliers.	X			
--------------------------------------------------------------------------------------------	---	--	--	--

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
General Operations - Service Level Agreements System Capacities and Performance 1. Provide capacity levels of each element of the IP Network his 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.	X			
	SLA 1 Bidder Response: 1. The AT&T ESInet core call routing centers are capable of processing more than twice the estimated busy hour rate for all 9-1-1 calls across the nation, meeting the above requirements. The AT&T ESInet IP network is continually monitored for capacity trends that indicate the need for proactive growth. We have established processes in place to augment the network as capacity needs are identified. The IP network transport used by the AT&T ESInet to deliver calls to the PSAP will initially be sized to comply with specified network bandwidth requirements. As the capacity needs change, this bandwidth will be scaled up or down by a change order process or through procedures as defined in the SLA and/or contract. AT&T ESInet is capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. As required, AT&T can easily scale IP capacities through simple provisioning processes, eliminating the need for additional network buildouts. This enables our customers to increase capacities within a few weeks instead of months. AT&T will work with the State of Nebraska to meet their capacity planning needs and to establish mutually agreed upon ordering timeframes. This methodology provides the State with a cost-effective solution in the near term and allows for growth based on coordinated agreements. 2. The IP network that AT&T will deploy is AT&T VPN which is an MPLS network that allows great flexibility in bandwidth speeds. The initial deployment of 100M service into most PSAPs allows for significant capacity to deploy additional PSAP applications. Changes in speed from the initial VLAN sizes of 3M-20M will be done via change orders and can be accomplished rapidly and well within the 30 days that has been specified by the State. The AT&T ESInet managed service includes utilization and bandwidth tracking and AT&T will reach out to the PSAP if said PSAP exceeds 80% of capacity at any given time. Understanding this AT&T ESInet system was pre-built to handle the entire country's busy 9-1-1 traffic, the expectation is that no new hardware would need to be put in place.			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Service Level Agreements - System Performance		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 2	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: The AT&T ESInet service level objective for network latency is a monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less between the data centers and the PSAP end points. AT&T's MPLS network carries more than 335.1 Petabytes of data traffic on an average day serving more than 1.5 million customer endpoints and assures round trip latency of less than 200ms across the entire network under full load conditions. AT&T ESInet™ service uses our own industry leading AT&T Virtual Private Network (AVPN) for all primary communication links to host sites. This MPLS switched network provides robust communications using nationwide switching points. These switches allow for traffic routing when network failure or congestion (increased latency) on any given link is detected by AT&T's Global Network Operations Center (GNOC). The GNOC is a 24x7x365 dedicated facility responsible for monitoring the AVPN network and collecting statistical information on all links. This allows AT&T to report actual monthly performance measurements alongside performance targets. AT&T ESInet measures latency based on "round trip time" e.g., the time it takes for a packet to get from one point on the network to another. AT&T leads the industry in IP/MPLS Network Performance Testing and AT&T Labs is considered an expert in the area of measuring IP/MPLS network performance. Unlike other providers who may use ping and trace route tests to show performance, AT&T has taken a leadership role in developing its own separate, standards-based network performance infrastructure and system to collect near real-time network performance information for its global IP/MPLS network. Today, during every 15-minute interval, AT&T tests its IP/MPLS network performance between approximately 6,700 city pair combinations. To do this, AT&T injects real traffic into its network and tests its performance in two ways: 1) By sending approximately 742,500 Best Effort probe packets between these city pairs, and 2) by sending approximately 20,542,500 Real Time probe packets between these city pairs. In addition, 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. AT&T then publishes these MPLS performance results on our public IP network health website available to anyone at www.att.com/ipnetwork . This data is refreshed every 15 minutes. From the Home Page you can link to greater levels of detail including Current Performance, Current Network Latency, Current Network Loss and Monthly Averages. In addition, a detailed explanation on the AT&T Global IP Network measurement methodology can be found on the Methodology page as well as a technical article that was published in the IEEE Communications Society magazine. These reports will be provided to the State of Nebraska, on a monthly basis by AT&T's dedicated Program Manager and Service Manager resources that are included as part of AT&T's RFP response.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Service Level Agreements - System Performance Point of Presence (POP) to POP Specify the guaranteed maximum latency from interconnection facility to interconnection facility, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SLA 3	<p>Bidder Response:</p> <p>The maximum acceptable delay for packets traversing the ESInet should be less than or equal to 37 ms. It is a best practice to design ESInets to operate with less than 15 to 20 ms of latency. This allows the original to encode and decode and a conference bridge in the middle of the path and still achieves the maximum 37ms or less packet delay.</p> <p>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.</p> <p>All SLAs will be gathered either automatically or manually based on monthly data, calculated based on established measurements and provided to the Commission as part of a monthly report.</p>				

Any additional documentation can be inserted here:

	Service Level Agreements - System Performance POP to Endpoints Specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SLA 4	<p>Bidder Response:</p> <p>The maximum acceptable delay for packets traversing the ESInet should be less than or equal to 37 ms. It is a best practice to design ESInets to operate with less than 15 to 20 ms of latency. This allows the original encode and decode and a conference bridge in the middle of the path and still achieves the maximum 37mS or less packet delay.</p> <p>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.</p> <p>All SLAs will be gathered either automatically or manually based on monthly data, calculated based on established measurements and provided to the Commission as part of a monthly report.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Service Level Agreements - System Performance Mean Opinion Score (MOS) Bidder shall guarantee, in the response, a consistent MOS of 4.0 or better across all network links transporting media streams from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	SLA 5 Bidder Response: AT&T ESInet and the associated AVPN network meet or exceed the average 4.0 MOS score as required by the State of Nebraska. This average MOS score applies across AT&T ESInet network endpoints that may also include secondary networks and applicable wireless links. Multiple network management components monitor network elements, IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. Traditional network management is complemented by active application monitoring and alerting. The AT&T ESInet application elements also report network failures as detected by their application messaging activity, some of which is specific to managing the availability and integrity of the solution. AT&T measures PMOS all the way through to the PSAP T-ESRP. AT&T measures the MOS scores as part of the AT&T ESInet Voice Quality SLA by monitoring the IP audio packets from Aggregation sites (from the AT&T ESInet demarcation point) into the Core Call Processing Nodes and from the PSAP (from the Customer demarcation point) into the Core Call Processing Nodes. The SLA objective, based on the industry standard Mean Opinion Score (MOS), measures a Daily Predicted Mean Opinion Score (PMOS) value per PSAP to not be less than a 4.0 average score for G.711 codec as measured by AT&T, where the ideal PMOS score for the G.711 codec is 4.3 as measured by AT&T. The Daily PSAP PMOS value will be based on an average of the per call PMOS scores over a 24-hour calendar day. A per call PMOS score is defined as the lowest score of the three (3) call legs defined as: <ul style="list-style-type: none"> • Ingress Call Leg A: Aggregation site LNG to IP network termination at Emergency Call Management Core (ECMC) • Core Call Leg B: Between the media server and the SBC at an ECMC • Egress Call Leg C: PSAP edge router to the SBC 	X		
<p>The diagram illustrates the network architecture for AT&T ESInet Voice Quality. It is divided into three main sections: Aggregation Sites, NGCS Data Centers, and PSAP. 1. Aggregation Sites: Contains two Local Network Gateways (LNGs) connected to a network of routers. Point 'a' is located at the start of this section. 2. NGCS Data Centers: Contains a Core Complex and several server racks. Points 'b' and 'c' are located at the beginning of this section, and points 'd' and 'e' are located at the end. 3. PSAP: Contains a PSAP CPE (Customer Premises Equipment) connected to a network of routers. Point 'f' is located at the end of this section. Call Legs: <ul style="list-style-type: none"> Ingress Call Leg A: A double-headed arrow connects point 'a' to point 'b'. Core Call Leg B: A double-headed arrow connects point 'c' to point 'd'. Egress Call Leg C: A double-headed arrow connects point 'e' to point 'f'. </p>				

Figure 15: AT&T ESInet Voice Quality

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<p>Voice quality for each leg is measured via Predicted MOS calculation by way of evaluation of Real-Time Transport Protocol (RTP) IP packet network characteristics (jitter, latency, packet loss). Per call Predicted MOS will be measured for leg A (a-b), B (c-d), and C (e-f).</p> <p>Regarding reporting of the Mean Opinion Score (MOS), AT&T's dedicated Program Manager and Service Manager resources that are included as part of AT&T's RFP response will compile this data and provide to the State of Nebraska. These two dedicated resources will provide this information in an agreed upon format along with the other required State of Nebraska reports on a monthly basis.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here

	Service Level Agreements - System Performance	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	<p>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.</p>	X			
SLA 6	<p>Bidder Response:</p> <p>The AT&T ESInet network maintains a maximum end-to-end packet loss across its network of less than 1 percent. Multiple IP transport paths are established between the Core sites and the CPE locations. The AT&T ESInet™ quickly detects impairment (packet loss, jitter, etc.) and soft failures (that is, loss of transit across an IP Layer 3 VPN instance with no detectable circuit loss or BGP route withdrawals at the edge) on one IP instance and moves traffic to the other unimpaired transport without interrupting existing data flows or voice RTP streams.</p> <p>Various connectivity metrics at each core site are measured, collected and tracked. Connectivity quality is based on statistics captured via IP transport metrics. These metrics include Jitter, Latency and Packet Loss:</p> <ul style="list-style-type: none"> • Jitter. The AT&T ESInet™ Jitter is calculated based on the network-wide average between the data centers and the PSAP end points. • Latency. The AT&T ESInet™ Latency is calculated based on the network-wide average roundtrip transmission between the data centers and the PSAP end points. • Packet Loss. The AT&T ESInet™ Packet Latency is engineered to keep the packet loss budget under 2.5 percent. It is designed without oversubscription and packet loss of less than 1 percent is expected. <p>AT&T VPN which serves as the underlying transport service for AT&T ESInet uses the "Data Delivery Performance Objective" metric which measures the ratio of the number of packets sent to the number of packets delivered. AT&T's performance objective for this metric is 99.95% packets delivered in the United States. These statistics along with other AT&T network statistics can be viewed in near real-time at our web portal.</p> <p>In addition, AT&T's dedicated Program Manager and Service Manager resources that are included as part of AT&T's RFP response will compile this data and provide to the State of Nebraska. These two dedicated resources will provide this information in an agreed upon format along with the other required State of Nebraska reports on a monthly basis.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Service Level Agreements - System Performance	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 7	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			
	<p>Bidder Response:</p> <p>AT&T ESInet™ service uses our own industry leading AT&T Virtual Private Network (AVPN) for all primary communication links to host sites. AT&T VPN maintains a Network Latency Performance of 37ms in the United States. This MPLS switched network provides robust communications using nationwide switching points. These switches allow for traffic routing when network failure or congestion (increased latency) on any given link is detected by AT&T's Global Network Operations Center (GNOC). The GNOC is a 24x7x365 dedicated facility responsible for monitoring the AVPN network and collecting statistical information on all links. This allows AT&T to report actual monthly performance measurements alongside performance targets. AT&T ESInet measures latency based on "round trip time" e.g., the time it takes for a packet to get from one point on the network and back.</p> <p>Additionally, The AT&T ESInet service guarantees network latency of fifty (50) milliseconds or less for the monthly network-wide average roundtrip transmission of fifty (50) milliseconds or less between the data centers and the PSAP end points.</p> <p>Finally, 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, sites designed with redundant 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.</p> <p>Various connectivity metrics at each core site are measured, collected and tracked. Connectivity quality is based on statistics captured via IP transport metrics. These metrics include Jitter, Latency and Packet Loss. The AT&T ESInet Latency is calculated based on the network-wide average roundtrip transmission between the data centers and the PSAP end points.</p>				

Any additional documentation can be inserted here

	Service Level Agreements - System Performance	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 8	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			
	<p>Bidder Response:</p> <p>Various connectivity metrics at each core site are measured, collected and tracked. Connectivity quality is based on statistics captured via IP transport metrics. These metrics include Jitter, Latency and Packet Loss. The AT&T ESInet Jitter is calculated based on the network-wide average between the data centers and the PSAP end points. The maximum end-to-end jitter across the network is 20 ms.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Service Level Agreements - System Performance		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 9	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: AT&T utilizes OSPF within our core network and BGP between CE and PE routers as our convergence protocol in our MPLS network. The GNOC is a 24x7x365 dedicated facility responsible for monitoring the AVPN network and collecting statistical information on all links. 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. AT&T can provide monthly network performance reports that substantiates our network performance at the core network level during monthly service meetings. These performance reports will be provided to the State of Nebraska, on a monthly basis by AT&T's dedicated Program Manager and Service Manager resources.				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SLA 10	<p>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.</p>	Comply	Partially Comply	Complies with Future Capability	Does Not Comply																	
	<p>Bidder Response:</p> <p>MTTR characteristics are commensurate with the appropriate level of service at which the ESInet system is functioning (i.e., system components in the call path are Life and Mission Critical Services (LCMS) while, peripheral systems are considered Business Critical Services (BCS). The MTTR characteristics are listed in the table below.</p> <ul style="list-style-type: none"> • Life and Mission Critical Services (LCMS) • Business Critical Services (BCS) • Business Essential Services (BES) • Business Support Services (BSS) • Unsupported Business Services (UBS) <p>MTBF and MTTR</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #ADD8E6;">Service Class</th> <th style="background-color: #ADD8E6;">MTBF (Service)</th> <th style="background-color: #ADD8E6;">MTTR (Service)</th> </tr> </thead> <tbody> <tr> <td>LMCS</td> <td>>5 years</td> <td><2 minutes</td> </tr> <tr> <td>BCS</td> <td>>1 year</td> <td><4 hours</td> </tr> <tr> <td>BES</td> <td>>3 months</td> <td><40 hours</td> </tr> <tr> <td>BSS</td> <td>>1 month</td> <td><3 days</td> </tr> <tr> <td>UBS</td> <td>Unspecified</td> <td>Unspecified</td> </tr> </tbody> </table> <p>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.</p> <p>All SLAs will be gathered either automatically or manually based on monthly data, calculated based on established measurements and provided to the Commission as part of a monthly report.</p>	Service Class	MTBF (Service)	MTTR (Service)	LMCS	>5 years	<2 minutes	BCS	>1 year	<4 hours	BES	>3 months	<40 hours	BSS	>1 month	<3 days	UBS	Unspecified	Unspecified	X		
Service Class	MTBF (Service)	MTTR (Service)																				
LMCS	>5 years	<2 minutes																				
BCS	>1 year	<4 hours																				
BES	>3 months	<40 hours																				
BSS	>1 month	<3 days																				
UBS	Unspecified	Unspecified																				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SLA 11	Service Level Agreements - System Performance Mean Time Between Failures (MTBF) Specify the MTBF characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTBF information will be gathered, calculated and provided to the Commission and affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply																		
	X																						
Bidder Response: MTBF characteristics are commensurate with the appropriate level of service at which the system is functioning i.e., systems in the call path are Life and Mission Critical Services (LCMS) while peripheral systems are considered Business Critical Services (BCS). The MTBF characteristics are listed in the table below. <ul style="list-style-type: none"> • Life and Mission Critical Services (LCMS) • Business Critical Services (BCS) • Business Essential Services (BES) • Business Support Services (BSS) • Unsupported Business Services (UBS) MTBF and MTTR <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #ADD8E6;">Service Class</th> <th style="background-color: #ADD8E6;">MTBF (Service)</th> <th style="background-color: #ADD8E6;">MTTR (Service)</th> </tr> </thead> <tbody> <tr> <td>LMCS</td> <td>>5 years</td> <td><2 minutes</td> </tr> <tr> <td>BCS</td> <td>>1 year</td> <td><4 hours</td> </tr> <tr> <td>BES</td> <td>>3 months</td> <td><40 hours</td> </tr> <tr> <td>BSS</td> <td>>1month</td> <td><3 days</td> </tr> <tr> <td>UBS</td> <td>Unspecified</td> <td>Unspecified</td> </tr> </tbody> </table> <p>Based on our public safety experience, AT&T 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. AT&T believes that the most relevant measure of service availability is evidenced by uninterrupted, reliable 9-1-1 call routing and delivery to the PSAPs.</p> <p>All SLAs will be gathered either automatically or manually based on monthly data, calculated based on established measurements and provided to the Commission as part of a monthly report.</p>						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
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																					

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 12	Specify in the response the overall reliability service level of the IP network, including all bidder-provided components and facilities.	X			
	<p>Bidder Response:</p> <p>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</p> <ul style="list-style-type: none"> • 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 <p>AT&T ESInet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. All i3 functions necessary for call processing are deployed in a highly available configuration. Each i3 element has multiple instances within a single core to provide redundancy for that core. The same redundant configuration is replicated at each of the six geographically diverse core sites. The nine Aggregation sites use the same design approach of redundancy within each individual site mirrored at the other sites. 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 AT&T ESInet components are designed and configured for continuous operation. AT&T ESInet availability is calculated from the time the outage begins that impacts call processing ability, until such time that the AT&T ESInet call processing ability is restored. This includes all AT&T ESInet downtime for the end-to-end service.</p> <p>In order to maintain reliability in a public safety grade network, maintenance of the AT&T ESInet 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.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Service Level Agreements - System Performance Network Availability 1. Specify the service level offered as a percentage of time when the service is available, and the maximum period of total outage before remedies are activated. Availability is defined as MTBF/(MTBF+MTTR). 2. Include how system availability information will be gathered, calculated and provided to the Commission and affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 13	<p>Bidder Response:</p> <ol style="list-style-type: none"> Based on our public safety experience, AT&T has found that measuring Service Availability from a call processing perspective is more applicable and relevant to 9-1-1 service versus traditional methods of calculating availability through Mean time between failure (MTBF) and Mean time to repair (MTTR) measures. Therefore, AT&T ESInet Service Availability SLA measures the system wide availability for Call Processing that encompasses network availability (Service Availability). Call Processing is the ability of the Service to deliver calls from the inbound Service demarcation point into the Core Call Processing Nodes and from the Service demarcation point to a Valid Destination (for example a PSAP). The Service Availability is calculated from the time an issue is reported that impacts Call Processing ability, until such time that the Service Call Processing ability is restored. <p>These reports will be provided to the State of Nebraska, on a monthly basis by AT&T's dedicated Program Manager and Service Manager resources that are included as part of AT&T's RFP response.</p> <p>Below is an example Service Availability report:</p>	X			

**Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

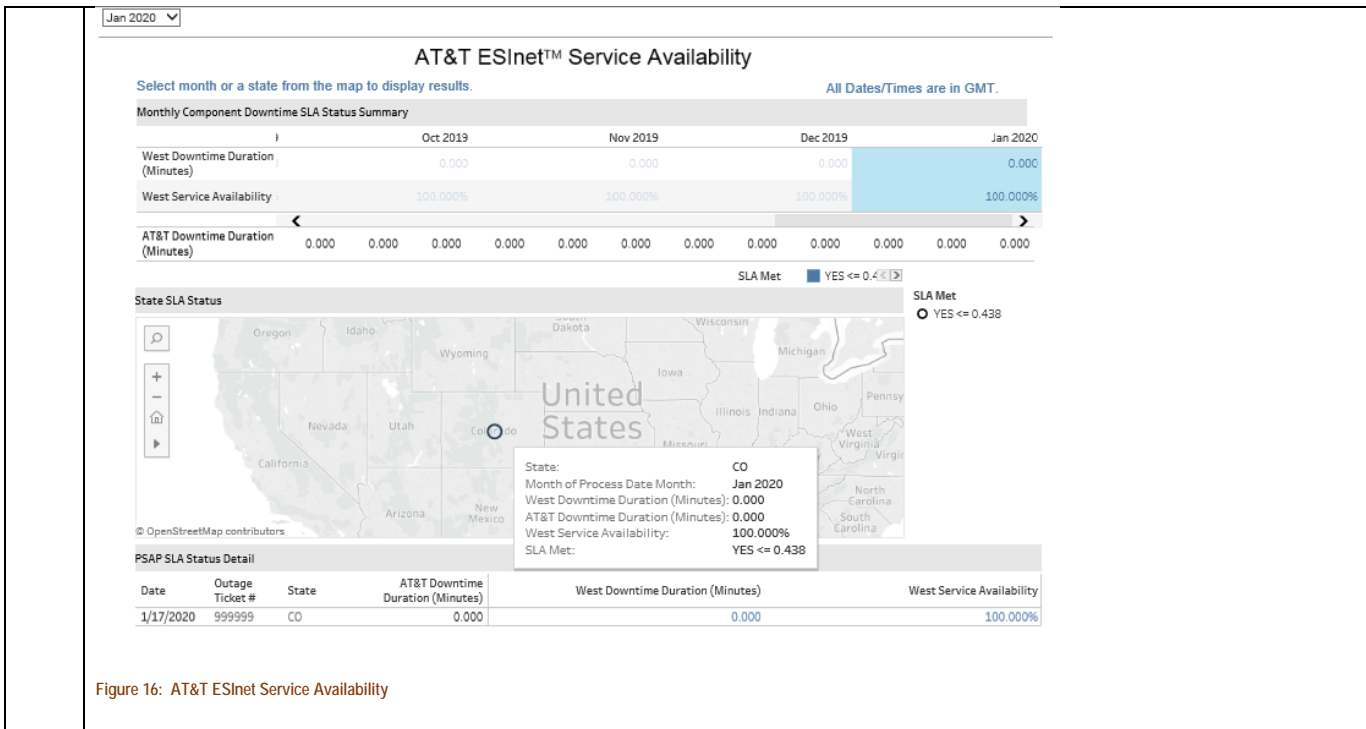


Figure 16: AT&T ESInet Service Availability

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SLA 14	Service Level Agreements - System Performance End-of-Support Equipment Contractor shall proactively replace, at Contractor's expense, any hardware that has reached end of support (EOS) no later than 90 calendar days prior to the manufacturer's EOS date. All equipment must be new and of current manufacture, not refurbished. Describe your procedures for End-of-Support Equipment.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: Key components within the AT&T ESInet™ are periodically renewed to enable PSAPs to operate on the most modern communications technology during the life of the contract. AT&T maintains and monitors all equipment and software within the solution, and it is AT&T's goal to replace End of Support (EOS) equipment prior to the EOS vendor published date.				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

SLA 15	<p>Service Level Agreements – SLAs for Incident Management</p> <p>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.</p>	Comply	Partially Comply	Complies with Future Capability	Does Not Comply																													
	<p>Bidder Response:</p> <p>As an industry-leading provider of 9-1-1 and public safety services for more than 30 years, AT&T has successfully implemented mature, proven processes and operational procedures for supporting a NOC/SOC that can rapidly triage calls.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Service Impact Level (SIL)</th> <th style="text-align: center;">Incident Type</th> <th style="text-align: center;">Communication method (all listed methods required)</th> <th style="text-align: center;">Ticket Initiation (Response)</th> <th style="text-align: center;">Update Frequency (Email)</th> <th style="text-align: center;">Restoration no later than (Resolution)</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;"> SIL 1 – Critical Full loss of critical functionality </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> ▫ Trunk outages ▫ Alternate Routing activation ▫ All calls misrouting ▫ No ANI/ALI ▫ Loss of service ▫ FCC reportable incidents ▫ PSAP unable to perform core functions ▫ Transfer failures (all calls) ▫ Circuit outage ▫ Ransomware or Malware attack </td> <td style="vertical-align: top;"> Phone Text Email </td> <td style="vertical-align: top; text-align: center;">15 Minutes</td> <td style="vertical-align: top; text-align: center;">1 Hour</td> <td style="vertical-align: top; text-align: center;">2 Hours</td> </tr> <tr> <td style="vertical-align: top;"> SIL 2 – Major Partial loss of critical functionality </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> ▫ Intermittent misroutes ▫ Intermittent transfer failures ▫ Intermittent ALI issues no/incorrect data ▫ WAN links bouncing intermittently ▫ Inability of PSAP to support 911 calls due to equipment failures </td> <td style="vertical-align: top;"> Phone Text Email </td> <td style="vertical-align: top; text-align: center;">30 Minutes</td> <td style="vertical-align: top; text-align: center;">2 Hours</td> <td style="vertical-align: top; text-align: center;">4 Hours</td> </tr> <tr> <td style="vertical-align: top;"> SIL 3 – Minor Does not have serious impact </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> ▫ Occasional calls misrouting Occasional transfers to other PSAPs failures ▫ PSAP equipment issues that do not impact call taker response </td> <td style="vertical-align: top;"> Email </td> <td style="vertical-align: top; text-align: center;">1 Hour</td> <td style="vertical-align: top; text-align: center;">24 Hours</td> <td style="vertical-align: top; text-align: center;">5 Calendar days</td> </tr> <tr> <td style="vertical-align: top;"> SIL 4 . Informational Does not have serious impact or informational </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> ▫ Non-critical and informational request ▫ Maintenance Activities </td> <td style="vertical-align: top;"> Email </td> <td style="vertical-align: top; text-align: center;">2 Hours</td> <td style="vertical-align: top; text-align: center;">Weekly</td> <td style="vertical-align: top; text-align: center;">15 Calendar days</td> </tr> </tbody> </table> <p>Please note the information AT&T has input into the table above.</p> <p>Severity Level 1 is defined as an incident whereby the Service or its components are completely inoperative or severely impacted:</p>	Service Impact Level (SIL)	Incident Type	Communication method (all listed methods required)	Ticket Initiation (Response)	Update Frequency (Email)	Restoration no later than (Resolution)	SIL 1 – Critical Full loss of critical functionality	<ul style="list-style-type: none"> ▫ Trunk outages ▫ Alternate Routing activation ▫ All calls misrouting ▫ No ANI/ALI ▫ Loss of service ▫ FCC reportable incidents ▫ PSAP unable to perform core functions ▫ Transfer failures (all calls) ▫ Circuit outage ▫ Ransomware or Malware attack 	Phone Text Email	15 Minutes	1 Hour	2 Hours	SIL 2 – Major Partial loss of critical functionality	<ul style="list-style-type: none"> ▫ Intermittent misroutes ▫ Intermittent transfer failures ▫ Intermittent ALI issues no/incorrect data ▫ WAN links bouncing intermittently ▫ Inability of PSAP to support 911 calls due to equipment failures 	Phone Text Email	30 Minutes	2 Hours	4 Hours	SIL 3 – Minor Does not have serious impact	<ul style="list-style-type: none"> ▫ Occasional calls misrouting Occasional transfers to other PSAPs failures ▫ PSAP equipment issues that do not impact call taker response 	Email	1 Hour	24 Hours	5 Calendar days	SIL 4 . Informational Does not have serious impact or informational	<ul style="list-style-type: none"> ▫ Non-critical and informational request ▫ Maintenance Activities 	Email	2 Hours	Weekly	15 Calendar days	X		
Service Impact Level (SIL)	Incident Type	Communication method (all listed methods required)	Ticket Initiation (Response)	Update Frequency (Email)	Restoration no later than (Resolution)																													
SIL 1 – Critical Full loss of critical functionality	<ul style="list-style-type: none"> ▫ Trunk outages ▫ Alternate Routing activation ▫ All calls misrouting ▫ No ANI/ALI ▫ Loss of service ▫ FCC reportable incidents ▫ PSAP unable to perform core functions ▫ Transfer failures (all calls) ▫ Circuit outage ▫ Ransomware or Malware attack 	Phone Text Email	15 Minutes	1 Hour	2 Hours																													
SIL 2 – Major Partial loss of critical functionality	<ul style="list-style-type: none"> ▫ Intermittent misroutes ▫ Intermittent transfer failures ▫ Intermittent ALI issues no/incorrect data ▫ WAN links bouncing intermittently ▫ Inability of PSAP to support 911 calls due to equipment failures 	Phone Text Email	30 Minutes	2 Hours	4 Hours																													
SIL 3 – Minor Does not have serious impact	<ul style="list-style-type: none"> ▫ Occasional calls misrouting Occasional transfers to other PSAPs failures ▫ PSAP equipment issues that do not impact call taker response 	Email	1 Hour	24 Hours	5 Calendar days																													
SIL 4 . Informational Does not have serious impact or informational	<ul style="list-style-type: none"> ▫ Non-critical and informational request ▫ Maintenance Activities 	Email	2 Hours	Weekly	15 Calendar days																													

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Examples: (including but not limited to)

- Trunk outages
- Alternate Routing activation
- All calls misrouting
- No ANI/ALI
- Loss of service
- FCC reportable incidents
- PSAP unable to perform core functions
- Transfer failures (all calls)
- Circuit outage
- Ransomware or Malware attack

For Severity Level 1 issues, AT&T will respond within 15 minutes of the State opening a trouble ticket with updates every one (1) hour and restoration within two (2) hours.

Severity Level 2 is defined as an incident whereby the Service is functioning at a limited capacity or critical functions are no longer redundant.

Examples: (including but not limited to)

- Intermittent misroutes
- Intermittent transfer failures
- Intermittent ALI issues no/incorrect data
- WAN links bouncing intermittently
- Inability of PSAP to support 911 calls due to equipment failures

For Severity Level 2 issues, AT&T will respond within 30 minutes of the State opening a trouble ticket with updates every two (2) hours and restoration within four (4) hours.

Severity Level 3 is defined as services are impaired and some functions are not operating, but the impairments are considered minor or cosmetic and have only a minor impact on usability. Examples: (including but not limited to)

- Occasional calls misrouting Occasional transfers to other PSAPs failures
- PSAP equipment issues that do not impact call taker response

For Severity Level 3 issues, AT&T will respond within one (1) hour of the State opening a trouble ticket with updates every 24 hours and restoration within five (5) calendar days.

Severity Level 4 is defined as informational, minor or cosmetic and have only a minor impact on usability.

Examples: (including but not limited to):

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

- Non-critical and informational request
- Maintenance Activities

For Severity Level 4 issues, AT&T will respond within two (2) hours of the State opening a trouble ticket with updates weekly and restoration resolution within 15 calendar days.

The incident response service level objectives, for all incident severity levels are measured by comparing the time of opening the trouble ticket to the time the Service was restored.

