



AT&T Response to Nebraska Public Service Commission RFP for Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS)

April 15, 2026





311 S Akard St.
Dallas, TX 75202

+1 214.991.0049
dustin.alexander@att.com
www.business.att.com

April 15, 2026

David Sankey
State 911 Director
Nebraska Public Service Commission
1200 N Street, Suite 300
Lincoln, NE 68508

Dear David Sankey:

As the Nebraska Public Service Commission (NPSC) advances public safety and telecommunications regulation, we recognize the critical importance of reliable, secure, and interoperable emergency communications. Protecting communities across Nebraska depends on robust 911 services that enable rapid, coordinated response.

We understand NPSC's objectives for a statewide NG911 solution require seamless design, implementation, and ongoing support. Your request for comprehensive services—including ESInet and NGCS deployment, 24x7 monitoring, migration, interoperability, GIS management, and strong security—reflects a commitment to operational excellence. AT&T's proposed solution is designed to address these needs while ensuring continuity, resilience, and future-ready capabilities.

Our solution is centered on AT&T ESInet™, a next-generation emergency services network that delivers:

- Secure, resilient, and scalable statewide IP-based call routing
- Seamless NGCS integration to support interoperability with PSAPs and regional systems
- 24x7 monitoring and support for proactive issue detection and rapid response
- GIS data management for accurate, location-based call routing
- Comprehensive security, logging, and analytics to protect data and enhance visibility

AT&T's experienced public safety team will support NPSC throughout implementation and ongoing operations, providing expert guidance, training, and responsive service management.

With decades of experience supporting public safety communications, AT&T is committed to partnering with NPSC to deliver a modern, resilient NG911 solution that strengthens emergency response across Nebraska. We look forward to the opportunity to discuss our proposed approach in greater detail.

Sincerely,

Regional Sales Director



AT&T'S GENERAL RESPONSE TO THE RFP FOR EMERGENCY SERVICES IP NETWORK (ESInet) and NEXT GENERATION CORE SERVICES (NGCS)

("AT&T's General Response")

AT&T Enterprises, LLC ("AT&T") is submitting this Response pursuant to the terms and conditions of (a) the attached proposed AT&T Master Agreement (sometimes referred to as the AT&T Unified Agreement); (b) corresponding Pricing Schedule(s); (c) any related transactional documents (collectively, the "Proposed Contract Documents"); and (d) the responses, answers, clarifications and supplemental terms and conditions set forth in and/or incorporated into this Response. State of Nebraska may be referred to as or "Customer" or "NPSC" within this Response.

The pricing submitted in this Response assumes use of the Proposed Contract Documents as the basis of any final, negotiated contract between the parties.

AT&T takes a general exception to all the terms and conditions contained in the RFP. This applies whether or not such exception is identified in the Response in the section of the RFP to which the exception corresponds. AT&T takes such a general exception primarily because the RFP does not contain the product-related contractual terms and conditions necessary for AT&T to properly deliver the products and services described in the Response. AT&T may have also taken specific exceptions to certain RFP provisions but has not made a final, complete comment on every such provision. Please note that AT&T's General Response, and the general exception above, applies in all instances, including those where specific comments/exceptions have been made and those where such comments/exceptions have not been made. The absence of any individual response to a specific section of the RFP cannot be considered a waiver of any objection or an agreement to that section's provisions. Similarly, the inclusion of any specific comment/exception does not remove the applicability of this general exception.

Note that included within this "AT&T's General Response" section of the Response, in the interest of efficiency, are statements that apply to provisions throughout the RFP and should be read as applicable to any and all such related provisions. In that regard, note that:

AT&T clarifies that only the physical response materials become Customer property. Any other pre-existing or newly developed intellectual property of AT&T, its suppliers or its third parties, provided in this Response or which is used or developed during the project remains the intellectual property of AT&T or its suppliers. AT&T would be willing to negotiate with Customer regarding rights to use that intellectual property.

The information and pricing in this Response is valid for a period of 90 days from the date on the Response cover page.

The Response is a direct reflection of the entire scope of work as presented here, as of the date of submission. Acceptance of only part of the quote may require mutual agreement/adjustment to the final configuration, subsequent pricing and implementation schedule.

Regarding any proposed waiver of informalities and irregularities, AT&T agrees, except to the extent the waiver of technicalities or informalities portions of this provision as used here and throughout this Response implies AT&T waives rights to protest the award decision. To that end, AT&T reserves all protest rights afforded bidders/respondents participating in the contracting process.



Any purchase orders issued for services as provided under any contract that results from the RFP must clearly provide that the purchase is made via the mutually agreed contract and not subject to the preprinted terms of that purchase order form.

Any third-party software used with the services will be governed by the written terms and conditions of the third-party software supplier's software license documentation applicable to such software.

Title to software remains with AT&T or its supplier and such software used with the services will be governed by the corresponding software license agreement to the extent not in conflict with law or any final contract between AT&T and Customer.

To the extent any portion of this project may be funded in whole or in part with grants, loans or payments from government funding sources other than Customer, AT&T and Customer will need to reach mutual agreement on AT&T's participation.

The information and pricing submitted with this Response is subject to change on account of any error or omission in the information provided by Customer or upon further investigation(s) as to the exact requirements of any order. For the price(s) quoted herein, AT&T will provide the items of equipment and services specifically listed in its Response. Work which is not shown or described in the Response will require mutual agreement/adjustment to the final configuration, subsequent pricing and Implementation schedule.

This Response is ©2026 AT&T Intellectual Property. All rights reserved. AT&T, AT&T logo, and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. This Response is AT&T Proprietary and, except to the extent required by law, confidential.

This Response is conditioned upon negotiation of mutually acceptable terms and conditions.

Pricing proposed herein is based upon the specific product and locations outlined in this Response. Any changes or variations in the proposed terms and conditions, the products/services/quantities, length of term, locations, and/or design described herein may result in different pricing. Prices quoted do not include applicable taxes, surcharges, or fees. In accordance with the tariffs or other applicable service agreement terms, Customer is responsible for payment of such charges.

Subsidiaries and affiliates of AT&T Inc. provide products and services under the AT&T brand. AT&T Enterprises, LLC is an AT&T company, is the proposer for itself and on behalf of its service-providing affiliates.

Notwithstanding anything to the contrary set forth in the RFP, neither AT&T nor Customer is under any obligation with respect to the RFP until both parties have agreed upon and executed a mutually acceptable final contract. It is AT&T's goal to provide the best communications services at the best value for all of our customers using the highest ethical and legal standards. Given the long and successful history of AT&T, we are confident, if AT&T is selected, this will be a successful contracting process, leading to a successful project performance.



Table of Contents

Executive Summary.....	8
RFP Response	19
1. CORPORATE OVERVIEW.....	19
a. BIDDER IDENTIFICATION AND INFORMATION	19
b. FINANCIAL STATEMENTS	20
c. CHANGE OF OWNERSHIP.....	21
d. OFFICE LOCATION	22
e. RELATIONSHIPS WITH THE STATE.....	22
f. BIDDER’S EMPLOYEE RELATIONS TO STATE	22
g. CONTRACT PERFORMANCE	23
h. SUMMARY OF BIDDER’S CORPORATE EXPERIENCE	24
i. SUMMARY OF BIDDER’S PROPOSED PERSONNEL/MANAGEMENT APPROACH	27
j. SUBCONTRACTORS	31
FACTORS USED TO EVALUATE CORPORATE OVERVIEW.....	33
2. RESPONSE TO SCOPE OF WORK.....	35
3. RESPONSE TO WORK PLAN AND PROJECT PLANNING	62
4. RESPONSE TO TECHNICAL REQUIREMENTS	95
1. ESInet Requirements	95
2. Next Generation Core Services (NGCS) Requirements	149
3. GIS and Database Services Requirements.....	187
4. Security Requirements	200
5. Reporting Services Requirements	257
6. Installation Requirements	296
7. Training	303
8. Operations and Service Management Requirements	310
9. Value Add and Optional Services	378
10. Use Case Examples for Use with Response	386
5. COST SHEET.....	397



6. RESPONSE TO TERMS.....	398
7. CONTRACTUAL AGREEMENT FORM	399
8. ADDITIONAL REQUESTED ITEMS	401
9. AT&T APPENDICES	402



Table of Figures

Figure 1: AT&T Key Project Personnel	28
Figure 2: AT&T NG911 Project Management & Governance Model.....	31
Figure 4: AT&T ESInet Architecture	36
Figure 5: AT&T ESInet NGCS Functional Elements.....	39
Figure 6: AT&T Key Project Personnel	70
Figure 7: Phased Project Approach.....	76
Figure 8: AT&T ESInet NGCS Architecture	86
Figure 9: AT&T ESInet NGCS Functional Elements.....	87
Figure 10: AT&T ESInet Functional Elements	100
Figure 11: AT&T ESInet NGCS Architecture	100
Figure 12: AT&T ESInet Redundancy by Design.....	101
Figure 13: AT&T ESInet NGCS Functional Elements	107
Figure 14: AT&T ESInet Redundancy by Design.....	108
Figure 15: Wireless OSP not using FG	128
Figure 16: Wireline OSP using AT&T LIS/ADR	129
Figure 17: Legacy VoIP OSP	130
Figure 18: NG OSP	131
Figure 19: NG OSP using AT&T LIS/ADR.....	133
Figure 20: NG OSP using FG	134
Figure 21: ESInet to ESInet Transfer/Handoff.....	136
Figure 22: Text Traffic Flow.....	137
Figure 23: GIS Provisioning Traffic Flow	138
Figure 24: Service Availability	142
Figure 25: MOS Score Measurement.....	180
Figure 26: MOS Score Measurement.....	182
Figure 27: PCA PKI Policy	205
Figure 28: Security and Trust Framework.....	230
Figure 29: Single Sign-On	235
Figure 30: Resiliency Design.....	333
Figure 31: i3 OSP w/LIS/ADR not using NFG	389
Figure 32: i3 OSP not using NFG using AT&T LIS/ADR	389
Figure 33: i3 OSP using NFG.....	390



Executive Summary

AT&T is widely recognized as America's Public Safety Communications Company, with major investments in Next Generation 911 Emergency Services IP Networks (AT&T ESInet) national solution, Cloud Based Call Handling CPE, and leadership in building and operating FirstNet, the nation's dedicated public safety broadband network. AT&T has a robust Public Safety Solutions practice that nationally serves public safety agencies with Legacy and Next Generation 911 call routing (AT&T ESInet), Call Handling, Location Services, Computer Aided Dispatch (CAD), GIS, 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 this experience to the Public Safety sector to more quickly and effectively manage emergency response. FirstNet and our AT&T ESInet platform are examples of our commitment to Public Safety.

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 Call Handling applications highlights our ability 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 CSRIC working groups.

A Commitment of Service to the State of Nebraska

AT&T is proud to present our comprehensive solution for the State of Nebraska's Next Generation 9-1-1 (NG9-1-1) needs. AT&T is uniquely positioned to deliver a state-of-the-art Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS).

Our extensive experience in the Public Safety segment, coupled with our proven track record as the market leader in deploying NG9-1-1 services, ensures that we can address the complex functions required for a



"Frost & Sullivan research indicates that AT&T remains the leading NG911 contract holder in the US, with a market share of approximately 34%. AT&T's ESInet™ is currently deployed in 18 states covering a population of 88 million."

- Brent Iadarola, Frost & Sullivan Practice Leader, ICT



successful transition from legacy 9-1-1 systems to a modern, IP-based network. AT&T's ESInet solution not only meets but **exceeds** the requirements outlined in the RFP, providing the State of Nebraska with unmatched reliability, flexibility, and support.

With AT&T ESInet, the State of Nebraska will benefit from our nationally available, pre-built cloud-based solution, which has demonstrated over 69,000 hours of continual service at a reliability level greater than 99.999%. Our solution is designed to facilitate an efficient transition to a mission-critical IP network capable of supporting the growing demands of our mobile society.

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

AT&T Nebraska Investment & Impact	
Financial Strength & Long-Term Investment	AT&T invested more than \$225 million in Nebraska network infrastructure from 2020–2024, reinforcing long-term stability, reliability, and capacity to support mission-critical communications statewide.
Statewide Network Coverage & Reliability	AT&T’s wireless voice and data network covers 99%+ of the U.S. population, with Nebraska benefiting from continuous enhancements across urban, suburban, and rural communities, ensuring dependable connectivity when it matters most.
Regional & Local Infrastructure Investment	Significant investments were made across Nebraska communities, including nearly \$110M in Omaha–Council Bluffs, \$15M+ in Lincoln, and \$4.3M+ in Grand Island, directly strengthening local network resiliency and performance.
Broadband Expansion & Digital Equity	Investment efforts focus on expanding fiber, 5G, and FirstNet® – Built with AT&T, supporting economic growth, workforce enablement, online learning, and access to critical communications services across the state.
Public Safety Communications Support	AT&T connects public safety agencies in 280+ Nebraska localities, including Omaha, Lincoln, Bellevue, Grand Island, and Kearney, delivering reliable connectivity that supports emergency communications and coordinated response.
FirstNet® – Public Safety Network Capability	FirstNet provides the largest public-safety network footprint in the U.S. (2.99M+ square miles). In Nebraska, nearly 600 Band 14 sites deliver dedicated public-safety coverage and capacity on spectrum reserved exclusively for first responders.



Technology Evolution & Innovation	AT&T continues to expand 5G services across Nebraska, including less-densely populated areas such as Norfolk, and is collaborating with AST SpaceMobile to enable future off-grid voice, data, text, and video connectivity.
Network Modernization & Future Readiness	AT&T is actively modernizing networks to support next-generation services, including transitioning away from legacy copper infrastructure while ensuring no loss of voice or 911 services during modernization efforts.
Alignment with Public Interest Objectives	AT&T's investments support the public interest by improving emergency response, strengthening economic development, enabling secure connectivity, and helping bridge the digital divide across Nebraska communities.

A Proven Solution for Nebraska

AT&T's ESInet™ solution is built from the ground up to comply with the National Emergency Number Association (NENA) i3 standards, ensuring seamless interoperability, scalability, and reliability. Our solution integrates with more call handling systems and voice interfaces than any other provider, offering PSAPs across the State of Nebraska unmatched flexibility and operational efficiency.

Key features of our proposed solution include:

- **NENA i3 Compliance** – Fully compliant with NENA, APCO, ANSI, and IETF standards, ensuring The State of Nebraska's NG9-1-1 system meets the highest industry benchmarks.
- **Geographically Diverse Infrastructure** – A fully meshed MPLS network with 99.999% service availability, supported by 12 geographically diverse cores for maximum redundancy and reliability.
- **Comprehensive Support** – Dedicated account teams, including a 9-1-1 Service Manager, will provide end-to-end support, ensuring consistent performance, rapid issue resolution, and proactive service management.
- **Customer Management Portal** – A secure, web-based portal offering PSAPs extensive control over routing policies, operational states, and alternate routing configurations.

AT&T's Solution Overview

AT&T ESInet™ Next Generation Core Services

To meet The State of Nebraska'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). AT&T ESInet™ is prebuilt with 6 geo-



diverse U.S. based locations, consisting of 12 NGCS cores. The solution has been in live production since 2018 with over 65K hours of operation. AT&T's ESInet solution provides the Public Safety community with an i3 architecture built from the ground up.

Our qualifications and innovation experience in 9-1-1 and public safety are unparalleled, starting over 50 years ago with the first 9-1-1 call and evidenced most recently through the implementation of our National AT&T ESInet™ call routing infrastructure, FirstNet public safety broadband network (PSBN), and rollout of 5G wireless technology.

AT&T's ESInet deployments now extend across 18 states and the nation's capital, serving more than 2,000 Public Safety Answering Points (PSAPs) that are either operational or under contract. No other provider offers comparable experience in designing and implementing mission-critical Next Generation 9-1-1 solutions like AT&T.

Call Handling Integration

Through its vendor-neutral architecture and compliance with NENA i3 standards, AT&T ESInet enables seamless integration with more call handling systems than any other NGCS provider. AT&T ESInet is a CHE agnostic solution that allows any CAMA, RFAI or i3 compliant CHE vendor to connect to the ESInet for call and data delivery. AT&T Labs thoroughly tests all hardware and 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 on the leading call handling suppliers: Motorola, Intrado, Carbyne and Comtech/Solacom. Additionally, AT&T and our partners have performed MSRP testing and deployment for i3 text for Intrado VIPER, Motorola Vesta and Carbyne APEX platforms. AT&T ESInet is currently deployed live with Intrado VIPER, Motorola VESTA and CallWorks, ATOS, Carbyne APEX, Central Square, Combix, Emergitech, Micro automation, Moducom, Nine One, Inc., Omni911, Proctor, Racom, Solacom (Comtech), Trittech, WestTel, and Zetron. AT&T's partner Intrado also offers an i3 interoperability lab to test compatibility with future CHE providers such as Ryzylant.

The platform utilizes established i3 geospatial routing, improved location accuracy, and text-to-9-1-1 delivery to ensure effective and compatible operation with Intrado VIPER environments. This robust integration allows the State's PSAPs to leverage reliable, advanced NG9-1-1 capabilities from major call handling providers present in the state and AT&T ESInet.

Text Control Center (TCC) Services

AT&T ESInet ensures reliable transport of Text-to-9-1-1 messages using the MSRP protocol through several key mechanisms:

- **Redundant Connections** – AT&T has pre-established, geographically diverse and fully redundant connections between the AT&T/Intrado-managed Text Control Center (TCC) and the ESInet



infrastructure. This redundancy eliminates single points of failure and ensures continuous service availability.

- **Policy-Based Routing** – The ESInet leverages Emergency Services Routing Proxy (ESRP) and Policy Routing Function (PRF) to determine and route MSRP traffic. This enables precise routing based on predefined policies, ensuring texts are delivered to the appropriate Public Safety Answering Point (PSAP).
- **i3 Compliance** – MSRP traffic is routed in compliance with NENA i3 standards, ensuring seamless interoperability and adherence to industry benchmarks.
- **End-to-End Integration** – Text messages traverse the ESInet's infrastructure via redundant paths and are handed off to Call Handling Equipment (CHE) at the PSAP, Host or POI locations. This integrated approach eliminates the need for over-the-top solutions.

AT&T Virtual Private Network (AVPN)

AT&T's proposal included two (2) AVPN Multi-Protocol Label Switching (MPLS) connections per designated Call Handling Host that will be engineered with Access Path Diversity and will take advantage of the existing dual entrances to the facilities where available. Dual AVPN circuits per Host will terminate on two (2) separate managed and monitored routers. In addition, AT&T has looked further into the network and designed these network services to utilize diverse Serving Wire Centers, Layer 2 and Layer 3 POPs, thus providing the greatest level of resiliency offered.

Standalone (non-hosted) PSAPs have been designed with Dual AVPNs as well as FirstNet wireless failover as a tertiary path to provide for additional redundancy. AT&T will work with the State of Nebraska to add dual entrance facilities into standalone PSAPs where requested.

The MPLS solution being offered is AT&T Virtual Private Network (AVPN), a VPN service used in public safety applications. The proposal outlines the significance of network diversity and describes measures for ensuring its implementation and ongoing maintenance throughout the duration of the contract.

Originating Service Providers (OSP) Migration

AT&T ESInet's proven processes and extensive experience in migrating Originating Service Providers (OSPs) to NG9-1-1 systems offer several key benefits:

- **Seamless Transition to NG9-1-1 Standards** – AT&T's expertise ensures a smooth migration from legacy systems to NENA i3-compliant NG9-1-1 systems, minimizing disruptions and maintaining service continuity during the transition.
- **Interoperability Leadership** – With over 2,000 OSP migrations completed, including 1,500 Wireless Direct IP connections and 500 TDM migrations, AT&T has demonstrated its ability to integrate diverse OSP networks into the ESInet. This ensures compatibility and interoperability with existing and future



systems. Furthermore, AT&T has direct IP connections to the three major wireless carriers – AT&T Mobility, Verizon Wireless and T-Mobile.

- **Support for Legacy Systems** – AT&T ESInet supports legacy OSP subscriber provisioning and Automatic Location Identification (ALI) database management without requiring changes to carrier systems. This allows OSPs to transition to NG9-1-1 without significant infrastructure modifications.
- **Enhanced Reliability and Redundancy** – AT&T's ESInet is built on a geographically diverse infrastructure with 99.999% service availability, ensuring that OSPs benefit from a highly reliable and resilient network.
- **Real-Time Text (RTT) and TTY Support** – AT&T ESInet supports RTT ingress from OSPs and provides seamless conversion to TTY for PSAPs that are not RTT-capable. This ensures accessibility and compliance with regulatory requirements.

Reporting

AT&T ESInet offers robust reporting capabilities through its Customer Management Portal, Executive Network Dashboard and i3 Logging Service, designed to enhance visibility, operational efficiency, and compliance with NENA i3 standards.