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 16	<p>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.</p>	X			
	<p>Regulatory Compliance Contractor shall comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract.</p> <p>Bidder Response:</p> <p>Outage Notification and Reason for Outage (RFO) Report Outage Summary and Lessons Learned</p> <p>AT&T considers its network outages and recovery time (including in the last calendar year) proprietary and confidential in accordance with the policies of the U.S. Department of Homeland Security and the Federal Communications Commission (FCC). For consistency with these policies, AT&T must decline to provide details about network outages and recovery time.</p> <p>AT&T considers the information in its outage reports to the FCC highly sensitive and therefore unsuitable for public availability, pursuant to the following FCC’s findings: “The overwhelming majority of the commenting parties, including the Department of Homeland Security, have demonstrated that the outage reports will contain sensitive data, which requires confidential treatment under the Freedom of Information Act.”</p> <p>This data, though useful for analysis, could be useful to hostile parties to attack our networks, which are part of our nation’s critical information infrastructure. The disclosure of outage reporting information to the public could present an unacceptable risk of more terrorist activity.</p> <p>For this reason, we treat network outage and recovery information as confidential and withhold it from disclosure to the public in accordance with the Freedom of Information Act, New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, ET Docket No. 04-35, FCC 04-188 (August 19, 2004).</p> <p>We make every effort to prevent outages and maintain a 99.99% network availability target.</p> <p>Regulatory Compliance</p> <p>AT&T complies with all FCC rules regarding outage notification, communication and Reason for Outage (RFO) reporting. In case of a service interruption and/or outage, we have instituted Incident Management processes and procedures for dealing with various severity levels during the course of an event. Our incident response tools include use of the Incident Command System (ICS modeled directly from the Federal Emergency Management Agency (FEMA) Emergency Management Institute. The ICS processes include resolution, documentation of any incident, communications, and post-event review and root cause analysis. We manage incidents and provide customers with up to the minute notification and status of ongoing service affecting issues that may impact the AT&T ESInet solution.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Service Level Agreements – Outage Notification and Reason for Outage (RFO) Report Outage Notification	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 17	<p>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.</p> <p>Bidder Response:</p> <p>AT&T's 9-1-1 Resolution Center shall notify the Commission, impacted PSAPs, and/or designated agencies as soon as possible but no later than 15 minutes of discovering an event or outage that may impact 9-1-1 services (Severity Level 1/Critical).</p> <p>AT&T's 9-1-1 Resolution Center uses the Everbridge system as a way of providing written and verbal mass notifications to communicate potential ESInet service-affecting or actual FCC significant events to the PSAP communities to meet the FCC mandates. We have the capability to provide notification by phone, email, SMS or Fax as directed by the customer.</p> <p>AT&T has customized the Everbridge system using notification templates as driven by FCC guidelines. Notifications can be sent to a PSAP, District, or other approved contact, depending on the needs of the customer and their capabilities. AT&T will work with the Commission to determine the appropriate contact list.</p> <p>At the time of initial notification, AT&T will include available information that may be useful, which will include but is not limited to: area/agencies impacted, type of Impact, options to mitigate 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.</p> <p>AT&T will coordinate data gathering, troubleshooting and reporting on behalf of Intrado.</p> <p>The AT&T ESInet solution is self-healing as every PSAP has connectivity to the entire AT&T ESInet infrastructure consisting of six geographically diverse ECMCs and eight diverse aggregation centers. Network connectivity is provided by AT&T's global MPLS network service AVPN. Served by 5 POPs in Nebraska and with diverse access to the regional ESInets, traffic will route around any network problems detected allowing for ultimate reliability for PSAP call delivery.</p> <p>In the event of an outage, AT&T applies immediate and sustained effort, 7x24, until the service is restored.</p>	X			

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 18	<p>Service Level Agreements – Outage Notification and Reason for Outage (RFO) Report Status Updates</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>AT&T will communicate any updated status information to the Commission, impacted PSAPs, and/or designated agencies no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 9-1-1 service is restored. AT&T will provide as much detailed information that is available at the time regarding the nature of the outage, cause, geographic scope of the outage, estimated time for repair and any other supporting information.</p> <p>AT&T uses the Everbridge system as a way of providing written and verbal mass notification to, impacted PSAPs, and/or designated agencies of updated status information during an event. Communication will be supplied to all parties provided to AT&T by the Customer and its entities. We provide notification by email and SMS.</p> <p>In the event of an outage AT&T applies immediate and sustained effort, 7x24, until a final resolution is in place. We use all reasonable efforts to provide a temporary workaround. We continue resolution activity until full service is restored. The primary objective of an incident is to mitigate impact. The Incident Commander and Incident Administrator are able to call upon additional resources as required to identify and restore functionality.</p>				

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		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. Bidder Response: Upon restoration of normal 9-1-1 service, AT&T will prepare a preliminary RFO report within three business days which will include an overview of all information known at that time. AT&T will prepare and submit a final detailed report to the customer, including root cause analysis (if applicable) will be provided to the Commission, that describes the impact of the event, the cause, resolution and any preventative steps that may be taken to eliminate future events. 1. AT&T’s 9-1-1 Resolution Center uses the Everbridge system as a way of providing written and verbal mass notifications to communicate potential ESInet service-affecting or actual FCC significant events to the PSAP communities to meet the FCC mandates. We have the capability to provide notification by phone, email, SMS or Fax as directed by the customer. AT&T has customized the Everbridge system using notification templates as driven by FCC guidelines. Notifications can be sent to a PSAP, District, or other approved contact, depending on the needs of the customer and their capabilities. AT&T will work with the Commission to determine the appropriate contact list. 2. The AT&T 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 AT&T 9-1-1 NOC. OpenView utilizes the HP Operations Manager (OM) module, which monitors systems and applications using agents, and the HP Network Node Manager (NNMi) network monitoring software module based on SNMP. Visual alerts are available 24x7x365 to the AT&T 9-1-1 NOC. In addition, our NOC also utilizes the following: <ul style="list-style-type: none"> • 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 Management Portal (MP) is a web-based application that allows authorized personnel from AT&T to view or edit the following information for one or more PSAP-level accounts deployed on the AT&T ESInet. <ul style="list-style-type: none"> ○ Provisioned PSAP contact information and feature subscription information ○ PSAP operational state and operational state change history ○ Primary route list ○ Abandonment route list 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

- | | |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none">○ Fixed transfer and bridge list○ ESN selective bridge list○ PSAP directory○ Access to Call Detail Records (CDR)s○ New PSAP Adds○ Insert/Update route lists (abandonment, backup, primary)○ Insert/Update transfer star codes○ Insert/Update audio treatment○ User Administration○ PSAP abandonment and un-abandonment○ Generation of test calls○ Ten-digit phone number reroute○ 9-1-1 call audio retrieval |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Service Level Agreements – Outage Notification and Reason for Outage (RFO) Report PSAP Notifications	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 20	<p>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.</p> <p>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.</p> <p>Provide a detailed description of how bidder will support such an outage notification service.</p>		X		
	<p>Bidder Response:</p> <p>Today the AT&T 9-1-1 Resolution Center uses a web-based application that utilizes a pre-populated template and distribution list per customer, to communicate potential or actual FCC significant events to the PSAP communities. The notifications can be sent to a PSAP, district, or state or multiples, depending on the requirements/needs of the customer and their capabilities.</p> <p>We provide multi-modal forms of notification e.g., voice, email and SMS. Presently, the system is not accessible to the PSAP community to select/deselect outage notification, however, AT&T will provide a resource to assist in the manual process until an automated process can be put in place. AT&T welcomes the opportunity to further explore the notification and customization requirements by the Commission and PSAPs as a future service capability.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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.	X			
	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. Bidder Response: Media Contact 1. AT&T Corporate Communications prepares appropriate messaging for media, internal stakeholders, and enterprise customers for any outage and service failure. Government & Regulatory Contact 2. Your local AT&T External Affairs would be the government and regulatory contact for any outage and service failure. As a global telecommunications company with a considerable governmental customer base, AT&T has provided Media and Government & Regulatory contacts when required. Some examples include instances of local and regional disasters, labor disputes, regulatory changes, and legal issues.				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 22	<p>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 violation report to the Commission on a monthly basis.</p> <p>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.</p> <p>Bidder Response:</p> <p>SLA Violations Read and understood.</p> <p>SLA Reporting AT&T has standardized processes and tools that measure performance objectives and provide reporting information on a monthly basis. SLA results shall be delivered by the AT&T Program Manager to the Commission on the 10th business day of each month. This monthly report shall include all performance items identified in AT&T's proposal.</p>	X			

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<p>Service Level Agreements – SLA Violation Financial Remedies</p> <p>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.</p> <p>For service-affecting incidents, a 10 percent (10%) discount shall be assessed 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.</p>	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 23	<p>Bidder Response:</p> <p>SLA Violation Financial Remedies</p> <p>As an industry leading provider of 9-1-1 and public safety services for over thirty years, AT&T has successfully implemented mature, proven processes and operational procedures for providing service assurance. AT&T has established service levels for AT&T ESInet Service. While AT&T does not guarantee the service levels. AT&T will provide credits to an eligible Customer when a service levels not met, subject to the terms, definitions and any potential exclusions that may apply. Customer may not receive credits totaling more than 100% of the monthly charge for any affected PSAP for a given calendar month.</p> <p>AT&T complies with the Incident Severity Level 1 and 2 Credits specified above as they apply in efforts to restore Severity Level 1 and Severity Level 2 issues defined below.</p> <p>Severity Level 1 is defined as an incident whereby the Service or its components are completely inoperative or severely impacted:</p> <p>Examples: (including but not limited to)</p> <ul style="list-style-type: none"> • PSAP not receiving calls • All network down to a PSAP • Total Service failure • Loss of ANI / ALI to a PSAP for 15 or more minutes <p>For Severity Level 1 issues, AT&T will respond within 30 minutes and restore Service within two (2) hours of opening a trouble ticket by Customer in the BusinessDirect portal.</p> <p>Severity Level 2 is defined as an incident whereby the Service is functioning at a limited capacity or critical functions are no longer redundant.</p> <p>Examples: (including but not limited to)</p> <ul style="list-style-type: none"> • PSAP reported line noise or interference 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

- Intermittent non delivery of voice
- Network to the PSAP one-sided (ESInet Network Connections)

For Severity Level 2 issues, AT&T will respond within 30 minutes and restore Service within four (4) hours of opening a trouble ticket by Customer in BusinessDirect portal.

AT&T ESInet Standard SLA for Incident Management is summarized in the table below:

Table 1: Incident Respond and Restore Intervals

AT&T ESInet™ SLA		
Incident	Respond	Restore
Severity Level 1	30 mins	2 hrs.
Severity Level 2	30 mins	4 hrs.
Severity Level 3	8 hrs.	48 hrs.
Severity Level 4	16 hrs.	96 hrs.

The incident response service level objectives, for all incident severity levels are measured by comparing the time of opening the trouble ticket to the time the Service was restored.

The AT&T ESInet™ Standard SLA for Incident Management provides restoration of Severity Level 1 and Severity Level 2 incidents 50% faster than the required time durations specified in the RFP.

If AT&T does not meet this performance objective for the Site Availability/Time to Restore SLA, Customer may be eligible for a Site Availability/Time to Restore SLA credit equal to the Customer's total discounted MRCs for call routing services for the affected PSAP sites, multiplied by a percentage based on the duration of (Time to Restore) the Outage, as set forth in the Site Availability/Time to Restore SLA Credit Table below.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Site Availability/Time to Restore SLA Credit Table		
Time to Restore - Equal to or Greater Than	Time to Restore - Less than	Credit Percentage
1 minute	2 hours	5%
2 hours	4 hours	10%
4 hours	8 hours	15%
8 hours	16 hours	20%
16 hours	> 16 hours	50%

AT&T looks forward to future discussions with the State of Nebraska to review our AT&T ESInet SLAs and service credits.

Bidder shall include how uptime information will be gathered, analyzed and provided to the Commission.

All SLAs will be gathered either automatically or manually based on monthly data, calculated based on established measurements and provided to the Commission as part of a monthly report.

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:

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 1	Scenario 1				
	<p>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.</p> <p>Bidder Response:</p> <p>Assumption the ingress calls are SS7.</p> <p>Risk Mitigation Strategy</p> <p>AT&T ESInet’s six-core solution has redundancy architected into not only the solution as a whole but also within in each core site. AT&T’s SBCs have the ability to failover within a core to provide the service with the 99.999% availability. Additionally, AT&T’s system not only has alarms set to notify the NOC and technical resources of an issue, but also alarms set to notify of even potential issues so AT&T can troubleshoot and resolve issues before a potential problem impacts the PSAPs.</p> <p>In addition, AT&T’s NOC is trained specifically for ESInet to ensure if issues arise, they understand call flow and potential impacts. AT&T has the ability to monitor server utilization statistics that can help predict issues before they arise.</p> <p>Issue Resolution Strategy</p> <ul style="list-style-type: none"> • 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 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. <p>*It should be noted that the alarms from 0300 may or may not be related to the garbled audio issue beginning at 0345.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Restoration and Resolution Timeframes

AT&T would designate this as Critical (service impacting) issue. AT&T 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.

Restoration and Resolution Timeframes

Severity Code	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	Client is able to access the system, or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor	Client is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent	Client has an informational request or questions of a general nature concerning the overall product suite functionality or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours
Informational	ORT Testing, SMOP Events, non-customer impacting problems or informational types of trouble	N/A	N/A	N/A

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Root Cause Analysis Report

Root Cause Analysis (RCA) report for Critical or Major service disruptions will be available following the resolution of a Critical or Major 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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Scenario 2 All originating service providers in the state are connected directly via Signaling System Number 7 (SS7) protocol to the bidder's LNGs that serve the PSAPs in Nebraska, as well as others outside the Commission's footprint. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. One of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of the prior day's logs, it is found that the two surviving LNGs only are processing 2,000 calls each.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 2	<p>Bidder Response:</p> <p>Risk Mitigation Strategy</p> <p>AT&T employs several strategies to mitigate risk to prevent such situations from happening. AT&T works with OSPs to establish redundant connectivity to the LNG (Aggregation Sites). During setup, AT&T recommends OSPs establish trunks with equal size so that should one trunk group become unavailable, the other trunk group can handle the full traffic load. Additionally, AT&T recommends OSPs test failover when establishing trunks. Finally, AT&T's LNGs are setup in an active-active configuration. The OSPs should utilize this function to send traffic to each of the LNGs so they do not have to manually failover should trunks be out of service or LNG functionality at one location be lost.</p> <p>Issue Resolution Strategy</p> <ul style="list-style-type: none"> • This situation is managed as a Major 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 OSP providers traffic to full capacity. Those steps are listed below. <ul style="list-style-type: none"> ○ 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. <p>This incident would be initially designated as a Major (routing services are impaired) issue, but upon review would change the classification to a Critical (severely impacted). Once the perceived call volume mismatch is detected AT&T will, until proven otherwise, assume that calls were/are being impacted by this outage.</p> <p>Restoration and Resolution Timeframes</p> <p>AT&T would designate this as a Critical (service impacting) issue. AT&T 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.</p>	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Restoration and Resolution Timeframes				
Severity Code	Description	Response Time	Customer Restore 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	Client is able to access the system, or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor	Client is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent	Client has an informational request or questions of a general nature concerning the overall product suite functionality or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours
Informational	ORT Testing, SMOP Events, non-customer impacting problems or informational types of trouble	N/A	N/A	N/A

Root Cause Analysis Report

A Root Cause Analysis (RCA) for Critical or Major service disruptions will be available following the resolution of a Critical or Major 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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none"> • 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.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here

GEN SCEN 3	Scenario 3	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
	<p>Bidder Response:</p> <p>Risk Mitigation Strategy</p> <p>The AT&T Spatial Interface (SI) is built to deal with this exact scenario. GIS submissions will be provided via the SI. AT&T's SI is known as the Enterprise Geospatial Database Management System (EGDMS). EGDMS allows 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.</p> <p>Issue Resolution Strategy</p> <p>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.</p> <p>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.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 4	<p>Scenario 4 At 0700, the NOC has received an alarm reporting loss of connectivity for a single path to PSAP A. At 0705, the NOC contacts PSAP 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 PSAP A. At 0900, the PSAP is reporting a decrease in typical call volume.</p>	X			
	<p>Bidder Response:</p> <p>Risk Mitigation Strategy</p> <p>As part of normal operations, the NOC actively monitors of 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 pretested during integration and turnout. Any issues with failover will be addressed prior to turning the PSAP live.</p> <p>Issue Resolution Strategy</p> <p>The presumed response of the NGCS vendor in scenario 4 differs from how AT&T 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. AT&T 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 AT&T 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.</p> <p>This incident would be initially designated as a Severity 2 (routing services are impaired) issue, but upon review would change the classification to a Severity 1 (severely impacted). Once the perceived call volume mismatch is detected AT&T will, until proven otherwise, assume that calls were/are being impacted by this outage.</p> <p>Restoration and Resolution Timeframes</p> <p>AT&T would designate this as a Severity 1 (service impacting) issue.</p> <p>AT&T 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.</p>				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Restoration and Resolution Timeframes

Severity Code	Description	Response Time	Customer Restore 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	Client is able to access the system, or ancillary products, but is experiencing a partial loss of critical functionality due to software or network problems and has no acceptable work around.	15 min	4 hrs	30 min
Minor	Client is able to access system, or ancillary products, but is experiencing a loss of non-critical functionality and has an acceptable work around.	30 min	8 hrs	60 min
Intermittent	Client has an informational request or questions of a general nature concerning the overall product suite functionality or is experiencing an operator inconvenience.	4 hours	24 hrs	2 hours
Informational	ORT Testing, SMOP Events, non-customer impacting problems or informational types of trouble	N/A	N/A	N/A

Root Cause Analysis Report

Root Cause Analysis (RCA) report for Critical or Major service disruptions will be available following the resolution of a Critical or Major 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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none">• 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.
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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 State of Nebraska will benefit from working with a skilled AT&T Global Project Manager from the AT&T Public Safety Group. The AT&T Project Manager is directly responsible for the project implementation and can reach out to other AT&T organizations to help smoothly transform Nebraska's service from its current environment to an AT&T i3 ESInet. The State will benefit from the skills and experience of our Global Project Manager and Transformation Team. The Project Manager will be guided by the principles established by the Project Management Institute (PMI®) in order to plan, schedule, and implement project activities, meeting industry recognized standards of quality, reporting frequency, and control. Nearly 75% of the AT&T Global Project Management (GPM) team is comprised of Project Management Institute certified Project Management professionals (PMP). AT&T's Global Project Management experience includes both domestic and international projects with overall project volumes ranging from 100 to 17,000 sites. The average on- time performance (OTP) on a GPM led project is 98%. The AT&T Project Manager will be responsible for multiple complex projects from conception through implementation, including: <ul style="list-style-type: none"> • Manage project team members including independent contractors. • Develop and implement project plans and design schedules. • Identify risks and alternate course of action to ensure projects are completed within corporate objectives exceeding customer expectations. Upon contract award, the AT&T Project Manager will engage team members throughout the AT&T organization to help ensure their commitment and understanding of the project requirements. The PM will schedule a kickoff meeting with the relevant jurisdiction 9-1-1 group and other required AT&T organizations. During the kickoff meeting, the PM will establish roles and responsibilities and reach a mutual agreement with the Commission on strategic objectives, plan of approach, priorities and timelines. Using the information gathered during the meeting, the PM and the customer will create an integrated master work plan that will be used as the implementation roadmap. Throughout the project, AT&T will focus on project planning and execution to help ensure a successful upgrade with minimal (if any) disruption to the customer's current Wireless/VoIP ESInet service. Project Management Tools AT&T's experienced Program Managers, Project Managers, Service Delivery Managers, Installation Technicians, Solutions Engineers and other supporting groups have worked together on many successful installations. We are determined to provide each customer with an installation that will exceed expectations. The NG 9-1-1 ESInet solution is an IP-based system that employs proven technology to deliver excellent 9-1-1 services. Given the mission critical nature of the network, greater safeguards are taken during installation, but from a practical point of view it is a network installation, and AT&T is able to leverage best practices of network installations to ensure success.				

PM 1

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

AT&T Project Managers will use the Microsoft suite of products to manage all projects as a standard operating procedure. Tools will include

- Microsoft Word
- Microsoft Excel
- Microsoft Project
- Microsoft Visio
- Microsoft Outlook

Project Management Methodology

The AT&T Worldwide Project Management Methodology is based upon the industry standard A Guide to the Project Management Body of Knowledge (PMBOK Guide®) Fourth Edition, produced by the Project Management Institute (PMI), as well as AT&T specific processes and procedures.

The characteristics of a project may be determined by many factors: strategic importance, size, scope, schedule, cost and duration, as well as many others. This methodology is scalable to accommodate all types of projects.

The Project Management Methodology utilizes a four-phase project life cycle:

- **Project Start Phase.** Recognition that a new project is being considered. During this phase, basic information is gathered, evaluated and based upon the information a decision is made to proceed with the project.
- **Project Plan Phase.** Establishing the project's approach and planning how to achieve the desired results and baselines for the project in terms of scope, schedule and cost.
- **Project Implementation Phase.** Implementing the Project Plan to produce the agreed upon deliverables, monitoring the project progress and ensuring that deliverables meet expectations.
- **Project Completion Phase.** Completing the project. Ensuring that the project was delivered as expected and ensuring that there is final/formal acceptance in order to close out the project.

These four phases of a project, plus the inputs and activities and deliverables key to the phases, comprise this methodology. Throughout each of the four distinct project phases, the five iterative process groups of Initiating, Planning, Executing, Monitoring and Controlling, and Closing will be used. Each of the five processes is applied within each project phase. Often changes occur within the life cycle of a project and process groups must be repeated.

2. The AT&T Project Manager will conduct regularly scheduled project status calls with the relevant State of Nebraska parties and key AT&T stakeholders. Normally, these status calls are held on a weekly basis and cover the following topics

- Overall Project Status – Red/Yellow/Green
- Project Timeline and Key Milestones
- Issues log review
- Key Deliverables status

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Also, during PSAP migration, the AT&T project manager will be available to discuss project-related elements with the State’s primary project contact on an informal schedule. If it is determined that formal daily meetings are required, the PM will schedule those meeting with the key stakeholders.

Monthly stewardship meetings can be held by the AT&T Account Team and the PM to provide the State with a holistic view of ongoing program.

3. We have included a high-level project plan as Exhibit 5, Project Plan and Project Schedule. All Project Plans are subject to negotiation and agreement with our customers. Upon contract award, AT&T will work with the State of Nebraska to develop an agreed upon implementation plan.

4. We have included a high-level project plan as Exhibit 5, Project Plan and Project Schedule. All Project Plans are subject to negotiation and agreement with our customers. Upon contract award, AT&T will work with the State of Nebraska to develop an agreed upon implementation plan.

Any additional documentation can be inserted here:



Exhibit 5_Region and
PSAP Implementation

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Project Management and Ongoing Client Management Services Post-Deployment Client Management Describe the post-deployment client management service, including client management reports, executive briefings and the fielding of ad hoc support requests.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
PM 2	<p style="margin: 0;">Bidder Response:</p> <p style="margin: 0;">AT&T 9-1-1 Service Management will be responsible for AT&T Customer Day Two Support for the service. AT&T 9-1-1 Service Management will collaborate with all parties to manage the customer relationship and basic routing changes as part of ongoing lifecycle management. The Service Manager is the single point of contact for escalation requests and performs the following tasks on a regular basis</p> <ul style="list-style-type: none"> • Lead monthly operations meetings. • Provide upgrade and maintenance event notifications. • Distribute software release notes, test cases, and test case results. • Coordinate software release lab testing. • Escalations. • RCA reporting. • Coordinate data center and aggregation site access for technical resources. • Coordinate new user access to operational support tools e.g., customer web portal. • Serve as Change Event Coordinators. • Outage communications. <p style="margin: 0;">The AT&T response includes a dedicated Nebraska-based Project Manager, Sr. Technology Manager, and ESInet Service Manager. These dedicated resources will work closely with the Nebraska-based AT&T Public Safety Service Management, Field Services and Account Teams. These groups along with our 9-1-1 Resolution Center will provide support during deployment and post-deployment to the Commission and to the PSAP's within the State of Nebraska. These resources will be on hand to provide ad hoc support, as applicable.</p>	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 1	<p>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:</p> <ol style="list-style-type: none"> 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. <p>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).</p> <p>Bidder Response:</p> <p>AT&T provides extensive training packages to support the rollout of NG9-1-1 systems including comprehensive training on AT&T ESInet Routing, AT&T ESInet ALI Management, metrics tools, and database management service support tool training to customer-designated users. 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 customer system and minimize operational impact on the end users and staff. We also provide appropriate training to telephone service providers to supplement TSP support information available online.</p> <p>The training plan for the customer 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 system, respective to each user's area of responsibility.</p> <p>Training sessions are designed to allow trainees to understand and effectively interact with AT&T and the web-based tools to maximize benefits of the system and tools for the customer. This is achieved by integrating well-designed technical documentation, practice exercises, and instruction into the overall training experience. We will provide a comprehensive set of training materials for each trainee.</p> <p>Training options include:</p> <ol style="list-style-type: none"> 1. Standard Customer Training. One on-site train the trainer session for up to 20 designated state and other representatives is included. Additional AT&T ESInet training is provided to customer-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. Upon request we can provide onsite training. 2. Supplemental Training. We are 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. We view the customer as a partner in overseeing the quality of the training and making ongoing recommendations for improvement. 3. Optional Training. We will work with the State to scope, design, develop, and deliver any additional AT&T ESInet training desired, including pertinent optional classes or training as it becomes available. 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<p>AT&T would coordinate training upon request to the State to educate their administrative personnel on the operational characteristics of the system and the tools available for overall system management. The training sessions are held via the Web and consists of two sessions.</p> <ol style="list-style-type: none">4. Session One (2 hours) is an overview of the customer web portal with instructions for logging in and uploading data.5. Session Two (2 hours) is to review the data output once the GIS data has been analyzed with employees trained on the access and use of GIS data portal, with specific training on data uploads and data reports. This is typically provided to the responsible party for maintaining the GIS data for the Customer. <p>Additionally, key contact information will be reviewed with each customer.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	General Requirements – Training Attendees and Curriculum	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 2	<p>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.</p> <p>2. Provide Examples of the proposed training plans.</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>1. AT&T will provide a Training Plan specific to Nebraska's PSAPs for the proposed solution. The number and type of attendees will be based on the needs of the State. The training will be comprehensive and will allow the PSAPs to understand the operational characteristics of the system and the tools available for overall system management. Training will include Network Status Reports, Help Desk, Trouble Ticketing and Root Cause Analysis/Review.</p> <p>2. Training sessions are designed to allow trainees to understand and effectively interact with AT&T and the web-based tools to maximize benefits of the system and tools for the customer. This is achieved by integrating well-designed technical documentation, practice exercises, and instruction into the overall training experience. We will provide a comprehensive set of training materials for each trainee.</p> <p>Training options include:</p> <ul style="list-style-type: none"> • Standard Customer Training. One on-site train the trainer session for up to 20 designated state and other representatives is included. Additional AT&T ESInet training is provided to customer-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. Upon request we can provide onsite training. • Supplemental Training. We are 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. We view the customer as a partner in overseeing the quality of the training and making ongoing recommendations for improvement. • Optional Training. We will work with the State to scope, design, develop, and deliver any additional AT&T ESInet training desired, including pertinent optional classes or training as it becomes available. <p>3. AT&T provides extensive training packages to support the rollout of NG9-1-1 systems including comprehensive training on AT&T ESInet Routing, AT&T ESInet ALI Management, metrics tools, and database management service support tool training to customer-designated users. 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 customer system and minimize operational impact on the end users and staff. We also provide appropriate training to telephone service providers to supplement TSP support information available online.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
SRAR 1	Bidder Response: The AT&T ESInet is designed and implemented as a fully managed service that eliminates the customer's need to constantly maintain, upgrade, and administer a complex hardware and software solution and it maximizes the customer's ability to focus on public safety. Key components within the AT&T ESInet are periodically renewed to enable PSAPs to operate on the most modern communications technology during the life of the contract. AT&T maintains and monitors all equipment and software within the solution, and it is AT&T's goal to replace End of Support (EOS) equipment prior to the EOS vendor published date. AT&T will replace any faulty equipment at no additional cost to the Commission that is not a direct result of negligence of on-site PSAP personnel. Support Maintenance 1. AT&T will conduct major and minor planned and critical unplanned changes for all AT&T ESInet system maintenance or upgrades that may impact customers. AT&T 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. AT&T 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. AT&T will include the required back-out time within the scheduled maintenance timeframe. Change Management / Maintenance Plan AT&T broadly classifies Change Management into 2 categories <ul style="list-style-type: none"> • Global Change Management Process for AT&T ESInet™ (Change Management) <ul style="list-style-type: none"> ○ How AT&T operates, administers and maintains our national call routing service e.g., Changes to network, hardware and software components affecting all users of the service • Local Change Management via Move, Add, Change and Disconnect (MACD) <ul style="list-style-type: none"> ○ How customers operate, administer and maintain their own PSAP specific information e.g., Provisioning data (Speed dial lists, Route changes, contact information etc.) 				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Global Change Management Process for AT&T ESInet™ (Change Management)

Change Management process governs the planning, coordinating, monitoring, reviewing, approving, auditing and communicating of change in the interest of maintaining service at target performance and availability levels for the AT&T ESInet™. AT&T 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. Our tool suite and built-in ITIL best practices enables us to understand and minimize risk while making Global changes, as well as allowing the environment to be stable, reliable, and predictable. This aligns us with ITIL and FCAPs (Fault, Configuration, Accounting, Performance, and Security) processes by allowing changes to be evaluated for their benefits and risks and considering all impacts.

The Change Management process ensures that all organizations impacting 9-1-1 will:

- Implement changes as scheduled and approved
- Perform deconfliction to reduce the number of concurrent changes that can be scheduled without impairing service
- Communicate planned change activity in a timely manner to allow accurate impact assessment and approvals
- Proactively eliminate or reduce incidents and outages caused by change
- Protect the production AT&T ESInet™ service
- Provide high availability for applications, network, services and infrastructure

The Change Management process cares for platform wide changes in the AT&T ESInet™ Core Routing platform. AT&T tracks scheduled changes to all components of the AT&T ESInet, which include Aggregation Sites, Core Call Routing Complexes, AT&T ESInet™ PSAP network edge equipment as well as the interconnections to each.

Most maintenance activities on the AT&T ESInet™ solution are completed with no scheduled downtime for the customer. AT&T follows the notification policies in the Change Event Definitions and Notifications Matrix below.

Change Event Definitions and Notifications Matrix

Event Type	Definition	Notification
Normal	<ul style="list-style-type: none"> • Pre-planned maintenance events or upgrades • Normal changes are categorized according to risk and impact 	<ul style="list-style-type: none"> • AT&T shall notify customers in advance when there are potential impacts identified to the service
Emergency	<ul style="list-style-type: none"> • Typically, unplanned events • Issues that have a potential for an immediate threat to the production environment or 9-1-1 service. 	<ul style="list-style-type: none"> • AT&T shall notify customers as soon as the need for emergency maintenance is identified and every effort is made to provide as much advanced notice as possible for any issues anticipated to result in a service disruption

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Change Management Steps

The AT&T Change Management process includes the following steps to ensure successful planning, governance and execution of implementing changes to help eliminate / minimize service impact.

Planning

AT&T Labs will thoroughly test all software updates and service packs as they are released by our suppliers and prior to releasing them into the live customer environment. This includes an Approval for Use (AFU) process which certifies new software releases. These upgrade and testing processes help ensure that our solution will work in a real-world environment and not just in test labs. The standard AT&T ESInet™ maintenance window is 12 a.m.-6 a.m. 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 12 a.m.-6 a.m. Central. MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

Review

AT&T utilizes a 9-1-1 Change Governance process to support 9-1-1 Change Management. Changes impacting 9-1-1 are submitted to a centralized 9-1-1 Governance Review Board for deconfliction and pre-approval. Planned events are scheduled in a manner that 9-1-1 operations are not impacted. All change requests submitted to the 9-1-1 Governance Review Board for pre-approval must include the following before being considered for scheduling:

- A Risk Assessed MOP that includes a step-by-step guide of the changes being made
- Clear definition of scope
- Clearly stated impacts, if any
- Detailed validation and back-out plan(s) to rollback changes and revert to the previous production configuration
- All event resources are clearly listed (includes escalation lists)

Approval

This 9-1-1 governance process includes reviewing service availability, capacity, configurations and hardware/software release levels prior to approving any changes in the Service. Once pre-approved, Change Requests with a potential large impact or any actual customer impact are submitted to our centralized 9-1-1 Governance Approval Board for executive review and approval. The 9-1-1 Governance Approval Board is a committee that consists of executive stakeholders and their representatives who review change requests and makes decisions regarding whether the change submitted should be implemented or not. The 9-1-1 Governance Approval Board meets weekly but is also engaged on an ad-hoc basis for emergency approvals should they be required.

Notification

AT&T's Service Management Organization will provide advanced notice of maintenance events, when there is possible customer impact identified. For questions during the maintenance window, the customer should contact the AT&T 9-1-1 Resolution Center.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Execution

The AT&T ESInet team conducts major and minor planned and critical un-planned events for all AT&T ESInet™ system maintenance or upgrades. Events are fully staffed and managed with a trained event management team, facilitating the change implementation and monitoring through the length of the event. For events that have potential for customer impact, additional steps are in place to ensure the co-ordination of the event via internal conference bridges and chat rooms.

Post Execution

The result of each change is tracked in AT&T's change management system and available for future reference in the system whether it was successful or unsuccessful. All unsuccessful events that result in a service impairment are tracked in AT&T's incident management system as incidents and follow our Incident Management Process where sustained effort is provided until service is restored.

AT&T ESInet Hardware/Software Maintenance Plan

The AT&T ESInet is designed and implemented as a fully managed service that eliminates the customer's need to constantly maintain, upgrade, and administer a complex hardware and software solution and it maximizes the customer's ability to focus on public safety.

Key components within the AT&T ESInet are periodically renewed to enable PSAPs to operate on the most modern communications technology during the life of the contract. AT&T maintains and monitors all equipment and software within the solution, and it is AT&T's goal to replace End of Support (EOS) equipment prior to the EOS vendor published date.

AT&T will replace any faulty equipment at no additional cost to the Commission that is not a direct result of negligence of on-site PSAP personnel.

Local Change Management Process (MACD)

MACD is an acronym used for PSAP Move, Add, Change, & Disconnect activities and is used to describe the processes and actions that take place on the existing live service.

MACDs are typically customer-initiated changes that allow and enable customers to operate, administer and maintain PSAP specific provisioned data such as speed dial lists, route changes and contact information.

Depending on complexity, MACD activities can be implemented either in a coordinated or non-coordinated manner.

- Coordinated MACDs include changes to call routing which may impact 911 call delivery. For coordinated MACDs there will be ongoing communication between AT&T and the customer regarding implementation, including timelines. Depending on the change requested, customers may be asked to participate in a conference bridge for immediate testing, which allows for unsuccessful changes to be promptly rolled back.
- Non-coordinated MACDs are limited to those that do not impact 911 call delivery. For non-coordinated MACDs, AT&T provides a completion notification to the customer once implemented.

MACD activities are not conducted under the control of the AT&T ESInet™ Change Management process, which is more geared towards global platform maintenance. As MACD activities are directly coordinated between AT&T and the customer, there are no MACD tickets created. MACD changes are noted in the AT&T customer database of record once completed and confirmed successful.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

1. The standard AT&T ESInet™ maintenance window is 12 a.m.-6 a.m. 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 12 a.m.-6 a.m. Central.

MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

2. The AT&T ESInet Network Operations Center (NOC) is staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage the AT&T ESInet associated services and connectivity.

Change Management

AT&T will conduct major and minor planned and critical un-planned events for all AT&T ESInet system maintenance or upgrades that may impact customers. AT&T ESInet uses the AT&T One Ticketing System–Change Management (AOTS-CM) service management suite for managing changes to the service including aggregation sites, core call routing complexes, PSAP equipment maintenance, circuit maintenance, and software upgrade events. AT&T will manage and complete these events with a trained ESInet event management team facilitating the change implementation, monitoring, and communication through the length of the event.

AT&T 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. AT&T includes the required back-out time within the scheduled maintenance timeframe.

The AOTS-CM module tracks changes in system hardware and software versions. Upgrade events can also be tracked via the Change Management module to establish a full version history of the system. Our AOTS system has been enhanced with specific templates created exclusively for AT&T ESInet to make entering data easier and to ensure change management tickets are routed efficiently. The AOTS-CM meets industry standards and is tailored to our work centers, e.g., ESInet Moves, Add, Changes, Deletes, etc.

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:** AT&T will provide a schedule of standard maintenance windows for activities defined below as: level 4 standard and level 3 normal.
- **Emergency:** Where reasonably practicable, AT&T will give the State 24 hours’ notice of the need for the maintenance and a summary of the potential impact. Emergency maintenance may occur at any time.

i3 Functional Elements, Layers 4-7

Change Event Type	Definition	Notification
Level 4 - Standard	A planned maintenance event that is a low risk and repeatable change that occurs frequently.	Courtesy notification will be provided for standard changes directly affecting the AT&T ESInet. These notifications will not require customer approval.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Repeatable Change plans / MOPs have been established. Example: PSAP Network failover testing (pre-production), replace a failed disk drive within an array.	
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 AT&T support will be reviewed with AT&T prior to the scheduled date. Example: Router replacement, PSAP activation, AT&T ESInet™ 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 AT&T to provide advance PSAP notification for this type of event. AT&T 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 Sev 1 or Sev 2 service disruption. For issues not anticipated to result in a Sev 1 or Sev 2 service disruption, notification shall be no less than twenty-four (24) hours.

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. AT&T 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 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 using a standard process. The Commission can choose the modality of this communication (i.e. text, email, etc.)

The AT&T Service Manager will provide notice of maintenance events, when there is possible customer impact identified. For questions during the maintenance window, the Commission should contact the AT&T 9-1-1 Resolution Center. The AT&T ESInet 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

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

be completed between 12am-6am CT. AT&T Customer PSAPs may require maintenance at the PSAP to be done outside of this maintenance window, in which case AT&T will coordinate an appropriate time to perform maintenance at the PSAP.

Problem Management

In addition to managing planned and emergent events, we maintain a problem management system for tracking and reporting trouble. AT&T provides a service portal [AT&T Express Portal \(https://expressticketing.acss.att.com/expressticketing\)](https://expressticketing.acss.att.com/expressticketing) 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. AT&T will send an email notification to the customer at the start and end of the pre- arranged maintenance interval. Listed below are the current AT&T 9-1-1 escalation procedures.

AT&T 9-1-1 Escalation Procedures

Escalation Intervals	Level	Responsibility
First Escalation SEV 1 - 2 Hours SEV 2 – 4 Hours SEV 3 – 6 Hours	Resolution Manager	<ul style="list-style-type: none"> Review Customer Request and keep customer updated Escalate as needed to the appropriate partner center
Second Escalation Customer Discretion	Area Manager Or Delegate	<ul style="list-style-type: none"> Review status of ticket Monitor ticket progress Notify Director - when appropriate
Third Escalation Customer Discretion	Director	<ul style="list-style-type: none"> Status Customer Escalate as needed to partner centers Monitor ticket Progress/ documentation Notify AVP when appropriate
Fourth Escalation	AVP	<ul style="list-style-type: none"> 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)

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none">• Trouble Location• Trouble description (e.g., out of service, service degraded, etc.)• The action or resolution requested <p>AT&T understands the requirement for integration and information sharing to the Customer for service management support. AT&T will work with the Commission to develop an appropriate integration design, plan and MOP for information sharing.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

General Requirements – Software Release Policy Scheduled Releases Frequency of Scheduled Releases 1. Describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release. 2. Include a current roadmap of feature updates and additions with projected release by quarter and year.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 1 Bidder Response: 1. 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 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 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 AT&T 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. One of AT&T’s distinctions compared to our competitors is that we employ rigorous steps to technically and operationally review all new software and patch releases end- to-end. All the software releases are tested by AT&T Labs. The testing program includes the following elements. <ul style="list-style-type: none"> • 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. A typical annual release schedule includes one major software release with up to two minor releases as required. Feature Release Testing Process The following information describes our product release cycle, outside of the Agile Scrum process.	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Deployment

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

- Finalize regression testing (if needed) (System Team).
- 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).
- Release candidate #1 may be 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 if applicable.

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. AT&T ESInet's draft product roadmap outline of NG 911 features considered for 2020 is illustrated in the figure below.

Product Roadmap**

AT&T ESInet™ Service

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Real-Time Text (RTT) Enhancements <ul style="list-style-type: none"> ◦ Mid call drop & continue text ◦ RTT transfers • NENA i3 Ingress Enhancements (e.g., missing location fallback) | <ul style="list-style-type: none"> • Network Based Firewall Managed Service • NetBond Cloud Managed Services |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|



**Items for consideration

Safe Harbor Statement
 Cautionary Language Concerning Forward-Looking Statements
 Specifics concerning the vision for future development are subject to change. This is not a timeline or a commitment to deploy any specific product, technology or feature. This document is not an offer, commitment, representation or warranty by AT&T and is subject to change without notice.

Figure 17: AT&T Roadmap for ESInet 2020

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	General Requirements – Software Release Policy Maintenance Releases Describe the frequency of defect-resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 2	<p>Bidder Response:</p> <p>The AT&T ESInet is designed and implemented as a fully managed service that eliminates the customer’s need to constantly maintain, upgrade, and administer a complex hardware and software solution and it maximizes the customer’s ability to focus on public safety.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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 AT&T Change Control Board.</p> <p>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.</p> <p>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.</p> <p>The AT&T ESInet solution is offered as a service; therefore, known issue and defects resolution are included at no cost. Enhancements and custom development could be at additional fees.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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: One of AT&T's distinctions compared to our competitors is that we employ rigorous steps to technically and operationally review all new software and patch releases end- to-end. AT&T Labs will thoroughly test all software updates and service packs as they are released by our suppliers and prior to releasing them into the live customer environment. This includes an Approval for Use (AFU) process which certifies new software releases. These upgrade and testing processes help ensure that our solution will work in a real-world environment and not just in test labs. The testing program includes the following elements. <ul style="list-style-type: none"> • 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. 				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
SRP 4	<p>Bidder Response:</p> <p>AT&T provides a problem management system for defect tracking and reporting trouble. AT&T provides a service portal AT&T Express Portal (https://expressticketing.acss.att.com/expressticketing) for opening trouble tickets, change requests and checking status of existing items e.g., tickets opened, resolved, and pending.</p> <p>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. AT&T will support the requirements of the State for the required “software defect tracking component”, and will utilize the Product Roadmap, and the Service Enhancement Request process to track the status and prioritize the enhancement with other Product Roadmap improvements.</p> <p>‘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.</p> <p>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.</p> <p>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 AT&T Change Control Board.</p> <p>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.</p> <p>Upon request, AT&T shall provide training to Commission 9-1-1 staff prior to final acceptance testing in order for the Commission to track the progress of defect resolutions.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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. AT&T will support the requirements of the State for the required "software defect tracking component", and 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 AT&T 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. AT&T provides a service portal, AT&T Express Portal (https://expressticketing.acss.att.com/expressticketing), 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:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
DOC 1	<p>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:</p> <ol style="list-style-type: none"> 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. <p>Network As-Built Documentation Upon implementation, Contractor shall provide a network or solution diagram that clearly depicts the Contractor’s solution as implemented.</p> <p>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.</p> <p>Bidder Response:</p> <p>AT&T will provide relevant documentation for the ESInet and NGCS as listed above. AT&T will provide and maintain as-built diagrams of the system and services. In the as-built diagrams, diversity will be clearly identified from the ingress BCFs to the PSAPs. Documentation will be maintained for all ingress and egress connections to the ESInet. Every ingress and egress connection will have at least one paired diverse connection to or from the ESInet. AT&T will work with the Commission to adjust documentation and “as-built” diagrams to meet the Commissions requirements. All documentation and as-built diagrams are viewed as living documents and kept current, updated and distributed as changes are made.</p> <p>Network As-Built Documentation</p> <p>AT&T will maintain the master as-built technical documentation for the program which includes the architecture of the provided system and will deliver it to the Commission within 30 days of system acceptance.</p>	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		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: AT&T ESInet is designed with diverse entrances into each core call processing facility and each aggregation site (e.g. data centers). AT&T uses MPLS networking between sites and avoids commonality of physical or virtual networks utilizing alternate POPs in all designs. PSAP connections are delivered via fiber optic cable where possible connecting to the global AT&T AVPN Network. The State of Nebraska “specified buildings” will have a second diverse landline connection avoiding the local wire center and connecting through a second POP for complete diversity into the MPLS backbone. The design adheres to level 7 diversity from the local serving central office to the customer building demarcation point avoiding any commonality end-to-end. Please note: If “Specified Buildings” do not have a secondary entrance into the building, it will be the customer’s responsibility to obtain permission from the building and/or landowner for AT&T to build entrance facilities. Should the Commission require secondary landline fiber connections for other PSAP locations, AT&T will work with the Commission to design those connections and provide information on availability and special construction costs if applicable.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: AT&T’s proposed AVPN MPLS network design provides fiber transport to all the Regional Host locations. In the State of Nebraska, AT&T is not a local access provider, we have existing Ethernet interconnection agreements in place with nearly all domestic and international carriers. The proposed Ethernet access utilizes fiber from all locations included in this RFP to the AVPN POP’s. AT&T will install one AVPN MPLS link into each of the 14 Regional Host locations with speeds ranging from 6Mbps - 20Mbps. The two host locations circuits in each region will be connected to different L2 ethernet access facilities and diverse AVPN POPs (L3 Routers location) to minimize the possibility of a single fiber outage taking out an entire region.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Emergency Services IP Network (ESInet) No Single Points of Failure The mission-critical ESInet shall be designed with no single points of failure. All equipment shall include redundant processors and power supplies and be supported by an uninterruptible power supply (UPS) system and alternate power source in a properly conditioned environment. Describe how the solution meets or exceeds the above requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 3	<p>Bidder Response:</p> <p>The AT&T solution is built on the basic principle of "no single point of failure." AT&T utilizes a fully redundant, multi-path, multi-protocol network linking all AT&T NG9-11/E9-1-1 network elements and PSAPs. Within each redundant node, there are redundant network elements. Failover within the system occurs automatically with no manual intervention. AT&T network connectivity handoffs enter each facility (minimum of two) via diverse facility transport paths and diverse points of interconnection.</p> <p>The geographically diverse AT&T data centers have multiple active power and cooling distribution paths, redundant components, and proven fault-tolerance. AT&T Data Centers employ the following:</p> <ul style="list-style-type: none"> • Heating, Ventilation, and Air Conditioning (HVAC) Systems—maintain proper temperature and humidity. Online stand-by units are available to help ensure a proper environment. • Uninterruptible Power Supply (UPS) Systems—eliminate spikes, sags, surges, and transients, and keep voltage consistent to help ensure that critical IT system loads have clean power. • Back-Up Generators—provide continuous power during a commercial power outage. On-site generators typically support multi-day operation at full load, and we maintain priority delivery contracts to replenish fuel supplies. <p>All the NGCS and network elements utilize these dual power supplies so that a failure on the primary circuit will not disable the operation of the device.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 4	Emergency Services IP Network (ESInet) IPv4 and IPv6 Support				
	<p>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 IPv6 and have the capability to run dual protocol stacks. Describe how the solution meets or exceeds the above requirement.</p> <p>Bidder Response:</p> <p>All deployed AT&T network equipment will be new and of current manufacture at the time of implementation. The AT&T ESInet can 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 can use 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.</p> <p>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.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

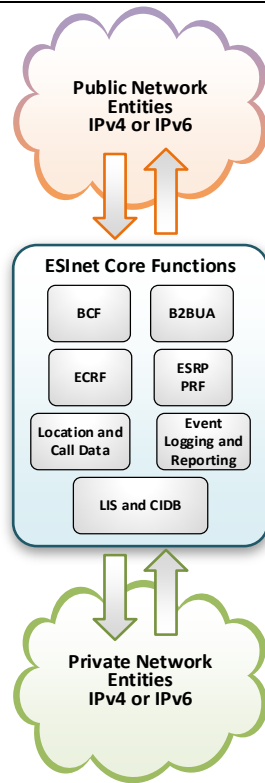


Figure 18: IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 5	<p>Emergency Services IP Network (ESInet) Open Standards Open standards-based protocols shall be used, and the use of proprietary routing protocols is prohibited.</p> <p>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.</p>				
	<p>Bidder Response:</p> <p>AT&T does not employ any proprietary protocols in our network design. All protocols used are industry standard. The AT&T ESInet solution is built on an open standards-based platform. The system complies with SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), NENA STA-010.2, IETF ECRIT best practices, and ANSI standards.</p> <p>IP packets are routable between any two points on the ESInet. The solution is deployed over IP-based Layer 3 VPN services that are used to provide connectivity between endpoint sites (LNGs and PSAPs) and core call processing sites. This provides a scalable point-to-multipoint WAN configuration. Any endpoint attached to a given IP VPN instance can be configured to reach any other endpoint due to the use of dynamic routing protocols that allow precise policy control over routing. Typically, individual endpoint sites use at least two IP instances for redundant connectivity to the six core sites.</p> <p>Resiliency</p> <p>All redundancy mechanisms for core applications and network elements that support delivery of emergency 9-1-1 calls across the AT&T ESInet solution (Routing LNG, ESRP, and ESInet components, LIS, ECRF, ADR, and ALI) employ “failover” procedures which are automatic and do not require human intervention. AT&T leverages the use of Bidirectional Forwarding Detection (BFD) on all network backbone links for fast failover purposes. Two LPGs are deployed to each PSAP for redundancy and failover. All supporting network routing infrastructure connected to the LPGs is designed and deployed in an N+1 model.</p> <p>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 AT&T ESInet 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.</p> <p>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.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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.				
	Bidder Response: ESInet routers and switches are capable of multicast routing and switching using Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) protocols.	X			

Any additional documentation can be inserted here:

		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.				
	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 AT&T ESInet 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.	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Emergency Services IP Network (ESInet) ESInet Properties	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 8	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>Private - The AT&T ESInet IP network uses a private, high-speed, MPLS IP backbone, not the public Internet, for transmission.</p> <p>Robust & Scalable - The AT&T ESInet is built with significantly more capacity than necessary to allow for component failures and/or maintenance that will not impact customer call processing. According to NENA 9-1-1 Statistics (http://www.nena.org/?page=911Statistics) approximately 290 million 9-1-1 calls occur annually in the United States, which equate to approximately 7.7 emergency calls originating every second. A "busy hour" call rate can be estimated at ten times the average call rate or approximately 77 calls per second.</p> <p>The AT&T ESInet can successfully process all State of Nebraska 9-1-1 calls even under severe loads that may occur during unusual events such as extreme weather.</p> <p>Secure - Core and Aggregation Site physical facilities are hardened with resilient power infrastructures and environmental systems designed such that a commercial power failure does not result in an interruption of service. These facilities are equipped with environmental monitoring of HVAC, power systems with battery backup, as well as generators permanently located at each site. Each facility is required to have priority fuel contracts in place, guaranteeing constant fuel supplies during extended outages for the power generators. Regular maintenance and full load testing is performed at each site to provide reliability. The facilities have documented fire plans, smoke and/or fire detection devices, sprinklers or other approved fire suppression systems as required by best practices and local code. Core Site data centers address requirements for physical access, security, diversity, and redundancy as defined in the Telecommunications Infrastructure Standard for Data Centers (TIA), TIA-942. Concerns addressed in data center selection include:</p> <ul style="list-style-type: none"> • Cabling infrastructure • Electrical systems (including UPS, battery, and utility) • Environmental systems • Lighting systems • Floor loading limitations • Seismic considerations • Physical security • Fire suppression • Network access <p>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.</p>				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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). Data center cabinet and physical floor space requirements are addressed within the pre-existing Core Sites. All equipment is mounted in four-post lockable cabinets.

Diverse- AT&T ESInet is designed with diverse entrances into each core call processing facility and each aggregation site (e.g. data centers). AT&T uses MPLS networking between sites and avoids commonality of physical or virtual networks utilizing alternate POPs in all designs.

PSAP connections are delivered via fiber optic cable where possible connecting to the global AT&T AVPN Network. The design adheres to level 7 diversity from the local serving central office to the customer building demarcation point avoiding any commonality end-to-end.

Redundant - The AT&T ESInet 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:

- Six core call processing sites located across the U.S.
- 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 ESInet to the Public Safety Answering Point (PSAP) for delivery 9-1-1 calls.
- Redundant Common Support Services (CSS) for management, monitoring, and reporting with a web-based Customer Management Portal that delivers real-time CDRs, call trace and solution testing.

Sustainable - The AT&T ESInet solution shall be maintained in its entirety for the initial contract duration without the need to totally replace or upgrade the applications, appliances, or CPE. The system is designed to be expandable, with the capability for expansion on an incremental basis, not a wholesale replacement of major platform(s).

Self-healing-the AT&T ESInet solution is self-healing as every PSAP has connectivity to the entire AT&T ESInet infrastructure consisting of six geographically diverse ECMCs and eight diverse aggregation centers. Network connectivity is provided by AT&T’s global MPLS network service AVPN. Served by 5 POPs in Nebraska and with diverse access to the regional ESInets, traffic will route around any network problems detected allowing for ultimate reliability for PSAP call delivery.

The AT&T ESInet core call routing centers are capable of processing more than twice the estimated busy hour rate for all 9-1-1 calls across the nation. The AT&T ESInet can successfully process 9-1-1 calls in Nebraska even under severe loads that may result from unplanned events such as natural or man-made disasters.

All PSAP locations served by fiber will be implemented with a minimum of 100M and most will have 1G ports. At turn-up, each PSAP will be provisioned with 150% of the expected bandwidth needed by current demand and current ESInet features

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
ESI 9	<p>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.</p>				
	<p>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.</p> <p>Network Design Documentation Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end-state designs for the ESInet.</p> <p>Bidder Response:</p> <p>Special Construction AT&T understands and complies. If special construction is required, then AT&T will ensure all construction permits, right-away negotiations and other subcontracted activities are included in the overall cost.</p> <p>Use of Existing Network Assets AT&T was one of the first carriers to implement the original 9-1-1 service, enhanced 9-1-1 and now Next Generation 911. No vendor has more experience with regards to Public Safety as AT&T. AT&T has over 35 years' experience installing, maintaining and hosting 911 call centers, 911 databases and 911 networks. AT&T ESInet™ is built upon the AT&T Global IP Private Network that is backed by industry leading SLAs. AT&T ESInet™ service provides the State of Nebraska a complete end-to-end solution monitored by a single provider to accelerate troubleshooting and eliminate vendor finger pointing.</p> <p>As a Public Safety solution and one of the most critical applications for the citizens of Nebraska, we have many concerns about the complexity of integrating the existing microwave network into AT&T's ESInet due to the potential effect it could have on performance and availability. We believe our solution, as designed, will meet or exceed the needs of the State to achieve the a highly available public safety grade network.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Network Design Documentation

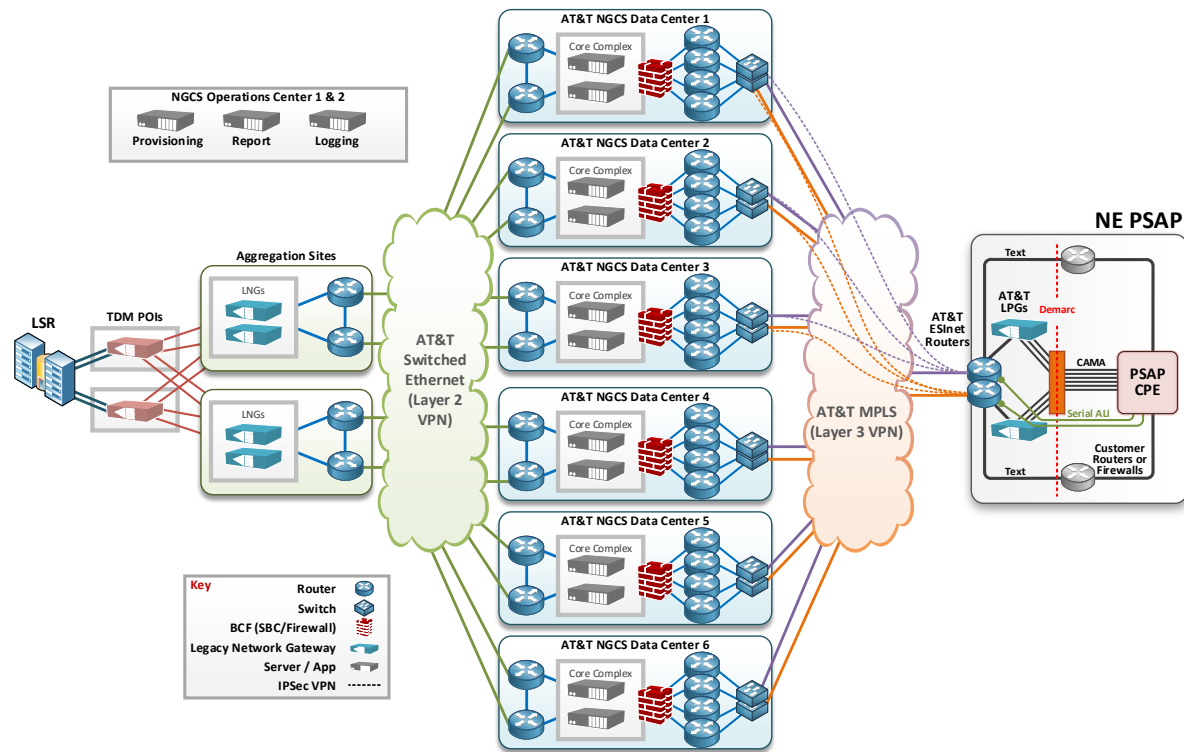


Figure 19: Network Design Diagram

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

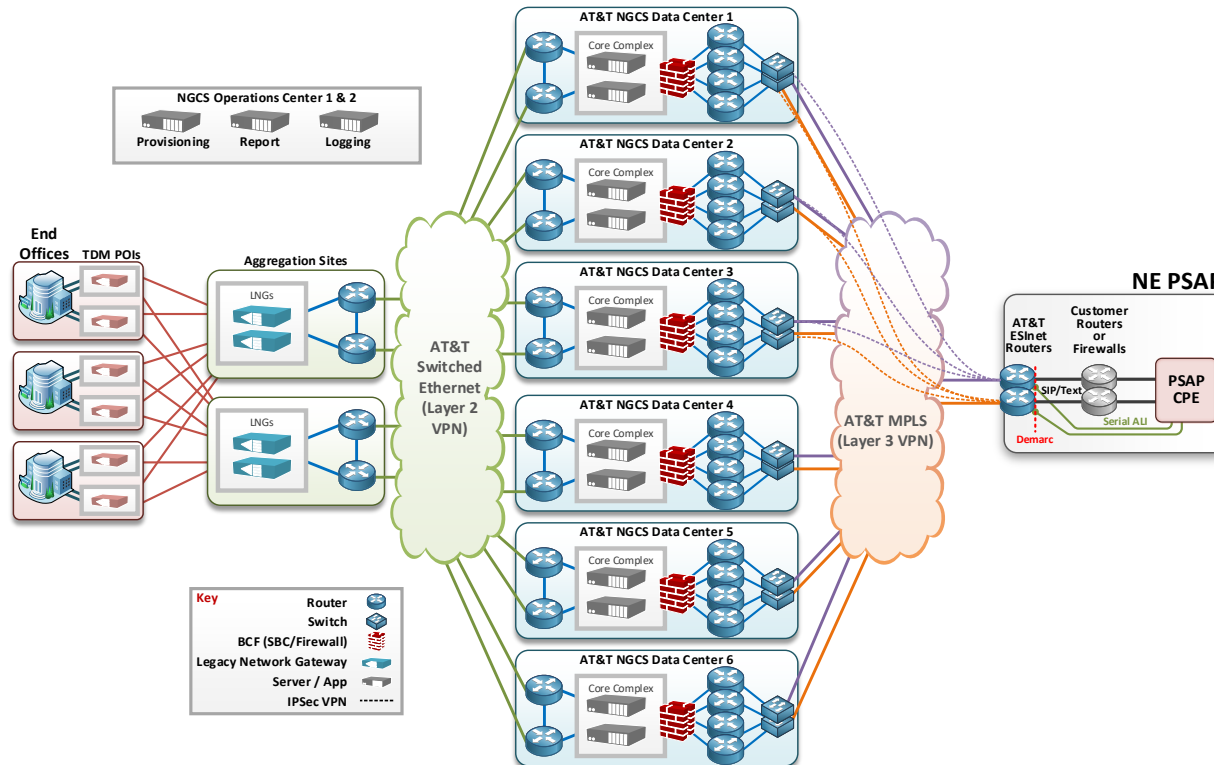


Figure 20: Network Design Diagram

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Emergency Services IP Network (ESInet) Provide Network to Network Interface with Other IP Networks Contractor shall provide an ESInet solution capable of interfacing with neighboring state and regional NG911 IP networks as they are established, and capable of transferring voice and data between PSAPs. Describe how the solution will meet these requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
ESI 10	<p>Bidder Response:</p> <p>AT&T will execute a commercial agreement, such as a memorandum of agreement, with IP Network provider(s). The agreement will identify the POI with the State's ESInet. The agreement includes lines of responsibility for network management and monitoring function between the authorized networks.</p> <p>AT&T establishes NNI commercial agreements with each ESInet provider with which it exchanges traffic.</p> <p>After receipts of the Letter of Authorization from the PSAP, AT&T sends an introductory package to the ESInet providers identified by the State of Nebraska. The package includes the LOA, notification, Interconnection agreement, NNI specifications and timelines. The Parties work cooperatively to establish the connections necessary to exchange IP traffic between the parties (6-9 months).</p> <p>The Interconnection agreements include but not limited to the following:</p> <ol style="list-style-type: none"> 1. Roles and responsibilities of the Parties related to the exchange of 9-1-1 traffic 2. Terms and Conditions 3. Establishing facilities and Exchange traffic 4. Basic SIP and i3 SIP interfaces 5. Network Architecture 6. Point of Interconnection (IP locations) 7. Bandwidth (Concurrent Call Sessions) traffic volume 8. IP network level 9. Application level 10. Call transfers 11. Split rate centers 12. Call transfers 13. Database 14. Troubleshooting 15. Fault Management and escalation procedures 				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

The Interconnection agreements include the roles and responsibilities of the Parties related to the exchange of 9-1-1 traffic including but not limited to, terms and conditions, split rate centers, Point of Ingress and NNI specifications. All terms, conditions, and procedures follow applicable State guidelines and rules as well as applicable telephone industry practices, NENA standards and all applicable US telecommunication law.