The **Reporting Suite** provides near real-time, PSAP-specific insights into:

- **Network Node and Connectivity Status** – Displays the availability and performance of PSAP ESInet IP connections.
- **Call Routing Activity** – Tracks call routing and processing in real time.
- **Utilization and Capacity Metrics** – Monitors PSAP capacity and usage.
- **Color-Coded Status Indicators** – Offers an intuitive, visual representation of overall system health for quick decision-making.

End-To-End Support

AT&T delivers comprehensive end-to-end support for its ESInet solution, ensuring high standards of reliability, security, and operational excellence. The platform is continuously monitored around the clock by AT&T's centralized Network Operations Center (NOC) and Security Operations Center (SOC), with dedicated tier 2 and tier 3 technical experts on hand. Its geographically diverse and redundant infrastructure, complemented by robust disaster recovery measures—including AT&T's Network Disaster Recovery (NDR) team—ensures uninterrupted service during even the most critical scenarios. AT&T utilizes established incident management and escalation protocols, as well as proactive maintenance and regular system upgrades, to achieve optimal performance. Furthermore, a dedicated 9-1-1 Service Manager and support team provide ongoing assistance, while tools such as the Customer Management Portal and Executive Network Dashboard offer real-time visibility and control, enabling PSAPs to maintain efficient and effective operations.



Why AT&T?

Unmatched Experience and Leadership

AT&T's leadership in the NG9-1-1 market is backed by decades of experience and a proven track record of successful deployments. Our ESInet™ solution is trusted by over 2,000 PSAPs nationwide, with 1,700+ already in live production. We leverage FirstNet wireless backup in 12 states, ensuring uninterrupted service even during emergencies.

The State of Nebraska can rely on AT&T's expertise, innovation, and commitment to public safety. Our solution is not just "i3-like" or "i3-aligned"—it is fully compliant and future-ready, designed to evolve with industry standards and the growing demands of a mobile society. With AT&T, The State of Nebraska will gain access to the most advanced NG9-1-1 solution available, supported by the nation's most experienced provider.

AT&T distinguishes itself as a leader in the NG9-1-1 market through several key attributes:

- **Market Leadership and Recognition** – AT&T has been recognized as the U.S. NG9-1-1 Market Leader by Frost & Sullivan for eight consecutive years, underscoring its dominance and expertise in the field.
- **Extensive Deployment and Reach** – AT&T ESInet™ serves over 88 million people across 18 states and Washington, D.C., making it the most widely deployed NG9-1-1 solution in the United States. It supports over 2,000 PSAPs, with 1,700+ in live production.
- **Proven Reliability** – AT&T ESInet™ boasts 99.999% service availability, with over 69,000 hours of uninterrupted operation. Its infrastructure includes 12 geographically diverse core centers, ensuring redundancy and resilience.
- **Advanced Technology and Standards Compliance** – AT&T's NG9-1-1 solutions are fully compliant with NENA i3 standards, offering geospatial call routing, GIS integration, and seamless interoperability with existing systems.
- **Interoperability Leadership** – AT&T has completed 2,000 migrations of Originating Service Providers (OSPs) to NG9-1-1, including 1,500 SIP/IP connections. It has established interconnection agreements with 80% of ESInet providers and supports interoperability with multiple ESInets and call-handling systems.
- **Commitment to Public Safety** – With decades of experience in emergency communications, to date, AT&T has processed over 150 million 9-1-1 calls through its NG9-1-1 system and provides mission-critical services with 24x7x365 readiness.





- **Scalability and Flexibility** – AT&T's ESInet™ integrates with more call-handling systems and voice interfaces than any other provider, offering unmatched flexibility for PSAPs.

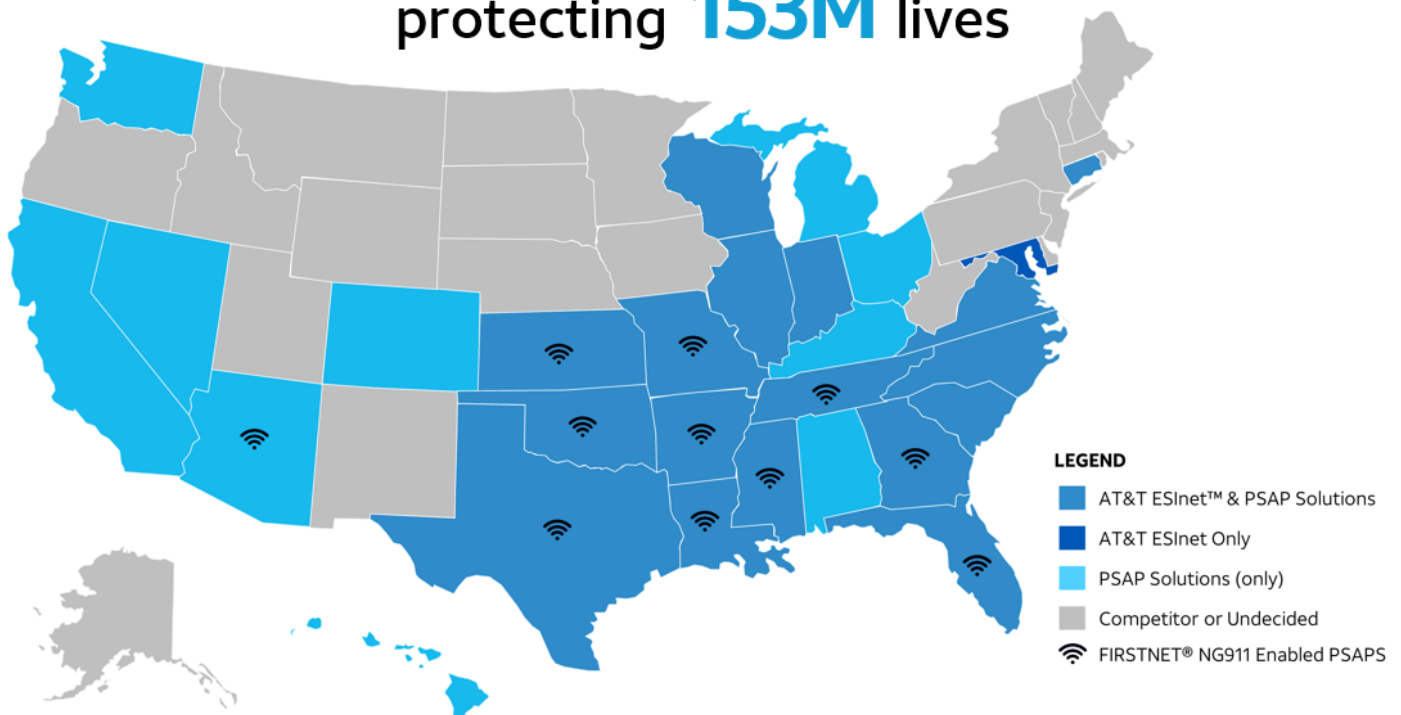
These factors collectively position AT&T as the **#1 provider of Next Generation 9-1-1** solutions in the United States, delivering transformative, reliable, and future-ready emergency communication systems.

Public Safety Solutions Leadership

AT&T maintains a robust Public Safety Solutions practice serving public safety agencies nationwide with a comprehensive portfolio that includes:

- Legacy and NG911 call routing services (AT&T ESInet™)
- Call Handling Equipment (CHE)
- Logging Recorders
- Location Services
- Computer Aided Dispatch (CAD)
- GIS
- Records, Jail, and Corrections Management systems
- Advanced security and cloud solutions
- IP networking, wireless, and IoT services

AT&T NG911 solutions deployed in **26 States** protecting **153M** lives





Through this portfolio, AT&T is driving the convergence of advanced communications technologies to help public safety agencies more effectively manage emergency response while preparing for future NG911 capabilities.

AT&T was among the first carriers to implement original 9-1-1, Enhanced 9-1-1 (E9-1-1), and now Next Generation 9-1-1. In 2015, AT&T announced its national vision for an i3-compliant NG911 Next Generation Core Services (NGCS) and ESInet architecture. This national NG911 platform is built, owned, and operated by AT&T and engineered to support more than twice the busy-hour 9-1-1 call volume for the entire United States, reflecting AT&T's commitment to scale, resiliency, and long-term viability.

*When a person dials 9-1-1, every passing second can be the difference between life and death. AT&T believes that when seconds count, public safety experience counts the most, therefore **AT&T is uniquely qualified to deliver NG911 services to help modernize public safety.***



AT&T Brings Day 1 Benefits to the State of Nebraska

State of Nebraska Benefits Delivered on Day One

- **ACCELERATED IMPLEMENTATION:** AT&T ESInet's pre-built solution accelerates deployment by eliminating the lengthy cycle times typically associated with equipment buildouts required by most NG911 service providers; reduced deployment time may also help the State of Nebraska meet their schedule for PSAP migrations.
- **Proven Reliability:** The AT&T ESInet guarantees 99.999% service availability through its robust and resilient architecture, ensuring consistent performance even during extreme events like experienced Hurricane Helene in North Carolina.
- **Seamless Interoperability:** On-net 9-1-1 AT&T ESInet call transfers with neighboring public safety agencies in Kansas and other NGCS providers serving South Dakota, Iowa and Colorado.
- **Advanced Call Routing:** Native SIP/IP call ingress for 100% of wireless 9-1-1 calls from national wireless carriers already interconnected with AT&T ESInet's national SIP POIs; helping to accelerate regulatory compliance with the FCC NG911 OSP Migration order.
- **Innovative Features:** Optimized AT&T ESInet integration and operations with many call handling providers, allowing the State of Nebraska to leverage the latest AT&T innovations, including native 9-1-1 picture messaging, if supported.
- **Uninterrupted Service:** Call processing continuity of operations using the optional FirstNet Wireless backup, providing automatic failover and seamless call delivery during unexpected wireline outages.
- **Emergency Backup:** Carbyne APEX Continuity ensures continuity of operations in extreme cases of PSAP abandonment or outage avoidance.

Personalized Support

The State of Nebraska will benefit from consistent, reliable, and coordinated support delivered by knowledgeable AT&T Account Teams. Furthermore, AT&T Public Safety Teams possess significant expertise across a comprehensive range of communication products and services tailored to public safety needs. This depth of experience enables us to expertly design and support solutions, including our proposal for Next Generation 9-1-1 services offered through AT&T ESInet.



Name	Title	Phone Number	Email
Jeff Bievenue	Application Sales Executive – Public Safety	314-775-3650	jeff.bievenue@att.com
Billy Blankenship	Sales Systems Engineer 3 – Public Safety	512-870-4111	billyb@att.com
Dustin Alexander	Regional Sales Director	214-991-0049	dustin.alexander@att.com
Keith Martin	Lead Product Management and Development	918-519-2634	Keith.martin@att.com
Jimmy Lichtenstein	Senior Public Safety Product Manager	615-521-6971	Jimmy.Lichtenstein@att.com

AT&T acknowledges the significance of this project. We recognize the need to consistently provide effective solutions for Public Safety customers and are committed to ongoing improvement. We anticipate continued collaboration with State of Nebraska as we implement this high-visibility, high-priority project.

The advertisement graphic features a woman in a call center headset working at a desk with multiple monitors displaying NG911 data. The AT&T logo is in the top left. The main headline reads 'CELEBRATING MARKET LEADERSHIP IN NG911'. Below this, several key statistics are presented: '1,750+¹ CALL CENTERS UPGRADED NATIONWIDE' with a map icon; 'ENHANCING SAFETY FOR 88+ MILLION PEOPLE' with a city skyline icon; 'AT&T ESInet™ DEPLOYMENTS SPAN 18 STATES' with a map of the US; a Frost & Sullivan '2026 BEST PRACTICES RECOGNITION' award for 'UNITED STATES NEXT GENERATION 9-1-1 MARKET LEADERSHIP'; and '#1 US PROVIDER (APPROX. 34% MARKET SHARE)' with a bar chart icon.

“The statewide ESInet was a literal lifesaver during and after Hurricane Helene,” said L.V. Pokey Harris, Executive Director of the N.C. 911 Board.¹

¹ North Carolina Department of Information Technology, October 18, 2024.



RFP Response

1. CORPORATE OVERVIEW

The Corporate Overview section of the solicitation response 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 Enterprises, LLC was formed May 2, 2024 as a Delaware LLC; the entity name/form has not changed since formation.

Company Name: AT&T Enterprises, LLC

Headquarters: 208 S. Akard St. Dallas, TX 75202

Entity Organization

AT&T is an independent, publicly traded corporation, and no individual owns more than 10% of the company.

State of Incorporation: Delaware

AT&T Enterprises, LLC is a Delaware limited liability company formed on May 2, 2024

The AT&T Corp. date of incorporation was March 3, 1885.

AT&T Inc. (our parent company) has been in business under its present name since 2005 when SBC Communications Inc. and AT&T Corporation merged.

However, our organization's history and the AT&T brand extend back to 1885 when Alexander Graham Bell's company adopted the name American Telephone and Telegraph Company, which was shorted to AT&T. Here's a selected history of our business names:

- 1877—Bell Telephone Company
- 1885—American Telephone and Telegraph Company (AT&T)



- 1983—AT&T divestiture results in AT&T and Southwestern Bell Corporation (SBC) becoming separate companies
- 2005—AT&T and SBC merge under the name AT&T Inc.

This timeline provides an illustrated history: www.att.com/Common/files/pdf/logo_evolution_factsheet.pdf

Various subsidiaries and affiliates of AT&T Inc. may operate under different names.

b. FINANCIAL STATEMENTS

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

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

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

AT&T Response:

Comply.

AT&T Inc. is a publicly held corporation and has provided its most recent audited financial report and statements in **Appendix L – AT&T 2025 Annual Report** (FY ended 12/31/2025).

With more than 146+ years of experience, AT&T draws on its expertise to champion innovation and develop comprehensive, reliable solutions. As the U.S. market leader in Next Generation 911, AT&T has developed a next generation offering of advanced call routing features, functions, and highly secure public safety network.

Financial / banking organization representative: As a matter of corporate policy, AT&T does not provide third-party banking references in competitive procurements. In lieu of a banking reference, AT&T provides the following fiscally responsible corporate representative for questions regarding AT&T's financial statements and financial capability to perform this Solicitation:



AT&T Corporate Treasury / Finance (Authorized Representative)
AT&T Inc., 208 S. Akard St.
Dallas, TX 75202

AT&T's Treasury team may be contacted at either cg5557@att.com or af7414@att.com.

The auditor of AT&T's financial organization is:

Ernst & Young LLP, Independent Registered Public Accounting Firm
2323 Victory Ave., Suite 2000
Dallas, TX 75219

Management has made available to Ernst & Young LLP all of AT&T's financial records and related data, as well as the minutes of stockholders' and directors' meetings. Furthermore, management believes that all representations made to Ernst & Young LLP during its audit were valid and appropriate.

You can find additional financial statements and reports at <https://investors.att.com/financial-reports/annual-reports>

Litigation / financial reversals: AT&T is not aware of any judgments, pending or expected litigation, or other real or potential financial reversals that might materially affect the viability or stability of AT&T.

c. CHANGE OF OWNERSHIP

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

AT&T Response:

In the last three years, AT&T's ownership structure has been unchanged.

No single person owns more than 10% of the company. It is an independent, publicly traded telecommunications services provider.

No change in ownership or control is anticipated during the twelve (12) months following the solicitation response due date. AT&T will notify the Commission if that changes.



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:

Upon award, AT&T's office location responsible for overall contract performance and customer coordination for the State of Nebraska will be AT&T Enterprises, LLC, 208 S. Akard St., Dallas, TX 75202. Day-to-day service delivery and operations support will be provided by AT&T's designated NG911/ESInet service management and 24x7 Network Operations Center (NOC) / Security Operations Center (SOC) resources supporting the AT&T ESInet™ platform.

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's solicitation response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

AT&T Response:

CONTRACT NUMBER 90610 04 - NASPO Mobility Contract- APRIL 01, 2021 THROUGH AUGUST 11, 2029

AT&T has an existing contractual relationship with the State of Nebraska under Contract Number 90610 04 (NASPO Mobility Contract) with a current term of April 1, 2021, through August 11, 2029. Under this agreement, AT&T provides statewide wireless mobility services, including AT&T mobility services and FirstNet® wireless capabilities, supporting reliable communications for eligible State agencies and authorized users. Other than Contract 90610 04, AT&T has had no other contracts with the State of Nebraska in the last 10 years.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's solicitation response is or was an employee of the State of Nebraska within the past six (6) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

If any employee of any agency of the State is employed by the bidder or is a subcontractor to the bidder, as of the due date for solicitation response submission, identify all such persons by name, position held with the



bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this solicitation. If no such relationship exists, so declare.

AT&T Response:

After reasonable inquiry, no Party named in this solicitation response who is or was an employee of the State of Nebraska within the past six (6) months.

After reasonable inquiry, no such relationship exists or has existed by employees employed by AT&T or its subcontractor.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past ten (10) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past ten (10) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's solicitation response accordingly. If no such termination for default has been experienced by the bidder in the past ten (10) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, nonperformance, 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:

To AT&T's knowledge after reasonable inquiry, AT&T has not had and is not aware of any proposed subcontractor having had, any contract terminated for default within the past ten (10) years, as defined in this RFP. Accordingly, there are no terminations for default to report.

To AT&T's knowledge after reasonable inquiry, AT&T has not had and is not aware of any proposed subcontractor having had, any contract terminated for convenience, non-performance, non-allocation of funds, or any other reason within the past five (5) years that would be required to be disclosed under this section. Accordingly, there are no such terminations to report.



h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

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

The bidder should address the following:

- i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this Solicitation. These descriptions should include:
 - a) The time period of the project,
 - b) The scheduled and actual completion dates,
 - c) The bidder's responsibilities,
 - d) For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and
 - e) Each project description should identify whether the work was performed as the prime vendor or as a subcontractor. If a bidder performed as the prime vendor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.
- ii. Bidder and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as subcontractor projects.
- iii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the bidders above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

AT&T Response:

Comply.

AT&T ESInet Project References and Work Performed

The following paragraphs include the identified similar in scope projects from current AT&T customers. Many of these demonstrate proven success with a regional deployment architecture like the State's 7-region model. AT&T considers meeting the customer requirements listed above with a go live cutover of service to include all applicable performance measures with results achieved. AT&T served as the prime contractor in all three of the referenced customer projects below. AT&T is unable to provide financial or contractual specifics related to



the projects referenced; however, the information may be obtained directly from the customer references listed.

Project status is noted below by PSAPs Deployed.

State of Kansas

Client's Name	Kansas 911 Board
Contract Number	20170323-2647
Contact Name	Sherry Massey, Executive Director
Telephone Number	785-280-1009
Email Address	Sherry.massey@ks.gov
Project Dates	2017 - Current
Contract Term	10 Years
Contract Type	Statewide
Population Served	2.9M
Concurrent Project	Yes
PSAPs Contracted	113
PSAPS Deployed	113
Description of Project and/or Technical Environment	The solution is AT&T ESInet(NGCS/ESINET), that is geographically diverse with 12 cores and i3 compliant. This is a fully meshed MPLS network AT&T Virtual Private Network (AVPN) which is designed for 99.999% service availability. AT&T provides the following additional services: Hosted Call Handling using Motorola VESTA, RapidDeploy Tactical Mapping, FirstNet Wireless backup.



State of Arkansas

Client's Name	Arkansas 9-1-1 Board
Contract Number	4600049010
Contact Name	C.J. Engel, Executive Director
Telephone Number	501-375-9911
Email Address	AR911Board@adem.arkansas.gov
Project Dates	2021 - Current
Contract Term	5 Years
Contract Type	Statewide
Population Served	2.8M
Concurrent Project	Yes
PSAPs Contracted	115
PSAPS Deployed	106
Description of Project and/or Technical Environment	The solution is AT&T ESInet(NGCS/ESINET), that is geographically diverse with 12 cores and i3 compliant. This is a fully meshed MPLS network AT&T Virtual Private Network (AVPN) which is designed for 99.999% service availability.

State of North Carolina

Client's Name	State of NC 911 Board
Contract Number	41-DIT-100086
Contact Name	(Ms.) L.V. Pokey Harris, MPA, ENP
Telephone Number	919-754-6621 Mobile: 276-759-6419
Email Address	pokey.harris@nc.gov
Project Dates	2017 - Current
Contract Term	7 Years
Contract Type	Statewide
Population Served	10.7M
Concurrent Project	Yes
PSAPs Contracted	192
PSAPS Deployed	192
Description of Project and/or Technical Environment	The solution is AT&T ESInet(NGCS/ESINET), that is geographically diverse with 12 cores and i3 compliant. This is a fully meshed MPLS



network AT&T Virtual Private Network (AVPN) which is designed for 99.999% service availability. AT&T provides the following additional services: Hosted Call Handling (As a Service) using Motorola VESTA & Intrado VIPER, RapidDeploy Eclipse Analytics, AT&T ESInet that is geographically diverse with 6 cores and i3 compliant.

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

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

The bidder should identify the specific professionals who will work on the Commission’s project if their company is awarded the contract resulting from this solicitation. The names and titles of the team proposed for assignment to the Commission project should be identified in full, with a description of the team leadership, interface, and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

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

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

AT&T Response:

AT&T has identified a dedicated team of key personnel to support the successful delivery, operation, and ongoing support of the proposed NG911 solution. An organizational chart outlining roles, responsibilities, and reporting relationships is included as part of AT&T’s proposal below. This team includes, at a minimum, a Project Manager, Technical Lead, Security Lead, Service Manager, Technical Engineer/Coordinator, and Provisioning Coordinator, each with demonstrated experience supporting complex, mission-critical public safety and NG911 environments. AT&T’s depth of resources and established NG911 delivery teams provide bench strength and succession planning to ensure continuity of service and project leadership throughout the life of the contract.



Resumes for all Key Personnel are provided in **Appendix A – AT&T Staff Resumes** and document relevant experience, qualifications, and applicable certifications. AT&T acknowledges and accepts that the State retains approval rights for all Key Personnel assignments and for any subsequent personnel changes. AT&T further commits to providing no less than thirty (30) days' written notice prior to the departure or replacement of any Key Person, except in circumstances beyond AT&T's reasonable control, and will work cooperatively with the State to ensure continuity of service and project stability. All personnel references whose resumes are included may be checked with the appropriate project reference customers listed above.

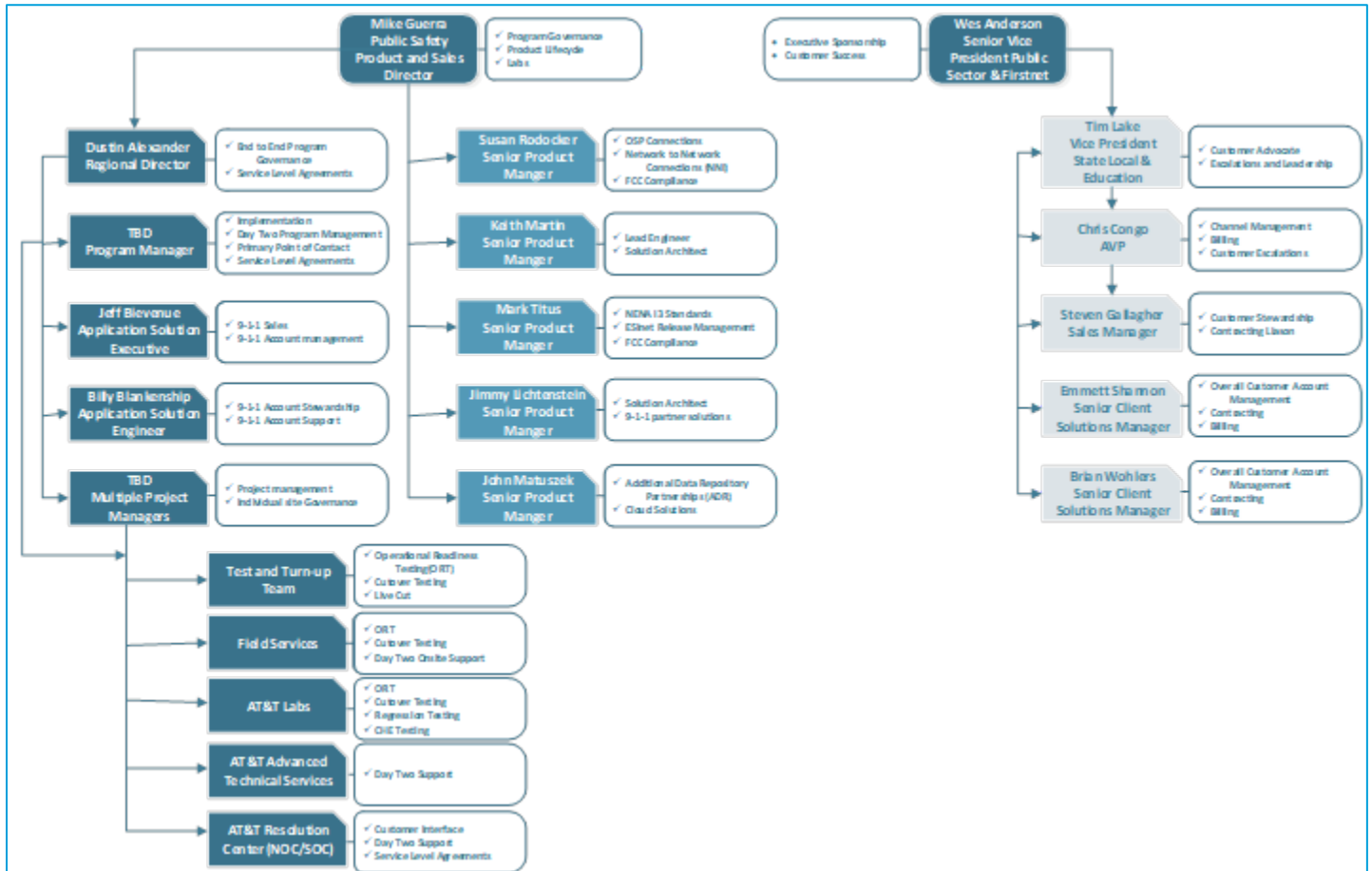


Figure 1: AT&T Key Project Personnel

Program Management and Approach

AT&T will manage this project using a proven, repeatable approach aligned to Project Management Institute (PMI) best practices and informed by ITIL service transition principles to ensure a controlled implementation and a smooth transition to steady-state operations. Following award, AT&T will provide a dedicated Program/Project Manager as the single point of contact to the Nebraska Public Service Commission (NPSC) and will coordinate all internal AT&T delivery teams and subcontractors (if any) to execute the approved project plan.



1) Governance and project organization

- **Project governance:** Establish a joint governance structure with the NPSC (and, as applicable, the State 9-1-1 Office/State 911 Director and the 9-1-1 Advisory Committee) that defines meeting cadence, decision rights, and escalation paths.
- **Defined roles and responsibilities:** Provide a RACI that identifies responsibilities across the NPSC, Nebraska PSAP stakeholders, AT&T, and external parties (e.g., Originating Service Providers (OSPs), neighboring ESInets, and other interfacing providers) for all major deliverables.
- **Single point of contact:** The AT&T Program/Project Manager coordinates schedule, deliverables, dependencies, and communications with the NPSC and maintains the integrated master schedule and action logs.

2) Phased delivery methodology

AT&T will execute the project through phased delivery with stage gates to confirm readiness before progressing:

- **Initiate / Mobilize:** Contract kickoff, stakeholder alignment, project charter, governance launch, and confirmation of objectives and constraints.
- **Plan / Define:** Requirements validation, PSAP and OSP discovery/data collection, site readiness review, dependency mapping, and baseline schedule and acceptance criteria.
- **Design / Engineer:** Finalize solution design details, interconnect and routing design, security design, and implementation runbooks/methods of procedure (MOPs).
- **Implement / Configure:** Provision circuits and interconnects, configure ESInet/NGCS elements, set up monitoring/reporting, and prepare migration assets.
- **Test / Validate:** Execute Operational Readiness Testing (ORT), interoperability testing, and cutover readiness reviews; remediate defects with regression testing.
- **Cutover / Transition:** Phased PSAP migration and OSP onboarding as scheduled, with defined rollback procedures and parallel operations as required.
- **Stabilize / Close:** Hypercare period, operational handoff to service management, final documentation delivery, and formal acceptance/closeout.

3) Scope, schedule, and deliverables control

- **Project Management Plan (PMP):** Maintain a living PMP that includes WBS, milestone schedule, deliverables, assumptions, dependencies, and a clear handoff from implementation to operations.
- **Integrated master schedule:** Track milestones, critical path, and PSAP-by-PSAP activities; identify impacts early and propose recovery plans when needed.



- **Deliverables management:** Maintain a deliverables register with owners, due dates, review/approval workflow, and version control.

4) Risk, issue, and dependency management

- **Risk register:** Identify, assess, and track risks (probability/impact) and mitigation actions from kickoff through acceptance.
- **Issue log and escalation:** Manage issues with owners, target dates, and escalation thresholds; provide visibility in status reporting.
- **Dependency tracking:** Actively manage external dependencies (e.g., PSAP readiness, OSP circuit ordering, third-party interconnects) and coordinate remediation plans.

5) Change and configuration management

- **Change control:** Evaluate scope, schedule, and operational impacts of proposed changes; obtain required approvals prior to implementation.
- **Configuration control:** Maintain controlled configuration baselines for routing, GIS-related inputs affecting call delivery, and system configurations, with traceability and auditability.

6) Communications and status reporting

- **Cadence:** Conduct regular status meetings (typically weekly during implementation, with additional working sessions as needed).
- **Reporting:** Provide written status reports that include accomplishments, upcoming work, milestone health, risks/issues, decisions needed, and change requests.
- **Stakeholder communications:** Coordinate PSAP and OSP communications for migrations, testing windows, and operational notifications consistent with an agreed communications plan and NPSC direction.

7) Quality, testing, and acceptance management

- **Quality management:** Apply defined QA/QC checkpoints across deliverables and configurations prior to cutover.
- **Test planning and execution:** Develop/maintain test plans and procedures, document results, and support retesting and regression testing following defect remediation.
- **Acceptance:** Support formal acceptance criteria and sign-off for major deliverables and cutover readiness, including NPSC participation and any required independent validation and verification.

8) Transition to operations



- **Operational handoff:** Execute a controlled transition to AT&T service management, including runbooks, as-built documentation, and operational procedures.
- **Hypercare:** Provide post-cut support to stabilize services and confirm performance and operational readiness.

9) Tools and project artifacts

AT&T will use standard project controls and documentation (e.g., schedule, RAID log, action items, meeting notes, deliverables register, change log, and test/acceptance documentation) and commonly used productivity tools (e.g., Microsoft Project, Excel, Word, and Visio) to provide transparent tracking and repeatable execution.

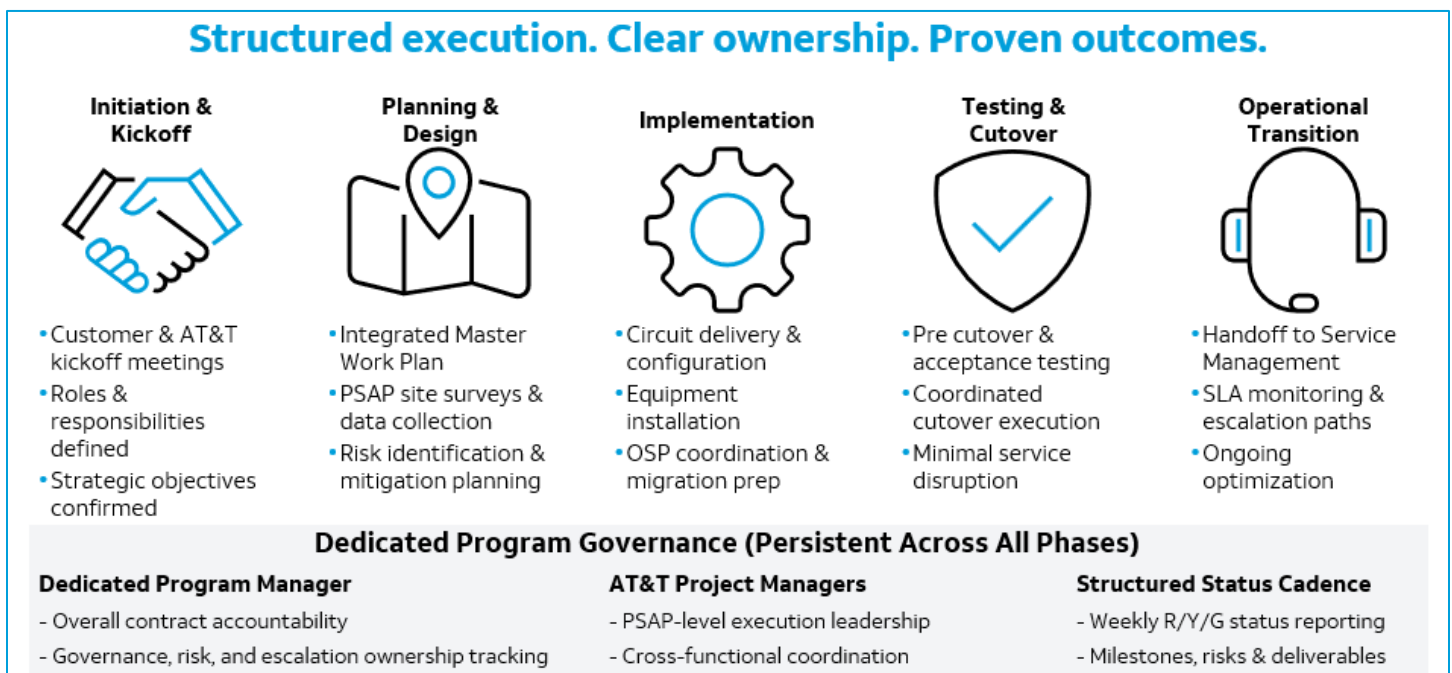


Figure 2: AT&T NG911 Project Management & Governance Model

j. SUBCONTRACTORS

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

- name, address, and telephone number of the subcontractor(s),
- specific tasks for each subcontractor(s),
- percentage of performance hours intended for each subcontract; and



- iv. total percentage of subcontractor(s) performance hours;
- v. whether the subcontractor is affiliated with the bidder or has common ownership.

Please note the definition of “subcontractor” in the glossary in providing a proper response to this.

AT&T Response:

AT&T intends to subcontract certain portions of its performance under this solicitation, as that term is defined in the RFP Glossary.

AT&T intends to utilize Intrado Life & Safety, Inc. (Intrado) as a subcontractor to support part of the proposed NG9-1-1 solution for the State of Nebraska. Intrado’s participation is provided in accordance with the RFP requirements and the Glossary definition of “Subcontractor.”

i. Subcontractor Name, Address, and Telephone Number

Intrado Life & Safety, Inc.
1601 Dry Creek Dr, Suite 250
Longmont, CO 80503
720-494-5800

ii. Specific Tasks to Be Performed by Subcontractor

Intrado Life & Safety, Inc. will support AT&T, the prime contractor(s) by providing Next Generation Core Services (NGCS) and Location Database (LDB) software and related services, including NGCS application functionality, system integration support, operational support services, and coordination necessary to support compliant NG9-1-1 call routing and delivery. All subcontracted activities will be performed under the direction of the prime contractor(s) and in coordination with AT&T.

iii. Percentage of Performance Hours Intended for Each Subcontractor

At the time of proposal submission, the final percentage of performance hours for Intrado is dependent on the State’s final implementation sequencing, PSAP onboarding schedule, and confirmed scope allocations established during post-award planning. AT&T will finalize and provide the percentage of Intrado performance hours within ten (10) business days of contract award (or by completion of project kickoff, whichever occurs first), and will manage subcontractor work under AT&T’s project governance and change control.

iv. Total Percentage of Subcontractor Performance Hours

AT&T will provide the total percentage of subcontractor performance hours within ten (10) business days of contract award (or by completion of project kickoff, whichever occurs first).

v. Affiliation / Common Ownership Disclosure



Intrado Life & Safety, Inc. is not affiliated with, and does not share common ownership with AT&T.

Prime accountability

AT&T will remain the State of Nebraska's single point of accountability for all deliverables, service levels, security obligations, and performance outcomes, including any work performed by subcontractors. Subcontractors will operate under AT&T-led governance, ticketing/escalation, change management, and acceptance testing, and AT&T will be responsible for ensuring subcontractor compliance with contract requirements.

AT&T's proposed solution delivers Nebraska a statewide, public-safety-grade NG911 platform backed by the scale, resiliency, and operational maturity of a national carrier—without sacrificing Nebraska's governance, control, or interoperability goals. For Nebraska, this means a standards-based ESInet and NGCS implementation that is already operating at scale across thousands of PSAPs, supported by 24x7x365 NOC/SOC monitoring, disciplined program governance, and proven migration methods that protect continuity of service during transition. AT&T will partner with the NPSC, PSAPs, and Originating Service Providers to execute a phased, test-driven cutover with defined acceptance criteria, rollback planning, and transparent reporting—while enabling future-ready capabilities such as multi-media, enhanced data delivery, and seamless interconnection to neighboring ESInets. In short, AT&T brings Nebraska a low-risk path to NG911 modernization that prioritizes reliability for citizens, operational confidence for PSAPs, and long-term sustainability for the State.

FACTORS USED TO EVALUATE CORPORATE OVERVIEW

Corporate Overview will be evaluated as follows:

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

In evaluating the corporate overview, the Commission may consider: past experiences with the vendor; references; the Department of Administrative Services' record of the vendor, which may include, but is not limited to Vendor Compliance Request, Contract Non-Compliance Notice, or vendor performance reports; and any information related to the vendor's historical or current character, integrity, reputation, capability, or



performance with the Commission, State or a third-party. Information obtained from any Contract Compliance Request or any Contract Non-Compliance Notice may be used in evaluating responses to determine the best value for the State.

AT&T Response:

AT&T Enterprises, LLC ("AT&T") provides this Corporate Overview response to demonstrate the qualifications the Nebraska Public Service Commission (NPSC) may consider in its evaluation. AT&T is committed to delivering a secure, resilient, standards-based NG911 solution and to performing all work in a manner consistent with applicable law, ethical business practices, and the requirements of this Solicitation.

- **Ability, capacity, and skill (i):** AT&T has the technical expertise, operational scale, and dedicated NG911 resources required to design, implement, integrate, and operate a statewide ESInet and NGCS solution consistent with NENA i3 requirements and the performance objectives described in this Response.
- **Character, integrity, reputation, judgment, experience, and efficiency (ii):** AT&T maintains established corporate governance, compliance, and security programs and brings substantial experience delivering mission-critical communications services. AT&T's project delivery approach leverages repeatable methods, disciplined controls, and continuous improvement to support efficient execution.
- **Ability to perform within the specified timeframe (iii):** AT&T will partner with the NPSC, PSAPs, and Originating Service Providers (OSPs) to develop and maintain an integrated master schedule, manage dependencies, and execute phased testing and cutover to meet required milestones.
- **Historical/current performance (iv):** AT&T's proposed solution is based on the AT&T ESInet™ platform and associated NG911 capabilities described in this proposal, which are in operational use supporting public safety communications. AT&T will provide service management, monitoring, reporting, and escalation processes to support SLA performance throughout the contract term.
- **Other relevant information (v):** Upon request, AT&T will provide customer references and additional information reasonably necessary for evaluation, consistent with confidentiality obligations. AT&T understands the State may review Department of Administrative Services vendor records (including any Vendor Compliance Request, Contract Non-Compliance Notice, and performance reports) and will cooperate as appropriate to support the State's best-value determination.



2. RESPONSE TO SCOPE OF WORK

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

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

Services to be Provided

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

1. ESInet Architecture and Design

- a. Contractor shall provide an ESInet design and implementation conforming to the NENA i3 ESInet architecture and functional requirements, including multi-site, geographically diverse redundant cores, session border control at boundaries, and tenant isolation. (This includes bandwidth provisioning, diagrams, availability, and reliability features).

AT&T Response:

Comply.

To meet The State of Nebraska RFP requirements, AT&T proposes its flagship multi-tenant isolated, 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). AT&T ESInet™ is prebuilt with 6 geo-diverse locations, consisting of 12 NGCS cores. The solution has been in live production since 2018 with over 69K hours of operation. AT&T's ESInet solution provides the Public Safety community with an i3 architecture built from the ground up.



Our qualifications and innovation experience in 9-1-1 and public safety are unparalleled, starting over 50 years ago with the first 9-1-1 call and evidenced most recently through the implementation of our National AT&T



ESInet™ call routing infrastructure, FirstNet public safety broadband network (PSBN), and rollout of 5G wireless technology.

AT&T's ESInet deployments currently reach into 18 states and the nation's capital serving over 2,000 PSAPs that are either in production or under contract. No other provider has the same depth of experience in architecting and delivering mission critical Next Generation 9-1-1 solutions.

With AT&T ESInet™, Nebraska can take advantage of a market proven solution capable of agnostic interoperability between the call-routing and call handling solutions. Our Network-to-Network Interface (NNI) will provide interoperability with third-party ESInet providers to enable IP call transfers to neighboring PSAPs outside of Nebraska.