A typical ESInet to ESInet implementation follows the following process:

1. Contract execution with the State
2. Overall project implementation plan mutually agreed to with the PSAP (State)
3. Letter of Authorization from the Customer to act of their behalf to migrate to AT&T ESInet™
4. AT&T sends notification (new NG 911 provider) and request to move traffic to AT&T ESInet™
5. Interconnection Agreements mutually agreed to executed by the Parties
6. MPLS circuits orders for interconnection
7. Test/Turn up on MPLS circuits
8. Operational Readiness (ORT) testing with the PSAP
9. PSAP goes live on AT&T ESInet™

This process will allow us to interconnect with additional ESInets in neighboring regions and states and FirstNet's NPSBN, as well as any other entities designated by the State.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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: We are committed to an AT&T ESInet™ 9-1-1 offering that requires interoperability with other vendors' systems and adheres to the various required interoperability protocols specified for use in the NENA i3 standards, such as HELD, LoST, Additional Data, MSRP, and others. AT&T's solution is compatible and complies with the following NENA specifications: <ul style="list-style-type: none"> • NENA-STA-010.2-2016 (formerly NENA 08-003), Detailed Functional and Interface Specification for the NENA i3 Solution. • NENA 08-002, NENA Functional and Interface Standards for Next Generation 911 Version 1.0 (i3). • NENA 08-751, NENA i3 Technical Requirements Document. • NENA 04-001, Recommended Generic Standards for E911 PSAP Equipment. AT&T has formalized interconnection agreement documents, processes and Network to Network Interface (NNI) specifications to govern connections with third-party ESInet providers. AT&T is currently working with third-party ESInet providers nationally to establish formal interconnection agreements.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 1	<p>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:</p> <ul style="list-style-type: none"> 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). <p>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.</p> <p>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.</p> <p>Bidder Response:</p> <p>Next Generation Core Services Elements (NGCS)</p> <p>AT&T ESInet™ provides an NGCS solution that eliminates LSR functionality. Today AT&T is the 9-1-1 system service provider to over half 6,000 PSAPs throughout the US. AT&T leverages this market leadership position along with our core Legacy E9-1-1 assets (e.g., dedicated network planners and 9-1-1 asset tracking database resources) as a competitive advantage to accelerate identifying wireline, wireless and Voice over IP (VoIP) Originating Service Providers (OSPs) connections to the LSR.</p> <p>AT&T has developed a transitional implementation strategy to migrate traffic off the LSR, as described below.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

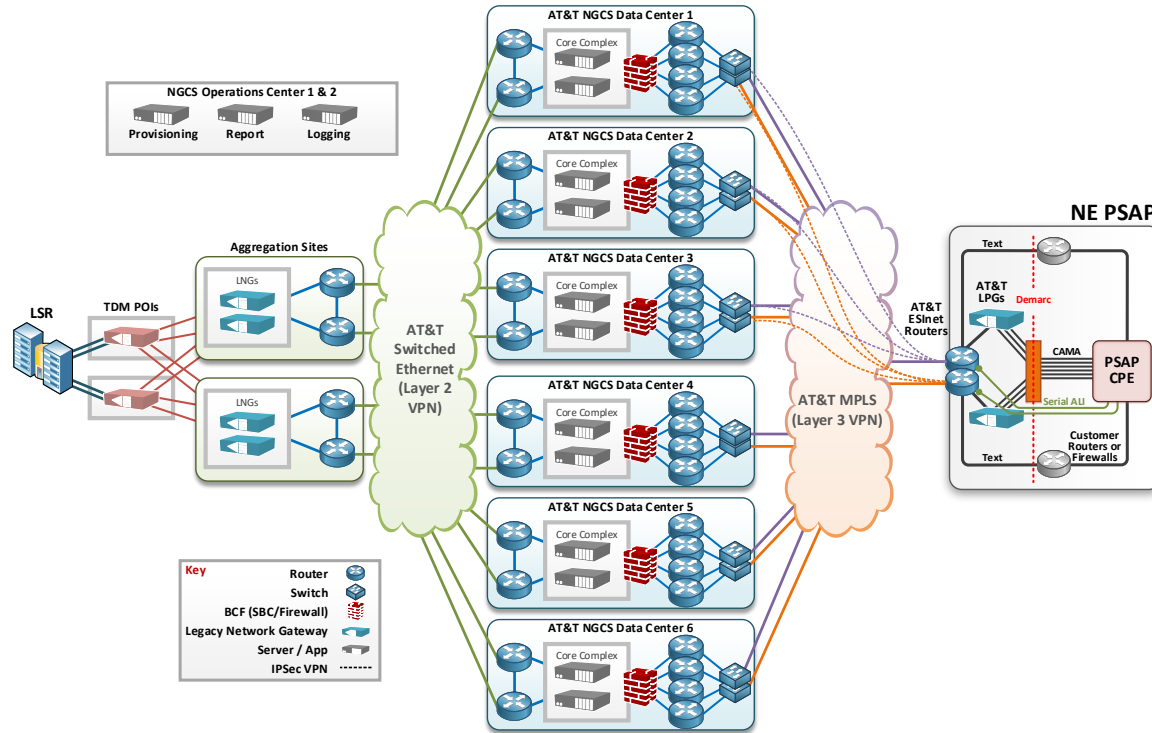


Figure 21: OSP Migration Approach—Phase 1 LSR Migration

During Phase 1, AT&T will work with the 9-1-1 authority to obtain a Letter of Agency (LOA) so AT&T may notify the OSPs to move trunks to the AT&T ESInet. The Phase 1 migration occurs during the PSAP on-boarding process and is done in parallel with establishing MPLS VPN connectivity to the remote PSAPs from the ESInet cores. AT&T's objective is to establish Point of Interface (POI) locations near existing ILEC LSR locations (as possible). During this transition, AT&T orders new trunk connections between the LSR and the newly established POIs. A routing change is performed at the LSR to route to 9-1-1 traffic to AT&T ESInet instead of the PSAP trunk. The LSR trunk connections to the PSAP remain in service

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

but not in use. 9-1-1 traffic is collected at the AT&T ESInet POIs and then backhauled to redundant Aggregation Sites that contain the Legacy Network Gateway (LNG) devices. During Phase 1 transition, OSP traffic continues to route thru the LSR and migration of the OSPs is not required to turn a PSAP up. In Phase 1 the PSAPs begin receiving all calls from the ESInet via the IP network. LSR and network providers are directly connected to the ESInet and direct calls to the ESInet based on PSAP ESN. In summary, this Phase 1 approach does not require the OSPs to move traffic and enables the PSAP to accelerate realizing the benefits of AT&T ESInet implementation.

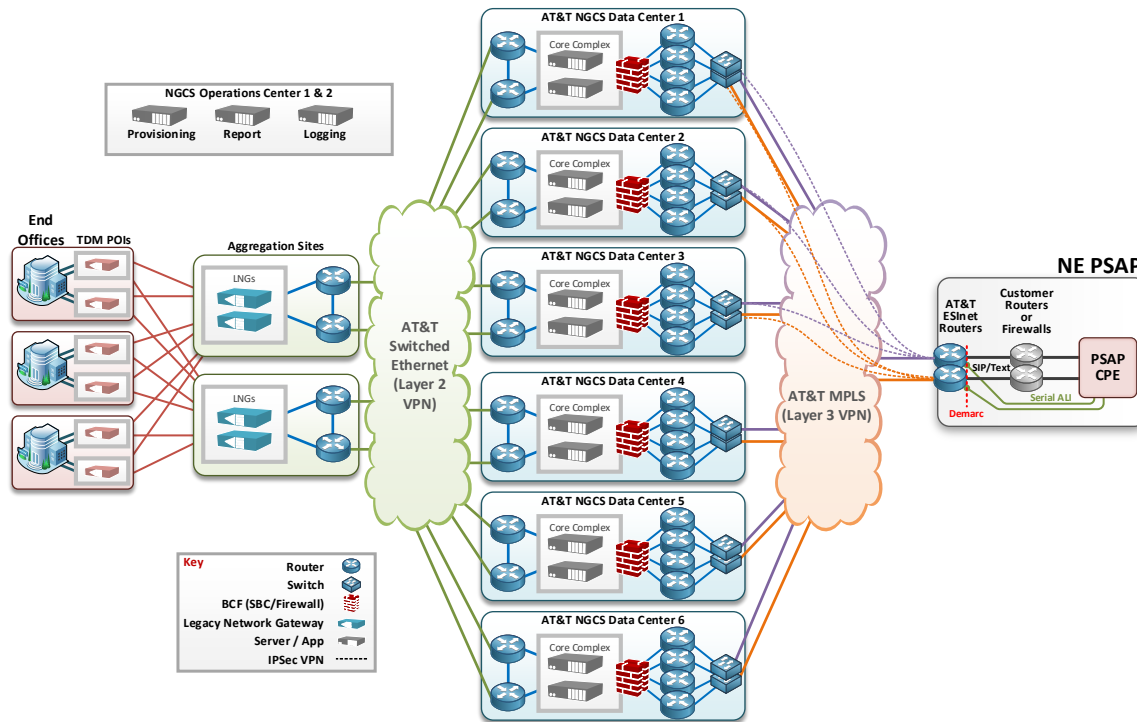


Figure 22: OSP Migration Approach - Phase 2 Direct Connectivity to ESInet

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

In Phase 2 of the AT&T ESInet™ implementation, the OSPs migrate to a direct connectivity model with the ESInet, bypassing the legacy selective routers and network providers. For each OSP, new emergency trunks are established from the OSP to AT&T ESInet POI (e.g., establish circuits from OSP to AT&T ESInet POIs, create SS7 trunk groups from OSP to AT&T ESInet LNGs). When the final OSP has been turned up and tested, the customer may disconnect trunks from the LSR to the PSAP (after 60 days). ESInet connectivity to the legacy selective routers and network providers is maintained only to support ingress and egress call transfers.

The timeline for migration from the LSR to the ESInet depends on the timely action by the OSP's and their ability to prioritize ordering and completing the installation of the new circuits. AT&T requests the OSP move within 6 months of notification. AT&T may request PSAP assistance in cases where OSPs are reluctant to move in a timely fashion.

Originating Service Provider (OSP) Connectivity

Due Authorization

AT&T does possess a certificate of public necessity to operate as a telecommunications provider in the state of Nebraska. AT&T will provide a copy of its current certificate of public necessity prior to award of contract.

Identification of Service Providers Connected to the Legacy Selective Router

AT&T will gather data about OSPs that are active in Nebraska and the associated rate centers from a multitude of data sources. Since OSP and customer information is considered sensitive CPNI data this information can be difficult to gather from one source. Subscription services such as LERG, TelcoData, and PSAP information will aid in data collection. Once a list of all OSPs covering Nebraska are gathered, they will be sent notices to rehome to the Agg Site (SS7) or Core Site (IP). If the OSPs have an aggregator, we expect the OSP to notify their aggregator of the new connection requirement. AT&T will work with the State commission to encourage any OSP stragglers to complete their network moves.

Information collected from or validated with OSP representatives during the Solution Definition phase includes:

- Comprehensive Inventory of OSPs serving the NCR; ILECs; Independent Operating Companies (ICOs); CLECs; Wireless; VoIP; Private Switch Customers
- OSP Contact Information; Network Planning; Trunk Ordering; ALI Data
- OSP Code Sets; CLLI Codes; Point Codes; ACNAs; OCN; NENA IDs
- OSP Switch Information; Type, CLLI Codes; Rate Centers Served
- OSP Trunk Information; Quantities; SS7; CAMA; PRI; SIP
- Embedded existing 9-1-1 service provider system interconnection
- Tariff Information
- Interconnection Agreements

This information will be updated quarterly and made available as requested by the State of Nebraska.

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 2	<p>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.</p>	X			
	<p>Bidder Response: AT&T has standard Interconnection and Trunking contract templates and has successfully negotiated agreements with nationwide carriers and regional ESInet providers. AT&T expects any new agreement needed will meet the 12-month of contract execution requirement, typically taking 6-8 months. The AT&T Carrier Negotiations organization will escalate to the State as appropriate regarding OSP stragglers.</p> <p>Interconnection Agreements The Interconnection agreements include the roles and responsibilities of the Parties related to the exchange of 9-1-1 traffic including but not limited to, split rate centers, tandem to tandem connections, IP connections and Function of Code R (FoCR) or a similar and appropriate method. LNP and NNP are cared through a mutually agreed to database management process to ensure the TNs are appropriately loaded and routed. All terms, conditions, and procedures follow applicable State guidelines and rules as well as applicable telephone industry practices, NENA standards and all applicable US telecommunication law.</p> <p>The AT&T ESInet™ solution provides interconnection to a variety of networks and physical locations. These include, as required, any/all data centers serving 9-1-1 traffic, any bordering legacy networks, or any bordering ESInet using IP interconnection, assuming the ESInet follows NENA i3 standards. AT&T will manage the migration of existing legacy 9-1-1 services already in place at the PSAP(s) onto the ESInet. AT&T will manage the implementation of NG 9-1-1 services between the 9-1-1 call originating networks and the ESInet so that 9-1-1 call delivery meets the quality and reliability required for emergency call networks. AT&T will cooperate with all impacted network operators to ensure a successful transition to the AT&T ESInet™ NG9- 1-1 call delivery solution.</p> <p>AT&T ESInet™ supports interconnection with regional intrastate and/or interstate ESInet providers and/or IP selective routers solutions and either CAMA or IP connection to the PSAP. AT&T will work with the State to develop a joint communication to each PSAP, government organization, and appropriate Originating Service Providers (OSPs) outlining the scope of services to be implemented, a high-level implementation schedule, and key contact information for each entity. AT&T can distribute this communication on behalf of the State. AT&T establishes expectations with each OSP and manages communication to the OSP for items related to the AT&T ESInet™ services on behalf of the State.</p>				

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 3	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>As part of our project management process, AT&T will assign a project manager to manage the entire project, including coordinating migration work with the OSPs. The State must provide AT&T with a Letter of Authorization (LOA), designating AT&T as its new 911 emergency services provider. This LOA will also authorize the OSP to provide information to AT&T to include, but not limited to:</p> <ul style="list-style-type: none"> • Types of facility transport currently in use • Signaling protocols • Quantities of trunk, DACs locations, etc. <p>Existing call transfer arrangements between the jurisdiction and any other that the customer can transfer to with ALI.</p> <p>Service Order Input (SOI) information. The data obtained by AT&T will be used solely for the purpose of provisioning, testing, migrating, activating and operating the State of Nebraska’s new 911 system in accordance with our agreements.</p> <p>AT&T will coordinate getting the OSPs records into the AT&T ESInet database. AT&T will also jointly plan the interconnecting network with the OSP. Circuits will be ordered and implemented between the OSP and the ESInet Point of Interconnection (POI). The ESInet POI may reside in an AT&T office or hub. AT&T will cooperatively test and turn up all trunking arrangements with the OSP. Traffic migrations from the legacy to new AT&T infrastructure will then begin.</p> <p>The AT&T ESInet™ service is monitored as a complete end-to-end operation via our NOCs. When a potential or actual Customer-affecting issue is identified and determined to be an incident, the 9-1-1 Resolution team is engaged by the NOC. The team uses established and proven processes for immediate escalation, notification, resolution, and reporting.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

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			
NGC S 4	Bidder Response: The AT&T ESInet includes redundant LNGs that provide signaling and median interconnection between callers utilizing legacy protocols such as SS7 as an example. The LNG collects full detail on TDM interfaces and upstream IP interfaces. LNG call detail is transmitted in real time to the AT&T ESInet management system for reporting and analysis. AT&T actively monitors Aggregation Site capacity using this reporting system. This allows for AT&T to see trends in network traffic and will cause alarms should predetermined thresholds be meet based on the LNG reporting. This system also allows AT&T operations teams to use ad hoc uploads of log files for troubleshooting and incident response. The AT&T ESInet is built to withstand sophisticated attacks, including DDoS. AT&T'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 necessary protocols/destinations, for both ingress and egress. The network can process 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). AT&T continually investigates and upgrades new advances in protective technology with tools such as Intrusion Detection Systems (IDS). The solution incorporates physical, network, and application security principles. Traffic between core processing sites and distributed sites, such as LNGs, 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.				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 5	<p>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.</p> <p>Describe the steps bidder will take to meet the transition timelines and minimize overlapping network costs.</p>	X			
	<p>Bidder Response:</p> <p>The AT&T ESInet solution will interconnect to legacy selective routers as defined per NENA standards using redundant LNGs. The AT&T aggregation sites that connect to both Legacy Originating Service Providers (OSPs) and Legacy Selective Routers (LSRs) are in use today and currently connect to LSRs to transfers calls between legacy PSAPs and PSAPs connected to AT&T ESInet. AT&T will interconnect to Legacy Selective Routers to transfer and/or receive calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to Nebraska's NGCS via legacy means through the LSRG provided as part of this solution. Interconnections will also allow legacy PSAPs served by legacy selective routers to serve as the abandonment route for Nebraska PSAPs served by the AT&T ESInet solution.</p> <p>Upon initiation of the project, AT&T will work to get connectivity to the LSRs as quickly as possible. This connectivity will not only be used for transfers between PSAPs on the ESInet and those still on the LSRs but will also enable a quicker transition to AT&T ESInet until the OSPs can move their connections to AT&T ESInet. The LNG to LSR connectivity follows the high-level steps below.</p> <ul style="list-style-type: none"> • Network Design <ul style="list-style-type: none"> ○ ILEC Interconnection Requirements Gathering ○ Facilitate inter-local agreements ○ Legacy SR interconnection path design • Interconnection Process <ul style="list-style-type: none"> ○ Create trunk model diagram ○ Submit originating and transfer trunk orders ○ Transfer trunk test and turn up ○ Provision Trunks in ESInet ○ Circuit Testing • Cutover Testing <ul style="list-style-type: none"> ○ During cutover of live 9-1-1 traffic, LSR translations are changed from Legacy PSAP connectivity to AT&T ESInet connectivity ○ Transfers via LSR are tested during cutover testing 				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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. AT&T has extensive experience with managing complex network moves. Currently AT&T has over 1,000 active AT&T ESInet™ deployments in 13 States and has successfully turned up over 200 PSAPs. AT&T has National interconnection agreements with various legacy 9-1-1 system service providers (SS7) as well as many of NG 9-1-1 Service providers (NNI-basic SIP). AT&T has successfully managed migration with multiple legacy 9-1-1 service providers in multiple States. Today, the legacy 9-1-1 system service providers connect to two AT&T POIs via TDM (SS7) then AT&T converts to IP for routing to the PSAP. AT&T is capable of direct IP (Basic SIP) into our core processing elements for delivery to the PSAPs. AT&T is actively working direct IP interconnection in multiple States. AT&T and the legacy system service providers and/or NG 9-1-1 system service providers have worked cooperatively to develop processes and procedures required to successfully migrate the services. In addition, AT&T communicates with each connecting carrier project timelines, ordering processes and milestone to ensure a smooth transition for the PSAPs. Once the connections are tested/turned up with the carriers, AT&T schedules ORT testing with each PSAP prior to going live on the Service AT&T's proposal provides the State of Nebraska 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 will provide standards-based interfaces to provide a network-to-network interface that interoperates with other ESInets via secure and highly reliable facilities. AT&T participates and monitors standards activities to ensure that the solution evolves with national industry standards. AT&T has always been, and intends to continue to be, a leader in the public safety solution and technology domain without compromising the quality and integrity of the 9-1-1 infrastructure. Recognizing the imperative for PSAP operations to continue uninterrupted during the implementation process, AT&T's coordination methodology approach prescribes the communications and activities necessary to ensure a safe and timely migration of services while paying special attention 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, AT&T 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 <ul style="list-style-type: none"> • 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.				

NGCS
6

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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
- 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 AT&T and Nebraska team members verify legacy and existing service installations to include in the system application and implementation requirements and refine the solution architecture to include and accommodate those existing systems and finalize the plan for end-to-end solution deployment.

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 customer.

2. Upon receipt of the Letter of Authorization from the PSAP, AT&T sends an introductory packet to the incumbent 9-1-1 System Service Provider (SSP). The packet includes the LOA, Interconnection agreement, trunk plan and timelines.

The Parties work cooperatively to establish the connections necessary to migrate traffic to the AT&T ESInet™. (est. 6-8 months)

The Interconnection agreements include the roles and responsibilities of the Parties related to the exchange of 9-1-1 traffic including but not limited to, terms and conditions, split rate centers, Point of Ingress and NNI specifications.

All terms, conditions, and procedures follow applicable State guidelines and rules as well as applicable telephone industry practices, NENA standards and all applicable US telecommunication law.

A typical implementation with a legacy 9-1-1 service provider follows the following process:

1. Contract execution with the State
2. Overall project implementation plan mutually agreed to with the PSAP (State)
3. Letter of Authorization from the Customer to act of their behalf to migrate to AT&T ESInet™
4. AT&T sends notification (new NG 911 provider) and request to establish connection to AT&T ESInet™
5. Interconnection Agreements mutually agreed to executed by the Parties
6. Circuits orders for interconnection
7. Test/Turn up on circuits
8. Operational Readiness (ORT) testing with the PSAP

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<p>9. PSAP goes live on AT&T ESInet™</p> <p>The AT&T ESInet™ solution provides interconnection to a variety of networks and physical locations. These include, as required, any/all data centers serving 9-1-1 traffic, any bordering legacy networks, or any bordering ESInet using IP interconnection, assuming the ESInet follows NENA i3 standards. AT&T will manage the migration of existing legacy 9-1-1 services already in place at the PSAP(s) onto the ESInet. AT&T will cooperate with all impacted network operators to ensure a successful transition to the AT&T ESInet™ NG9- 1-1 call delivery solution.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 7	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>The capacity of each of the redundant Aggregation Site is engineered to exceed the traffic for the entire State of Nebraska. AT&T uses a combination of current call capacity and transfer capability to determine the number of trunks between the Legacy Selective Router (LSR) and the two geographically diverse Aggregation sites. AT&T will work with each PSAP within the State of Nebraska to determine the existing number of PSAP trunks and PSAP call capacity. AT&T will continue to validate trunk capacity as Originating Service Providers migration to direct connections to the Aggregation Site. AT&T designs the trunks to each Aggregation Site so that each Aggregation Site can accommodate 100% of the traffic in case of a failure with the redundant site.</p>				

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 8	Next Generation Core Services Elements (NGCS) Legacy Network Gateway (LNG) Location Information				
	<p>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.</p> <p>Bidder Response:</p> <p>The AT&T ESInet solution complies with NENA 08-003 which itself is based upon IETF RFCs such as SIP (RFC 3261), HELD (RFC 5985/6155), PIDF-LO (RFC 4119 and successive updates), and IETF ECRIT best practices documents and ANSI standards.</p> <p>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.</p> <p>The HELD interface into the AT&T ESInet Location Database (LDB) is leveraged by the LNG to retrieve PIDF-LO, either by value 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.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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				
	<p>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.</p> <p>Bidder Response:</p> <p>The 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.</p> <ul style="list-style-type: none"> • 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) <p>AT&T's <i>Originating Service Provider (OSP) Interface Specification</i> provides OSPs with guidance when using TDM connections to interface with the AT&T ESInet. The interface specification provides OSPs with information on best practices, details on signaling for each of the protocols mentioned above, interface requirements, and trunk group requirements. This allows for an easier transition for OSPs from the Legacy Selective Router to the AT&T ESInet TDM POIs.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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				
	<p>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.</p> <p>Bidder Response:</p> <p>AT&T ESInet's BCF supports transcoding of Baudot tones to Real-Time Text (RTT) as described in IETF RFC 4103 as well as RFC 5194 as mentioned in the NENA STA 010.2 interface standards. As PSAPs with CPE capable RTT are rare, the following information describes the current RTT and TTY support. For those PSAPs wanting to deploy RTT, AT&T will work with them to determine when to enable RTT and as such transcode TTY to RTT.</p> <p>AT&T ESInet supports TTY transport to the PSAP. PSAPs requesting TTY instead of MSRP or Web Interface text messaging will request OSPs in their jurisdiction deliver TTY. In this case, the OSPs TCC provider will send TTY into the ESInet. AT&T ESInet supports TTY both for Text-to-911 purposes and legacy OSPs that still support TTY devices. In these cases, AT&T ESInet will deliver TTY to the PSAP in two possible methods. NG PSAPs capable of IP will receive TTY equivalent over SIP while legacy PSAPs will be connected to an LPG to deliver TTY to the PSAPs CPE.</p> <p>AT&T's ESInet also supports RTT ingress from OSPs. OSPs using RTT will connect IP to AT&T's ESInet. AT&T ESInet allows IP capable OSPs to connect directly to the AT&T ESInet NGCS locations and bypass the LNG. OSPs that enable RTT will not need to connect via a TCC provider. For an RTT call from an OSP destined for a PSAP that does not have an RTT capable CPE, the AT&T ESInet will convert the RTT call to TTY. To this end, AT&T's ESInet will be configured to know a PSAP's capability to receive RTT.</p>	X			

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) Legacy Network Gateway (LNG) Callback Number The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the Contractor to obtain the callback number from the wireless or VoIP provider and may include additional recurring and non-recurring costs that are independent of this RFP. The Contractor shall be responsible for all recurring and non-recurring costs associated with this requirement. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 12	<p>Bidder Response:</p> <p>Prior to OSPs providing location and additional data with the call, AT&T will continue to manage the location data and ANI on behalf of the OSP. The migration of ALI and MSAG data from the current CenturyLink and Windstream databases is included in the transition to AT&T ESInet and is included at no additional costs. For wireless or VoIP providers, the OSP will continue to send the pseudo ANI with the originating call to the AT&T ESInet POI. Once received by the LNG, the AT&T ESInet will perform the proper NIF, LIF, and PIF functions to query the location database and steer queries to the external OSP database to acquire the callback number and location information. When that is returned to the ESInet Core, routing will be determined and delivered to the appropriate PSAP.</p> <p>At this point if an OSP is i3-compliant, all calls originating from their network will leverage their LIS and an ADR to provide location and CBN information, 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 AT&T for ALI provisioning, though they will be required to utilize the ESInet LVF for location validation before provisioning records to their LIS. Carriers who do not have a LIS will continue to send SOI records for validation and provisioning into the State's ALI database.</p> <p>A carrier LIS is considered outside of the ESInet, while the State's ALI and its associated LIS interface is located inside the ESInet within the secured zone protected by firewalls and authentication.</p> <p>The AT&T transitional ADR solution leverages an interface into the ALI database that supports ADR queries. During carrier transition to NENA i3 compliance, AT&T will maintain the ADR interface into the ALI platform to simultaneously support legacy PSAPs and i3 PSAPs with CBNs for wireline and static VoIP calls.</p> <p>Note that not all ALI fields map to PIDF-LO, for example Class of Service and Customer Name. As such, AT&T will also provide an ADR interface to retrieve this information to be included in the SIP signaling. For these fields, the LNG supports the Additional Data protocol (draft-ietf-ecrit-additional-data-28) to provide these data fields via the Additional Data Repository (ADR). In the case of any significant changes to the Additional Data specification, updates will be placed on the roadmap, as it is critical that implementations are coordinated with the different i3 functional elements (ADR, LNG, Terminating ESRP) that leverage this protocol.</p>	X			

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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. Bidder Response: The AT&T ESInet service provides an i3 logging capability per the NENA STA-010.2 specification. AT&T can support near real-time log delivery and web service interfaces for log retrieval from authorized clients. The AT&T ESInet 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 AT&T ESInet is setup to send i3 log files to the ECaTS reporting system. As the State of Nebraska has a separate contract with ECaTS, it is the understanding that ECaTS would format and make this report available. 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 selective router to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics. AT&T's standard reporting suite provides the following reports through a web-based interface. <ul style="list-style-type: none"> • 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. • 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 information below shows the required reports to the corresponding AT&T provided report:	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Timing = Event Count Reports per Hour
- Call-delivery time = Event Setup Time
- Call-processing time between elements = AT&T will provide i3 logs to ECaTS. ECaTS reports show processing times between elements
- Volumes = Event County by Routing Reason and Destination
- Call volumes by call type = Event Count by Type
- Alternate-routed calls = Event Count by Routing Reason and Destination
- Text-to-911= Event Count by Type
- All NGCS element usage volumes = AT&T has internal reports server, network capacity and utilization; AT&T i3 logs sent to ECaTS can provide details on each NGCS element utilized, it is the assumption based of answers from the Commission that ECaTS will provide this report using the i3 logs provided by AT&T
- Bandwidth/trunk utilization = Event Count by Incoming Trunk Group
- Calls per trunk = Event Count by Incoming Trunk Group
- Trunk utilization = PSAPs can view near real-time trunk utilization using the “PSAP Call, IP Contact, and Trunk Status” screen in the Customer Management Portal
- Circuit utilization = PSAPs can view near real-time trunk utilization using the “PSAP Call, IP Contact, and Trunk Status” screen in the Customer Management Portal

The AT&T 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. AT&T 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.

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

NGCS 14	Next Generation Core Services Elements (NGCS) Legacy Network Gateway (LNG) Extraction of Log Files	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	<p>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.</p>	X			
<p>Bidder Response:</p> <p>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. AT&T’s LNG log files are collected at the redundant Common Support Services (CSS) locations. The CSS provide a central point for log files for all functional elements. AT&T’s Resolution Center has access to these logs for monitoring, troubleshooting, and incident reporting purposes.</p>					

Any additional documentation can be inserted here

NGCS 15	Next Generation Core Services Elements (NGCS) Legacy Network Gateway (LNG) High-Availability Design	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	<p>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.</p>	X			
<p>Bidder Response:</p> <p>The AT&T ESInet achieves 99.999% service availability 24x7x365 for call processing and has no single point of failure that will disrupt the ability to provide on-going call processing. The LNG complies with the reliability, availability, security, and network traffic restrictions described in Section V.D.1.b. The LNG has a MTBF that will result in a reliability of .99999. The LNG availability is architected so that it has less than five minutes of downtime per year to meet the availability requirement. The LNG is secure and uses AES 256 encryption when communicating to the Core Sites. The LNG meets the Network Traffic Restrictions requirement by ensuring 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.</p> <p>The AT&T ESInet components are designed and configured for continuous operation. AT&T ESInet availability is calculated from the time an outage begins that impacts call processing ability, until such time that the AT&T ESInet call processing ability is restored.</p> <p>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.</p>					

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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				
	<p>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.</p> <p>Bidder Response:</p> <p>The LNG and LSRG are signaling and media interconnection points between callers in the legacy originating networks and AT&T ESInet. The LNG converts calls from TDM to SIP signaling for ingress to the ESInet. The LSRG converts calls from SIP to TDM signaling for egress from the ESInet to the Legacy Selective Routers.</p> <p>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 AT&T's next generation emergency network. 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.</p> <p>Two or three-digit star codes are supported for ESN-based routing with AT&T's IP Selective Routing option. The AT&T ESInet 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.</p> <p>A call taker can use a single button on the call taker's display to complete either a transfer or three-way conference. They can transfer an incoming 9-1-1 call to another agency by pressing a button labeled with the type of agency; for example "Fire"-on the PSAP premises equipment. These transfers utilize pre-provisioned codes on a per-PSAP basis.</p> <p>While star codes are not required for i3 routing, the AT&T ESInet can support star codes (2- or 3-digit) for i3 routing upon request for an additional charge.</p>	X			

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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: AT&T provides regional and redundant Aggregation Sites in NEBs-compliant AT&T Central Office locations driven by customer demand. Legacy Network Gateways, and other Network equipment reside in these Aggregation Site locations and convert Local Legacy TDM 9-1-1 calls to IP(Protocol Interwork Function). The NG9-1-1-specific Interwork Function (NIF) and Location Interwork Function (LIF) are both located within each of the six core sites. AT&T Data Center locations with Core Processing Node equipment are regionally located, and geographically separated within our current 21-state footprint. AT&T core sites are location within class IV equivalent data centers. PSAPs within Nebraska will utilize the existing Aggregation Sites located in Chicago, IL and San Antonio, TX. In addition to the Aggregation Sites, AT&T offers local Points of Interconnect (POI) for OSPs to connect to. These local POIs keep costs to the OSPs down with mileage-sensitive TDM circuits. AT&T offers TDM POIs in Davy, Grand Island, Scotts Bluff, and at two sites in Omaha, NE. AT&T recommends legacy OSPs connect to at least two POIs for redundancy.				

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.	X			
	Describe how bidder's solution meets this requirement. Bidder Response: As stated earlier in AT&T responses to NGCS 2 and 3; AT&T has established national interconnection agreements and standardized on-boarding processes in place to support the transition from the legacy selective routers. AT&T has successfully worked with carriers like Century Link, Verizon, Frontier, Windstream and others to interconnect 911 traffic. AT&T is willing to accept responsibility for delays caused by AT&T. AT&T does not have authority over wireline, wireless or VoIP originating service providers (OSP) and will rely on the regulatory power of the Commission or other State regulatory authority to assist in obtaining cooperation to rehome OSP traffic off the legacy selective routers. AT&T would anticipate working with the Commission to finalize contractual language defining the extent of financial responsibility during contracting phase upon award.				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 19	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p>	X			
<p>Bidder Response:</p> <p>As part of the AT&T ESInet solution, AT&T provides a Border Control Function (BCF) that detects and intercedes any non-trusted network components and is responsible for the logical network security functions between external networks and the ESInet, as well as between the ESInet and intrastate/interstate and regional agency networks. AT&T's BCF provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2 (replacing NENA 08-003) 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 call sessions as they traverse IP networks between callers and Public Safety Answering Points (PSAPs).</p> <p>Both AT&T and our partner, Intrado recognize the critical importance of compliance with as well as on-going adherence to all relevant industry frameworks and specifications including but not limited to NENA, NIST framework and specifications, and the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) "Best Practices." Therefore, we utilize these documents as part of product development and initial design of our Next Generation 9-1-1 solutions as well as the on-going policies and procedures utilized to support them. As the technology and threat</p>					

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

landscape continue to evolve, we closely and continually monitor and any changes or newly released content to adapt and continually improve upon our product and service offerings. We maintain active roles through engagement in collaborative industry events, including membership on the Councils convened for the development of the FCC’s Communications Security, Reliability and Interoperability Council (CSRIC) “Best Practices,” reviews and updates to NENA framework and specification documents, including the Detailed Functional and Interface Specification for the NENA i3 Solution and the active project to refresh of the Security for Next-Generation 9-1-1 Standard (NG-SEC). As the industry leading provider of NG 9-1-1 solutions, we have built a standards-based platform that offers the reliability, resiliency, and security our customers expect for the delivery of life mission critical call traffic.

As a provider of the critical infrastructure supporting the backbone of the nation’s 9-1-1 network, we have evaluated our security program processes against the NIST Cybersecurity Framework and have the people, processes, and technology in place to support the Framework core lifecycle components to identify, protect, detect, respond and recover.

Highlights of the key functions provided are:

- **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 border control and security functions including firewalls, intrusion detection systems, and intrusion protection systems. Security management personnel specialize in managing and operating these facilities and validate their operation.

The AT&T ESInet 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, 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). The AT&T SOC continually investigates and upgrades with new advances in protective technology with tools such as Intrusion Detection System (IDS).

- **Session Border Control (SBC).** The SBC supports SIP over Transmission Control Protocol (TCP) primarily and recommended, User Datagram Protocol (UDP), Transport Layer Security over TCP (TLS-over-TCP), and Stream Control Transmission Protocol (SCTP). The SBC populates Layer 3 headers in order to facilitate priority routing of packets and enables interworking between networks utilizing IPv4 and IPv6.
- **Opening and closing of pinholes.** AT&T ESInet BCFs are set to deny by default all traffic. Rules are built in the BCF/Firewall as necessary to allow pinholes between the firewalls to allow trusted/known traffic. Allowances go through rigorous scrutiny before being approved by the SOC. Once approved, changes are made on a regular basis following standard procedures to ensure no other pinholes are opened. AT&T SOC also does on-going traffic studies on the firewalls. Should a pinhole be opened but not utilized, AT&T SOC will coordinate the closure of the pinhole if necessary.
- **Limiting access to critical components through the use of VLANs.** The proposed ESInet is a Quality of Service (QoS)-managed private IP network which can prioritize any type of IP traffic; voice, data, and multi-media. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic.
- **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 AT&T ESInet solution.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Video/Audio Codecs including G.711 in addition to testing G.729, G.723, and AMR-WB
- Voice Quality controls including adaptive jitter buffers, automatic gain control, echo cancellation, and RCTP-XR
- Loss of RTP detection which when network-caused loss of RTP is detected, RTP will automatically converge to other available network paths.
- **Network Address Translation (NAT).** AT&T ESInet uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. When the SBC receives a message the rules are applied, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message.
- **Codec negotiation.** The AT&T ESInet system performs codec negotiation and upgrades all calls to a codec of G.711.
- **Support for QoS and priority markings.** AT&T ESInet uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic.
- **Media proxy.** The AT&T ESInet BCF supports the media proxy function. In addition, the AT&T ESInet provides a media server secured by the BCF to provide additional media functions

Each core emergency call processing site includes border control and security functions including firewalls and intrusion detection systems. Security management personnel specialize in managing and operating these facilities and validate their operation.

AT&T's 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, for both ingress and egress.

The network is capable of processing ingress 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).

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 secure the various communication elements of the proposed solution.

The following diagram depicts how the ESInet BCF is deployed.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

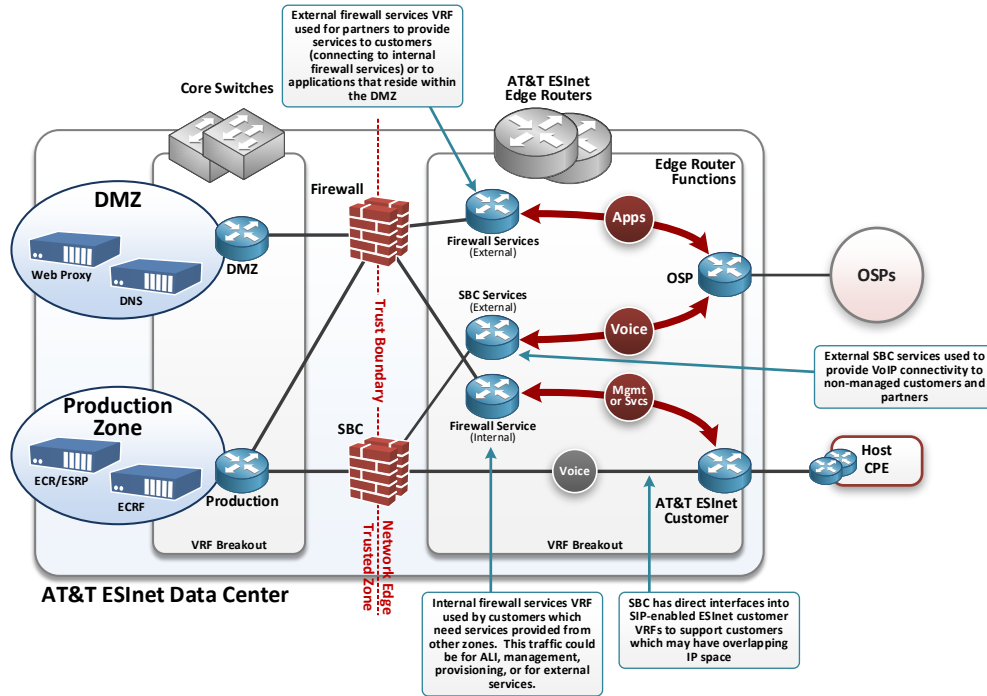


Figure 23: ESInet Boarder Control Function

Local authentication must be available as a fallback for cases in which the remote authentication server is inaccessible.

Any additional documentation can be inserted here

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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: Each of the six AT&T Core sites have redundant BCFs. The redundant BCF design and the overall six-Core architecture of the AT&T ESInet solution allows for availability to meet or exceed 99.999%.					

Any additional documentation can be inserted here

NGCS 21	Next Generation Core Services Elements (NGCS) Border Control Function (BCF) Auditing of System Log Files Management of the BCF shall include continuous auditing of the system log files for anomalies, and processes for responding to and managing security incidents. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	X				
Bidder Response: AT&T 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 AT&T ESInet environment. This capability assists in troubleshooting and anomaly resolution as well as providing assurance of reliable performance. The AT&T ESInet also provides a Network Operations Center (NOC)/Security Operations Center (SOC) staffed 24 hours a day, seven days a week, 365 days a year to actively monitor and manage the AT&T ESInet end-to-end service. When a potential or actual Customer-affecting issue is detected, the Incident Administration team is engaged by the NOC/SOC. The team uses established processes that are ISO 9001:2008-compliant for immediate escalation, notification, resolution, and reporting. The primary function is the review of log information, IDS alerts, alerting from advanced malware protection systems and other sources (broadly known as the Network Security Monitoring, or NSM, function). In addition to this, the SOC is continually searching for anomalous activity which could indicate compromise or precursor actions (“active hunting”). The results of these activities either sometimes (hunting) or always (Security Information Event Management [SIEM]/IDS alerts) are an ‘event’. One or more events, with corroborating information, may be an incident. This triage and escalation process is done within the SOC. There is no single set of criteria used to determine when a set of events or other data points are designated an incident. The SOC staff makes this determination based on the best information available at the time. Based on experience, the SOC staff is generally predisposed to designating an incident at the earliest possible time. Any single staff member may initiate an incident, based on indicators he or she sees on the ground even while event handling and normal reconnaissance take their course.					

Any additional documentation can be inserted here

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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				
	<p>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.</p> <p>Bidder Response:</p> <p>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.</p> <p>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)."</p> <p>To that end the AT&T ESInet does not enable silence suppression for any calls that use the AT&T service. Currently, when the AT&T ESInet receives an emergency call with silence suppression requested, the ingress BCF answers with silence suppression disabled. Since we don't know if silence suppression was active or inactive for the upstream links, disabling silence suppression on the link into the AT&T ESInet prevents us from potentially being the only link with silence suppression active and dropping potentially important low-level background sounds.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
NGCS 23	Bidder Response: The AT&T ESInet 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 standards. The AT&T ESInet ingress specification that supports these standards is the <i>AT&T Originating Service Provider (OSP) Network SIP Interconnection Specification v1.6</i> (available under separate NDA). The AT&T ESInet specification is not only compliant with the NENA and ATIS standards, but also supports a transitional approach to accommodate the period until OSPs conform to the prerequisites identified in these standards. This transitional option is referred to as Selective Router Interface using SIP and it emulates SS7. The OSP Network SIP Interconnection option accepts emergency ingress calls to the ESInet via the BCF using SIP and then processes the call according to the routing logic determined by the 9-1-1 Public Safety Authority. Calls are routed either in conformance with the i3 specification or by equivalent legacy Selective Router logic. Calls from i3 compliant OSP networks interact with the ESRP and are processed in conformance with the i3 specification. Ingress SIP calls may only include the TN or pANI (ESRK or ESQK) or may include Location by Value or Location by Reference. The AT&T ESInet will process these calls accordingly.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	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. AT&T will support near real-time log delivery and web service interfaces for log retrieval from authorized clients.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: The AT&T ESInet uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. When the SBC receives a message the rules are applied, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network. When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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. Bidder Response: The AT&T ESInet will provide either an IPv6 or IPv4 interface to external entities as desired for ingress to and egress from the service. IPv6 interfaces are supported according to NENA i3 standards. All network equipment has the capability to utilize IPv4 and IPv6 addresses and is configurable to support dual stack operation. Whereas some components of internal systems only support IPv4; this will not be a limitation for this solution. When an IPv6 external device sends a request packet to an internal IPv4 device, the ESInet Core strips down the IPv6 packet, removes the IPv6 header and adds the IPv4 header and passes it through. The reverse happens when the response comes back from the IPv4 device to the IPv6 device. The IPv4 network and IPv6 interfaces are continuously monitored for availability and performance. This is accomplished with the use of a back-to-back user agent session border controller, rather than Network Address Translations (NATs). All devices within the network shall be assigned static addresses.	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

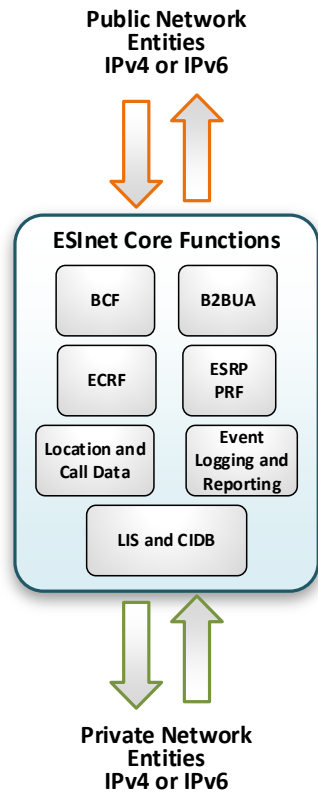


Figure 24: IPv4 and IPv6 Support Model

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		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: AT&T uses Transmission Control Protocol (TCP) within the ESInet and highly recommends that PSAP call handling solutions support TCP. If the size of the SIP INVITE is within 200 bytes of the maximum transmission unit (MTU) of an Ethernet frame, fragmentation is likely to occur. Fragmentation may have impacts ranging from call setup delays of unknown duration and quantity, to blocked or abandoned calls. In some instances, fragmentation has no discernible impact to the call. Packet fragmentation is not unexpected, and it can be handled appropriately with the use of Transmission Control Protocol (TCP). Another protocol, User Datagram Protocol (UDP), is commonly used in VoIP implementations. This protocol differs from TCP, and its mechanisms for handling packet fragmentation are weaker. While AT&T's ESInet solution can support both UDP and TCP, AT&T recommends that TCP be used. This recommendation is based upon the packet size experienced within AT&T's ESInet solution, the anticipated growth of such packet sizes with forward-looking NG9-1-1 message sets, and applicable standards including the NENA i3 specification and IETF RFC 3261. Transport Layer Security over TCP (TLS-over-TCP), and Stream Control Transmission Protocol (SCTP) are supported and selectable for each SBC interface to external systems.				

Any additional documentation can be inserted here:

		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 AT&T ESInet 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 <i>AT&T ESInet™ Originating Service Provider (OSP) Network SIP Interconnection Specification v1. 6</i> , available under separate NDA.				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: AT&T provides a Border Control Function for encryption and interface with any non-trusted network components. AT&T's Border Control Function (BCF) provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification. The BCF inspects, modifies and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect and where the ESInet connects with service provider networks. The solution for border control functions includes both security functions for the ESInet as well as the applications that ride the ESInet which include but are not limited to the SIP traffic on the ESInet. AT&T employs encryption-in-transit where possible on networks not under direct AT&T control. Encryption is achieved either using SSL/TLS or IPSEC VPN. AT&T does not encrypt data-at-rest at the database level; as a compensating control, database servers are hardened at the operating system and application level and employ Principle of Least Privilege when assigning access for users and applications to database tables. Tunnels are encrypted for security with IPSEC tunnel protection.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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 BCF inspects, modifies, and controls SIP signaling and associated media where Emergency Services IP Networks (ESInet) and agency networks interconnect and where the ESInet connects with service provider networks. The BCF mitigates security threats, resolves interoperability problems and ensures reliable SIP-based communications. It is designed to protect and control real-time voice, video, and text sessions as they traverse IP networks between callers and Public Safety Answering Points (PSAPs). BCFs are included in the solution and interface to external components traversing through redundant BCF components. Each of the six AT&T Core sites will have redundant BCFs. The redundant BCF components are market leading products that provide high reliability and high availability. The BCFs work so that only authorized traffic to authorized end points are allowed. The redundant BCF design and the overall 6-Core architecture of the AT&T ESInet™ solution allows for availability to meet or exceed 99.999%. As part of the AT&T ESInet solution, AT&T provides a Border Control Function to interface with any non-trusted network components. AT&T's Border Control Function provides session border control and border firewall functionality in accordance with the National Emergency Number Association (NENA) STA-010.2-2016 specification. Customer access to the BCF is provided via the Customer Management Portal allowing for review of real-time CDR data.				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

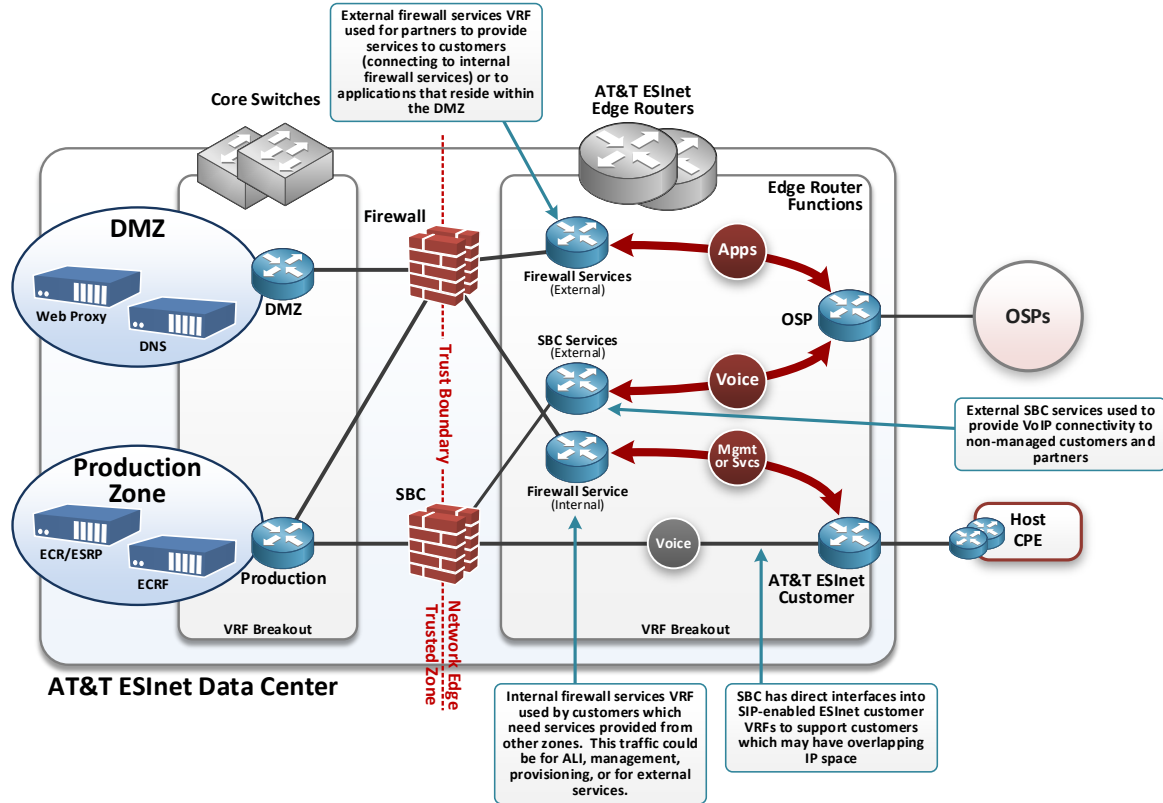


Figure 25: Border Control Function

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

<p>2. AT&T's BCF has minimal requirements from the Commission and/or PSAPs. AT&T's BCF is set up to assume anything outside the ESInet/NGCS should be treated as untrusted. Therefore, only known traffic is allowed (whitelisted) to be allowed into the solution. AT&T 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; AT&T can assign an ASN for those that do not. Additionally, AT&T supports and recommends the use of BGP passwords. AT&T can generate these for those PSAPs not wanting to provide their own.</p> <p>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.</p> <p>AT&T ESInet allows users to access the AT&T ESInet Portal for access to the Customer Management Portal and additional reporting via secure internet connections using dual factor authentication. AT&T will provide the users with a username/password credentials and associated Entrust token to securely access the AT&T ESInet Portal. The users do not have to supply their own tokens and setup is included in the cost of AT&T ESInet.</p>

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) ESRP Description	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 31	<p>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.</p> <p>Bidder Response:</p> <p>AT&T’s Emergency Service Routing Proxy (ESRP) provides i3 compliant routing functionality including full integration with geographically determined routing, carrier grade voice quality, and demonstrated reliability. AT&T’s ESRP is utilized today in a live environment and processes i3 calls using geospatial routing received from the ECRF.</p> <p>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 ESRP and routes calls to the appropriate terminating ESRP (PSAP) according to the caller’s location and the PSAP-configured routing policy.</p> <p>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 LIS/LRF or LDB 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.</p> <p>Additionally, the ESRP provides PSAPs with peace of mind by supporting multiple routing fallback options that can be used until carriers fully transition to i3 call delivery. Fallback to legacy ESN or No Record Found routing is supported to ensure every call is routed even if VoIP or wireless carriers do not deliver or pre-provision routable location values or if carrier-provisioned records are not error treated. If the ESRP has to utilize the fallback ESN or NRF routing scheme, it will continue to deliver the call and location information. This innovative solution provides extreme reliability for the routing of calls.</p> <p>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.</p> <p>Policy route determination includes evaluation of the PSAP-configured routing policy, the operational state of the PSAP, the caller’s location (for geospatially determined alternate routing policies), the PSAP operational state, and the ring-no-answer timer configuration.</p> <p>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/LRF and ADR interface responses.</p> <p>In addition to call delivery to i3-compliant PSAPs, the ESRP supports call delivery to legacy PSAPs. A subset of i3 routing policies can be provisioned for legacy PSAPs along with a 10-digit telephone number for delivery.</p> <p>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 as desired.</p>	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

The diagram below illustrates the ESRP/PRF functional components and the interfaces with other AT&T i3 solution elements.

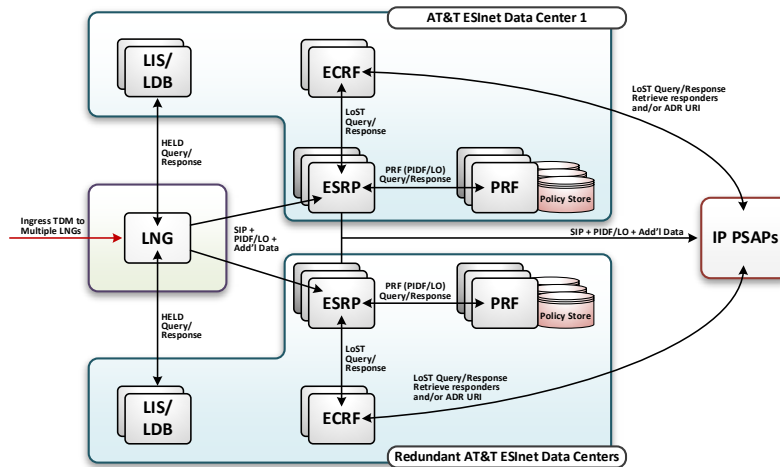


Figure 26: ESRP/PRF Diagram

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) Transition to Geospatial Routing Bidder understands that all PSAPs and regions may not be ready for geospatial routing on day one of operations and shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. In bidder's separate cost proposal response, indicate the pricing difference between tabular and geospatial routing. Describe the process for transitioning each PSAP or region from tabular routing to geospatial routing as PSAP's becomes ready and the manner in which the solution provides for routing by both means simultaneously.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 32	Bidder Response: AT&T ESInet includes both IPSR and Geospatial Routing in the base price. This allows a PSAP to transition from tabular routing to geospatial routing at the PSAP's pace and without additional costs. AT&T ESInet is a live system and currently supporting both tabular and geospatial routing. AT&T has also completed tabular-to-geospatial conversions for multiple PSAPs. The i3 solution is NENA's Next Generation solution to support IP calls using new protocols and GIS-based routing. This solution is now available to the PSAP, but the PSAP will need to take some things into consideration. Understanding that the Originating Service Providers are not yet ready to send calls into the infrastructure, the PSAP will need to maintain both the existing MSAG (for carrier location validation) as well as the GIS information for the ESInet solution. The operational procedure of comparing and completing a 98% match rate between these data sets will need to be created. Once that is created, the process of continually maintaining and loading this data into the infrastructure will need to be implemented. Additionally, the CPE will need to be able to support the new protocols for i3. All of these items will need to be investigated by the PSAP to move forward with i3. Once the PSAP's CPE is capable of supporting i3 and the PSAP's GIS data is ready, AT&T will kick off a project to convert the PSAP from RFAI to i3. AT&T provides the NENA Spatial Interface (SI) as a function of the 9-1-1 Enterprise Geospatial Database Management System (9-1-1EGDMS). AT&T will start by assisting the PSAP in loading their data through the EGDMS. The Onboarding service is included with AT&T ESInet without any additional charges and is managed by Intrado's GIS resources. The Onboarding services included with NG9-1-1 GIS Managed Services can also be purchased as a standalone service. AT&T's NG9-1-1 GIS Onboarding delivers essential services, training, and support needed to successfully deploy NG9-1-1 GIS data and the EGDMS within a NG9-1-1 environment. Intrado will provide web-based training and setup of the EGDMS system and assist with the initial GIS data load, clarifying the role of the EGDMS as the NENA Spatial Interface, and defining its features and functionality. NG9-1-1 GIS Onboarding services establish communication between the end customer, Intrado, and the NG9-1-1 service provider throughout the GIS onboarding phase and the EGDMS implementation. NG9-1-1 GIS Onboarding includes EGDMS setup and the following services: <ul style="list-style-type: none"> • Assignment of an i3 GIS Coach • NG9-1-1 GIS Onboarding kickoff meeting • EGDMS overview, user training, and field mapping training (web-based) • EGDMS report interpretation and error correction consultation training (web-based) • ALL-to-GIS report review and error correction consultation training (web-based) • GIS data testing and remediation • General NG9-1-1 GIS Q&A support • EGDMS and NG9-1-1 GIS go-live support 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Once GIS data has been loaded through and validated by the EGDMS, the data is loaded to AT&T's ECRFs and LVFs. The next step is to schedule migration testing to test the between the AT&T ESInet and the PSAPs CPE. Testing will occur without using live 9-1-1 traffic. Once all the test cases have been passed to ensure both call delivery (SIP with PIDF-LO) and data delivery (HELD and LoST), a cutover to this new configuration is completed. Additional test calls are made to ensure calls are routing using the GIS data provided by the PSAP and call and data are delivered to the PSAP's CPE using i3 protocols.

Additionally, the ESRP provides PSAPs with peace of mind by supporting multiple default routing fallback options until carriers transition to 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 not error treated. If the ESRP has to utilize the fallback ESN or NRF routing scheme, it will continue to deliver the call and location information. This innovative solution provides extreme reliability for the routing of calls.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) Policy Routing Function (PRF) Description	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 33	<p>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.</p> <p>Bidder Response:</p> <p>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.</p> <p>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.</p>	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 34	<p>Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) PRF Policy Store and User Interface</p> <p>The PRF shall allow defining of policy rules for distributing a wide range of calls in an efficient manner.</p> <p>1. Describe the solution’s Policy Store and the PSAP’s ability to effect changes to the PRF.</p> <p>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.</p>	X			
	<p>Bidder Response:</p> <p>The AT&T policy store/policy routing function provides the PSAP with extensive flexibility to define and update standard and alternate routing policies. PSAPs can modify routing policies, set priorities, and modify their operational state through a customer management portal. The tight integration of the AT&T ESInet PRF with ESRP call processing logic alleviates the requirement for PSAPs to retrieve and manage policies directly.</p> <p>Multi-factor authentication and role-based access control are used to restrict user access to the ESInet management portal. User access via the public Internet requires two-factor authentication, where one factor is provided through username and password and the second factor is provided through a dynamic, randomly changing secure access code from an AT&T-provided security token. Users are configured in the AT&T identity management system, linked to a specific security token, and configured for access to a defined list of applications.</p> <p>The routing proxy and policy store include the following elements:</p> <ul style="list-style-type: none"> • PSAP-defined routing policies. • ESInet Management Portal – A feature-rich web tool that allows PSAPs to customize ESRP configurations, define and edit their routing policies, and modify their state (normal, abandoned, diverted). Secure user access is provided via the AT&T portal. <p>The ESInet management portal is a user-friendly tool that provides information by jurisdiction(s) and/or PSAPs on service configuration and resource utilization, operational state and policies. Policies have attributes such as active/inactive, one-time or recurring time window, priority, URI, or a set of URIs of the destination(s) to send the call to as examples. Routing destinations can be pre-provisioned or can be constructed in real time to handle incidents.</p> <p>The following types of routing policies are supported.</p> <ul style="list-style-type: none"> • Abandonment/Night Service Routing – The abandonment policy is engaged whenever the terminating ESRP (PSAP) operational state is defined as ‘disabled’. The PSAP operational state may be modified by contacting the AT&T NOC, triggered via a device installed at the PSAP. • Overflow Routing – The overflow routing policy is applied during overflow scenarios when a PSAP is receiving more calls than its occupied workstations can accommodate. Upon reaching the designated call capacity for the call type, cumulative calls, or if the target is unreachable, the ESRP engages the primary PSAP’s overflow routing policy. Similarly, the alternating routing policy will be invoked if the terminating ESRP call handling system does not accept the SIP invite or for a ring-no-answer timeout. • 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 AT&T NOC or online. 				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	<ul style="list-style-type: none"> • 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. <p>Additionally, abandonment, overflow, and diversion policies can be configured to use any of the following policies.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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.	X			
	<p>Bidder Response:</p> <p>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. AT&T 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.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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 six-core architecture of the AT&T ESInet solution allows for availability to meet or exceed 99.999%. ESRP high availability is achieved through an application processing complex consisting of multiple application servers, each of which operates independently of the others so that a single application processor failure does not disrupt the processing of the complex. There are six application processing complexes that operate independently of each other and are geographically distributed. Each component at an application processing complex has redundancy and high availability within its own domain. The ESRP application is highly redundant within each of the geographically separate sites. There are multiple computers running the ESRP application and the failure of any one or two of those computers do not affect calls in progress. Failure of a data center results in all future calls being processed by another geographically diverse data center and will still provide the total required call processing capacity requirement.				