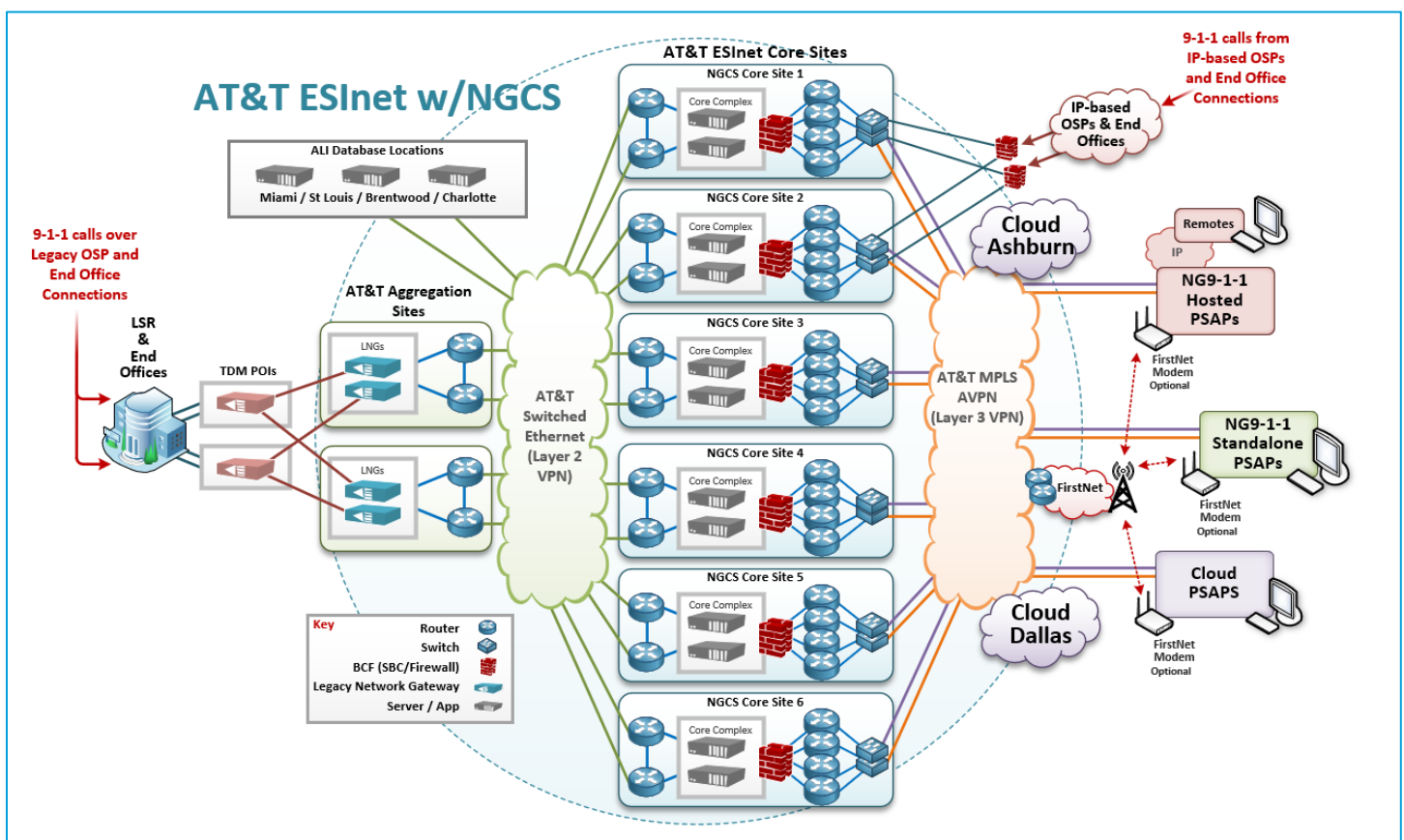


Figure 3: AT&T ESInet Architecture

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



AT&T Response:

Comply.

AT&T supports both IPv4 and IPv6 addressing and implements Quality of Service mechanisms, including DiffServ or equivalent, to ensure priority handling of emergency signaling and media traffic. Bandwidth and capacity requirements for all services will be documented, and applicable 99.999% availability objectives will be incorporated into the Service Level Agreement.

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

AT&T Response:

Comply.

AT&T supports SIP signaling in accordance with RFC 3261 and applicable NG911 SIP extensions, including the use of SIP over TLS for signaling and SRTP for media, where applicable. The solution supports end-to-end SIP call flow across the ESInet, ensures calls are not lost, and provides SIP interconnection and mediation with external peers, including protocol conversion where required.

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

AT&T Response:

Comply.

AT&T provides documented peering and interconnect interfaces, including LNG, LSRG, LPG, SBCs, other edge elements, and defined Points of Interconnection. AT&T will also provide APIs and documented procedures to support peering with other ESInets and third-party providers, including supporting configuration management data, network diagrams, and IP addressing schemas.

The following interface specifications are provided to 3rd parties connecting to the AT&T ESInet and can include Call Handling Equipment vendors, Originating Service Providers as well as other ESInet providers. The following specifications assist 3rd parties in connecting to the ESInet.

- AT&T ESInet ESRP-Terminating ESRP Interface Specification v2.0
- AT&T ESInet LIS-HELD Interface Specification v2.1



- AT&T ESInet ADR-AdditionalData Interface Specification v1.3.4
- AT&T ESInet ECRF-LoST Interface Specification v1.4.6
- AT&T ESInet-to-ESInet SIP Interconnection Specification-i3_v3.2
- AT&T ESInet-to-ESInet Interface Specification SIP Basic_v3.4.1
- AT&T LVF-LoST Interface Specification_v1.2.2
- AT&T Interface Standards_OSP Networks_Foreign ESInets_v1.3.1
- AT&T OSP Network Interface Specification SIP Basic_v.2.4_Final
- AT&T OSP SIP NNI i3_v2.1

2. NG911 Core Services (NGCS)

- a. Contractor shall provide or interoperate with NGCS functional elements (BCF, ESRP, ECRF, LVF/LIS, MSAG/ALI-equivalent services, ESRP/ESRP-like routing proxy, etc.) as defined in the NENA i3 Standard and shall map which product components implement each NGCS function.

AT&T Response:

Comply.

AT&T will provide and/or interoperate with all required NG911 Core Services (NGCS) functional elements in accordance with the NENA i3 Standard. The proposed solution supports standards-based integration with core NGCS functions, including the Border Control Function (BCF), Emergency Services Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Location Validation Function / Location Information Server (LVF/LIS), MSAG/ALI equivalent services, and ESRP like routing proxies.

Each NGCS function is implemented through clearly defined product components or interoperates via NENA i3compliant interfaces to ensure seamless call routing, location validation, and policy-based decision making across the NG911 ecosystem. AT&T will provide a functional mapping that identifies which solution components deliver or interoperate with each NGCS element, ensuring full alignment with NENA i3 architecture and functional requirements.

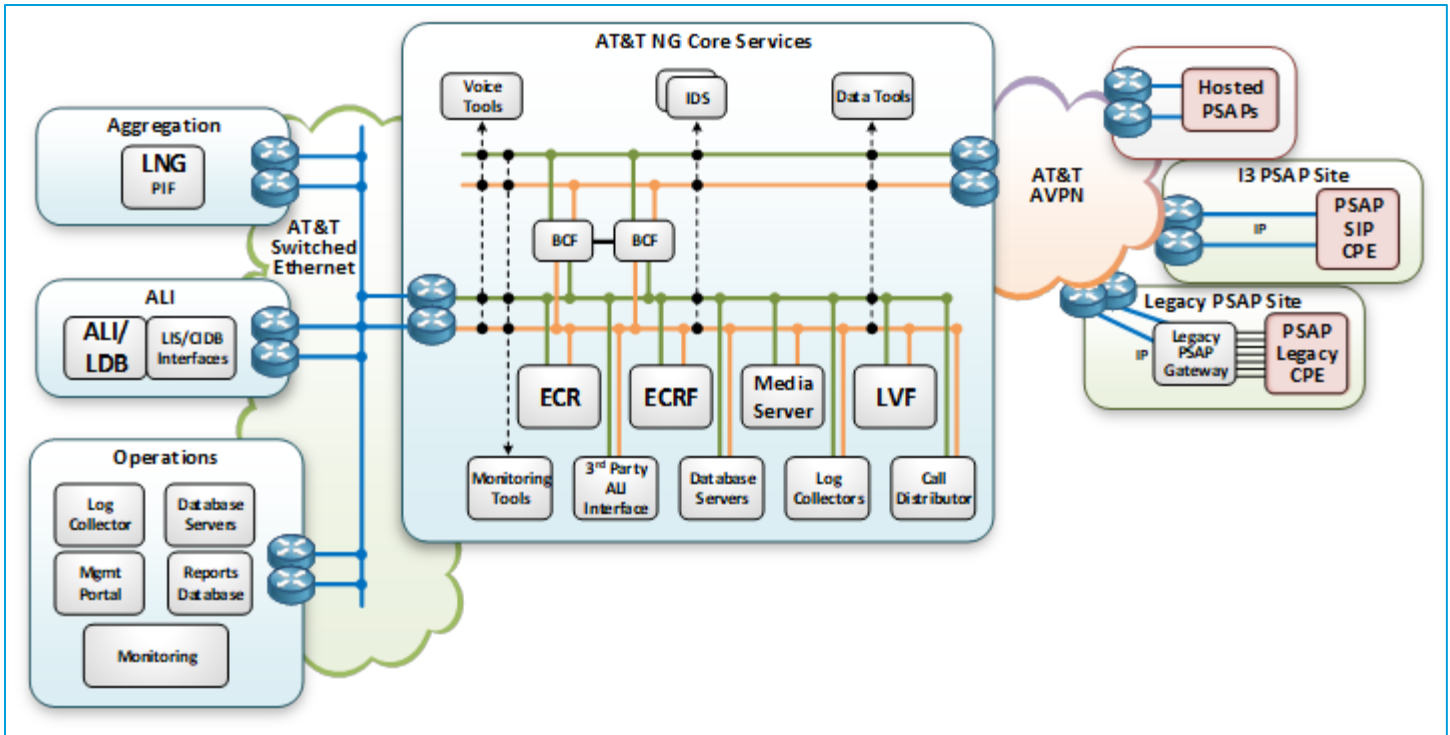


Figure 4: AT&T ESInet NGCS Functional Elements

Component Location	Component	NGCS Function
Aggregation	LNG	LNG - PIF
ALI	LDB	ALI equivalent services
ALI	LDB	MSAG equivalent services
NG Core Services	Logger	i3 Logging
NG Core Services	Database Servers	Data rights management
NG Core Services	ECR	ESRP
NG Core Services	ECR	PRF
NG Core Services	ECR	LNG - LIF / NIF
NG Core Services	BCF	BCF
NG Core Services	ECRF	ECRF
NG Core Services	LVF	LVF
NG Core Services	Media Server	Bridging

b. Contractor shall implement NGCS interfaces per the NGCS Interface Standard (SIP and REST interfaces, expected message formats including PIDF-LO where applicable) and shall provide interface documentation, schemas, and test harness endpoints.



AT&T Response:**Comply.**

AT&T implements NG911 Core Services (NGCS) interfaces in accordance with the NGCS Interface Standard, utilizing standards-based SIP and REST interfaces and supporting required message formats, including PIDF-LO where applicable. The proposed solution adheres to NENA i3 interface specifications to ensure interoperable call signaling, location conveyance, and policy-driven routing across the NG911 ecosystem.

Comprehensive interface documentation is provided, including interface descriptions, schemas, and applicable message definitions. AT&T also supports integration testing through the provision of test harness endpoints, enabling validation of interface behavior, message handling, and interoperability with external NG911 systems.

- c. Contractor shall meet stated latency and throughput SLAs for NGCS lookups and routing decisions. (99.999 from caller to call-taker unless specified in writing between the PSC and Contractor.)

AT&T Response:**Comply.**

AT&T's NG911 Core Services (NGCS) are engineered and operated to meet the stated latency and throughput service level agreements for NGCS lookups and routing decisions. The proposed solution is designed to support end-to-end call processing performance consistent with a 99.999% availability objective from caller to call taker, unless otherwise specified in writing.

Performance is continuously monitored across NGCS components to ensure timely routing, location resolution, and policy execution. AT&T's operational controls and service management practices are aligned to maintain SLA compliance and to support reporting and verification as required.

3. GIS and Location-Based Routing

- a. Contractor shall accept, store, and use GIS data in the NENA GIS data model/schema and SHALL maintain the required NENA layers (PSAP boundaries, ESN/service boundaries, address points, civic addressing, emergency routing attributes). GIS data shall conform to normative language identified in NENA-STA-006.2-2022. The Contractor may utilize NENA-REF-006.2-2023 (NENA NG9-1-1 GIS Data Model Templates) to assist in conformance to the Standard.

AT&T Response:**Comply.**



AT&T accepts, stores, and utilizes Geographic Information System (GIS) data in full accordance with the NENA NG911 GIS Data Model and schema. The proposed solution maintains all required NENA GIS layers, including PSAP boundaries, ESN and service boundaries, address points, civic addressing, and emergency routing attributes, to support accurate location-based routing and NG911 call processing.

All GIS data conforms to the normative requirements defined in NENA-STA-006.2-2022. AT&T may also leverage the NENA NG911 GIS Data Model Templates (NENA-REF-006.2-2023) to assist in maintaining conformance and ensuring consistency across required GIS layers and attributes.

- b. Contractor shall use authoritative GIS data for routing decisions (ECRF) and shall accept location in PIDF-LO format (and convert civic/geodetic input) for routing and display.

AT&T Response:

Comply.

AT&T utilizes authoritative GIS data to support Emergency Call Routing Function (ECRF) routing decisions in accordance with NENA i3 requirements. The proposed solution accepts location information in PIDFLO format and supports the conversion of civic and geodetic location inputs to ensure accurate routing and call delivery.

Location data is processed for both routing and call taker display, enabling precise location validation, policy-based routing decisions, and consistent presentation of location information across NG911 systems.

- c. Contractor shall provide GIS data versioning, change tracking, import/export in NENA formats (e.g., GML/GeoJSON or NENA schema), and support automated incremental updates.

AT&T Response:

Comply.

AT&T provides GIS data versioning and change tracking capabilities to support control management of NG911 GIS datasets. The proposed solution supports import and export of GIS data using NENA recognized formats, including GML, GeoJSON, and NENA defined schemas, to ensure standards-based data exchange and interoperability.

AT&T also supports automated incremental GIS updates, enabling efficient propagation of changes to authoritative datasets while maintaining data integrity, version history, and routing accuracy within the NG911 environment.

4. Call Flow and Media Session Handling



- a. Contractor shall implement NENA i3 call flows (incoming SIP INVITE → ESRP/ECRF lookup → PSAP routing) preserving required SIP headers (P-Asserted Identity, Diversion, History Info, etc.) and shall deliver PIDF-LO location payloads with calls where required.

AT&T Response:

Comply.

AT&T ESInet will implement NENA i3 call flows for NG911 call processing, including receipt of incoming SIP INVITE requests, execution of ESRP processing with ECRF lookups as required, and routing to the appropriate PSAP. AT&T will preserve and properly convey required SIP headers throughout call setup and subsequent routing actions, including P-Asserted Identity, Diversion, History Info, and other applicable i3 call-signaling headers. AT&T will also deliver PIDFLO location payloads with calls when required to support accurate routing and call taker presentation.

- b. Contractor shall support real-time multimedia as defined by NENA (voice, IP text-to-911, real-time video, and supplemental data) with media negotiation, fallback behaviors, and preservation of metadata across transfers.

AT&T Response:

Comply.

AT&T supports real time multimedia communications as defined by NENA, including voice, IP based textto911, real time video, and supplemental data. The solution provides standards-based media negotiation and supports defined fallback behaviors to ensure continuity of emergency communications when preferred media types are unavailable.

All associated call metadata, location information, and supplemental data are preserved throughout call handling, transfers, and handoffs between PSAPs and NG911 systems to ensure consistent situational awareness and call integrity.

- c. Contractor shall support PSAP call transfer (warm or attended and blind transfers) while preserving call metadata and location.

AT&T Response:

Comply.

AT&T supports PSAP call transfers, including warm (attended) and blind transfers, in accordance with NENA i3 call handling requirements. All call metadata and associated location information are preserved and conveyed



throughout the transfer process to ensure continuity of call context and accurate information delivery to the receiving PSAP.

5. Security, Privacy, and Trust

- a. Contractor shall implement the NENA ESInet security and trust model including mutual TLS between NG911 elements, strong authentication and RBAC for administrative interfaces, and secure boundary elements (SBCs).

AT&T Response:

Comply.

AT&T implements the NENA ESInet security and trust model across its NG911 solution. This includes the use of mutual TLS (mTLS) for secure communication between NG911 functional elements, strong authentication mechanisms, and role-based access control (RBAC) for administrative and management interfaces.

Security controls are further enforced through the deployment of secure boundary elements, including Session Border Controllers (SBCs), to protect NG911 interfaces, manage trust relationships, and safeguard signaling and media traffic within the ESInet.

- b. Contractor shall encrypt sensitive data in transit (TLS 1.2+ / TLS 1.3) and at rest (AES-256 or equivalent), provide PKI/certificate lifecycle management, and protect cryptographic keys using a hardware security module or equivalent. Contractor shall support certificate revocation.

AT&T Response:

Comply.

AT&T encrypts sensitive data both in transit and at rest in accordance with industry best practices. Data in transit is protected using TLS 1.2 or higher, including TLS 1.3 where supported, and data at rest is encrypted using AES256 or equivalent encryption standards.

AT&T provides public key infrastructure (PKI) and certificate lifecycle management, including certificate issuance, renewal, and revocation. Cryptographic keys are protected using hardware security modules (HSMs) or equivalent secure key management technologies to ensure confidentiality, integrity, and compliance with NG911 security requirements.

- c. Contractor shall provide incident response and vulnerability management processes and supply recent third-party penetration test reports and remediation plans.



AT&T Response:**Comply.**

AT&T maintains formal incident response and vulnerability management programs aligned with industry best practices. These processes include detection, analysis, containment, remediation, and post incident review to ensure timely and effective response to security events.

AT&T provides recent third-party penetration testing reports upon request, along with documented remediation plans that address identified findings and track corrective actions to resolution.

- d. Contractor shall satisfy Neb. Rev. Stat. 86-125 by completing the affidavit provided by the State regarding the use of prohibited communications equipment by communications providers.

AT&T Response:**Comply.**

AT&T will comply with Neb. Rev. Stat. § 86125 by completing and submitting the affidavit provided by the State regarding the use of prohibited communications equipment by communications providers, as required.

6. Logging, Reporting, and Call Detail Records

- a. Contractor shall produce end-to-end logs and Call Detail Records (CDRs) for every emergency transaction containing timestamps and share with the data analytics engine, correlation IDs, call identifiers, caller identity (if available), location used for routing, PSAP destination, media types, and call disposition.

AT&T Response:**Comply.**

AT&T produces comprehensive end-to-end logs and Call Detail Records (CDRs) for every emergency transaction. These records include timestamps, correlation IDs, call identifiers, available caller identity, routing location, PSAP destination, media types, and call disposition, and are shared with the data analytics engine to support monitoring, troubleshooting, and reporting.

- b. Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats.

AT&T Response:



Comply.

AT&T provides secure storage for logs and Call Detail Records (CDRs) with appropriate protections to maintain confidentiality and integrity. Access to log and CDR data is controlled through role based access controls (RBAC), ensuring that only authorized users can view or manage this information. AT&T also supports export of logs and CDRs in open, nonproprietary formats to facilitate reporting, analysis, and data sharing.

- c. Contractor shall provide operational reports (call volume, answer times, transfers, location failure rates, outage reports) and support ad-hoc queries.

AT&T Response:**Comply.**

AT&T provides a comprehensive set of operational reports to support NG911 oversight and performance management. Standard reporting includes call volume metrics, answer times, call transfers, location failure rates, and outage reporting, with data available for operational review and analysis. AT&T also supports ad-hoc queries to enable customers to obtain additional operational insights as needed.

7. Interoperability, Testing, Conformance, and System Acceptance

- a. Contractor shall participate in jurisdiction-specified interoperability and conformance testing, independent third-party validation and verification, demonstrate NGCS and ESInet interfaces in a test harness, and provide test results and logs.

AT&T Response:**Comply.**

AT&T will participate in jurisdiction specified interoperability and conformance testing activities, including independent third-party validation and verification, testing of all elements required in this procurement. AT&T will demonstrate ESInet, NGCS, GIS, security, logging and operational support components.

- b. Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals.

AT&T Response:**Comply.**



AT&T will provide complete product documentation for the proposed NG911 solution, including detailed API specifications, operator and administrator manuals, and operational runbooks. AT&T also delivers role appropriate training to support system operations, administration, and ongoing maintenance.

8. Operational Support and Service Level Agreements (SLAs)

- a. Contractor shall negotiate with the PSC to establish firm SLAs for availability, incident response, escalation, mean time to repair (MTTR), change management procedures, and maintenance windows.

AT&T Response:

Comply.