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 AT&T ESInet 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 AT&T ESInet LNGs and OSP switching equipment before a circuit is established.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 38	<p>Next Generation Core Services Elements (NGCS) Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF) TCP/TLS Implementation</p> <p>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.</p> <p>Provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.</p>	X			
	<p>Bidder Response:</p> <p>AT&T uses Transmission Control Protocol (TCP) within the ESInet and highly recommends that both ingress and egress partners support TCP as well.</p> <p>While AT&T's ESInet solution can support both UDP and TCP, AT&T recommends that TCP be used. This recommendation is based upon the packet size experienced within AT&T's ESInet solution, the anticipated growth of such packet sizes with forward-looking NG9-1-1 i3 message sets and applicable standards including the NENA i3 specification and IETF RFC 3261.</p> <p>The AT&T ESInet 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. Support for Stream Control Transmission Protocol can be added for an additional charge.</p>				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	<p>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.</p>				
<p>NGCS 39</p>	<p>Bidder Response:</p> <p>Overview Section 5.2.1.1</p> <p>Comply. Intrado supports the Emergency Service Routing Proxy (ESRP) as the base routing function for emergency calls for i3.</p> <p>The Intrado ESRP manages routing per the Nena standard and supports the hierarchy of originating, intermediate and terminating ESRPs. It receives 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 the Policy Routing Function (PRF).</p> <p>For typical 9-1-1 calls with a Request URI starting with “urn:service:sos” received, the Intrado ESRP will:</p> <ol style="list-style-type: none"> 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. <p>The result of the policy rule evaluation is a URI. The ESRP forwards the call to the URI.</p> <p>The ESRP also handles calls to “administrative lines,” meaning calls directed to, for example, a 10-digit number listed for a particular PSAP.</p> <p>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.</p> <p>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.</p> <p>Call Queueing Section 5.2.1.2</p> <p>Partially Comply; full compliance road mapped for 2Q 2022.</p> <p>Queue State Event Package Section 5.2.1.3</p> <p>Comply with Future Capability 2Q 2022</p>				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

De-queue Registration Event Package Section 5.2.1

Comply with Future Capability 2Q 2022.

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.

Before a call is directed to a specific URI (representing a T-ESRP), the PRF examines the target URI and extracts an Origination Policy from the PRF Policy Store for that URI and executes the rule set. The rules may be constructed in multiple ways. The rule may act on non-geographic information such as Date/Time information, type of call (wireline, wireless, VolP, Text) and/or may invoke a LoST findService request using a specific Service URN. This Service URN points to specific GIS data sets that have been created by the GIS entity responsible for this geographic area and loaded into the ECRF (by the Spatial Interface). 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 2Q 2022.

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.

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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. Intrados’ ESRP processes CANCELS per RFC 3261.

OPTIONS Transaction Processing Section 5.2.1.10

Comply with Future Capability 4Q 2021

Upstream Call Interface Section 5.2.2.1

Comply with Future Capability 2Q 2021.

Downstream Call Interface Section 5.2.2.2

Comply with Future Capability 2Q 2021.

ECRF Interface Section 5.2.2.3

Comply with Future Capability 4Q 2021.

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 uses 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:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- 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.
- 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 2Q 2021

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 2Q 2022.

Policy Elements Section 5.2.4

Comply with Future Capability 2Q 2022.

Provisioning Section 5.2.5

Partially Comply; full compliance road mapped for 2Q 2022

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;

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	<ul style="list-style-type: none"> • 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
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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	
Queue State Event Package Section 5.2.1.3			X	
De-queue Registration Event Package Section 5.2.1.4			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	

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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. 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, AT&T 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 AT&T ESInet, 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. 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 AT&T ESInet ECRF and ECRFs outside the AT&T ESInet also require credentialing/authentication.	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) ECRF Description	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 41	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			
	<p>Bidder Response:</p> <p>The AT&T ESInet ECRF provides full i3 compliance and contains the 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 (formerly NENA 08-003) requirements. 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.</p> <p>There are also different considerations associated with transitional i3 deployments within NENA STA-010.2. AT&T will work with the State to establish a consistent means to handle the transitional deployment until such time that legacy data stores are no longer required and carriers within the region are compliant with the NENA i3 standards. Note that the NG9-1-1 Data Model document is still in draft form. That said, it will take precedence over older NENA documents describing GIS data models. The ECRF has been supporting production Next Generation 9-1-1 call routing solutions since 2009, and the technology core has been supporting wireless and VoIP 9-1-1 call routing since 2003. The ECRF LoST interface was tested during the NENA Industry Collaboration Event (ICE 4).</p> <p>At least two ECRF servers will exist at up to six geographically diverse locations, all with redundant and secure IP connections. Even if one server or even one location has a failure, the workload will be distributed to the other ECRF servers within the system.</p> <p>The system is designed such that standard maintenance and upgrades will never leave the ECRF system single-sided.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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. Bidder Response: The redundant ECRF design and the overall six-core architecture of the AT&T ESInet solution allows for availability to meet or exceed 99.999%. For the system, including all subsystems, to be available 99.999% of the time, the network as well as the NG9-1-1 applications and appliances are designed and deployed using a high-availability model. The ECRFs exist within a highly available and geographically distributed application processing environment. A single hardware component failure at one of the application processing complexes will not interrupt processing of the ECRF. A single geographic site failure (either the communication to the site or elimination of the site itself) will not prevent further call processing from occurring. High availability is achieved through high-availability software design, redundant ECRF instances, and transactions using dynamic client/server connections with multiple ECRF serving entities. The geographically diverse ECRFs utilize redundant data stores to support high availability. These systems are monitored 24x7x365 by 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.	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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 utilize digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA), once available. Until that time, AT&T 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 AT&T ESInet, including access to the LIS interface, ADR interface and ECRF. 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 AT&T ESInet ECRF and ECRFs outside the AT&T ESInet also require credentialing/authentication.				

Any additional documentation can be inserted here:

		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 AT&T ESInet is considered safe, so the ECRF does allow LoST queries from any entity inside the ESInet. It is understood that ECRFs provided by other entities may have their own policies regarding who may query them and as such there is no guarantee that a query to another ECRF will provide a useful result. As a matter of practice, the AT&T ESInet ECRF should 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 National Forest Guide and the PSAP Credentialing Agency (PCA) have been established, there will no longer be a need for A&T to manage the digital certificates.				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) Origination Network ECRF An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Describe the functionality of such an ECRF equivalent and document where this functional element resides within the proposed solution.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 45	<p>Bidder Response:</p> <p>The origination network ECRF would typically reside within its own network and at its own cost, as noted. AT&T 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-AT&T ESInets within the state.</p> <p>AT&T will provide the Spatial Interface. Since there is not yet an established standard for the Spatial Interface to provision ECRFs with GIS data, internal or external, the mechanism for provisioning must be negotiated between AT&T, as the Spatial Interface provider, and non-AT&T ECRF providers.</p>				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) Routing Query Interface The ECRF shall support a routing query interface that can be used by an endpoint, ESRP or PSAP to request location-based routing information from the ECRF. Additionally, it shall support both iterative and recursive queries to external ECRF sources. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 46	<p>Bidder Response:</p> <p>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.</p> <p>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.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 47	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) LoST Protocol Support The ECRF shall interface with the Location-to-Service Translation (LoST) protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CHE, or any other permitted IP host. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		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 AT&T ESInet must be authenticated.					

Any additional documentation can be inserted here:

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.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		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. For obvious reasons, rate limiting any "call path" requests will not be allowed.					

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) Supported Functions The ECRF shall support each of the following items. Describe how the solution meets or exceeds each of the requirements below:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 49	<p>Bidder Response:</p> <p>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 ECRF has been supporting production Next Generation 9-1-1 call routing solutions since 2009, and the technology core has been supporting wireless and VoIP 9-1-1 call routing since 2003.</p> <p>The 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.</p> <p>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.</p> <ul style="list-style-type: none"> • Location error identification. The 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 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. 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 validations include road centerline, address point, and polygon for each data upload. <p>Features with critical errors cannot be loaded into the AT&T ESInet 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.</p> <ul style="list-style-type: none"> • Critical Errors: 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. <ul style="list-style-type: none"> ○ 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. 	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

<ul style="list-style-type: none"> ○ 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 <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>				
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

<p>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.</p> <p>Routing of calls based on geographic coordinates, geodetic shapes and civic addresses: For expediency during call processing, the geodetic location, if available, is utilized by the ESRP for routing determination of using a point-in-polygon lookup. Latitude and longitude (XY) circle and sphere are the geodetic shapes currently supported. Other geodetic shapes will be considered in future developments as markets demand. Routing and other services can also be determined based on civic address when geodetic locations are unavailable.</p> <p>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.</p> <p>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.</p> <p>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 are not the responsibility of the ECRF provider.</p> <p>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 AT&T ESInet 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.</p> <p>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.</p>				
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

<p>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.</p> <p>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.</p> <p>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 AT&T Spatial Interface.</p> <p>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.</p>				
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

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			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 50	<p>Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) User Interface and Provisioning Define bidder's method for:</p> <ol style="list-style-type: none"> 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			
	<p>Bidder Response:</p> <p>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 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 and re-projected, if necessary, to comply with the World Geodetic System 1984 (WGS84) datum 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.</p> <p>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.</p> <p>GIS data is submitted to the AT&T ESInet via the web-based SI portal. The portal provides secure GIS file transfer. 9-1-1 Authorities can maintain their local database schema and configure database changes using the attribute field mapping tools. The SI portal provides:</p> <ul style="list-style-type: none"> • Secure file transfer via the SI portal using secure two-factor authentication • Updates submitted to the SI will be comprised of one or more complete feature classes • GIS file format support for File Geodatabase and Shapefile • Automated schema change detection and error notification • Attribute field mapping configuration driven by the 9-1-1 Authority/local data source • Automated email notifications for upload, error, and processing status • Logging of uploads and any associated errors and provisioning status (succeeded/failed) • GIS data upload and validation report retrieval 				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Data validations include Gap/Overlap detection, reporting and error logging
- A configurable threshold for triggering gap and overlap alarms/reports

The 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 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.

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 logs errors and 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 AT&T ESInet 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

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.

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Additional ECRF Features

- 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.
- 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.
- standard.
- 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.

Architecture and Availability

The AT&T ESInet 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 six 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 utilize 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 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. 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.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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				
	<p>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.</p> <p>Bidder Response:</p> <p>At the State's discretion, the AT&T ESInet 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:</p> <ul style="list-style-type: none"> • 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." <p>AT&T ESInet ECRFs and LVFs can be deployed to support both approaches.</p> <p>Using the coordinated, intergovernmental approach, coverage areas for any other ECRFs or LVFs would be provisioned into the AT&T ESInet ECRF and LVF, and the AT&T ESInet 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.</p> <p>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 AT&T ESInet™ ECRF and LVF can potentially be utilized as a statewide or multi-state parent system to support this task.</p> <p>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, AT&T 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.</p> <p>AT&T 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.</p>	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Emergency Call Routing Function (ECRF) Forest Guide Provide explanations of any tradeoffs between aggregations of data at higher-level ECRFs versus the use of Forest Guides (as defined in NENA-INF-009.1-2014) to refer requests between ECRFs that possess different levels of data. As part of that explanation, provide details on how the appropriate ECRF/LVF data will be managed and provisioned for use in overload and backup routing scenarios in the current environment, and any dependencies that might impact provisioning.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 52	<p>Bidder Response:</p> <p>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.</p> <p>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.</p> <p>Either scenario is acceptable and meets the NENA guidelines and is supported by RFC 5222.</p> <p>It is arguable that the latter scenario is more efficient. Regardless, the AT&T ESInet 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.</p> <p>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</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 53	Next Generation Core Services Elements (NGCS) Location Validation Function (LVF)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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 AT&T LVF will be a public-facing LVF provisioned for use by service providers outside the ESInet. Since PSAP access to validate locations will be limited, 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.					

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 54	Next Generation Core Services Elements (NGCS) Location Validation Function (LVF) LVF Description				
	<p>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.</p> <p>Bidder Response:</p> <p>As part of the AT&T ESInet i3 solution, the Location Validation Function (LVF) is available to TSPs operating in the region via the LoST protocol (RFC 5222). This will allow them to pre-validate customer records against the GIS data to ensure that the civic addresses are 9-1-1 valid and will route and plot properly.</p> <p>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.</p> <p>Since the ECRF and LVF share a common code base, the customer is ensured that a location that has passed LVF validation will also route properly when the civic location element is presented to the ECRF because the exact same logic is used for both purposes. This assumes the LIS operator properly provisions their LIS with the subscriber's location.</p> <p>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.</p> <p>It is anticipated that when carriers first attempt to communicate with the LVF, problems may occur, even though the LVF fully meets the requirements defined in RFC 5222. Therefore, AT&T has developed a LoST interworking specification which identifies the specifics of AT&T's implementation along with LoST Request and Response examples to aid the carriers with their LVF client implementations.</p> <p>The AT&T ESInet LVF is secure. In lieu of the NENA PSAP Credentialing Agency (PCA), which does not exist at this time, AT&T will issue digital certificates to LVF clients for authenticated access to the LVF.</p> <p>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.</p> <p>Note that any User Interface or LoST client required to interact with the LVF will be the responsibility of the Carrier making the LVF LoST requests.</p>	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

NGCS 55	Next Generation Core Services Elements (NGCS) Location Validation Function (LVF) Location Validation The LVF shall be available to validate civic locations at the time a wireline device is ordered— e.g., Service Order Interface (SOI) validation—when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB shall be allowed to periodically revalidate the civic location information against the GIS data contained within the LVF. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
Bidder Response: The LVF is available for civic location validations and subsequent revalidations for authorized LVF clients. It is the responsibility of the LIS / LDB operators to validate and periodically revalidate their subscriber records using the LVF.					

Any additional documentation can be inserted here:

NGCS 56	Next Generation Core Services Elements (NGCS) Location Validation Function (LVF) High-Availability Design The LVF shall support all functionality as defined in NENA-STA-010.2-2016, shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability, and shall be provisioned with the same data as the ECRF. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
Bidder Response: The standard LVF utilized for service provider validation of their subscriber records is provided in a 99.999+% environment due to the provisioning nature of the LVF. It is implemented the same way the ECRF is, but is only available from two geodetically diverse locations, each with redundant processing elements. 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:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
Bidder Response: The AT&T ESInet LVF will be a public-facing LVF provisioned for use by service providers outside the ESInet.					

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) Location Validation Function (LVF) User Interface and Security Describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined in NENA-STA-010.2-2016, with particular attention to: 1. the arrangement of the proposed components; 2. user interface and features; 3. and security aspects.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 58	<p>Bidder Response:</p> <p>As part of the AT&T ESInet i3 solution, the Location Validation Function (LVF) is available to TSPs. It utilizes the LoST protocol (RFC 5222), which is a machine-to-machine interface that will allow service providers to pre-validate customer records against the state's GIS data to ensure that the civic addresses are 9-1-1 valid and will route and plot properly.</p> <p>Since the ECRF and LVF share a common code base, Nebraska is ensured that a location that has passed LVF validation will also route properly when the civic location element is presented to the ECRF because the exact same logic is used for both purposes.</p> <p>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.</p> <p>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.</p> <p>It is anticipated that when carriers first attempt to communicate with the LVF, problems may occur, even though the LVF fully meets the requirements defined in RFC 5222. Therefore, AT&T has developed a LoST interworking specification which identifies the specifics of AT&T's implementation along with LoST Request and Response examples to aid the carriers with their LVF client implementations.</p> <p>The AT&T ESInet LVF is secure. In lieu of the NENA PSAP Credentialing Agency (PCA), which does not exist at this time, AT&T will issue digital certificates to LVF clients for authenticated access to the LVF.</p> <p>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.</p> <p>Note that any User Interface required to interact with the LVF will be the responsibility of the service provider making the LVF LoST requests.</p>	X			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS) Spatial Interface (SI) SI Description	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 59	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>AT&T 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:</p> <ul style="list-style-type: none"> • NG9-1-1 GIS data compliancy checks • Ongoing GIS data accuracy validation (QA/QC) • GIS data error reporting • Provisioning to i3 systems (ECRF/LVF) <p>The SI undergoes 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 utilized.</p> <p>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).</p> <p>Section 4.6 of STA-010.2 states the following:</p> <p>"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."</p> <p>While the SI provides a consistent means to update the ECRF and LVF, a means to update other vendor's 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.</p>				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

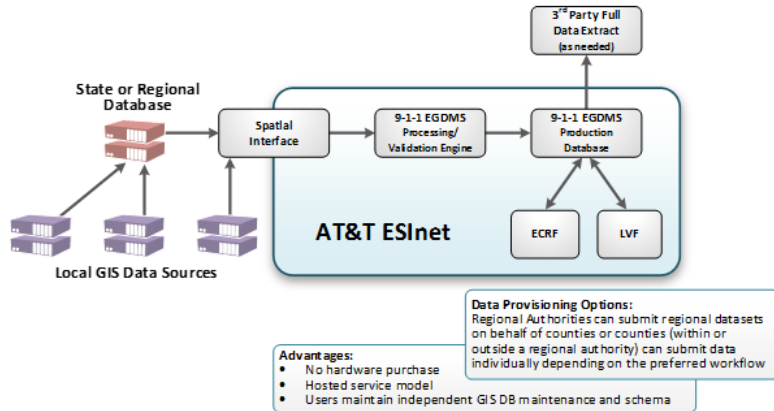


Figure 27: Spatial Interface

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 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:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 60	<p>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.</p>	X			
	<p>Bidder Response:</p> <p>The SI will normalize the GIS data, converting it into a consistent format, which will meet the ECRF/LVF Lost protocol requirements.</p> <p>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).</p> <p>Section 4.6 of STA-010.2 states the following:</p> <p>"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.</p> <p>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.</p> <p>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.</p>				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		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. 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 AT&T ESInet 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 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. <ul style="list-style-type: none"> • 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. 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

- 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 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:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 62	<p>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 D) 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.</p> <p>Bidder Response:</p> <p>AT&T 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. 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).</p> <p>The SI provides:</p> <ul style="list-style-type: none"> • NG9-1-1 GIS data compliancy checks • Ongoing GIS data accuracy validation (QA/QC) • GIS data error reporting • Provisioning to i3 systems (ECRF/LVF) <p>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 AT&T ESInet GIS data model, without any adjustment to customer’s data model. Unless the local data model changes, this is a one-time operation. 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.</p> <p>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 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.</p> <p>The GIS layers supported include:</p> <ul style="list-style-type: none"> • 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. 	X			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none"> • 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:

	Next Generation Core Services Elements (NGCS)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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.	X			
NGCS 63	Bidder Response: Currently, the AT&T LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can support the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or gateway mobile location center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols. AT&T's Location Database Services (ALDS) provides a suite of feature rich services that allows for the eventual replacement of legacy ALI services. AT&T Location Database Services, in conjunction with AT&T's Emergency Call Routing Services, provides all the necessary services to eliminate any need for a fully featured i3 end point to interface with a legacy ALI database. AT&T ESInet includes the LDB service. Prior to PSAPs migration onto the system, AT&T will work with the PSAPs to load their MSAGs onto the AT&T ESInet. AT&T will also work on behalf of the PSAPs with the OSPs to build a database that matches the current Legacy ALI DB providers database. Once all the MSAG and OSP ALI Data has been loaded into AT&T ESInet, PSAPs can be migrated to AT&T ESInet. At point, data loaded in the AT&T LDB will be used. The PSAPs and OSPs will now provision data onto the AT&T LDB and no longer will be required to provision the legacy LDB. AT&T ESInet can also support LDB-to-LDB connectivity should an LDB provider need connectivity for transferring calls between ESInets.				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 64	<p>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.</p> <p>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.</p> <p>Bidder Response:</p> <p>AT&T’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. AT&T Location Database Services, in conjunction with AT&T’s Emergency Call Routing Services, provides all the necessary services to eliminate any need for a fully featured i3 end point to interface with a legacy ALI database.</p> <p>The AT&T 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.</p> <p>While the AT&T 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.</p> <p>The AT&T 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.</p> <p>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.</p> <p>Currently, the LDBs used for the AT&T ESInet 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.</p> <p>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 AT&T ESInet platform buildout and acceptance.</p>				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

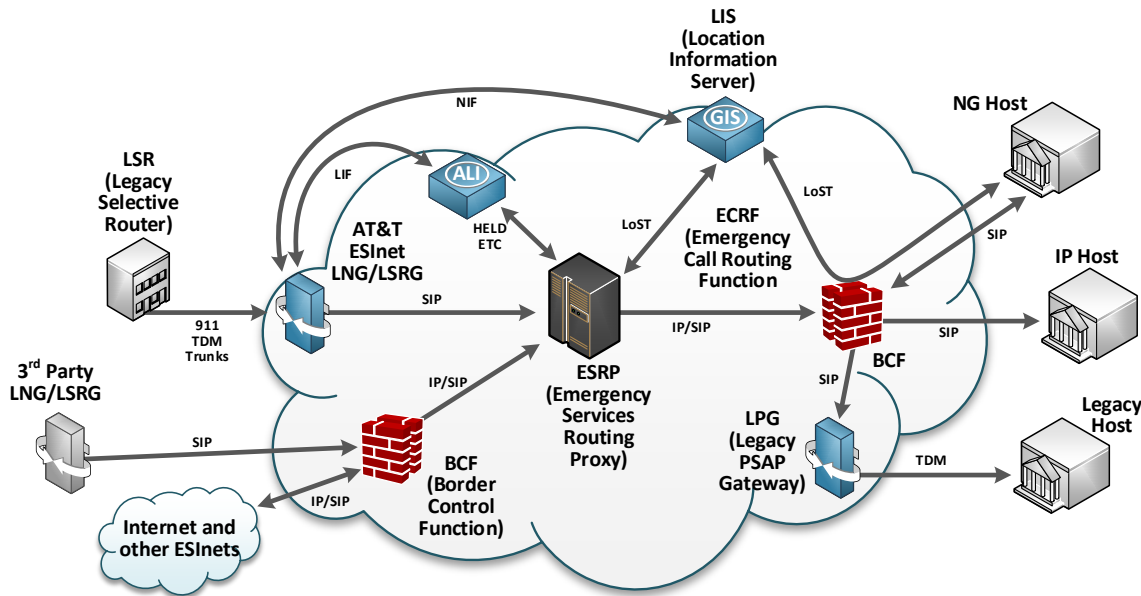


Figure 28: i3 Transitional State with Location Database Components

Support for LIS Functionality and NENA i3 Interfaces

The AT&T ESInet 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 Credentialing Agency (PCA), once available. Until that time, AT&T 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 AT&T ESInet, including access to the LIS interface, ADR interface, and ECRF.

Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

During carrier transition to NENA i3 compliance, AT&T will maintain the HELD interface into the ALI platform to simultaneously support legacy PSAPs and i3 PSAPs. The HELD interface into the AT&T 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, AT&T 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 AT&T ALI system until all PSAPs in the State are served by i3-compliant TSPs. 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 AT&T 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 AT&T 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.

The AT&T 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 AT&T 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.

AT&T 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

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

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. 9-1-1 NET is accessed via a web-based portal following secure sign-on.

Synchronization of GIS and LDB

The AT&T ESInet 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.

AT&T 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, AT&T 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 the AT&T Spatial Interface and simultaneous support for NG9-1-1 GIS and legacy address standards.

AT&T'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 TSP provisioning and ALI
- Full i3 readiness – Streamlines deployment to AT&T ESInet 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 AT&T LVF.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

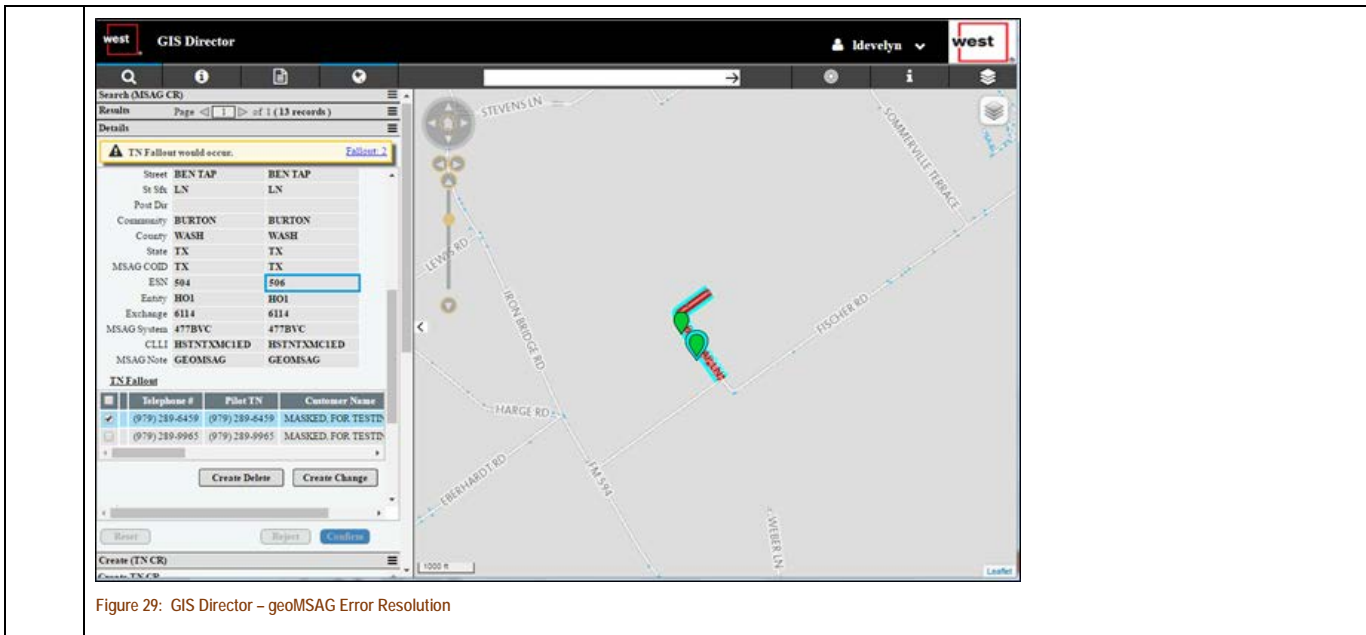


Figure 29: GIS Director – geoMSAG Error Resolution

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			
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			

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

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			

	Next Generation Core Services Elements (NGCS)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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.	X			
NGCS 65	Bidder Response: 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:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Discrepancy Reporting 1. Provide details regarding the proposed solution’s report functions for notifying PSAPs any time a discrepancy is detected concerning the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, explain how a report will be sent for the purpose of reporting the discrepancy to multiple responding PSAPs, as determined by the Commission. Discrepancy reporting is outlined in Section 4.7 of NENA-STA-010.2-2016. 2. Describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 66	<p>Bidder Response:</p> <p>AT&T has a full featured solution for Discrepancy reporting for legacy and Next Generation PSAPs. Once the NENA requirements are hardened AT&T will review for buildability and market demand. It is expected that i3 compliant discrepancy reporting will be a future development.</p> <p>Until such time, the AT&T ESInet 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.</p> <p>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 AT&T ESInet ESRP and PRF provide safeguards around how routing policies are entered to help ensure that only valid policies are configured to prevent the need for discrepancy reporting. Policies and rules are tested prior to enabling in production. Fall-back routing (e.g., default trunk group routing) due to policy rules inaccurate data such as No Record Found is reported via a 9-1-1 NET ALI DR for research and correction.</p> <p>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: incorrect GIS provisioned to the ECRF/LVF, incorrect policy routing rules, etc.</p> <p>Access to 9-1-1 NET requires two-factor authentication for all users.</p> <p>The following list, as provided in STA-010.2, lists the types of discrepancies that will need to be addressed in i3. 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.</p> <p>The following list, as provided in STA-010.2, lists the types of discrepancies that will need to be addressed in i3. 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.</p> <ul style="list-style-type: none"> • The LIS needs to file a Discrepancy Report on the LVF. • Customers with AT&T 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. 	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- 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 AT&T ESInet 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.
- The PSAP needs to file a DR on the GIS when issues are found in a map display.
- Not applicable for the services requested in this RFP.
- 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 AT&T 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.
- Future capability.
- 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
- Future capability.
- 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.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	<ul style="list-style-type: none"> 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. <p>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.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: AT&T's ESInet can support additional uses such as logging recorders. At all times 9-1-1 voice and location ESInet traffic will be designated as priority one. Secondly, AT&T will set up separate tunnels or "VRFs" for segmentation of additional traffic through the AT&T ESInet and will prioritize them using QoS and priority markings. Our process and ability to support additional statewide systems is itemized below: Additional network pathways between Nebraska PSAPs and Nebraska data centers are used to support additional Public Safety applications such as Logging Recorders, and CAD. <ul style="list-style-type: none"> The solution provides that Intrado routers and AT&T circuits are used to support the pathways. The solution will provide QoS queues. The customer is responsible for ensuring packets are appropriately marked before sending to the ESInet. 9-1-1 Call delivery will always be the priority traffic on the ESInet Customer is responsible for providing accurate circuit sizing requirements for their application flows Customer is responsible for interfacing additional systems to the ESInet infrastructure All traffic traversing the ESInet is encrypted and will inherit the same high availability and redundancy used for emergency call traffic AT&T ESInet supports the statistical data gathering of ESInet/NGCS logs via ECaTS. AT&T customers today utilize ECaTS and the AT&T solution is tested and verified to deliver i3 logs to ECaTS for NGCS-specific elements such as ESRP, ECRF, and others.				

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) Event Logging and Management Information System (MIS) Event Logging Description	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	<p>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.</p>	X			
NGCS 68	<p>Bidder Response:</p> <p>The AT&T ESInet 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.</p> <p>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.</p> <p>A standard reporting suite provides reports through a web-based interface.</p> <p>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.</p> <p>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 ESInet entry point to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics.</p> <p>AT&T's standard reporting suite provides the following reports through a web-based interface.</p> <ul style="list-style-type: none"> • 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. • Bridge Call Summary. Provides metrics for calls bridged in or out by bridge type (fixed, selective, manual, refer). Call detail is available for each bridged call. • 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 				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	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			
NGCS 69	Bidder Response: 1. The AT&T solution will integrate with the PSAP's call-handling MIS solution (ECaTS) to provide the PSAPs with a complete, end-to-end view of the call. No additional equipment to provide this functionality is required at the PSAP. AT&T's ESInet is set up to send i3 logs to the i3 log collectors maintained by ECaTS. All i3 logs are sent to ECaTS and they segregate this traffic by PSAP to provide the PSAP with their i3 reports 2. The AT&T Customer Management Portal (CMP) provides participating PSAPs and approved personnel 24x7x365 access to a reporting suite including call detail records and AT&T ESInet Routing and Location Data Management reports through a secure, web-based portal. Access is provided to authorized users via two-factor authentication. 3. Based on the Question and Answer feedback that the existing ECaTS contract will be used by the State to create the i3 reports, it is assumed no additional equipment, software licensing agreements, or interfaces will need to be supplied to allow the PSAPs and the Commission to access this data. AT&T is currently set up to send i3 logs from the ESInet solution to the ECaTS servers that collect and correlate this data. Should the State need to purchase additional ECaTS reports and services, AT&T as a reseller of the ECaTS services can assist the State should they choose to change their procurement procedures.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

	Next Generation Core Services Elements (NGCS)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 70	<p>Event Logging and Management Information System (MIS) Access to Event Logging Data</p> <p>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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> 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			
	<p>Bidder Response:</p> <p>1. The PSAPs and Commission can gain access to event logging data through the web-based AT&T 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 statistics, while another user may be provided authorization to view all PSAPs in a county, region, state, or other appropriate grouping.</p>				

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

AT&T will coordinate with ECaTS, the State, and the PSAPs to deliver event logging data to the ECaTS solution.

2. The AT&T ESInet service provides an i3 logging capability per the NENA STA-010.2 specification. AT&T can support near real-time log delivery and web service interfaces for log retrieval from authorized clients. The AT&T ESInet 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 AT&T 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 selective router to be delivered to the PSAP. This event data tracking by functional element allows for call diagnostics.

Reporting

AT&T'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.
- **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

The information below shows the required reports to the corresponding AT&T provided report:

- Timing = Event Count Reports per Hour
- Call-delivery time = Event Setup Time
- Call-processing time between elements = AT&T will provide i3 logs to ECaTS. ECaTS reports show processing times between elements
- Volumes = Event County by Routing Reason and Destination

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

- Call volumes by call type = Event Count by Type
- Alternate-routed calls = Event Count by Routing Reason and Destination
- Text-to-911= Event Count by Type
- All NGCS element usage volumes = AT&T has internal reports server, network capacity and utilization; AT&T i3 logs sent to ECaTS can provide details on each NGCS element utilized, it is the assumption based of answers from the Commission that ECaTS will provide this report using the i3 logs provided by AT&T
- Bandwidth/trunk utilization = Event Count by Incoming Trunk Group
- Calls per trunk = Event Count by Incoming Trunk Group
- Trunk utilization = PSAPs can view near real-time trunk utilization using the “PSAP Call, IP Contact, and Trunk Status” screen in the Customer Management Portal
- Circuit utilization = PSAPs can view near real-time trunk utilization using the “PSAP Call, IP Contact, and Trunk Status” screen in the Customer Management Portal

The AT&T 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.

CMP also provides the PSAP with the ability to download the audio stream associated to a call. The PSAP can either download only the caller's audio or the conference audio of all the participants (up to 10). Both types of audio streams can be used for troubleshooting the service. Audio recordings are available to download for up to 14 days.

For ALI management, users can create customized reports and perform real-time data and trend analysis, including graphing, based on daily data updates. AT&T 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. AT&T 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.

AT&T has provided some additional management reports that would be available to the State below.

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1



Figure 30: PSAP Resource Availability and Statistics

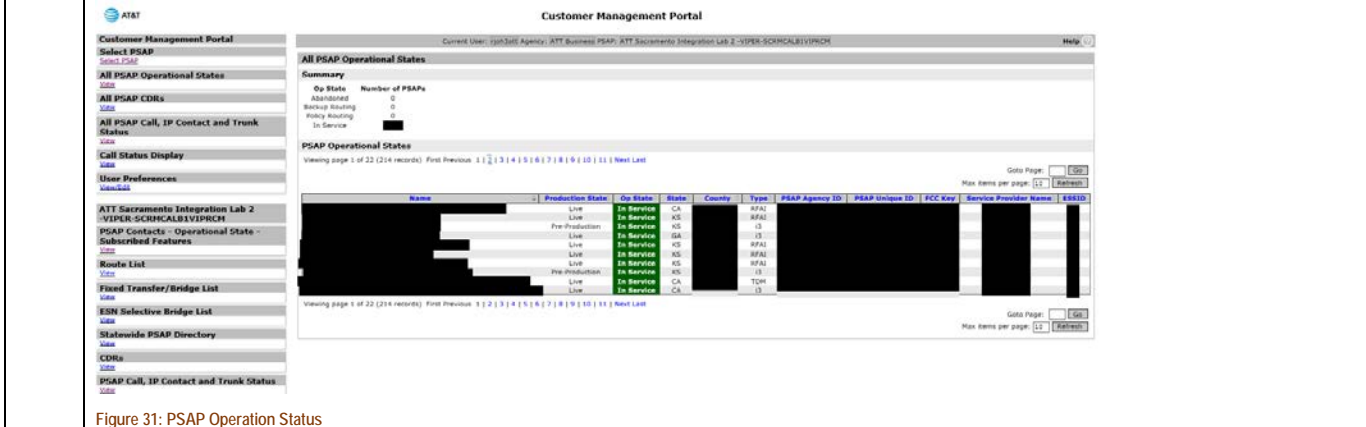


Figure 31: PSAP Operation Status

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

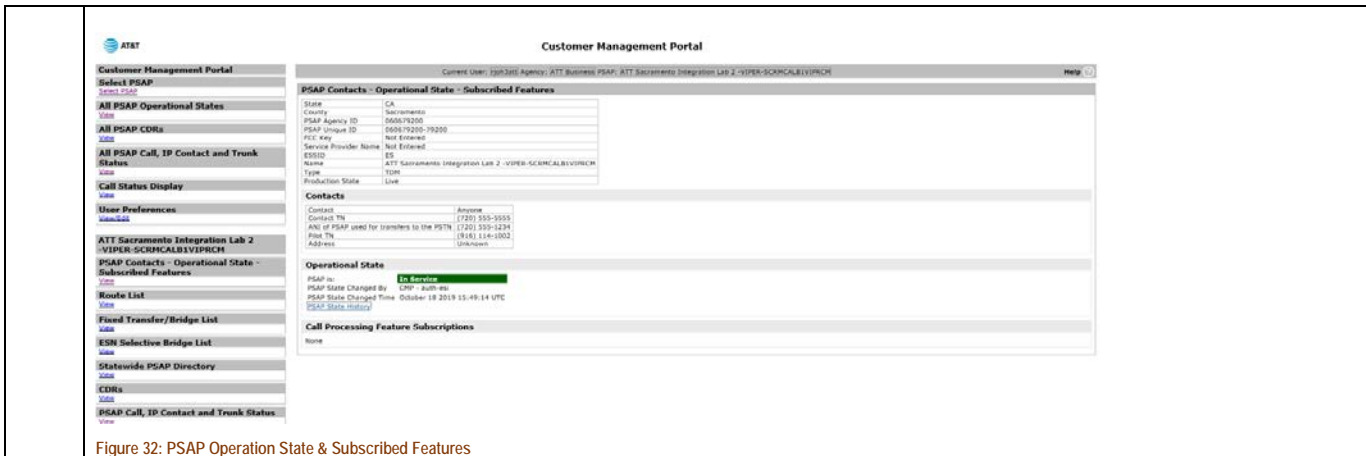


Figure 32: PSAP Operation State & Subscribed Features

Any additional documentation can be inserted here:

		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 AT&T ESInet service provides an i3 logging capability per the NENA STA-010.2 specification. Additionally, i3 logs from all ESInet i3 components will be available per the NENA STA-010.2 specification. Third-Party Certification Fees The AT&T ESInet service includes third-party certification fees.				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

NGCS 72	Next Generation Core Services Elements (NGCS) Network Time Protocol (NTP) and Time Source Bidder's solution shall sync with existing time sources to maintain consistent time stamps across the network and systems. Describe how bidder's solution complies with this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
Bidder Response: The AT&T ESInet solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the NTP time services interface, accurate to 1 millisecond. AT&T will work with the Commission and PSAPs to assess how to support interoperability with existing time sources.					

Any additional documentation can be inserted here:

NGCS 73	Next Generation Core Services Elements (NGCS) Network Time Protocol (NTP) and Time Source Master Clock Description The bidder shall provide redundant, resilient network-attached Stratum 2 time sources ("master clocks") capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
Bidder Response: AT&T ESInet processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the AT&T ESInet domain. Time stamps are included in logs, system traces, and user reports.					

Any additional documentation can be inserted here:

NGCS 74	Next Generation Core Services Elements (NGCS) Network Time Protocol (NTP) and Time Source Accessibility by PSAP Equipment The master clock time source(s) shall be accessible to the PSAPs for synchronizing call-handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the NTP for maintaining system clock accuracy. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
Bidder Response: AT&T ESInet processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the AT&T ESInet domain. PSAPs will be offered use of the NTP service to synchronize the clocks on their 9-1-1 CPE, workstations, etc. The AT&T ESInet 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:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) NG911 Application Integration Bidder shall describe other NG911 applications, additional data integrations, and personal safety applications that may be integrated with the NGCS solution. The bidder’s system must be capable of integration with Additional Data Repositories (ADR), Identity-Searchable Additional Data Repositories (IS-ADR) or commercial third-party LIS, as described in NENA STA-010.2-2016, within two years of the deployment of the first PSAP. Describe how the solution will accomplish integration, information storage, and use/transmission of data to PSAP CHE.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 75	<p>Bidder Response:</p> <p>AT&T and its partners have had 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. AT&T is excited to have the opportunity to fully understand and implement additional lifesaving technologies within its NGCS Infrastructure. AT&T looks forward to working with the State and the OSPs on how to deploy those technologies within a redundant and reliable next generation solution.</p> <p>AT&T ESInet will interwork seamlessly with OSPs by supporting and adhering to NENA and ATIS standards. 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 (AT&T). If a location by reference is provided, the AT&T ESInet will query for location using the HELD protocol as required. The AT&T ESInet 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.</p> <p>Integration with Additional Data Repositories (ADR), Identity-Searchable Additional Data Repositories (IS-ADR) or Commercial Third-party LIS</p> <p>There are two types of solutions listed within the requirement above. Typical integration will be discussed for each of the solutions</p> <ol style="list-style-type: none"> 1. LIS/ADR - Carrier Provided <ol style="list-style-type: none"> a. 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 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, AT&T 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. 2. LIS/ADR – Third Party <ol style="list-style-type: none"> a. 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 911 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 AT&T ESInet as the path to the 3rd party providers ADR, some other requirements will need to be determined. Those requirements include the network path from the AT&T ESInet core infrastructure to the 3rd party 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. 	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

Information Storage

The carrier approved LIS/ADR is used as the primary source of routable and displayable 911 location information. All information provided by the OSP used for routing by the AT&T Core ECRF and transmitted to the PSAP is stored and available in the AT&T ESInet CMP. Additionally, any re-requests and updated information communicated by the carrier provided LIS/ADR is also available for retrieval through the AT&T CMP.

Leveraging the redundancy, reliability and security in the ESInet, AT&T 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 AT&T system does not capture the elements of those direct third party to PSAP ADR/LIS messages. AT&T will, of course, continue to monitor the network path over which the ADR/LIS 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 AT&T 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 AT&T ESRP – Terminating ESRP Interface for ESInet Specification v1.2 document included with this response contains a 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.

- AT&T ECRF-LoST Interface Specification v1.4
- AT&T LIS Held Interface Specification v1.3.1
- AT&T ADR Additional Data Interface Specification v1.3

Please refer to Exhibit 6 for copies of these documents.

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

		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. The AT&T ESInet 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 AT&T ESInet implementation and can transition to utilize 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 ESInet ESRP functions and benefit from a common and centrally controlled set of PSAP routing policies, such as PSAP Abandonment/Evacuation routing. The AT&T/Intrado-managed TCC has interconnections to all current TCC providers and their respective customers. Carrier initiated emergency text messages can be aggregated at the AT&T/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 utilizing ESInet transport. “SMS to 9-1-1” industry defined service delivery mechanisms are: <ul style="list-style-type: none"> • TTY calls are sent into the AT&T ESInet™ 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 – AT&T has established redundant connections between the AT&T/Intrado-managed TCC and the AT&T ESInet. When a text is initiated, the text will traverse the ESInet infrastructure. The ESRP/PRF will be used to determine and route any text 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. The service includes the following elements: <ul style="list-style-type: none"> • Redundant interconnection with TCC • Redundant, secure IP connectivity between the end user PSAP and AT&T ESInet • Support for the TCC transfer of a text session to another PSAP • SIP-based communication protocol compliant to existing standards, NENA i3 and ATIS J-STD-110 MSRP protocol • Ability to display Request Initiator (RI) cell sector location and Carrier Identifier as an in-band message • Log retention of text dialogues 				

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

The following diagram illustrates "SMS to 9-1-1" interconnection between the Intrado TCC, AT&T ESInet™ and each of the three "SMS to 9-1-1" service delivery types.

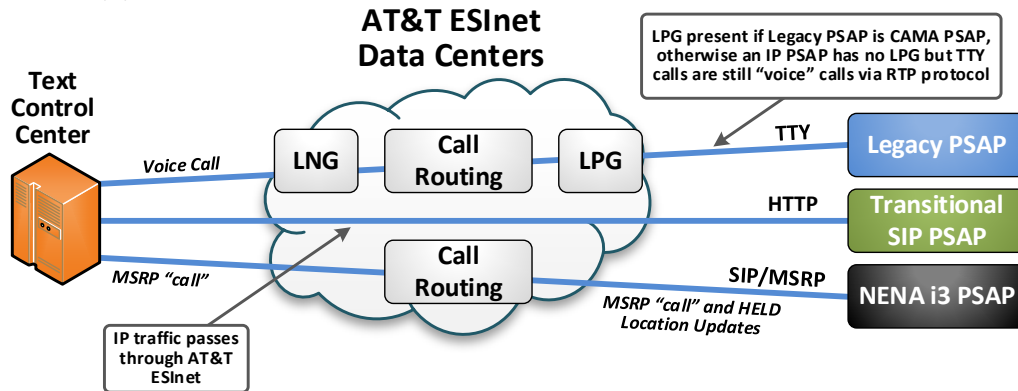


Figure 33: AT&T ESInet Text to 9-1-1 High Level Diagram

The following is a sample message flow:

- An RI sends a text message to 9-1-1.
- The text request is routed through the wireless carrier's network to the TCC.
- TCC determines location of the RI via a Mobile Location Protocol (MLP).
- TCC determines the ESInet by using the cell sector or caller's latitude and longitude and sends the call to the AT&T ESInet™ or PSAP Web Browser interface.
- If using a TTY or integrated solution, the AT&T ESInet determines PSAP by querying the ECRF. The AT&T ESInet sends the call to the PSAP where tones are recognized and converted into displayable characters.

2. For location, a call will include either location-by-value or location-by-reference when passed to the NG Service Provider. If a location-by-reference is provided, the system will query for location using the HELD protocol as required. The system 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.

If location-by-value is provided, that value will be passed to the PSAP.

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

Next Generation Core Services Elements (NGCS)		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 77	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: <ol style="list-style-type: none"> 1. AT&T can support the make-busy functionality. AT&T ESInet will allow 9-1-1 calls to be re-routed to a pre-provisioned alternative destination. This can be accomplished via the AT&T Resolution Center or the PSAPs may also utilize the Customer Management Portal. This provides the Commission with the ability to invoke abandonment themselves for a specific PSAP. Alternate routing plans are defined as part of the implementation process. 2. The AT&T Solution that includes AT&T ESInet supports ring-down functionality. As ringdown requires connections to each physical PSAP and not the CPE hosts, AT&T would require more information to properly scope this for the State of Nebraska as their solution provides separate CPE with capabilities that are unknown at this time. AT&T would need to work with the PSAPs to determine which agencies need ringdown, how many ringdown lines they will need, and what use cases these will be used in. Once scope is provided, AT&T can provide pricing to the PSAPs. 3. The AT&T 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. AT&T has enabled PSAPs to transfer calls to PSAPs both on-net (connected to AT&T ESInet) and also PSAPs off-net (connected to a L-SR or ESInet). 				

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 78	<p>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:</p> <ul style="list-style-type: none"> a. SIP calls b. NGCS call delivery c. Web services d. All baseline media and multimedia (as described in NENA STA-010.2-2016, Section 4) e. NTP time services interface, accurate to 1 ms f. Transport layer security g. Discrepancy reporting <p>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.</p> <p>Bidder Response:</p> <p>The AT&T ESInet solution supports PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the following:</p> <ul style="list-style-type: none"> • SIP call • NGCS call delivery • Web services • All baseline media and multimedia as described in NENA STA-010.2-2016, Section 4 • NTP time services interface, accurate to 1 millisecond • Transport layer security • Discrepancy reporting • HELD and LoST queries and responses, including queries for supplemental location to a third-party LIS hosted by commercial providers of additional data services • Queries to and responses from additional data repositories (ADR), including queries to ADRs hosted by commercial providers <p>The AT&T ESRP – Terminating ESRP Interface for ESInet Specification v1.2 document contains a detailed description of the functionality of the PSAP interfaces, specifically including the user interface, additional features, and security aspects. We can provide this document upon request and under separate NDA. Specifications for the following interfaces are also available upon request and under NDA.</p> <ul style="list-style-type: none"> • AT&T ECRF-LoST Interface Specification v1.3 • AT&T LIS Held Interface Specification v1.2 • AT&T CIDB Additional Data Interface Specification v1.1 	X			

Any additional documentation can be inserted here:

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

	Next Generation Core Services Elements (NGCS) PSAP Interfaces and Backroom Equipment Requirements Support of Call Handling Equipment (CHE) Platforms	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 79	<p>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.</p> <p>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.</p> <p>3. Describe the physical interface handoff required at the PSAP CHE demarcation point.</p> <p>Bidder Response:</p> <p>1. AT&T Labs has worked to validate that the AT&T ESInet is CPE-agnostic. AT&T has completed ESInet interoperability testing with multiple vendors including Intrado, Motorola, and Solacom call handling equipment for i3. The versions of CPE listed below are the latest version of CPE with manufacturer's software.</p> <ul style="list-style-type: none"> • Intrado VIPER Release 5.1 and VIPER 7 • Motorola Vesta Release 7.2 • Solacom Guardian 19.2.4 <p>Today, AT&T ESInet is deployed using i3 call delivery with Intrado VIPER and Motorola VESTA with planned Solacom Guardian deployment in progress with a completion in 2020.</p> <p>AT&T publishes RFAI and T-ESRP interface specifications for CPE vendors. AT&T and Intrado also support cooperative interoperability testing for RFAI and i3.</p> <p>AT&T NG Routing RFAI service supports the following CPE types:</p> <ul style="list-style-type: none"> • Intrado VIPER • Airbus/Motorola Vesta • Solacom • Comtech xT911 • Central Square <p>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.</p> <p>AT&T and Intrado offer an interoperability lab-to-lab test program for i3 (T-ESRP) vendors. Ongoing discussions are occurring with Call Handling vendors to encourage testing in the AT&T/Intrado Lab environment for i3 protocol verification. Verification testing is provided at no additional charge to Call Handling vendors. AT&T/Intrado have developed standard test cases and testing methodology that meets the industry i3 standards.</p> <p>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. Connectivity for this method of testing uses internet VPN and follows a suite of suggested test cases within a defined</p>	X			

**Attachment “C”
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1**

testing window. Intrado would assist with 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.

The Intrado *i3 CPE Testing Service Guide* provides the following required and recommended test cases to validate the ability to receive, answer, transfer, conference and terminate calls and/or text (where applicable) with voice and data. These test cases are for Lab-to-Lab interoperability testing.

Test Case #	Test Case Description	Required or Recommended
1.1.2	i3 invite with PIDF-LO+ADR LbV only	Recommended
1.1.3	i3 invite with No location references (bad/no ANI results in voice only call)	Required
1.1.3.1	Verify Subscribe Notify from T-ESRP (Conference)	Required
1.1.4	Verify Subscribe Notify between ESRP and T-ESRP (Conference)	Required
1.1.5	Verify Subscribe Notify between ESRP and T-ESRP (Refer bridges)	Required
1.1.6	Verify 18x Response (with SDP [early media])	Required
1.1.7	Verify PRACK/ACK for 18x	Required
1.1.8	Verify 200 ok with SDP	Required
1.1.9	Verify Wireline Call	Required
1.1.10	Verify Wireless Call with Point, Circle, Sphere geometry	Required
1.1.11	Verify VoIP Call	Required
1.1.12	Verify MSRP Text Call	Recommended
1.1.13	Re-Invite from ESRP	Required
1.1.14	Re-Invite from T-ESRP	Required
1.1.15	Verify TDD/TTY call	Required
2.1.0	Verify initial HELD/LIS location query from T-ESRP	Required
2.1.1	Verify initial ADR query(s) from T-ESRP	Recommended
2.1.2	Verify Police LoST query from T-ESRP (with display text)	Required
2.1.3	Verify Fire LoST query from T-ESRP (with display text)	Required
2.1.4	Verify EMS LoST query from T-ESRP (with display text)	Required
2.1.5	Additional LoST Data-for a PSAP layer-additional layers	Recommended
2.1.6	Verify automatic HELD query after initial location	Recommended
2.1.7	Verify manual HELD query after initial location	Required
2.1.8	Verify manual HELD query after call hang-up	Recommended
2.1.9	Verify HELD/T-ESRP error processing (e.g. NRF)	Required
2.1.10	Verify LoST/T-ESRP error processing	Required
2.1.11	Verify ADR/T-ESRP error processing	Required
3.1.0	Verify mid call DTMF from caller	Required

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

4.1.0	Refer using URI from Police LoST query (SIP/TEL)	Required
4.1.1	Refer using URI from Fire LoST query (SIP/TEL)	Required
4.1.2	Refer using URI from EMS LoST query (SIP/TEL)	Required
4.1.3	Refer using URI from T-ESRP fixed bridge list (SIP/TEL)	Required
4.1.4	Refer using manual bridge request (TEL)	Required
4.1.5	Initial T-ESRP drops from bridge	Required
4.1.6	Initial T-ESRP drops newly added member from bridge	Required
4.1.8	Verify when T-ESRP is added to a bridge by another T-ESRP (with add/drop)	Required
4.1.9	Verify mid-call DTMF (T-ESRP bridges on a VRU) from the T-ESRP	Recommended
4.1.10	Verify Error Code on Bridge attempt (486 and 4xx,5xx)	Required
4.1.11	Verify that any EIDD received in a Refer is passed to the target of the Refer; if no EIDD-none is passed	Recommended
5.1.0	Verify T-ESRP disconnect	Required
5.1.1	Verify Caller disconnect	Required
6.1.0	Verify LoR call	Recommended
6.1.1	Verify LoR interaction with caller on hold	Recommended
7.1.0	Verify Abandon Call routing to T-ESRP	Required
7.1.1	Verify RNA Call Handling	Required
7.1.2	Verify Alternate Routed call to T-ESRP	Required
8.1.0	T-ESRP Busy (coordinated/segreated?)	Required
8.1.1	T-ESRP Internal Processing Error (coordinated/segreated?)	Required
9.1.0	Long Duration Call (up to 5 minutes)	Recommended
10.1.0	Options Heartbeat Monitor-Success	Required
10.1.1	Options Heartbeat Monitor-Failure	Required

3. Intrado supports the Ethernet port on the Terminating Router or the TDM port on the Legacy PSAP Gateway.
Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.			
	X			
	Bidder Response: AT&T ESInet supports call transfers via the PSTN network. AT&T also supports using 7/10-digit numbers for alternate routes should a PSAP want to failover to an administrative line if a catastrophic failure disables their CPE. AT&T Resolution Center can test these PSTN numbers prior to utilizing them using a Test Call function in the ESInet. This confirms the number is active, works through the system and is available on the PSTN network and is not an internal PBX number only			

Any additional documentation can be inserted here:

Attachment "C"
Option C
Technical Requirements
Public Service Commission ESInet
Request for Proposal Number 6264 Z1

OPTIONAL SERVICE

		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: AT&T and its partners have had 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. With the information available today, it seems as though alarm data and call center support would fit the NG mold well. In order to fully understand the support (and therefore financial) impacts, AT&T would need to know the interoperability requirements from the Alarm Provider, as well as the expectation for the end result from the PSAP. If the alarm companies provide either legacy TDM/ALI or i3 standard protocols, the integration would be seamless, and the call flow should be identical to that of a typical legacy and/or i3 call. If for some reason, the alarm company is unable to provide the voice and location information in an industry-standard format, additional resources would need to be expended to design, test and implement a non-standard solution. AT&T is excited to have the opportunity to fully understand and implement additional lifesaving technologies within its NGCS Infrastructure. AT&T looks forward to working with the Commission and the OSPs on how to deploy those technologies within a redundant and reliable next generation solution. AT&T can work through engineering requirements discovery with the Commission to develop a mutually agreed upon scope of work that would be priced separately upon completion of functional requirements analysis.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
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.	X			
	Bidder Response: Upon request by the Commission, Bidder will allow for network and validation by a third-party entity as mutually agreed upon.				



Proposed High-Level Project Plan

The State of Nebraska will benefit from working with a skilled AT&T Global Project Manager from the AT&T Public Safety Group. The AT&T Project Manager is directly responsible for the project implementation and can reach out to other AT&T organizations to help smoothly transform Nebraska's service from its current environment to an AT&T i3 ESInet. The State will benefit from the skills and experience of our Global Project Manager and Transformation Team.

We have included a high-level project plan and project schedule in the next section. All Project Plans are subject to negotiation and agreement with our customers. Upon contract award, AT&T will work with the State of Nebraska to develop an agreed upon implementation plan.

The Project Manager will be guided by the principles established by the Project Management Institute (PMI®) in order to plan, schedule, and implement project activities, meeting industry recognized standards of quality, reporting frequency, and control. Nearly 75% of the AT&T Global Project Management (GPM) team is comprised of Project Management Institute certified Project Management professionals (PMP). AT&T's Global Project Management experience includes both domestic and international projects with overall project volumes ranging from 100 to 17,000 sites. The average on-time performance (OTP) on a GPM led project is 98%.

The AT&T Project Manager will be responsible for multiple complex projects from conception through implementation, including:

- Manage project team members including independent contractors.
- Develop and implement project plans and design schedules.
- Identify risks and alternate course of action to ensure projects are completed within corporate objectives exceeding customer expectations.

Upon contract award, the AT&T Project Manager will engage team members throughout the AT&T organization to help ensure their commitment and understanding of the project requirements. The PM will schedule a kickoff meeting with the relevant jurisdiction 9-1-1 group and other required AT&T organizations. During the kickoff meeting, the PM will establish roles and responsibilities and reach a mutual agreement with the State on strategic objectives, plan of approach, priorities and timelines.

Using the information gathered during the meeting, the PM and the customer will create an integrated master work plan that will be used as the implementation





roadmap. Throughout the project, AT&T will focus on project planning and execution to help ensure a successful upgrade with minimal (if any) disruption to the customer's current Wireless/VoIP ESInet service.

Project Management Meetings

The AT&T Project Manager will conduct regularly scheduled project status calls with the relevant State of Nebraska parties and key AT&T stakeholders. Normally, these status calls are held on a weekly basis and cover the following topics

- Overall Project Status – Red/Yellow/Green
- Project Timeline and Key Milestones
- Issues log review
- Key Deliverables status

Also, during PSAP migration, the AT&T project manager will be available to discuss project-related elements with the State's primary project contact on an informal schedule. If it is determined that formal daily meetings are required, the PM will schedule those meeting with the key stakeholders.

Monthly stewardship meetings can be held by the AT&T Account Team and the PM to provide the State with a holistic view of ongoing program.

Project Management Tools

AT&T's experienced Program Managers, Project Managers, Service Delivery Managers, Installation Technicians, Solutions Engineers and other supporting groups have worked together on many successful installations. We are determined to provide each customer with an installation that will exceed expectations.

The NG 9-1-1 ESInet solution is an IP-based system that employs proven technology to deliver excellent 9-1-1 services. Given the mission critical nature of the network, greater safeguards are taken during installation, but from a practical point of view it is a network installation, and AT&T is able to leverage best practices of network installations to ensure success.

AT&T Project Managers will use the Microsoft suite of products to manage all projects as a standard operating procedure. Tools will include

- Microsoft Word





- Microsoft Excel
- Microsoft Project
- Microsoft Visio
- Microsoft Outlook

Project Management Methodology

The AT&T Worldwide Project Management Methodology is based upon the industry standard A Guide to the Project Management Body of Knowledge (PMBOK Guide®) Fourth Edition, produced by the Project Management Institute (PMI), as well as AT&T specific processes and procedures.

The characteristics of a project may be determined by many factors: strategic importance, size, scope, schedule, cost and duration, as well as many others. This methodology is scalable to accommodate all types of projects.

The Project Management Methodology utilizes a four-phase project life cycle:

- **Project Start Phase.** Recognition that a new project is being considered. During this phase, basic information is gathered, evaluated and based upon the information a decision is made to proceed with the project.
- **Project Plan Phase.** Establishing the project's approach and planning how to achieve the desired results and baselines for the project in terms of scope, schedule and cost.
- **Project Implementation Phase.** Implementing the Project Plan to produce the agreed upon deliverables, monitoring the project progress and ensuring that deliverables meet expectations.
- **Project Completion Phase.** Completing the project. Ensuring that the project was delivered as expected and ensuring that there is final/formal acceptance in order to close out the project.

These four phases of a project, plus the inputs and activities and deliverables key to the phases, comprise this methodology. Throughout each of the four distinct project phases, the five iterative process groups of Initiating, Planning, Executing, Monitoring and Controlling and Closing will be used. Each of the five processes is applied within each project phase. Often changes occur within the life cycle of a project and process groups must be repeated.





Schedule for the Lifecycle of this Project

Attached is a high-level Project Plan and Project Schedule.



Exhibit 5_Region and
PSAP Implementation

Cost Proposal

Please see the separate Cost Proposal for AT&T's pricing details.





II. Terms and Conditions

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

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

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:

1. If only one Party has a particular clause then that clause shall control;
2. If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;
3. If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

AT&T's Response:

Notwithstanding anything contained in this RFP to the contrary, AT&T Corp., on behalf of itself and its service-providing affiliates (AT&T) submits this RFP response (the Response) subject to the provisions of this Response. In that regard, please note that AT&T takes a general exception to the terms and conditions contained within or referenced to in this RFP document. This exception is taken regardless of whether AT&T has specifically responded to any individual provision in the RFP.





Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the **State of Nebraska** to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T’s Response to it.

A. General

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

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

1. Request for Proposal and Addenda;
2. Amendments to the solicitation;
3. Questions and Answers;
4. Bidder’s proposal (Solicitation and properly submitted documents);
5. The executed Contract and Addendum One to Contract, if applicable; and,
6. Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

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

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





B. Notification

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

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

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

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

C. Buyer's Representative

The State reserves the right to appoint a Buyer's Representative to manage (or assist the Buyer in managing) the contract on behalf of the State. The Buyer's Representative will be appointed in writing, and the appointment document will specify the extent of the Buyer's Representative authority and responsibilities. If a Buyer's Representative is appointed, the Contractor will be provided a copy of the appointment document, and is required to cooperate accordingly with the Buyer's Representative. The Buyer's Representative has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

D. Governing Law (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must





be brought in the State of Nebraska per state law; (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity, limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

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

AT&T's Response:

AT&T's Response is submitted under applicable codes, laws and regulations current at the time of contract execution. AT&T shall comply with all codes, laws and regulations applicable to AT&T. Changes in codes, laws and regulations may require changes in pricing and performance.