AT&T will work collaboratively with the Public Service Commission (PSC) to define and formalize service level agreements governing system availability, incident response, escalation procedures, mean time to repair (MTTR), change management processes, and scheduled maintenance windows. SLAs will be mutually agreed upon and documented to support reliable operations and clear performance expectations.

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

AT&T Response:

Comply.

AT&T has documented rollback and contingency plans for major system upgrades. AT&T will provide documented rollback and contingency plans for that impact routing, GIS data, or call handling functionality as necessary. These plans are designed to minimize operational risk and support timely restoration of services should an update require reversal.

Applicable Standards

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

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



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

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

Federal Communications Commission Rules

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

Other Industry Standards

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

- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- Open Systems Interconnection (OSI)
- Telecommunications Industry Association (TIA)
- Underwriters Laboratories (UL) Respondents must propose a system that utilizes an Open Standards Methodology:

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

- The proposed system shall be subject to standards that enhance open standards and increase interoperability such as ITU, IEEE 802 at OSI Layer 2, and IP and TCP, as defined by the IETF in the applicable RFCs, at OSI Layer 3 and above.
- If proprietary standards or protocols are used within a proposed solution, Respondents shall disclose the proprietary nature and discuss any limitations that may result.

AT&T Response:

Comply.



AT&T and its partner, Intrado, are committed to supporting the NENA standards, both current and future.

AT&T is committed to supporting the NENA STA-010.3 standards for all external interfaces included in our solution that require interoperability with other vendors' systems. AT&T adheres to the various required interoperability protocols specified for use in the NENA i3 standards, such as HELD, LoST, Additional Data, MSRP, and others.

All applications, equipment, services, and systems that will be performing NG9-1-1 related functions use open standards. The AT&T ESInet system does not use proprietary software or hardware.

AT&T's solution is compatible with is working to fulfilling our obligation toward compliance with NENA-STA-010.3-2021, Detailed Functional and Interface Specification for the NENA i3 solution.

Our proposed solution is built on an open, standards-based platform utilizing standards such as IEEE 802 at ISO Layer-2, and IP and TCP, as defined by the Internet Engineering Task Force (IETF) in the applicable RFCs, at ISO Layer-3 and above. The system complies with SIP (RFC 3261), LoST (RFC 5222), PIDF-LO (RFC 4119 and successive updates), NENA STA-010.3, IETF ECRIT best practices, and ANSI standards.

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

AT&T's solution complies with the FCC 911 Reliability rules and requirements (FCC Report and Order FCC 13-158), including the audit requirements and submitting an annual report to the customer.

AT&T ESInet also complies with the following:

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

Conformance to Standards Baseline Conformance

AT&T Response:



Comply.

AT&T understands the State's preference for full conformance with NENA-STA-010.3 at System Acceptance and proposes a solution designed to meet that baseline wherever practicable. AT&T will ensure the solution remains current with NENA standards as they evolve over the contract term. Where certain capabilities require additional development, AT&T will clearly identify any gaps and provide a plan and timeline to achieve full conformance.

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

Gap Identification (Proposal Requirement)

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

AT&T Response:

Comply.

AT&T sees no gaps with NENA-STA-010.3.

Note:

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

Standards Updates (Post-Award)

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

AT&T Response:

Comply.



AT&T will work with The State to implement updated NENA standards within 9 months where possible.

Non-Disclosure and Breach

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

AT&T Response:

Comply.

AT&T has read and understood the requirement.

Deviation Classification (Proposal Requirement)

Each deviation must be classified as one of the following:

- **NENA-STA-010.3 upgrade, proposed date:** The delivered system conforms for the feature, and the proposal includes an estimated date for providing the **NENA-STA-010.3** upgrade to the State (no later than **Contract Year 2**).
- **Missing capability, proposed date:** The delivered system does **not** conform to NENA-STA-010.3 for the feature; the proposal includes an estimated upgrade date (no later than **Contract Year 2**).
- **Missing capability, no proposed date (will be provided):** The delivered system does not conform to **NENA-STA010.2** or **NENA-STA-010.3** for the feature; the proposal commits to provide the capability but does not specify a date.
- **Missing capability, no plans:** The delivered system does not conform and there is no intention to conform. An alternative to the **NENA-STA-010.3** feature may be proposed for State consideration.

AT&T Response:

Comply.

AT&T has read and understood the requirement.

Remediation Plan and Progress



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

Interoperability

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

- If the Contractor is required to make changes, it shall propose a completion date acceptable to the State.
- If the issue lies with the other vendor, the Contractor shall cooperate in testing but has no further responsibility.
- If the other vendor conforms to **NENA-STA-010.2**, the State's system conforms to **NENA-STA-010.3**, and the issue falls outside the **010.3** backward-compatibility statements for **010.2**, the Contractor is **not** required to make changes.

AT&T Response:

Comply.

The proposed solution is fully designed to interoperate with any system conforming to NENA-STA-010.3, using only open standards and proven interfaces for SIP, LoST, HELD, MSRP, and related NG911 functions. When interoperability issues arise, AT&T will collaborate with the State and any involved vendors to jointly identify the source of the problem and determine corrective actions, following the intent of NENA-STA-010.3. If changes are required within AT&T's system, AT&T will propose a remediation timeline acceptable to the State and complete all necessary updates and regression testing. If the issue is determined to originate with another vendor, AT&T will continue to support testing and diagnostics but will not be responsible for making system changes. Likewise, if both the other vendor and AT&T are conformant to their required NENA versions and the issue falls outside NENA-STA-010.3 backward-compatibility provisions, no AT&T modifications will be required.

NENA NG911 i3 Standard Conformance

The following section includes references to conformance with **NENA-STA-010.3**. The absence of an explicit reference **DOES NOT** imply the State does not require conformance to that portion of the Standard. The State



requires conformance to the full standard, while recognizing the practicalities of achieving conformance within the contract period as described above.

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

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

Status must be presented with one of the following options:

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

Remainder of page intentionally blank



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

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



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
	Includes BCF, Bridge and logging service support	
MSRP	Instant Messaging Service	Implemented
Non-Human Initiated Calls	Support for IoT devices, alarms, etc.	Implemented
TLS (Transport Layer Security) transport of SIP	Provides secure call signaling	Implemented
SRTP	Provides secure media (voice, video, text) for calls	Implemented
RTCP support on all SIP entities	Provides secure control of RTP (Real Time Transport Protocol) streams	Implemented
RTCP Extended Reports	Provides diagnostic information on media streams	Implemented
PSAP detection of loss of RTP vs silence	Differentiates silent calls from mechanical loss of audio media stream	Implemented
Element Overload (RFC 7339)	Graceful coping with too many SIP calls	Implemented
STUN/TURN/ICE	Standards based mechanisms for NAT Traversal	Implemented
NG-AACN Support	Update to Automatic Car Crash Notification standards	Implemented
SIP Presence for location	Allows OSPs to send location updates for mobile devices without manual rebid (requires OSP to implement also).	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Policy Store i3v3 interface	Interoperable policy repository that allows 3rd party editors/verifiers/etc.	Implemented
Multiple Geolocation	Accepts more than one location reported in a 911 call	Implemented
Discrepancy Reporting mechanism + i3v3 defined DRs (Discrepancy Report)	Standardized way to report discrepancies with standardized responses	Implemented
Bad Actor mechanism	Allows PSAP to stop repeated bad calls from a source	Implemented
Call Suspicion mechanism	Allows the system to mark calls that MAY be bad, and then treat them specially at the PSAP (warnings, special queues, etc.)	Implemented
QueueState	Allows Policy routing based on queue congestion	Implemented
DequeueRegistration	Allows multiple PSAPs and other entities to dequeue from a queue	Implemented
ESRPnotify	Allows policy routing rule to notify some entity that a condition was encountered	Implemented
AbandonedCall	Standardized way to report a call that was hung up before PSAP got the call	Implemented
Service/Agency Locator	Service that allows discovery of things on any ESInet rather than provisioning it.	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
XACML based data rights management	Standardized way to control who has access to what data	Implemented
EIDO on Transfer	Mechanism to transfer call state to a PSAP along with the call	Implemented
3rd Party Origination	Allows a 3rd party, like Video Relay Interpreter, to be automatically added to a call as a 3 way	Implemented
RTT	Real Time Text support, includes multiparty RTT (Real Time Text) support (RFC 9071) and mixer support for nonaware devices	Implemented
Resource Priority header	Allows SIP Resource Priority handling of SIP messages. All SIP entities support it, BCF polices/inserts it.	Implemented
Incoming Baudot is converted to RTT	TTY to/from OSP converted to Real Time Text by LNG (Legacy Network Gateway) (Baudot to RFC 4103)	Implemented
Outgoing Baudot is converted to RTT	TTY to/from PSAP converted to Real Time Text by LPG (Legacy PSAP Gateway) (Baudot to RFC 4103)	Implemented
Multipart MIME (BCF, bridge, media server)	Allows multiple SIP bodies. Typically, this is Location by Value plus SDP.	Implemented
SRV records for SIP interface resolution (BCF/ESRP and PSAP)	Standard mechanism to derive SIP connection address from a domain name	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Support for Outbound (RFC 5626)	SIP Protocol fixes for outbound calls	Implemented
i3v3 Syntax and Semantics for Policy Routing Rules	Standardized Syntax and Semantics for Policy Routing Rules	Implemented
SBC inserts NENA-Source parameter	Allows PSAP to identify which SBC (BCF component) handled a call. Used with Bad Actor	Implemented
ESRP supports AdditionalData dereference for PRR	Allows policy routing based on additional data	Implemented
ESRP handles incoming admin calls	Allows policy routing of admin calls	Implemented
ESRP policy routes calls to other agencies	Allows calls to other PSAPs, responders, to be policy routed. Includes extraction of location from an EIDO	Implemented
Support for incoming identity validation	STI-VS implemented to return STIR/SHAKEN validation on incoming calls.	Implemented
Gap/Overlap	Tells agencies about gap or overlap discovered by ECRF/LVF in GIS data	Implemented
ECRF handles any standard shape	Location can be specified by polygon, circle, ellipse, or arc band, in addition to point	Implemented
ECRF returns service boundary	ECRF can return a polygon, within which, the response will still be valid	Implemented
ECRF Supports lost-planned-changes	allows planned changes in GIS to occur on a schedule	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
matchType and degradedMatch implemented	Allows querier to know how validation was determined and receive a warning that validation was not necessarily as good as intended	Implemented
i3v3 Appendix B/NG GIS implemented	Updated GIS provisioning data model	Implemented
Support CLDXF location	US profile of PIDF-LO, FGDC conformant.	Implemented
Internal and External ECRF/LVF supplied	ECRF and LVF (Location Validation Function) for public and OSP support available on the Internet, separate from internal ECRF/LVF available on ESInet	Implemented
ECRF/LVF replica support	Interface that allows an OSP or other entity to maintain a local copy of the ECRF/LVF	Implemented
Interconnected ESInet support	Allows neighboring ESInets to connect to the State ESInet. Supports bidirectional ECRF/LVF query, call transfer, etc.	Implemented
Forest Guide Support	Entry in FG for State ECRF/LVF, and recursive resolution of out of area queries via the FG	Implemented
MCS (MSAG Conversion Service) and GCS (Geocode Conversion Service) are implemented	MCS = MSAG (Master Street Address Guide) Conversion Service, converts between MSAG form of address and PIDF-LO. GCS=Geocode conversion service,	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
	provides civic to geo, or geo to civic conversion for any system	
Change in GIS results in routing change in minutes	A change in the GIS data can affect routing within minutes of the GIS authority releasing the change	Implemented
MDS implemented	Map Database Service returns maps (as images) or features to support both local and out of area maps	Implemented
Spatial Interface is implemented	Standard was to provision ECRF/LVF/MDS/GCS/MCS	Implemented
Changes to PRR effective on next call	Update of PRR policy in Policy Store causes changes in routing immediately	Implemented
i3v3 DR interface and all defined DRs implemented	Automated Discrepancy Reporting mechanism and several standard DR formats	Implemented
i3v3 Test call is supported	Automated mechanism to test the call path. No human required. Includes media check (loopback)	Implemented
i3v3 Test Call Generator supported	Automated mechanism to generate test calls (can text PRR sets)	Implemented
IS-ADR search supported at PSAP	Standardized way to check outside sources to see if they have additional data for a telephone number (like RapidSOS)	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
humintlang tag supported	Signals request for language used on a call	Implemented
Call Transfer follows i3v3 call flows	Either Ad hoc or Route All Calls Via a Conference Aware UA (User Agent) model is followed for bridge based attended transfer	Implemented
Transfers between ESInets with different bridge models supported	Transfer of calls between ESInets that have different bridge models work as defined in the i3V3 standard	Implemented
Media server supports i3v2 IMR	Standardized multimedia "Interactive Voice Response" unit (auto answer with menus). Includes audio, video, text, RTT. Includes VXML for control.	Implemented
Logging service supports all i3v3 LogEvents	Logging Service supports all i3 defined log events	Implemented
NGCS elements create the specified LogEvents	All NGCS elements generate all V3 standardized log events they should implement	Implemented
Logger logs media per the standard	Logging service logs all media per the standard	Implemented
Logger retrieval interface follows standard	Logging Service implements i3 standardized log retrieval interface	Implemented
Logger can be used as IRR (Instant Recall Recorder)	Logging Service implements the Instant Recall Recorder function	Implemented



v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
LNG supports P-Preferred-Identity + ESN/IMEI for non-initialized mobile	LNG retrieves IMEI for non-initialized phones and passes it in SIP P-Preferred Identify header	Implemented
Outgoing Call Interface Function	Supports call backs and other outgoing calls with all media supported on the incoming emergency call. Includes support for STIR/SHAKEN signing of Identity.	Implemented

Remainder of page intentionally blank



3. RESPONSE TO WORK PLAN AND PROJECT PLANNING

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

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

C. WORK PLAN AND PROJECT PLANNING

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

1. Project Management

a. Project Management Approach

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

AT&T Response:

Comply.

AT&T understands and complies with the required project management approach.

The Dedicated Program 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 percent of the Global Project Management (GPM) team is comprised of certified Project Management Professionals (PMP) as certified by the Project Management Institute. Experience includes both domestic and international components with project volumes ranging from 100 to 17,000 sites.

The AT&T Program Manager will be responsible for multiple complex projects from conception through implementation. Manage project team members including independent contractors. Develop and implement



project plans, design schedules, identify problems and alternate course of action to ensure projects are completed within corporate objectives exceeding customer expectations.

Upon contract award, the AT&T Program 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, we will establish roles and responsibilities and reach a mutual agreement with the jurisdiction 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 the implementation schedule. 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.

The AT&T Program Manager will conduct regularly scheduled project status calls with State of Nebraska 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

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 Program Managers will use the Microsoft Suite of Products to manage all projects as a standard operating procedure. Products 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
- Project Plan Phase
- Project Implementation Phase
- Project Completion Phase

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. Many times, changes occur within the life cycle of a project and process groups must be repeated.

The four project phases are briefly characterized by:

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.



Deployment

AT&T has been delivering ESInet solutions prior to the NENA i3 standards ratification and have continually updated and enhanced our service offerings with market, technology, and standards development. We are well versed in all aspects of system design, delivery, and ongoing lifecycle management. Combined, AT&T and have more than 500 resources dedicated to the national AT&T ESInet™ solution, of which the State of Nebraska will be a major benefactor. These resources are highly experienced and skilled in actual deployments.

Well-defined and coordinated cutover plans and rollback contingency plans are created in preparation for each PSAP migration. The joint AT&T and Customer team members verify system application and implementation requirements, refine the solution architecture, and finalize the plan for a successful solution deployment. Sequencing is not mandatory, but AT&T recommends to initially migrate the State of Nebraska PSAPs starting with the primary PSAP jurisdiction containing the smallest population. The migration event would include all associated secondary and back-up PSAPs. The following migrations would be scheduled based on population until the largest primary PSAP and associated secondary and back-up PSAPs were deployed.

During the Solution Deployment phase, all network components and equipment connectivity is validated, and acceptance tests are performed, and metrics tracking, and reporting are initiated. After all non-live call testing is completed, a series of transition events are executed to cut-over live 9-1-1 traffic to the AT&T ESInet™.

In preparation for deployment and in partnership with the State, the AT&T ESInet™ Program Manager finalizes the cutover plan, including procedures for notification concerning schedule specifics. To minimize impact to the PSAPs, each PSAP is cutover by receiving traffic directly from the legacy selective routers as well as any OSP end offices that have completed pre-migration provisioning and testing prior to the date of the scheduled cut. The PSAP is flash cut using procedures outlined below, and then any additional OSP traffic and end offices are rehomed post-PSAP cut. Prior to the commencement of the cutover event for the legacy selective router and OSP switches, the project team members hold a cutover meeting, and OSPs are provided a set of methods and procedures for the switch transition. The purpose of this meeting is to discuss the progress of activities, cutover readiness, and the cutover plan.

During the scheduled cutover, all parties both on- and off-site join a bridge that will be managed by an AT&T ESInet™ Change Manager. Legacy selective router and end office migration of live traffic is performed on a switch-by-switch basis. At the scheduled time and in accordance with the 9-1-1 service transition plan, the OSP translations representative executes a predefined set of switch translations (script) to redirect calls from their legacy trunks to the new trunk groups to the AT&T ESInet™. Generally, the OSP will busy-out their primary legacy call path, thus sending all calls to the alternate legacy call path. The OSP then cuts over the primary trunk group to the AT&T ESInet™ and calls are validated. The OSP then repeats the procedure for the alternate call path. The actual switch transition event occurs smoothly and transparently to 9-1-1 callers as all systems have been previous tested with non-live calls.



After live traffic has been cut, the system will then undergo a system acceptance test and quality walkthrough, including re-validation of a subset of testing that had been performed prior to the migration, including call transfers. Once complete, and in agreement with the Customer, the service is accepted, and the maintenance period begins.

In the event that the PSAP must revert back, this may be accomplished by the OSPs reversing the translations and directing traffic sent to the new LNGs back to the prior legacy network paths.

PSAPs can choose from one of the following deployment configurations:

- Legacy PSAP - Supports non-IP enabled PSAPs that require the use of Centralized Automated Message Accounting (CAMA) signaling for the PSAP CPE.
- Locally Hosted IP PSAP - Supports locally hosted PSAP IP call handling controller utilizing either NENA i3 or ATIS RFAI protocols.
- Host/Remote - Supports PSAP customers that utilize a centrally hosted call handling controller to provide call delivery to multiple PSAPs e.g., multi-node deployments.

Deployment Timeline

AT&T would estimate a 4-to-6-month lead time prior to the first PSAP deployment in order to establish ingress trunking, egress circuits and work through data collection and provisioning. Upon first PSAP deployment, we would suggest an average of ten (10) deployments a month.

Risk Management

The AT&T ESInet™ systems are highly robust and tested extensively prior to release. In any implementation and cutover, there are always risks. We have event plans that are used to mitigate the risks. In addition, we have checkpoints built into the event plan to ensure a smooth deployment. We utilize a risk register to identify, assess, and prioritize any potential risks to minimize the probability and/or impact of unfortunate events or maximize the realization of opportunity.

Schedule

Customer AT&T ESInet™ projects currently on-going are utilizing the project framework to allow for customer modification requests. In one such example, the state PSAP consolidation mandate required the customer to change the number of PSAPs to be implemented as well as several location changes after the design phase was completed. Through the utilization of the flexible and iterative nature of the project methodology, the associated schedules and scope of the project were adjusted in-flight to accommodate the requirements of the customer.



Scope

This project methodology has been successfully used to implement both customer end-user project as well as internal AT&T network product roll outs. The AT&T ESInet™ product itself leveraged this same project methodology successfully to design, build, test and deliver services. The AT&T ESInet™ is the first and only nationwide ESInet service offering that has been pre-built with respect to core infrastructure enabling customers to procure and implement an ESInet solution in months as opposed to years.

Quality Management

Quality management is an on-going collaborative process with both AT&T and the State evaluating each phase of the project. Applicable testing and performance measures are employed to evaluate the meeting each of the stated goals within each phase. 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. Many times, changes occur within the life cycle of a project and process groups must be repeated.

b. Project Manager

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

AT&T Response:

Comply.

AT&T understands and complies with project manager requirement.

AT&T refers to the primary implementation position and single point of contact to the State as the Program Manager. AT&T further assigns additional Project Managers to individual PSAP implementations coordinating with the Program Manager who is the overall project lead.

As is the normal course of the relationship, AT&T maintains with our ESInet customers, the Program Managers are required to make themselves available to their ESInet customers with a preference of one or two primary points of contact with customer leadership. The Program Manager will be tasked with a focus on the Nebraska project implementation singularly. The AT&T Program Manager will make themselves available to the State and its consultant in the manner that they deem appropriate.