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:





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

AT&T’s Response:

AT&T’s proposal hereunder is a direct reflection of the scope of work as presented here, as of the date of submission. Changes /modifications made after submission will require mutual agreement/adjustment to the new scope, subsequent pricing and performance requirements. For the prices quoted AT&T will provide services for the listed sites. Any additional services will be provided at additional cost.

H. Vendor Performance Report(s)

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





--	--	--	--

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:

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.

AT&T's Response:

Notice should be within a reasonable prompt time after Contractor is made aware of the matter, not immediately.

AT&T will not commit to provide "immediate notification", as that term is somewhat undefined in this context. AT&T will provide the services as outlined in its proposal and resulting contract documents in a manner mutually agreed by the parties

J Breach

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





		Solicitation Response (Initial)	

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 in the event of the State’s failure to make payment.~~

AT&T Response:

AT&T complies subject to the interlineations noted above.

AT&T’s proposal is submitted subject to negotiation of a mutually agreeable limitation of AT&T’s liability and insertion of the liability limitations into the final contract documents. AT&T suggests the following wording:

LIMITATION OF LIABILITY

- (a) EITHER PARTY’S ENTIRE LIABILITY AND THE OTHER PARTY’S EXCLUSIVE REMEDY FOR DAMAGES ON ACCOUNT OF ANY CLAIM ARISING OUT OF AND NOT DISCLAIMED UNDER THIS AGREEMENT SHALL BE:





- (i) FOR BODILY INJURY, DEATH OR DAMAGE TO REAL PROPERTY OR TO TANGIBLE PERSONAL PROPERTY PROXIMATELY CAUSED BY A PARTY'S NEGLIGENCE, PROVEN DIRECT DAMAGES;
 - (ii) FOR BREACH OF ANY CONFIDENTIALITY, PUBLIC OR TRADEMARK OBLIGATIONS, IF ANY, PROVEN DIRECT DAMAGES;
 - (iii) FOR ANY THIRD-PARTY CLAIMS, THE REMEDIES AVAILABLE UNDER The Agreement;
 - (iv) FOR CLAIMS ARISING FROM THE OTHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, PROVEN DAMAGES; OR
 - (v) FOR CLAIMS OTHER THAN THOSE SET FORTH IN THIS SECTION (a)(i)-(iv), PROVEN DIRECT DAMAGES NOT TO EXCEED, ON A PER CLAIM OR AGGREGATE BASIS DURING ANY TWELVE (12) MONTH PERIOD, AN AMOUNT EQUAL TO THE TOTAL NET CHARGES INCURRED BY CUSTOMER FOR THE AFFECTED SERVICE IN THE RELEVANT COUNTRY DURING THE THREE (3) MONTHS PRECEDING THE MONTH IN WHICH THE CLAIM AROSE.
- (b) EXCEPT IN THE CASE OF A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES OR FOR INCREASED COST OF OPERATIONS.
- (c) THE LIMITATIONS IN THIS SECTION SHALL NOT LIMIT CUSTOMER'S RESPONSIBILITY FOR THE PAYMENT OF ALL PROPERLY DUE CHARGES UNDER THIS AGREEMENT.

Disclaimer of Liability. AT&T WILL NOT BE LIABLE FOR ANY DAMAGES ARISING OUT OF OR RELATING TO: INTEROPERABILITY, ACCESS OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, DATA, EQUIPMENT, SERVICES, CONTENT OR NETWORKS PROVIDED BY CUSTOMER OR THIRD PARTIES; SERVICE DEFECTS, SERVICE LEVELS, DELAYS OR ANY SERVICE ERROR OR INTERRUPTION, INCLUDING INTERRUPTIONS OR ERRORS IN ROUTING OR COMPLETING ANY 911 OR OTHER EMERGENCY RESPONSE CALLS OR ANY OTHER CALLS OR TRANSMISSIONS (EXCEPT FOR CREDITS EXPLICITLY SET FORTH IN THIS AGREEMENT); LOST OR ALTERED MESSAGES OR TRANSMISSIONS; OR UNAUTHORIZED ACCESS TO OR THEFT, ALTERATION, LOSS OR DESTRUCTION OF CUSTOMER'S (OR ITS AFFILIATES', USERS' OR THIRD PARTIES') APPLICATIONS, CONTENT, DATA, PROGRAMS, INFORMATION, NETWORKS OR SYSTEMS





K. Non-Waiver of Breach

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

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:

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:





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-bodily~~ injury, death, or ~~real or tangible~~ 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.

~~Notwithstanding the foregoing, Contractor reserves and does not waive any immunities or qualified immunities afforded the provider of 911 service; Contractor’s indemnity obligation will not be construed so as to abridge or otherwise undermine such immunity.~~

Formatted: Font: 12 pt, Font color: Gray-50%

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.~~





Notwithstanding the foregoing, Contractor shall have no obligation to defend, indemnify or hold harmless where the claimed infringement arises out of or results from: (a) the State's, Customer's, or a user's content; (b) modifications to the Service by the State, Customer, or a third party not controlled by Contractor, or unauthorized combinations of the Service with any non-Contractor services or products by Customer or others; (c) Contractor's adherence to Customer's or State's written requirements; or (d) use of a Service in violation of this Agreement.

Formatted: Font: 12 pt
Formatted: *RFPBody, Indent: Left: 0", Space After: 0 pt

AT&T's Response:

AT&T complies subject to the interlineations noted above.

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.

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

N. Attorney's Fees

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





--	--	--	--

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:

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:

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:

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:





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.

AT&T's Response

AT&T cannot agree to this Section R as written. AT&T suggest the following as a complete replacement for this Section R.

- R. Force Majeure. Except for payment of amounts due, neither party will be liable for any delay, failure in performance, loss or damage due to fire, explosion, cable cuts, power blackout, earthquake, flood, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism, acts of God, acts of a public enemy, acts or omissions of carriers or suppliers, acts of regulatory or governmental agencies or other causes beyond such party's reasonable control.

S. Confidentiality

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

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.

AT&T's Response:

AT&T will not commit to provide "immediate notification", as that term is somewhat undefined in this context. AT&T will provide the services as outlined in its proposal and resulting contract documents in a manner mutually agreed by the parties.

T. Early Termination

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

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, **plus any unrecouped amortized costs.**
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;
- 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 in which case the State shall provide 30 days written notice prior to termination.

Formatted: Font: 12 pt, Font color: Gray-50%

4. In the event of termination under this section, AT&T shall be entitled to recover all demonstrated, unrecouped amortized costs of the Service, less amounts paid under the Contract by the State as of the date of termination."

Formatted: Font: 12 pt, Font color: Gray-50%

Formatted: *RFP#List1

Formatted: Font color: Gray-50%

AT&T Response:

AT&T complies subject to the interlineations noted above.

U. Contract Closeout

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

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.





III. Contractor Duties

A. Independent Contractor / Obligations

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

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.~~

AT&T’s Response:

AT&T cannot agree to this clause as it excessively restricts our ability to manage our employees and our business.

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.

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.

AT&T's Response:

AT&T suggests the following as a complete replacement for this Section.

The State may notify AT&T when the State believes an AT&T employee providing support to the State is unacceptable for assignment to the provision of Services to the State for any lawful reason, including the States reasonable determination that he or she is not qualified to perform the work to which he or she is assigned. Upon receipt of





such notice AT&T shall review the matter with the State. The State may not exercise this right on grounds unrelated to job performance or in a manner that obligates AT&T to commit an unlawful act. In the event that any such AT&T employee is transferred from a position, AT&T shall have a reasonable time to replace any such transferred employee.

B. Employee Work Eligibility Status

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

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:

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:





--	--	--	--

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.~~

AT&T's Response:

AT&T complies as edited.

AT&T does not warrant against IP infringement but we provide for full indemnity against it.

F. Ownership of Information and Data / Deliverables

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

The State shall have the perpetual, non-exclusive, personal and non-transferable unlimited right under Contractor's copyrights to ~~publish, modify,~~ duplicate, use, and as required by law disclose copies of any deliverable, excluding software, which are furnished to the State by Contractor which contain all information and data developed ~~or obtained~~ by or for the Contractor on behalf of the State pursuant to this contract.

Formatted: Font: 12 pt, Font color: Gray-50%

Formatted: Font: 12 pt, Font color: Gray-50%

The State shall own and hold exclusive title to copies of any deliverable, excluding software, developed as a result of this contract which are furnished to the State by Contractor. Contractor shall have no ownership interest or title in such copies, and shall not patent, license, or copyright, duplicate, transfer, sell, or exchange, the design, specifications, concept, or deliverable.





AT&T Response:

AT&T takes exception. AT&T does not anticipate that any work product will be created for this engagement. However, if it were, all intellectual property and proprietary rights arising by virtue of AT&T’s performance of the Services are and will be the sole and exclusive property of AT&T, and neither ownership nor title to any such property will pass to Customer.

G. Insurance Requirements

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

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

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

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

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





contract and one (1) year ~~beginning from the time the work is completed following termination or expiration of the contract.~~

Formatted: Font: 12 pt, Font color: Gray-50%

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/carry~~ 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~~ ~~include~~ subrogation waiver ~~language found hereinafter~~ ~~endorsement~~. 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-eligible to do business~~ 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/carry~~ 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 ~~per ISO form CG 00 01~~, 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, as Additional Insured(s) by endorsement as respects to this Agreement. 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~~ include the required endorsements. The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles. Notwithstanding these requirements, Contractor may, in its sole discretion, self-insure any of the required insurance under the same terms as required by this Agreement.

Formatted: Font: 12 pt, Font color: Gray-50%





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
<i>If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.</i>	
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 Coverage under Professional Liability Insurance	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	\$10,000,000
MANDATORY COI SUBROGATION WAIVER LANGUAGE	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
MANDATORY COI LIABILITY WAIVER LANGUAGE	
"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self insurance carried by the State shall be considered secondary and non-contributory as additionally insured."	

3. Evidence of Coverage





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

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

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

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

4. Deviations

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

AT&T Response:

AT&T does not carry all the coverages listed in this section. AT&T, as a large, financially secure corporation, self-insures some coverages. AT&T does not agree to share copies of its insurance policies.

H. Antitrust

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





--	--	--	--

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.

AT&T's Response:

AT&T will work with the State of Nebraska ("Customer") to reach agreement on a mutually acceptable assignment of anti-trust claim provision.

AT&T counter proposes and will agree to the following language: "Contractor hereby assigns to Customer any and all antitrust claims for overcharges to the extent associated with the volume of products and services provided to Customer under any contract resulting from this RFP, when such claims arise under the antitrust laws of the United States, 15 U.S.C. Section 1, et seq. (1973), as amended, and the antitrust laws of the State of Nebraska."

I. Conflict of Interest

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

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.

AT&T's Response:

AT&T is not aware of any conflict of interest that could materially and adversely affect AT&T's ability to perform under a proposed agreement with the State of Nebraska. AT&T is publicly owned, and with millions of shareholders, it is impossible for AT&T to determine whether any State of Nebraska employee or any member of his or her immediate family may be a shareholder in AT&T, Inc. Further, AT&T and its affiliates' employ approximately 240,000 individuals and AT&T cannot practically identify possible connections between all AT&T employees and any employees of the State of Nebraska or any component office.

In lieu of the certification proposed above, the undersigned can affirm to the best of the undersigned's knowledge and belief, after a reasonable inquiry, that none of the individuals directly involved in the preparation of this RFP have a familial relationship with any employee of the State of Nebraska; however, the State of Nebraska should make such an inquiry of its own employees, directors, and officers prior to entering into an agreement with AT&T and take the necessary steps to ensure such individuals remain in compliance with these requirements.

J. State Property

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

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.

AT&T's Response:

For clarification, AT&T will repair or replace any damage to the State of Nebraska's premises proximately caused by installation efforts of AT&T or its agents, as promptly as reasonably practicable, in an effort to return the site to its pre-installation condition.





K. Site Rules and Regulations

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

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:

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.

AT&T Response:

AT&T suggests the following as a complete replacement for this Section L.

- L **ADVERTISING.** Neither party may issue any public statements or announcements relating to the terms of this Agreement or to the provision of Services without the prior written consent of the other party.





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:

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:

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:

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.

AT&T's Response:

The warranty and remedies above does not seem to apply fully to a contract under which a provider will provide a continuing service from month to month for a specified term, but seem to apply to a service project. AT&T would like the opportunity to negotiate this language to take into account the benefit of the services the State would receive. Ordinary damage provisions would appear to be adequate in this regard.





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~~

AT&T's Response:

AT&T complies as edited.

C. Invoices

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

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:

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.~~

AT&T's Response:

With regard to inspecting AT&T's premises, AT&T will be pleased to answer any questions regarding the provisioning of the services requested in the Solicitation; however, AT&T would like to better understand why a tour of AT&T facilities would be useful to the State. For security and policy reasons, AT&T does not typically host tours of its network facilities to third parties. Accordingly, once AT&T understands the customer's specific issues, AT&T will work with the State to find an alternative way to address these concerns.

E. Payment (Statutory)

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





F. Late Payment (Statutory)

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

G. Subject to Funding / Funding out Clause for Loss of Appropriations (Statutory)

The State's obligation to pay amounts due on the Contract for a fiscal 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:

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.





V. Project Description and Scope of Work

A. Background and Project Scope

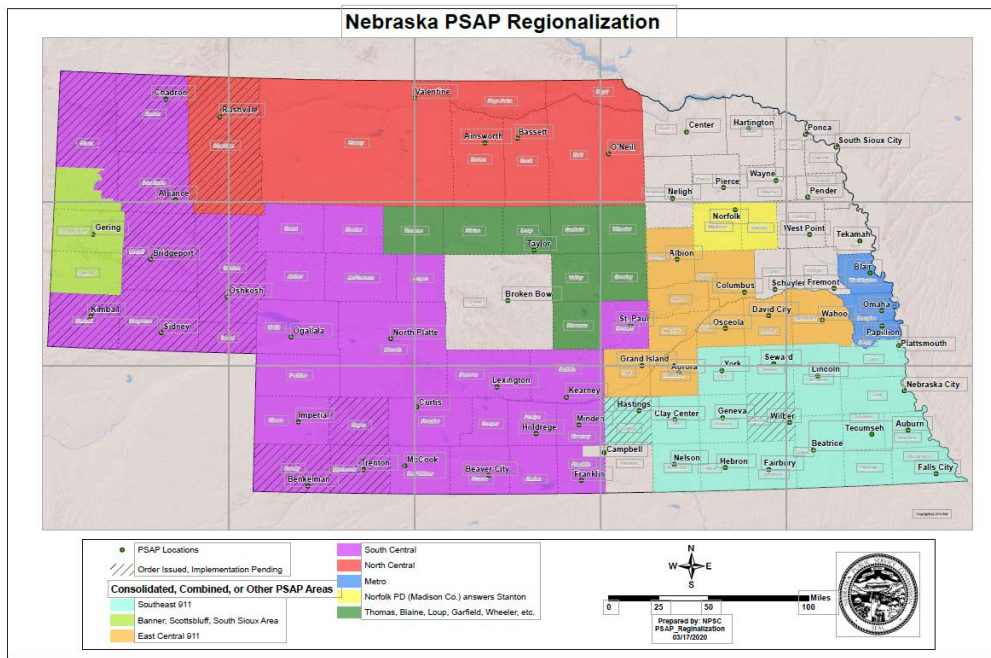
The Nebraska Public Service Commission, State 911 Department (The Commission) is the statewide authority responsible for implementing and coordinating 911 service in the state. The Commission is seeking proposals for a statewide ESInet and NGCS to help advance Next Generation 911 (NG911) across the state.

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

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

FIGURE 1





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

AT&T Response:

AT&T has read and understands.

B. Composition of the Request for Proposal

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





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

1. Option A: Deployment of an ESInet

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

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

2. Option B: Deployment of Next Generation Core Services (NGCS)

The Commission is seeking an NG911 call-delivery system that provides highly available call routing and delivery to the regional end points throughout the state. Key project elements for NGCS deployment include but are not limited to:

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

3. Option C: Deployment of an ESInet and NGCS

Includes all requirements of both Option A and Option B.

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

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





AT&T Response:

AT&T is submitted a response to Option C.

C. Bidder Requirements:

1. Bidders should include with their response:
 - a. Configuration Solution – A diagram showing the major components (hardware, software, and network layout) for the proposed system, accompanied by tables containing short descriptions of the diagrammed components in terms of their value or benefit to the Commission and the Public Safety Answering Points (PSAPs).
 - b. Attachments – Cost Proposal, with a detailed description of its firm fixed pricing.
 - c. Appendices – The Bidder may include appendices and reference them from within the proposal response. This is particularly appropriate for lengthy responses on a single subject. Understanding the intent of the Bidder shall be possible without the reading of the appendices.
 - d. Brochures – Hardware, software, or service brochures may be submitted with response where appropriate.

AT&T Response:

AT&T has provided the required information.

D. General Requirements – Technical

1. General requirements – Commission Requirements
 - a. Industry Standards

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

 - i. [Association of Public Safety Communications Officials \(APCO\)](#)
 - ii. [The Monitoring Association \(TMA\)](#)





- iii. [National Emergency Number Association \(NENA\)](#)
- iv. [Alliance for Telecommunications Industry Solutions \(ATIS\)](#)
- v. [Department of Justice \(DOJ\)](#)
- vi. [Internet Engineering Task Force \(IETF\)](#)
- vii. [North American Electric Reliability Corporation \(NERC\)](#)
- viii. [National Institute of Standards and Technology \(NIST\)](#)
- ix. [Telecommunications Industry Association \(TIA\)](#)

Table 2: Adopted Standards

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
ATIS	ATIS-0500017	Considerations for an Emergency Services Next Generation Network (ES-NGN)	Identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next-generation telecommunications networks.	Version 1 June 2009
DOJ	CJISD-ITS-DOC-08140-5.6	Criminal Justice Information Services (CJIS) Security Policy	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information.	Version 5.6 June 5, 2017
IETF	RFC 3261	SIP: Session Initiation Protocol	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	Version 1 July 7, 2002
IETF	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Defines the generic URI syntax and a process for resolving URI references, along with guidelines and security considerations for the use of URIs on the Internet.	Version 1 January 2005
NENA/ APCO	REQ-001.1.2-2018	Next Generation 911 PSAP Requirements	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP.	Version 1.2 April 5, 2018
NENA/ APCO	INF-005	Emergency Incident Data Document (EIDD) Information Document	Provides a recommended list of data components, their relationships to each other, the data elements contained within each data component, and the registries that control the available values for appropriate data elements. Initiates the process to create a National Information Exchange Model (NIEM).	February 21, 2014 Scheduled to be replaced by a standards document
NENA	STA-015.10-2018	Standard Data Formats for 911 Data Exchange & GIS Mapping	Establishes standard formats for Automatic Location Identification (ALI) data exchange between service providers and Database Management System (DBMS) providers, a GIS data model, a data dictionary, and formats for data	Version 10 August 12, 2018





SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date or The Most Current
			exchange between the ALI database and PSAP controller equipment.	
NENA	STA-008.2-2014	Registry System Standard	Describes how registries (lists of values used in NG911 functional element standards) are created and maintained.	Version 2 October 6, 2014
NENA	STA-010.2-2016	Detailed Functional and Interface Specifications for the NENA i3 Solution	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards.	Version 2 September 10, 2016
NENA	INF-016.2-2018	Emergency Services IP Network Design for NG911 (ESIND)	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInd.	Version 1 April 5, 2018
NENA	75-001	Security for Next Generation 911 (NG-SEC)	Establishes the minimal guidelines and requirements for levels of security applicable to NG911 entities.	Version 1 February 6, 2010
NENA	INF-015.1-2016	NG911 Security Information Document	Provides mechanisms and best practices for cybersecurity for i3 systems	Version 1 December 8, 2016
NERC	CIP 002-CIP 009	Critical Infrastructure Protection	Addresses the security of cyber assets essential to the reliable operation of the nation's critical infrastructure.	Version 1 December 16, 2009
NIST	FIPS 140-33	Security Requirements for Cryptographic Modules	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information.	Version 2 March 22, 2019
NIST	Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure.	Version 1.1 April 16, 2018
TIA	TIA-942-A	Telecommunications Infrastructure Standard for Data Centers	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers.	Revision A March 2014

As industry standards evolve, the Bidder's solution shall be upgraded to maintain compliance with the current version of established industry standards. The Bidder's solution shall support new ESInd, NGCS and security industry standards within 18 months of ratification of applicable industry standards at no additional cost to the State. Compliance requirements apply also to the supporting standards referenced within each standard. As solution updates are made to maintain compliance, the solution shall not





abandon services or feature functionality in place at the time of the solution upgrade. The Bidder shall uncover any performance or feature changes prior to the upgrade and report them to the Commission for approval.

b. Public Safety-Grade Definition

The national standards listed in this document provide standards and requirements an IP network and core functions shall meet or exceed to be considered an ESInet. The term “public safety-grade” has been utilized to refer to this level of standards compliance; however, a universal definition of this term has not been proposed by a Standards Development Organization (SDO) or accepted by the public safety community. For the purpose of the requirements associated with this ESInet and NGCS design and deployment, the following metric is used to define public safety-grade:

i. Reliability:

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

ii. Availability:

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

iii. Security:

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

- d) 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.
- e) An eXtensible Access Control Markup Language (XACML)-based Data Rights Management (DRM) system to control authorization.





- f) Advanced Encryption Standards (AES) based encryption to provide confidentiality.
 - g) Secure Hash Algorithm (SHA)-based digest-based digital hashing to provide integrity protection.
 - h) Dsig-based digital signatures to provide non-repudiation.
- iv. Network Traffic Restrictions:

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

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

AT&T Response:

AT&T has read and understands.



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.

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:	AT&T Corp.
COMPLETE ADDRESS:	3033 Chain Bridge Road, Oakton, VA 22124
TELEPHONE NUMBER:	571-205-6730
FAX NUMBER:	N/A
DATE:	June 3, 2020
SIGNATURE:	<small>DocuSigned by:</small> <i>Stacy Schwartz</i> <small>25A9D487C742473...</small>
TYPED NAME & TITLE OF SIGNER:	Stacy Schwartz, VP-Global Public Sector

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	0.00
Milestone 2: Region 2 deployments complete	0.00
Milestone 3: Region 3 deployments complete	0.00
Milestone 4: Region 4 deployments complete	0.00
Milestone 5: Region 5 deployments complete	0.00
Milestone 6: Region 6 deployments complete	0.00
Milestone 7: Region 7 deployments complete	0.00
TOTAL	0.00

Bidder Name:		AT&T Corp.													
Date (MM/DD/YYYY):		6/3/2020													
INITIAL CONTRACT PERIOD															
Emergency Services IP Network	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	MRC'	MRC'	MRC'	MRC'	MRC'
Region One Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1123		0.1123		0.1123		0.1123		0.1123	0.1123	0.1123	0.1123	0.1123	0.1123
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 1 TOTAL	0.0000	349,423.3367	0.0000	349,423.3367	0.0000	349,423.3367	0.0000	349,423.3367	0.0000	349,423.3367	349,423.3367	349,423.3367	349,423.3367	349,423.3367	349,423.3367
Region Two Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1097		0.1097		0.1097		0.1097		0.1097	0.1097	0.1097	0.1097	0.1097	0.1097
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 2 TOTAL	0.0000	673,976.7394	0.0000	673,976.7394	0.0000	673,976.7394	0.0000	673,976.7394	0.0000	673,976.7394	673,976.7394	673,976.7394	673,976.7394	673,976.7394	673,976.7394
Region Three Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1088		0.1088		0.1088		0.1088		0.1088	0.1088	0.1088	0.1088	0.1088	0.1088
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 3 TOTAL	0.0000	1,007,733.7013	0.0000	1,007,733.7013	0.0000	1,007,733.7013	0.0000	1,007,733.7013	0.0000	1,007,733.7013	1,007,733.7013	1,007,733.7013	1,007,733.7013	1,007,733.7013	1,007,733.7013
Region Four Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1507		0.1507		0.1507		0.1507		0.1507	0.1507	0.1507	0.1507	0.1507	0.1507
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 4 TOTAL	0.0000	51,042.3139	0.0000	51,042.3139	0.0000	51,042.3139	0.0000	51,042.3139	0.0000	51,042.3139	51,042.3139	51,042.3139	51,042.3139	51,042.3139	51,042.3139
Region Five Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1134		0.1134		0.1134		0.1134		0.1134	0.1134	0.1134	0.1134	0.1134	0.1134
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 5 TOTAL	0.0000	245,561.9489	0.0000	245,561.9489	0.0000	245,561.9489	0.0000	245,561.9489	0.0000	245,561.9489	245,561.9489	245,561.9489	245,561.9489	245,561.9489	245,561.9489
Region Six Milestone															
AT&T ESInet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1173		0.1173		0.1173		0.1173		0.1173	0.1173	0.1173	0.1173	0.1173	0.1173
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC REGION 6 TOTAL	0.0000	160,771.9607	0.0000	160,771.9607	0.0000	160,771.9607	0.0000	160,771.9607	0.0000	160,771.9607	160,771.9607	160,771.9607	160,771.9607	160,771.9607	160,771.9607
Region Seven Milestone															

AT&T ESinet (Includes Ingress trunking, call routing, Managed primary & secondary AVPN ports, local access network connections, LNG, BCF, ESRP, PRF, ECRF, LVF, SI, LDB and geospatial routing capabilities as standard service)		0.1291		0.1291		0.1291		0.1291		0.1291		0.1291		0.1291		0.1291
Bidder Input																
Bidder Input																
Bidder Input																
Bidder Input																
NRC/MRC REGION 7 TOTAL	0.0000	97,775.2489	0.0000	97,775.2489	0.0000	97,775.2489	0.0000	97,775.2489	0.0000	97,775.2489	97,775.2489	97,775.2489	97,775.2489	97,775.2489	97,775.2489	97,775.2489
ESinet Total	0.0000	2,586,285.2498	0.0000	2,586,285.2498	0.0000	2,586,285.2498	0.0000	2,586,285.2498	0.0000	2,586,285.2498	2,586,285.2498	2,586,285.2498	2,586,285.2498	2,586,285.2498	2,586,285.2498	2,586,285.2498

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:		INITIAL CONTRACT PERIOD														
Date (MM/DD/YYYY):		YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
Legacy Network Gateway		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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input																
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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
LNG Total		0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:		AT&T Corp.													
Date (MM/DD/YYYY):		6/3/2020													
Border Control 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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input															
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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:		INITIAL CONTRACT PERIOD														
Date (MM/DD/YYYY):		YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
Emergency Services Routing Proxy & Policy Routing Function		NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	MRC'	MRC'	MRC'	MRC'	MRC'
Region One Milestone																
Included in AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input																
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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
ESRP & PRF 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:		AT&T Corp.													
Date (MM/DD/YYYY):		6/3/2020													
Emergency Call Routing Function & Location Validation Function	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	MRC'	MRC'	MRC'	MRC'	MRC'
Region One Milestone															
Included in AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input															
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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:		AT&T Corp.													
Date (MM/DD/YYYY):		6/3/2020													
Spatial Interface	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	MRC'	MRC'	MRC'	MRC'	MRC'
Region One Milestone															
Included in AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input															
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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:	AT&T Corp.														
Date (MM/DD/YYYY):	6/3/2020														
Location Database	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	MRC ¹	MRC ¹	MRC ¹	MRC ¹	MRC ¹
Region One Milestone															
Included in AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bidder Input															
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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 AT&T ESInet Service	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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
LDB Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

6264 Z1 Cost Proposal Option C ESInet NGCS Revision One

Bidder Name:		AT&T Corp.													
Date (MM/DD/YYYY):		6/3/2020													
Miscellaneous	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	NRC	MRC'	MRC'	MRC'	MRC'	MRC'	MRC'
Region One Milestone															
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															
Bidder Input															
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															
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															
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															
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															
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															
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
MISC Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Bidder Name: AT&T Corp.
 Date (MM/DD/YYYY): 6/3/2020

Optional Svc for NGCS	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	NRC	MRC ¹	MRC ¹	MRC ¹	MRC ¹	MRC ¹	MRC ¹
Region One Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	15,394.1100	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	15,394.1100	25,192.5876	0.0000	25,192.5876	0.0000	25,192.5876	0.0000	25,192.5876	0.0000	25,192.5876	25,192.5876	25,192.5876	25,192.5876	25,192.5876	25,192.5876
Region Two Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	30,417.6000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	30,417.6000	49,778.6472	0.0000	49,778.6472	0.0000	49,778.6472	0.0000	49,778.6472	0.0000	49,778.6472	49,778.6472	49,778.6472	49,778.6472	49,778.6472	49,778.6472
Region Three Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	45,853.1100	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	45,853.1100	75,038.9832	0.0000	75,038.9832	0.0000	75,038.9832	0.0000	75,038.9832	0.0000	75,038.9832	75,038.9832	75,038.9832	75,038.9832	75,038.9832	75,038.9832
Region Four Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	1,676.5400	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	1,676.5400	2,743.6644	0.0000	2,743.6644	0.0000	2,743.6644	0.0000	2,743.6644	0.0000	2,743.6644	2,743.6644	2,743.6644	2,743.6644	2,743.6644	2,743.6644
Region Five Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	10,716.1800	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	10,716.1800	17,537.1156	0.0000	17,537.1156	0.0000	17,537.1156	0.0000	17,537.1156	0.0000	17,537.1156	17,537.1156	17,537.1156	17,537.1156	17,537.1156	17,537.1156
Region Six Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	6,783.0600	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	6,783.0600	11,100.5316	0.0000	11,100.5316	0.0000	11,100.5316	0.0000	11,100.5316	0.0000	11,100.5316	11,100.5316	11,100.5316	11,100.5316	11,100.5316	11,100.5316
Region Seven Milestone															
AT&T ESinet™ includes support for i3, geospatial routing as part of the standard service offering and is not broken out as an additional cost over time.	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
Optional - NG9-1-1 Transitional Data Management Service (TDMS)	3,747.8100	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0000	0.0081	0.0081	0.0081	0.0081	0.0081	0.0081
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	3,747.8100	6,133.3200	0.0000	6,133.3200	0.0000	6,133.3200	0.0000	6,133.3200	0.0000	6,133.3200	6,133.3200	6,133.3200	6,133.3200	6,133.3200	6,133.3200
Opt. Svc NGCS Total	114,588.4100	187,524.8496	0.0000	187,524.8496	0.0000	187,524.8496	0.0000	187,524.8496	0.0000	187,524.8496	187,524.8496	187,524.8496	187,524.8496	187,524.8496	187,524.8496