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



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

Minimum PMP contents:

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

Notes:

*The PMP will be referenced regularly during implementation to ensure timely completion.
Any schedule or work-plan changes require prior State approval through the Change Management process.*

AT&T Response:

Comply.

AT&T has provided a preliminary Project Management Plan in **Appendix M - PSAP Implementation Project Plan Nebraska** AT&T identifying major activities to complete the deliverables as well as due dates. This plan can form the basis of the required formal plan. The Project Plan includes WBS.

The AT&T Project Manager will conduct regularly scheduled project status calls with State of Nebraska 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

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.

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

- Project Start Phase
- Project Plan Phase
- Project Implementation Phase
- Project Completion Phase

2. Staffing and Qualifications

a. Key Personnel

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

AT&T Response:

Comply.

AT&T has identified a dedicated team of key personnel to support the successful delivery, operation, and ongoing support of the proposed NG911 solution. An organizational chart outlining roles, responsibilities, and reporting relationships is included as part of AT&T's proposal below. This team includes, at a minimum, a Project Manager, Technical Lead, Security Lead, Service Manager, Technical Engineer/Coordinator, and Provisioning Coordinator, each with demonstrated experience supporting complex, mission-critical public safety and NG911 environments. AT&T's depth of resources and established NG911 delivery teams provide bench strength and succession planning to ensure continuity of service and project leadership throughout the life of the contract.

Resumes for all Key Personnel are provided in **Appendix A – AT&T Staff Resumes** and document relevant experience, qualifications, and applicable certifications. AT&T acknowledges and accepts that the State retains approval rights for all Key Personnel assignments and for any subsequent personnel changes. AT&T further commits to providing no less than thirty (30) days' written notice prior to the departure or replacement of any Key Person, except in circumstances beyond AT&T's reasonable control, and will work cooperatively with the State to ensure continuity of service and project stability.

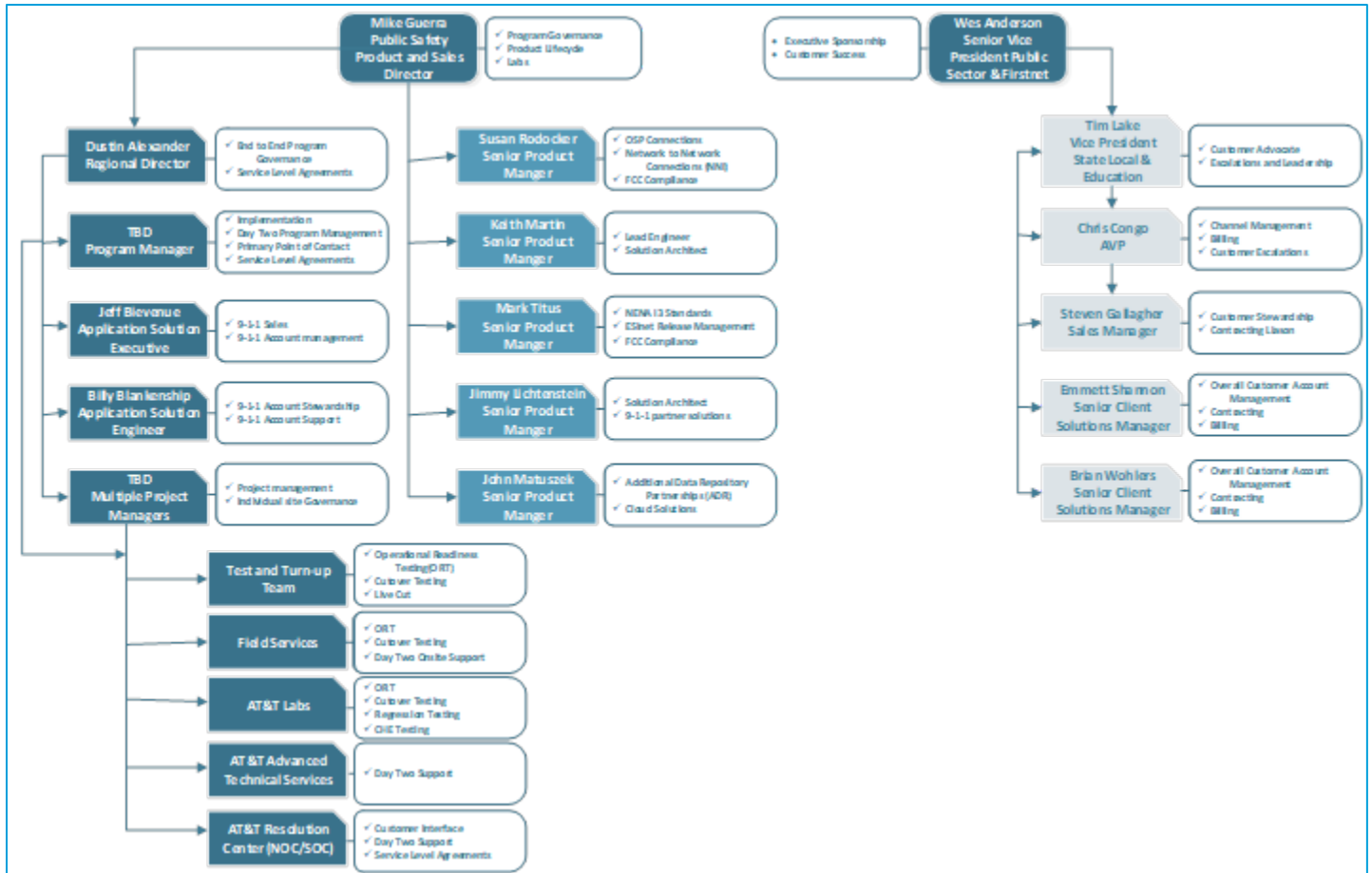


Figure 5: AT&T Key Project Personnel

b. Staff Qualifications

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

AT&T Response:

Comply.

AT&T shall employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with Customer's operations and use of telecommunications services, to provide and support Customer's use of the Services in accordance with the terms of AT&T's response to this RFP. The identities and titles of specific persons and their availability to provide and support Customer's needs will be separately established by authorized representatives of AT&T upon award of the RFP to AT&T. If required after contract award, AT&T will supply documentation to authenticate technical expertise, within the parameters of confidentiality limits.



c. Designations, Certifications, and Licenses

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

AT&T Response:

Comply.

Please see **Appendix A – AT&T Staff Resumes** for key project personnel.

3. Implementation

a. Implementation Approach

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

AT&T Response:

Comply.

AT&T has deployed over 1,700 PSAPs in live production using AT&T ESInet. AT&T has followed a similar blueprint for success across these deployments by implementing a proven scope of work hardened by decades of experience in the 9-1-1 industry.

The typical scope of work across our customer base includes satisfying a nearly identical set of performance criteria. Our detailed description of work performed is captured in the following set of functional requirements summarized below:

- **Standards Based ESInet and NGCS**
 - Provide a Next Generation 911 Core Services (NGCS) and Emergency Services IP Network (ESInet) solution configured in a manner that utilizes and complies with the latest NENA and Association of Public Safety Communications Officials (APCO) Next Generation 9-1-1 collection of standards e.g., NIST, NG-Sec, IETF, NENA i3, etc.
 - Delivery of a fully functional and comprehensive system set of NGCS and fully integrated ESInet solution architecture based on a geo-diverse, geo-redundant, and high availability design consisting of the following components:
 - Legacy Network Gateway (LNG)/Legacy Selective Router Gateway (LSRG)/Legacy



- PSAP Gateway (LPG)
- Border Control Function (BCF) to include Session Border Controller (SBC)
- Emergency Services Routing Proxy (ESRP)
- Policy Routing Function (PRF)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Spatial Interface (SI)
- Location Database (LDB)
- Additional Data Repository (ADR) and/or Identity Searchable-ADR (IS-ADR)
- Incident Data Exchange (IDX)
- An open-vendor ecosystem that provides quick implementation of new integrated services as public safety technologies and capabilities advance
- Integration to third-party commercial ADR and/or IoT gateways
- Integration to third-party commercial location information servers (LIS)
- Network Time Protocol (NTP) time source
- Solution architecture is 100 percent geo-redundant with no single point of failure for facility, hardware or software and delivers an end-to-end service level that meets a standard of 99.999% service availability rate.
- Ability to convert to NG9-1-1 core functionality without interruption of any existing legacy functions and provide seamless ingress and egress to and from the legacy network including support of legacy database management.
- Provide NG9-1-1 Core Services and capabilities interconnecting all Public Safety Answering Points (PSAPs) who subscribe with Next Generation 9-1-1 or continue with a legacy 911 system.
- The system must be capable of the primary receipt, routing, and delivery of 9-1-1 calls and all traffic to PSAPs from Originating Service Providers (OSP) via an ESInet to any PSAP as designated.
- Support both TDM and Voice over Internet Protocol (VoIP), wireless, incumbent local exchange carriers (ILECs), competitive local exchange carriers (CLECs), and future media providers to connect directly to the ESInet without the use of the existing legacy selective routers.
- Provide Network to Network (NNI) to 3rd party NGCS providers.



- Provide a 24x7x365 Network and Security Operations Center (NOC/SOC) responsible for management of alarm, reports, monitoring, security and support all NG9-1-1 system components including ingress circuits from OSPs, all NGCS components and egress circuits to the PSAP DMARC.
- Employ proactive measures to recognize, alert, log and report all security issues, as well as establish a plan, such as an Intrusion Prevention System (IPS) and Distributed Denial of Service (DDoS), that will avoid, limit and minimize disruptions to the network due to security incidents and work with customers to provide reports as requested.
- Secure and resilient to cyber-attack, penetration, abuse, or misuse.
- Process inbound Text to 9-1-1 emergency requests and originate outbound Text from the PSAP.
- Allow PSAPs to integrate their call processing equipment (CPE) with AT&T core services and ESInet.
- Support increased fault tolerance, reliability, resiliency, continuity of operations and disaster recovery for the PSAPs.
- Supply and support enterprise-wide call accounting and data collection of the end-to-end service.
- Utilize a common NG9-1-1 GIS data set available for all PSAPs when a common NG9-1-1 GIS data set is established.
- Provide Customer Training – AT&T Project Managers assigned to each PSAP implementation will coordinate and provide information to the for each of the below categories:
 - Customer Management Portal (web user interface guide) for PSAP provisioning
 - System Dashboard, Reporting and logging tools
 - 9-1-1 Resolution Center incident reporting and ticketing tools
 - GIS Tools and procedures for GIS data provisioning, spatial interface, data validation, etc.
- Project Implementation and Turn Up Plan covers the following topics:
 - Project Phases
 - Customer and AT&T Responsibilities
 - Customer and AT&T Contacts
 - Connection to PSAP/Host Location
 - PSAP Abandonment Devices
 - Text to 9-1-1
 - Originating Service Providers (OSP's)



- Test and Turn-Up
- System and Pre-Cutover acceptance test plans are reviewed by the AT&T Project Manager and PSAP coordinator.
- Product Cutover Coordination – AT&T Project Managers provide a detailed cutover plan to coordinate schedule and resource availability.
- Project Staffing – AT&T makes available the entire team of skilled NG911 professionals including leadership, account execs, technical architects, project managers, installation technicians and tier 2 & 3 technical engineering support.
- PSAP OSP Migration Plan - provide and coordinate OSP and database migration services to include:
 - Coordinate with PSAPs to obtain letters of authority.
 - Establish required interconnection agreements, commercial agreements, and required trunking with OSPs and current 911 service provider to manage and maintain NG911 services across the state.
 - Coordinate with all telecommunications providers and manage circuit order processes to include testing and integration.
 - Contractor shall manage all adds, moves, changes, and deletions of connections to OSPs, both TDM and IP-based, monitor these connections, and proactively work with the respective OSPs to resolve problems as they occur.
 - Contractor shall complete the transition from TDM to SIP ingress to the ESInet.
 - Support the collection, routing, and delivery of 9-1-1 calls and traffic to PSAPs that may use either Legacy 9-1-1 systems or have some form of a NG91-1 system and with a variety of Call Processing Equipment (CPE) types and vendors.
 - Provide management to maintain Automatic Location Identification (ALI) database information and transition to Location Database (LDB)
 - Support service order input (SOI) process for subscriber records.
 - Provide integration and provisioning of existing and future MLTS databases.
 - Manage the transition to include coordination of all provider records from the current location database to the replacement LDB, and any dual provisioning necessary during the transitional phases of the project.
- Software Release and Change Management support including:
 - Provide change management governance in support of operations, administration, maintenance, and provisioning of their NG911 services; including but not limited to software release upgrades/updates, maintenance hour activities, method of procedure approvals & testing, issue & outage notification processes, etc.



- Deliver business and service continuity, disaster recovery, and emergency procedures e.g., Risk Assessment, Service Continuity Strategy, Risk Reduction and Recovery Measures, Plans and Procedures, etc.
- Progress Reports and status information are provided at regular intervals coordinated with customers.
- Support for Performance Standards and Service Level Agreements (SLAs) to meet the needs of AT&T ESInet customers.

Results are captured and measured by our experienced team of skilled NG911 project managers that work with our customers to develop acceptance test plans, coordinate all testing and cutover activities while holding regular communication meetings to advise customers of project status/progress. **AT&T ESInet service includes a Service Level Agreement ensuring on-time project completion**, that is backed by financial remedy in the event AT&T does not meet the agreed upon implementation schedule key milestones.

b. Elements of Implementation

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

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

AT&T Response:

Comply.

AT&T ESInet employs a solution lifecycle implementation methodology (see description below) to ensure that all project areas of change are properly defined, designed, integrated, and deployed. The solution lifecycle implementation methodology has been developed and refined based on experience and the lessons learned migrating hundreds of agency systems to next generation 9-1-1. The methodology provides a blueprint for managing system migration and includes a project plan, templates, examples, diagrams, forms, and project communications. These project tools are tailored during the project definition phase to address the specific attributes of each next generation system implementation, and then refined during the subsequent project phases.



The chart below provides a visual of the phased approach that will be used for the State of Nebraska, with specifics that will be discussed in the following sections.

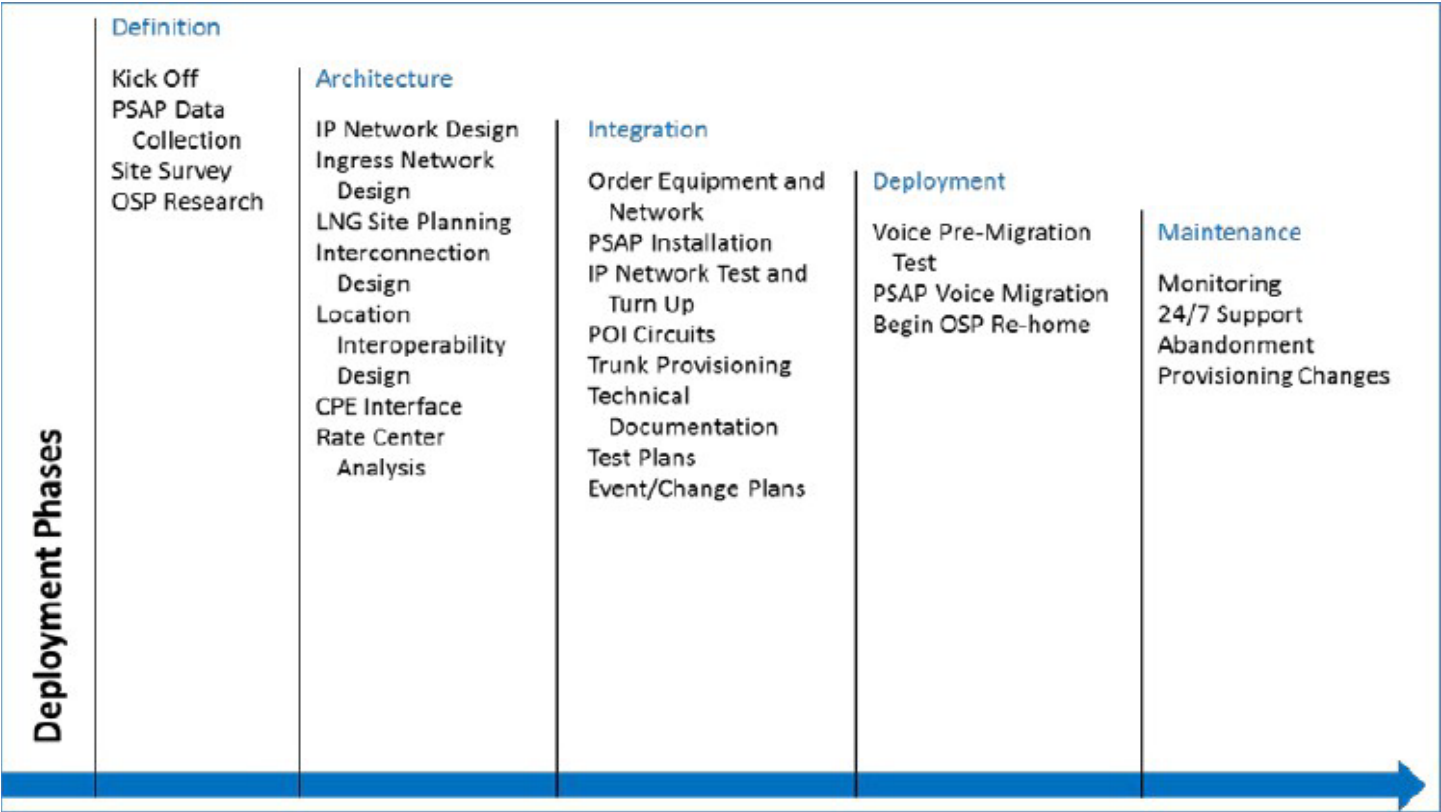


Figure 6: Phased Project Approach

Solution Definition

The first phase in the solution lifecycle is the Solution Definition phase, which begins with the kickoff and alignment process and is critical to the overall success of the next generation 9-1-1 initiative within the State of Nebraska. During this process, key members of the joint project team unite to identify roles, responsibilities, critical success factors, project challenges, elaborate on specific strategies and project options, confirm E9-1-1 project scope, and finalize plans to expedite solution delivery plans and resources. The proposed solution is reviewed in order to align each primary stakeholder with a common vision and strategy for unified team design and planning.

The Solution Definition phase principally represents administrative, organization, and discovery tasks necessary to align the team’s roles and responsibilities with project deliverables. During this phase, the team determines the aspects of the 9-1-1 system that are subject to change within the scope of the project. Much of this entails identifying and collecting information from project stakeholders such as the State of Nebraska, existing 9-1-1 service providers, public safety agencies, and Originating Service Providers (OSPs).



Prior to collecting detailed information that will be used during the project, it is important for the team to understand the overall project goals and the criteria that will govern their decision-making. Project “Principles and Constraints” represent beliefs that span and guide all phases of the project, and which will eventually determine the success of the project. The project principles and constraints are communicated to all team members so that all design, integrations, and deployment decisions can be assessed in their light. Guided by the project principles and constraints, more detailed information is then collected during the Solution Definition phase. This includes conducting site visits and readiness assessments of Public Safety agency facilities. Information also may be obtained by telephone and email exchange. Where it is possible, the team provides information ahead of time for the agency personnel to validate. A high percentage of PSAP data can be verified in this manner rather than collected from scratch. Every effort is made to obtain the necessary data in a manner that is efficient, respectful, and does not interfere with PSAP operations.

Information collection methods include interviews, questionnaire forms, review of documentation developed by the State of Nebraska during earlier project phases, and research utilizing both public and proprietary data sources. The information is captured in Microsoft Office documents including Word, Excel, Project, and Visio. It is then organized, correlated, and stored in a secure project repository. Some of the information is plotted using geographic information systems (GIS) so that relationships between public safety agency jurisdictions and communication service provider networks can be more readily analyzed and communicated. The project Communications Plan guides the dissemination and sharing of this information based on a project RACI chart.

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

- PSAP Contact Information
- PSAP Jurisdiction Boundaries
- Existing 9-1-1 Service Provider and Legacy Selective Router Information
- PSAP Services and Trunk Types
- PSAP CPE and Positions
- PSAP Equipment Configuration; Power; HVAC
- PSAP ALI Information; Format
- PSAP GIS Layers
- PSAP Community; Back-Up; Alternate; E9-1-1 and PSTN Transfers

In parallel with the above PSAP data collection tasks, a corresponding research and data collection effort is conducted to gather Originating Service Provider (OSP) information. Again, much of this information is first obtained from public or proprietary industry databases, and subsequently augmented and annotated with feedback from service provider representatives.





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

- Comprehensive Inventory of OSPs serving Nebraska; 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
- Site Surveys

Based upon the project principles and constraints, as well as information collected during the Solution Definition phase, the team begins to distribute “network change” notifications to communications service providers. Network change notifications generally provide at least six months lead time for carriers to meet new trunking arrangements. Notifications may be issued on Nebraska or agency letterhead and may be emailed as well as posted online. The initial notification to communications service providers may provide general information and time frames, with details to follow as additional instructions are developed during the architecture phase.

The “network change” notifications will be specifically tailored for OSPs. It likely also will be necessary to provision outbound circuits from the LNGs to the embedded existing 9-1-1 service provider systems and legacy selective routers to support interoperability of the legacy and next generation systems during the migration process.

Solution Architecture

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

The Solution Architecture phase represents the design and documentation of all solution components and interrelationships. The objective of the Solution Architecture phase is for all project stakeholders to understand the requirements for which they are responsible and have the information necessary to obtain approvals, procure equipment, submit trunk orders, and arrange connectivity during the Solution Integration



phase. During this phase, the team creates and distributes more detailed communications to OSPs that provide trunk ordering instructions and due dates.

To achieve these objectives, Solution Architecture entails creating logical and physical network diagrams and spreadsheets that depict the entity relationships between all system components. Logical entities include the OSP end offices, legacy selective routers, other 9-1-1 service provider systems, data centers, legacy network gateways (LNGs), points of interface (POIs), next generation selective routers, etc. Additional dimensions considered during Solution Architecture are LATAs, rate centers, exchange boundaries, and PSAP jurisdiction boundaries. Using information collected during the Solution Definition phase, the team estimates the type and quantity of network capacity required to accommodate ingress trunks from all OSPs to the LNGs. The team designs and sizes egress trunk groups from the LNGs back to the legacy systems in accordance with interconnection agreements to support interoperability of the legacy 9-1-1 system with the next generation system during the system migration period. The team identifies service addresses where Common Line Location Identifier (CLLI) codes will be required from Telcordia.

Solution Integration

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

Coordination with originating service providers is an essential part of this stage to plan for the 9-1-1 services management transition. OSPs receive all necessary information and detail to order trunks/circuits to the LNGs or IP POIs.

Based on the due dates the project team provides, OSPs utilizing legacy connections submit facility orders (usually DS1) to point of interface (POIs) to access the LNGs and trunk group orders (DSOs) to the next generation selective routers. The trunk types include CAMA, PRI, and SIP. If possible, some pre-provisioning may be performed to collapse time frames. An example of this might be the collection of OSP point code information necessary to begin ISUP orders to support pre-provisioning of the OSP SS7 signaling to facilitate trunk group builds. It may be determined that OSPs already connected to the AT&T ESInet to serve non-Nebraska PSAP jurisdictions may be able to leverage such connectivity to deliver traffic intended for Nebraska. This would jump-start the connection process for some OSPs by allowing them to add trunk groups for PSAPs to existing facilities.

In general, most OSPs are likely to order trunk groups in quantities and configurations that replicate their existing connectivity to the legacy selective routers. OSPs may be able to aggregate more trunk groups on fewer overall facilities due to changes in the number and location of the LNGs. OSPs will be instructed to order diverse (primary and alternate) trunk groups to the next generation selective routers. OSPs will be instructed to configure their primary and alternate call paths so as to achieve a balance between the AT&T ESInet point codes in order to distribute the load between the pair.



The team coordinates with the State of Nebraska and OSPs to ensure that each trunk group is associated with the appropriate default PSAP. The default PSAP is the PSAP where calls received over the trunk group will be routed in the event that the ANI is missing or location information for routing is not found. Agencies generally determine the default PSAP based on the relationship between the OSP's originating rate center, the PSAP jurisdiction(s) boundaries, and the PSAP(s) call-taker capacity and ability to dispatch or transfer calls. A baseline for default PSAP determination may be the legacy system relationship between OSP trunk groups, rate centers, and PSAPs.

As trunk orders complete, OSPs contact the AT&T ESInet team to schedule call-through testing. Each trunk is tested as well as overflow and alternate call path logic. Depending on the timing relative to the planned in-service date, traffic may be cut over to the new trunk groups or the trunks may be turned down until the PSAP(s) served by the groups are ready to receive calls from the new system.

In parallel with network provisioning, the project team implements the PSAP connectivity and works with the PSAP to ensure CPE configuration is complete. PSAPs are provisioned in the AT&T ESInet to support call transfers, star code lists, alternate, overflow, and abandonment routing. A common statewide PSAP directory may be utilized to enable 9-1-1 call transfers to any PSAP as authorized.

Working closely with the State of Nebraska and stakeholder groups, the project team designs customized provisioning plans (including incoming trunk route plans, bridge lists, alternate and backup policies and dialing plans). Additionally, the documentation developers customize the user and process documents to meet the needs of the State and PSAPs.

Solution Deployment Site Cutover Approach

During the Solution Deployment phase, all network components and equipment connectivity is validated, and acceptance tests are performed, and metrics tracking, and reporting are initiated.

After all non-live call testing is completed, a series of transition events are executed to cut-over live 9-1-1 traffic to the AT&T ESInet.

In preparation for deployment and in partnership with the State of Nebraska and their PSAPs, the AT&T ESInet Project Manager finalizes the cutover plan, including procedures for notification concerning schedule specifics. To minimize impact to the PSAPs, each PSAP is cutover by receiving traffic directly from the legacy selective routers as well as any OSP end offices that have completed pre-migration provisioning and testing prior to the date of the scheduled cut. The PSAP is flash cut using procedures outlined below, and then any additional OSP traffic and end offices are rehomed post-PSAP cut. Prior to the commencement of the cutover event for the legacy selective router and OSP switches, the project team members hold a cutover meeting, and OSPs are provided a set of methods and procedures for the switch transition. The purpose of this meeting is to discuss the progress of activities, cutover readiness, and the cutover plan.





During the scheduled cutover, all parties both on- and off-site join a bridge that will be managed by an AT&T ESInet Project Manager. Legacy selective router and end office migration of live traffic is performed on a switch-by-switch basis. At the scheduled time and in accordance with the 9-1-1 service transition plan, the OSP translations representative executes a predefined set of switch translations (script) to redirect calls from their legacy trunks to the new connections to the AT&T ESInet. Generally, the OSP will busy-out their primary legacy call path, thus sending all calls to the alternate legacy call path. The OSP then cuts over the primary trunk group to the AT&T ESInet and calls are validated. The OSP then repeats the procedure for the alternate call path. The actual switch transition event occurs smoothly and transparently to 9-1-1 callers as all systems have been previously tested with non-live calls.

After live traffic has been cut, the system will then undergo a system acceptance test and quality walkthrough, including re-validation of a subset of testing that had been performed prior to the migration, including call transfers. Once complete, and in agreement with the Customer, the service is accepted, and the maintenance period begins.

In the event that the PSAP must revert back, this may be accomplished by the OSPs reversing the translations and directing traffic sent to the new LNGs back to the prior legacy network paths.

Testing

The AT&T ESInet Acceptance Test Plan is customized and utilized to certify that each system component functions as required, and all data is provisioned and configured properly. The plan is customized to include the customer's specific requirements as well as to support pre-cutover validation testing, acceptance testing, and pre-migration provisioning testing for each PSAP. The plan is designed to demonstrate that the individual components, when combined as described in the proposed solution, meet expectations.

The AT&T ESInet Operational Readiness Test Plan provides a detailed list of test cases for the implementation of AT&T ESInet™ services. This plan will be customized to include the customer's specific requirements as well as to support pre-cutover validation testing, acceptance testing, and pre-migration provisioning testing for each PSAP.

The Project Manager will participate in all testing and certification. The technical staff will vary based on the solution module being tested. The customer will be provided with copies of the acceptance test forms specifying what is being tested and the expected results.

We will manage the testing process and coordinate all test calls documented in the test plan. This testing is scheduled in accordance with the PSAP's availability. The PSAP is required to provide a resource to answer the test calls and provide documentation (i.e., screen prints and recordings) for certain calls. Once the System Acceptance Testing is completed the Site is officially accepted and standard warranty and maintenance services start.



We use a structured approach to migrate the customer into the new system. This is reflected on a cutover plan that serves as a checklist or guide to our cutover team to ensure that the system is ready to go live. The focus of the System Migration Strategy is on the activities, tasks, and timing of the days prior to going live on the new system.

All deployment steps are performed with well-defined and coordinated cutover plans and rollback contingency plans. Next Generation 9-1-1 capabilities are validated prior to moving live traffic to Next Generation 9-1-1 facilities. Equipment and network transport is validated prior and during Next Generation 9-1-1 capability deployment. Elements and transport are further validated on a continuous ongoing basis. Proven methods that we have successfully used in previous NG9-1-1 deployments are utilized.

In addition, we will work with State of Nebraska to develop a joint communication to each provider outlining the scope of services to be implemented, a high-level implementation schedule, and key contact information for each entity. AT&T can distribute the communication on behalf of the State.

Risk Management

The AT&T ESInet systems are highly robust and tested extensively prior to release. In any implementation and cutover, there are always risks. We have event plans that are used to mitigate the risks. In addition, we have checkpoints built into the event plan to ensure a smooth deployment. We utilize a risk register to identify, assess, and prioritize any potential risks to minimize the probability and/or impact of unfortunate events or maximize the realization of opportunity.

Process Audits

AT&T conducts process review sessions as part of the completion phase of every PSAP implementation project. The output from these process review sessions informs changes as needed to our baseline project and process plan templates. The baseline templates are used as a starting point for each new project and are then customized to the individual needs of each project.

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

Ongoing OSP rehomes will occur during this phase as well. Any OSP traffic that continues to route to the PSAP through the legacy selective router to the AT&T ESInet must be moved to direct connections to the AT&T ESInet. AT&T will continue to manage these individual migrations at no impact to the PSAPs.



AT&T's IP networks are known for their reliability, security, and redundancy. Employing private, high-speed, MPLS IP backbones for transmission; the AT&T ESInet supports an availability target of 99.999 percent. Additionally, it has the following core capabilities:

- Is a secure TCP/IP virtual private network with PSAP to ESInet connections that are resilient, physically diverse when possible, and logically separate.
- Actively tests all network pathways for degradation and automatically re-routes traffic to healthy pathways.
- Operates on IPv4 or IPv6 network infrastructures.
- Manages and measures voice quality.

An ESInet application layer runs over the base IP transport products and provide management, security, and high availability. ESInet transport protocols and techniques include BGP, IPSEC, iGRE, Virtual Routing and Forwarding (VRFs), SNMP, and SIP messaging to validate component readiness. The AT&T solution employs AES 256 encryption-in-transit. Encryption is achieved either using SSL/TLS or IPSEC VPN. AT&T will utilize our wholly owned backbone network, that uses Multiprotocol Label Switching (MPLS) technology to integrate multiple network services. Border Gateway Protocol (BGP) is used within the ESInet to facilitate multi-protocol label switching (MPLS) and as an exterior gateway protocol (EGP) to interface with external networks. This EGP functionality allows inter-connectivity between the AT&T NGCS core, and the Hosted Call Handling/Logging subsystem components.

The proposed solution ensures performance using traffic shaping and traffic policing. Standard internet protocols are used to prioritize IP traffic (BGP, IPSLA) and constantly test and verify IP path availability. Authorization and security protocols ensure only valid and preauthorized traffic traverses the ESInet.

The AT&T ESInet service utilizes AT&T's MPLS private IP network that may include use of third-party network providers that provide the local access and path diversity. These networks are comprised of different components, multiple technical solutions, and various types of interfaces. Due to the nature of MPLS-based transport, WAN failures (within the carrier network or last-mile) may not be immediately detected by Next Generation Core Services (NGCS) network equipment at the physical layer. Knowing this, the AT&T solution employs a more robust means of end-to-end failure detection to ensure the reliable delivery of 9-1-1 traffic. These methods include creating a tunnel overlay through the MPLS-based carrier networks, as well as running heartbeats from the NGCS Core equipment to the PSAP. All of this, combined with additional accounting for false positives/network degradation, creates a backbone convergence time of less than 500ms.

The proposed solution is a Quality of Service (QoS)-managed network providing the capability to prioritize any type of IP traffic (voice, data, and multi-media). The solution provides QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. 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. 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



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 infrastructure prefers the use of a public IP addressing schema. AT&T further understands that existing PSAP-side equipment may not currently use public IP addresses. Typically, PSAP-side call handling equipment is deployed using private IP addresses. Furthermore, these private addresses are reused from deployment to deployment. Although, as stated previously, AT&T prefers the use of Public IPs, the AT&T solution allows for the use of private IP addressing by creating encrypted VPN tunnels through the provided network.

AT&T ESInet uses a Private MPLS network that provides all the benefits of IP with built in security. For scalability of the UCA ESInet offering, AT&T's MPLS IP networks are known for their reliability, security, and redundancy. AT&T ESInet supports an availability target of 99.999 percent.

AT&T's implementation approach in regard to the ESInet and the Functional Elements (FEs) included as part of the NGCS utilizes several key factors to produce the best possible solution for the PSAPs. Past experience, rigorous testing, and NGCS architecture designed to have no single point of failure are keys to implementing NG9-1-1 that ensures each FE is delivering functionality as expected even in a world of mixed PSAP capabilities.

Past Experience

In 2015, AT&T made a bold national product announcement that detailed our vision for a national i3-compliant ESInet solution. This solution is funded and built by AT&T to support twice the busy hour 9-1-1 call volume for the entire United States. AT&T is the industry leader in terms of ESInet systems contracted and delivered. At the time of this writing, AT&T has **more than 2,000 PSAPs** connected and/or contracted to ESInet solutions, with **over 1,700 live** and in service today. These systems and contracts cover **more than 88 million** U.S. residents in aggregate. No other provider has the same depth of experience in architecting and delivering mission-critical Next Generation 9-1-1 solutions. AT&T has used this experience to create a solution that allows the PSAPs to join an ESInet that is already built and has the customization capabilities to provide each PSAP with the ability to deploy the solution they are ready for.

AT&T understands building a PSAP or region-specific NG9-1-1 solution is time consuming with a majority of the time spent deploying the NGCS elements. AT&T's existing ESInet with NGCS provides PSAPs the ability to quickly integrate onto an ESInet and gain the reliability, redundancy, and functionality of a NG9-1-1 system quickly.

Testing

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 of the software releases are tested by AT&T Labs. The testing program includes the following elements.



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

AT&T Labs completed extensive acceptance testing of the ESInet and associated NGCS prior to the launch of the product. This testing ensured the system in production was functioning as expected and not only providing NENA i3 compliant FEs but also could properly handle calls if a specific element failed. Over 1,000 test cases were completed prior to launch. Test cases were categorized as functional, failover, or load testing.

Functional test cases validated that each element was not only completing the requirements of the FE, but also successfully interacting with other components. Failover testing went deeper on each FEs ability to not only perform its task, but to ensure if an FE (or multiple FEs) failed, then a redundant FE completed the task without interruption to service. Finally, testing was completed to validate load, performance, and stability of the system. In addition to the testing prior to go-live, AT&T Labs is dedicated to testing new functionality prior to implementation in production.

All software deployed to the AT&T ESInet next generation service is thoroughly vetted by exhaustive regression testing in settings that emulate the production environment. The code base, hardware, operating systems, network and monitoring equipment, and related firmware used to test new software are of the same make, model, and version as is deployed in production. There is no requirement to take a production component out of service for testing new software.

AT&T Labs has also worked to validate that the AT&T ESInet is CPE-agnostic. AT&T has completed ESInet interoperability testing with multiple vendors including Intrado VIPER, Motorola VESTA and Solacom Guardian call handling equipment. Today, AT&T ESInet is deployed using i3 call delivery with Intrado VIPER and Motorola VESTA with planned Solacom Guardian deployment in early 1Q2020. AT&T's subcontractor offers an i3 Customer Integration Lab (CIL) for all other CPE vendors to validate their i3 code against the AT&T ESInet code for easier implementation without the need to validate in a production environment.

NGCS Architecture

The AT&T ESInet solution employs a multi-tenant, highly redundant, geographically diverse architecture as illustrated in the figure below.

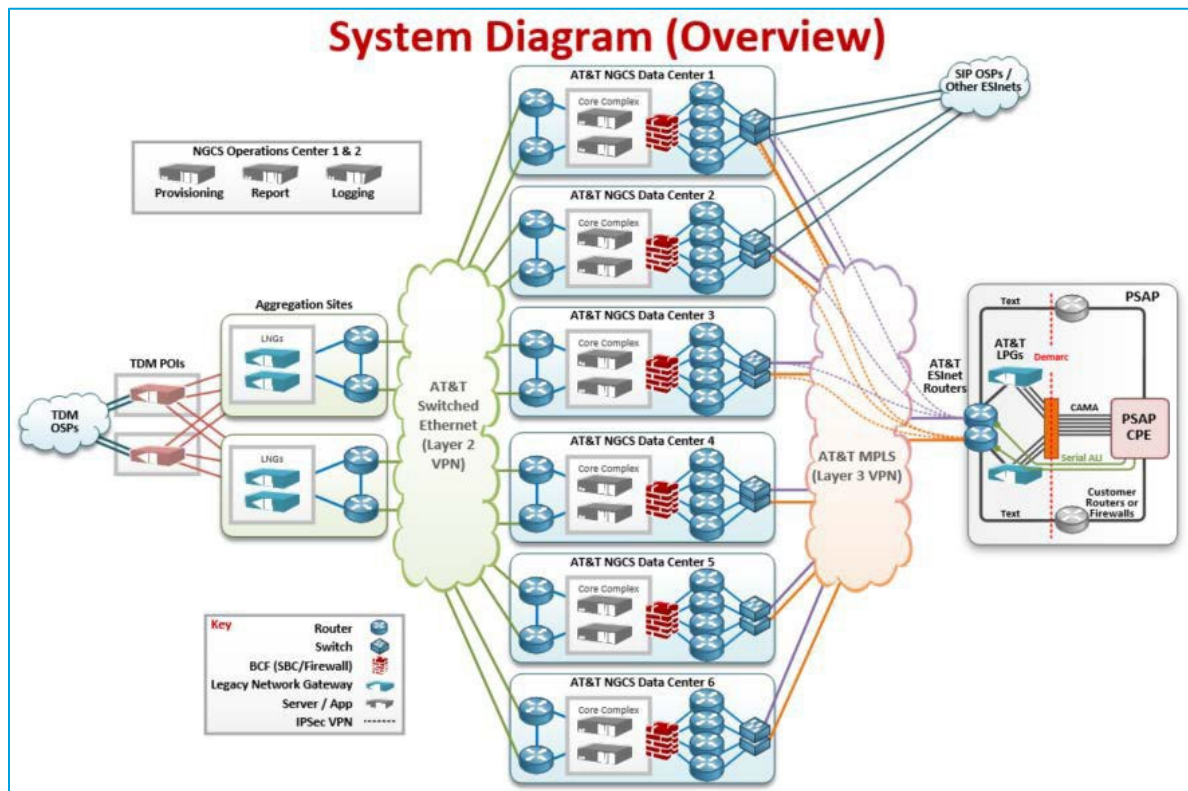


Figure 7: AT&T ESInet NGCS Architecture

The AT&T ESInet provides a market-leading deployment architecture based on a foundation of six strategically located data centers, also known as Core Sites, with NGCS functions. The Core Sites combined with regional Aggregation Sites, for example LNG locations, and AT&T's robust broadband transport network create a high quality NG9-1-1 product offering. Any 9-1-1 call can be processed at any of the AT&T Core Sites; each Core Site contains highly available architecture with multiple levels of redundancy as well as focused operations and management for self-sufficiency. The AT&T ESInet is an infrastructure that is public safety grade in terms of capacity, reliability, scalability, and redundancy, and does not require an individual 9-1-1 authority to invest in stand-alone Core Sites.

The AT&T ESInet provides a shared processing environment where individual 9-1-1 authorities perceive a dedicated ESInet deployment, but benefit from the investment possible by a common environment. This shared Core Site strategy has produced a highly available solution with redundancy upon redundancy and extremely high service availability. The shared environment provides straightforward integration and enhanced interoperability between all PSAPs served by the AT&T ESInet offering, whether they are neighboring PSAPs or PSAPs across the county. Integration with other ESInet providers is achieved through industry standard interfaces.

The solution deploys redundant and diverse components providing the i3 architecture, such as but not limited to, ECRF, ESRP, PRF, BCF, and LNG functionality. The solution has no single point of failure, positioning the

State of Nebraska with a unique foundation to deploy future NG9-1-1 functions as and when they become available. The AT&T ESInet solution has been designed solely for the purpose of completing every 9-1-1 call 24x7x365. The AT&T ESInet can withstand the failure of individual components or the failure of core processing sites and continue to successfully process 9-1-1 calls.

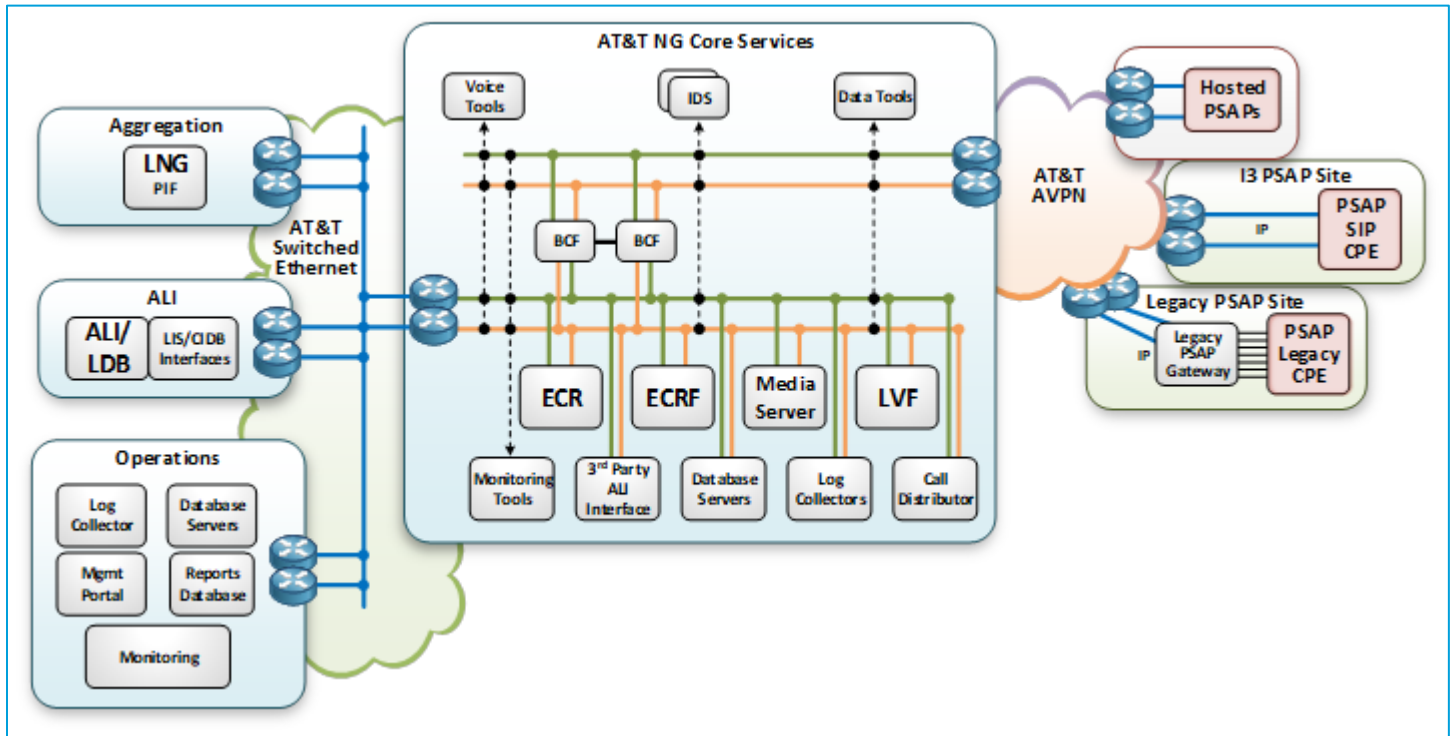


Figure 8: AT&T ESInet NGCS Functional Elements

4. Transition

a. Transition Plan: Current and Future

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

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



- **OSP interface** transition and service migration to the NG911 system.
- Integration with other systems, services, and providers.

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

AT&T Response:

Comply.

AT&T's Implementation Project Manager will oversee and manage all aspects of the project that enable transition to the AT&T ESInet platform. AT&T will work with the Board in developing the transition plan, will seek final approval and authorization from the Board before beginning the transition, and will give notice to the Board before engaging PSAPs. Any changes to the plan will follow change management processes.

Transition activities include:

- Create PSAP Migration Timeline and manage/escalate any issue that may block an on-time deployment
- Coordinate and communicate with legacy 9-1-1 service providers; ILECs; rural LECs or independent operating companies; competitive local exchange companies (CLECs); wireless service providers; VoIP; and PS-ALI providers to ensure calls originating from each TSP's networks will be received and delivered into the AT&T ESInet system
- Evaluate ALI data and GIS data readiness
- 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 system
- Schedule field technicians for site visits, network equipment installation, and the test and turn up of the new network
- Dedicate as much time as is needed for a successful PSAP migration onto the AT&T system.

We use a structured approach to migrate the customer into the new system. This is reflected in a cutover plan that serves as a checklist or guide to our cutover team to ensure that the system is ready to go live. The focus of the system migration strategy is on the activities, tasks, and timing of the days prior to going live on the new system.



All deployment steps are performed with well-defined and coordinated cutover plans and rollback contingency plans. ESInet capabilities are validated prior to moving live traffic to ESInet facilities. Equipment and network transport is validated prior and during ESInet capability deployment. Elements and transport are further validated on a continuous, ongoing basis. Proven methods that we have successfully used in previous ESInet deployments will be utilized.

5. Testing and Acceptance

a. Testing (Comprehensive Test Plan)

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

- Test environment, facilities, and equipment.
- Test configurations and thresholds.
- Simulators and test-call processes.
- Final documentation of all tests and results. **System Testing must address, at minimum:**
- NENA-STA-010.3 Functional Element testing.
- 911 call flow: primary, alternate, last route.
- End-to-end traffic flow.
- Functional Element ↔ Functional Element tests.
- Protocol ↔ Protocol tests.
- Port ↔ Port tests.
- Load testing: unexpected surge, short burst, sustained overflow.
- ESInet throughput and capacity.
- ESInet end-to-end connectivity (fault tolerance, failover, alternate routing, monitoring systems, fault notification).
- Security controls: firewalls, intrusion detection systems, intrusion prevention systems.
- Throughput acceptance testing of ≥24 hours, simulating 200% peak traffic load.



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

AT&T Response:

Comply.

AT&T has extensive experience with operational readiness, cutover, and system final acceptance planning and testing. We will provide comprehensive and customized test plans to the State for approval at least 30 days before planned execution.

The attached test plans include our current test plan for individual PSAPs to assess operational readiness to proceed with cutover, as well as our current individual PSAP cut plan template that is used as a MOP for the traffic migration and validation on cut day.

Included in the current plans are the methods and documentation space for how each test is executed and on what equipment, where it is executed and the expected results.

Please see the following appendices for additional information:

- ***Appendix B - ATT ESInet Operational Readiness Test Plans i3 PSAPs***
- ***Appendix C - ATT ESInet Operational Readiness Test Plans RFAI PSAPs***
- ***Appendix D - ORT-Acceptance Test Plan***

b. Test Plan Methodology

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

AT&T Response:

Comply.

AT&T ESInet has been in production since 2018 and has completed **over 69,000 hours of operation**. Prior to production launch, AT&T Labs tested and certified the operation of all NG911 functional elements, system components and capacity testing that are further described in the components listed below.

- Individual functional element testing for elements that are live on AT&T ESInet were tested prior to our first PSAP turnup in 2018. Each element is retested when software/hardware upgrades are performed. New elements to be added are tested individually prior to being introduced into the



live environment and are also functionally tested for interoperability confirmation when introduced. Also note, AT&T has a lab PSAP environment where calls from the production AT&T ESInet can be terminated to, and that can query individual AT&T ESInet elements as part of standard call flow testing at any time.

- 911 call flow (primary, alternate, last route) – These call flows will be tested as part of each individual PSAP's ORT and cut testing, based on the decisions they have made during data collection about where calls should route. AT&T also routinely tests this functionality on the platform in general as part of routine automated call testing through the platform.
- End to end traffic flow – AT&T routinely tests this functionality on the platform in general as part of routine automated call testing through the platform. Additionally, end to end testing is performed as part of both ORT and the PSAP live traffic cutover event plans.
- Functional Element to Functional Element tests – All functional elements that are live on the AT&T ESInet platform today went through rigorous interoperability testing in 2018 prior to our first PSAP turnup. With live traffic today, the functionality is constantly being utilized in real-time for live calls. Each new element that is introduced will be interop tested in a non-live environment prior to be introduced to the production platform and will then be introduced against an isolated production node for testing prior to being exposed to all nodes.
- Protocol to protocol tests – Protocol translations are live in production as part of many production applications. With live traffic today, the functionality is constantly being used in real-time for live calls. For protocol testing against new PSAPs, the ORT and cut plans executed on a per PSAP basis will be used.
- Port to port tests - Port to port communication is live in production as part of many production applications. With live traffic today, the communication is constantly being used in real-time for live calls. For port-to-port testing against new PSAPs, the ORT and cut plans executed on a per PSAP basis will be used.
- Load testing - all elements that are live on the AT&T ESInet platform today went through rigorous load testing in 2018 prior to our first PSAP turnup - including surge, burst, and sustained overflow traffic. With live traffic today, these conditions happen from time to time for live calls and the ability for the AT&T ESInet to handle this is proven.
- Regression testing - AT&T has a lab PSAP environment where calls from the production AT&T ESInet can be terminated to, and that can query individual AT&T ESInet elements as part of standard call flow testing at any time. When new CPE versions are introduced into the lab, regression testing is performed. Regression testing also takes place upon the introduction of any new element or software into the AT&T ESInet as part of our change management procedures.
- ESInet throughput and capacity testing - Throughput and capacity testing were performed on the live AT&T ESInet platform in 2018 prior to our first PSAP turnup. Additionally, we perform capacity



testing to each PSAP to validate the CPE line limits as well as failover routing in the case of resource exhaustion.

- ESInet end to end connectivity testing - ESInet end to end connectivity testing was performed on the live AT&T ESInet platform in 2018 prior to our first PSAP turnup. For each new connection that we add, including to a new 911 service provider, a new OSP or a new PSAP, we perform connectivity testing with test calls prior to the introduction of any live traffic. The connectivity testing for new PSAP circuits is detailed in our ORT plan.
- ESInet and NGCS failover testing - ESInet and NGCS failover testing was performed on the live AT&T ESInet platform in 2018 prior to our first PSAP turnup. For each new connection that we add, including to a new 911 service provider, a new OSP or a new PSAP, we perform network failover testing with test calls prior to the introduction of any live traffic. The failover testing for new PSAP circuits is detailed in our ORT plan.
- ESInet monitoring systems including fault notification – Validation of all ESInet monitoring systems including fault notification was performed on the live AT&T ESInet platform in 2018 prior to our first PSAP turnup. With live traffic today, our monitoring systems are live and alarming and fault notification happen regularly when needed; the ability for the AT&T ESInet to handle this is proven.
- Firewalls, intrusion detection systems, intrusion protection systems – – AT&T performs continuous network traffic monitoring (passive vulnerability monitoring) and annual external penetration testing of the AT&T Network. AT&T employs a combination of internally and commercially developed tools to detect and mitigate threats e.g., Distributed Denial of Service (DDoS) and attempts by unauthorized persons to penetrate the AT&T IP network.
- AT&T ESInet throughput and acceptance testing were certified by AT&T Labs against the production AT&T ESInet platform in 2018 prior to our first PSAP turnup. AT&T Labs acceptance testing certified system stability and load testing to successfully validate system capabilities operation for a period of greater than 24 hours. During testing AT&T Labs was able to generate automated test calls to simulate 200% peak traffic conditions.

c. System Acceptance Testing

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

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

- TP – Test Passed
- TF – Test Failed



- RTP – Retest Passed
- RTF – Retest Failed
- NA – Feature not applicable to the final configuration

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

AT&T Response:

Comply.

AT&T understands and complies with the System Acceptance Testing requirements.

AT&T shall complete Acceptance testing prior to the final acceptance of the System. AT&T agrees that certification considered complete, only after acceptance testing results have been supplied to the State and the State certifies that the testing satisfactorily meets all requirements.

AT&T agrees to work with the State of Nebraska and allows for independent validation and verification of their installed system upon acceptance. The IV&V can be completed by third party, who is acceptable to the State and AT&T, specifically to test the system as installed.

AT&T has established standard proven and documented processes for ESInet system acceptance testing that we've used to successfully on-board 1,700+ PSAPs onto our national infrastructure. Our standard processes include Operational Readiness Testing (ORT) test cases for each PSAP that demonstrate the solution prior to cutting over to the ESInet. AT&T will work to remedy any issues resulting from testing failures. Once the testing is completed the PSAPs are ready to cutover for live call processing and at that point are transitioned to full ESInet operational support.

AT&T's Labs group manages all PSAP ORT testing and documents all testing on the supplied ORT plan. The lead tester documents the date/time of each test, and notes whether the case passed (TP) or failed (TF). If a failure occurs, an evaluation will be performed to determine root cause, and the issue will be remedied by the responsible party. Then, when the case is retested, a new date/time will be added, documenting a pass (RTP) or failure (RTF). Regression testing is performed for any additional cases related to configuration changes made. The lead tester will also note if a feature/test case is NA for a particular PSAP.

d. Independent Validation and Verification (IV&V)

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



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

AT&T Response:

Comply.

AT&T shall complete Acceptance testing prior to the final acceptance of the System. AT&T agrees that certification considered complete, only after acceptance testing results have been supplied to the State and the State certifies that the testing satisfactorily meets all requirements.

AT&T agrees to work with the State and allows for independent validation and verification of their installed system upon acceptance. The IV&V can be completed by third party, who is acceptable to the State and AT&T, specifically to test the system as installed.

AT&T has established standard proven and documented processes for ESInet system acceptance testing that we've used to successfully on-boarded over 1,750 PSAPs onto our national infrastructure. Our standard processes include Operational Readiness Testing (ORT) test cases for each PSAP that demonstrate the solution prior to cutting over to the ESInet. AT&T will work to remedy any issues resulting from testing failures. Once the testing is completed the PSAPs are ready to cutover for live call processing and at that point are transitioned to full ESInet operational support.

AT&T's Labs group manages all PSAP ORT testing and documents all testing on the supplied ORT plan. The lead tester documents the date/time of each test, and notes whether the case passed (TP) or failed (TF). If a failure occurs, an evaluation will be performed to determine root cause, and the issue will be remedied by the responsible party. Then, when the case is retested, a new date/time will be added, documenting a pass (RTP) or failure (RTF). Regression testing is performed for any additional cases related to configuration changes made. The lead tester will also note if a feature/test case is NA for a particular PSAP.

Remainder of page intentionally blank



4. RESPONSE TO TECHNICAL REQUIREMENTS

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

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

1. ESInet Requirements

The Emergency Services IP Network (ESInet) must comply with NENA-STA-010.3-2021 (i3 Standard) and follow the recommendations in the NENA Emergency Services IP Network Design (ESIND) Information Document

(NENA-INF-016.2-2018). The ESInet shall interconnect all NG911 components with Public Safety Answering Points (PSAPs) and Originating Service Providers (OSPs) using Internet Protocol (IP), and, where necessary, legacy methods.

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

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

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

The ESInet shall incorporate geographically diverse, redundant network cores; duplicate session border/edge elements; and automatic, transparent failover for signaling and media so that failure of any single component (e.g., link, router, or server) does not disrupt 911 service. The Respondent shall define and guarantee a



Recovery Point Objective (RPO) of less than one (1) minute and a **Recovery Time Objective (RTO)** of less than five (5) seconds for critical paths, with active-active or active-passive configurations across data centers separated by at least 100 miles.

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

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

The Respondent must provide a description and/or documentation that supports the requirements in this section, including a clear description of:

- Network operations management (operational policies, staffing, incident response, and system management procedures).
- Detailed physical and logical security measures (encryption protocols, access controls, secure access points, and physical security for data centers); strategies for achieving 99.999% uptime with contingency plans.
- Continuous performance monitoring mechanisms with logging and alert systems; real-time alarm generation and notification strategies.
- Guidelines for routine, updates, and emergency maintenance; comprehensive disaster recovery plan with RTO and RPO details.
- Procedures for service restoration post-incident.
- Proactive outage prevention and response strategies including redundancy testing.
- Technical specifications for core routing architecture with diverse paths and load balancing.
- Interfaces with hosted solutions or third-party providers.
- Fault zone design methodology identifying critical components and failure points.
- Bandwidth management protocols prioritizing emergency traffic.
- And any bandwidth sharing arrangements with implications for priority traffic.
- Any limitations in the “span of control” over connections to the OSPs or PSAPs that are linked to the ESInet to establish a risk register for future reference.



Additionally, the Respondent must investigate and document potential single points of failure, explain detection and activation of standby systems if not active-active, and detail ESInet interconnection points with OSPs and PSAPs for full IP-based NG911 functionality.

AT&T Response:

Comply.

AT&T ESInet™ is a prebuilt twelve core solution in live production. AT&T's ESInet solution provides the Public Safety community with an i3 architecture built from the ground up. AT&T ESInet™ meets/exceeds the requirements in NENA-STA-010.3 and conforms to the recommendations in NENA-ESIND. AT&T ESInet™ will interconnect all elements of the NG911 system to be supplied by the respondent, all PSAPs and all origination service providers (OSPs) who desire to connect to State of Nebraska ESInet. AT&T ESInet is designed to automatically reroute traffic to alternate routes, systems or PSAPs in order to bypass network outages, system failures, or if the primary PSAP is unable to be reached. Calls from i3 compliant OSP networks interact with the ESRP and are processed in conformance with the i3 specification.

"Our successful ongoing operations and support with AT&T is built on 24x7x365 monitoring, and clearly defined governance to ensure reliability, transparency, and accountability throughout the life of the contract."

- CJ Engel, Executive Director, Arkansas 911 Board

The AT&T solution is designed as a highly available service through an active-active processing methodology, geographically diverse and distributed components, highly available component architecture, and redundant IP transport. The AT&T solution has no single point of failure.

Design, installation, testing, interconnection, and operation of ESInet components required to operate or support the operation of a Statewide ESInet.

The AT&T ESInet™ design requires a minimum of two geographically diverse circuit connections by the OSPs for connectivity into the NGCS cores. PSAP connections are delivered via fiber optic cable where possible. A second diverse connection is provided which avoids the local wire center by connecting to a second POP for complete diversity into the MPLS backbone. An optional third tertiary connection is available utilizing a FirstNet connection in case the primary/secondary connections are compromised. Once these steps have been completed, AT&T Labs will conduct Operational Readiness Testing (ORT) prior to the PSAP being cutover live to AT&T ESInet™. AT&T will provide ongoing support, reporting and maintenance for all PSAPs on the AT&T ESInet™ solution (see details below).



Maintenance and repair of those elements of the ESInet and interconnections owned, operated, installed, or controlled by respondents as part of their solution.

AT&T ESInet is a fully managed NG911 Call Routing platform with established support organizations. Once the service is implemented, AT&T's Resolution Center and AT&T's 911 Service Management organizations become the primary support organizations to ensure the solution is fully operational, maintain consistent performance, meeting the required service levels, to address open issues, ticketing and restoration of the service if an outage should occur. As part of the solution offer, AT&T will assign a dedicated Service Manager to the State of Nebraska. During the life of the contract, AT&T will maintain and monitor all equipment and software within the NGCS solution. AT&T will replace any faulty equipment (that wasn't a direct cause of negligence of on-site PSAP personnel) at no additional cost to the jurisdiction.

Completion of as-built drawings, sketches and/or schematic materials related to the ESInet.

AT&T will provide as built drawings, sketches, and/or schematic materials related to the State of Nebraska AT&T ESInet™ solution.

A data collection and reporting system for all ESInet elements that monitor, report, and analyze the operational metrics of the ESInet.

AT&T will provide the AT&T ESInet™ Customer Management Portal (CMP) and a standard reporting suite for the data collection and reporting system for all ESInet elements that monitor, report, and analyze the operational metrics of the ESInet.

1.1. Architecture and Topology

1.1.1. ESInet Diagrams

The contractor must submit comprehensive diagrams that visually represent the proposed ESInet architecture. **These diagrams must be kept current and be included in a configuration management database that the 911 Advisory Committee and the State may access at any time during the contract to validate the deployment and system functionality.**

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive diagrams illustrating network maps (logical and physical topologies).
- Physical and logical path diversity for redundancy.
- One-time and transitional network elements.
- Network ingress and egress points with connections to OSPs, PSAPs, and external interfaces.



- Transport types (e.g., MPLS or Ethernet) with port speeds.
- Capacities and estimated bandwidth at ingress, core, and egress points.
- Interconnection locations (nodes, data centers, POIs, LRGs); and any additional technologies and interfaces.

AT&T Response:

AT&T will provide comprehensive ESInet architecture diagrams that visually represent the proposed Nebraska deployment and will maintain these diagrams as living artifacts throughout the contract term. Diagrams will be controlled under AT&T's configuration management process and maintained in the ESInet documentation repository/CMDB so that the State and the 9-1-1 Advisory Committee may access the current approved versions at any time to validate the deployment configuration and system functionality. Updated diagrams will be published following any approved change that impacts topology, routing, interconnection, capacity, or security boundaries, and at minimum will be reviewed and revalidated on a regular cadence as agreed during project governance.

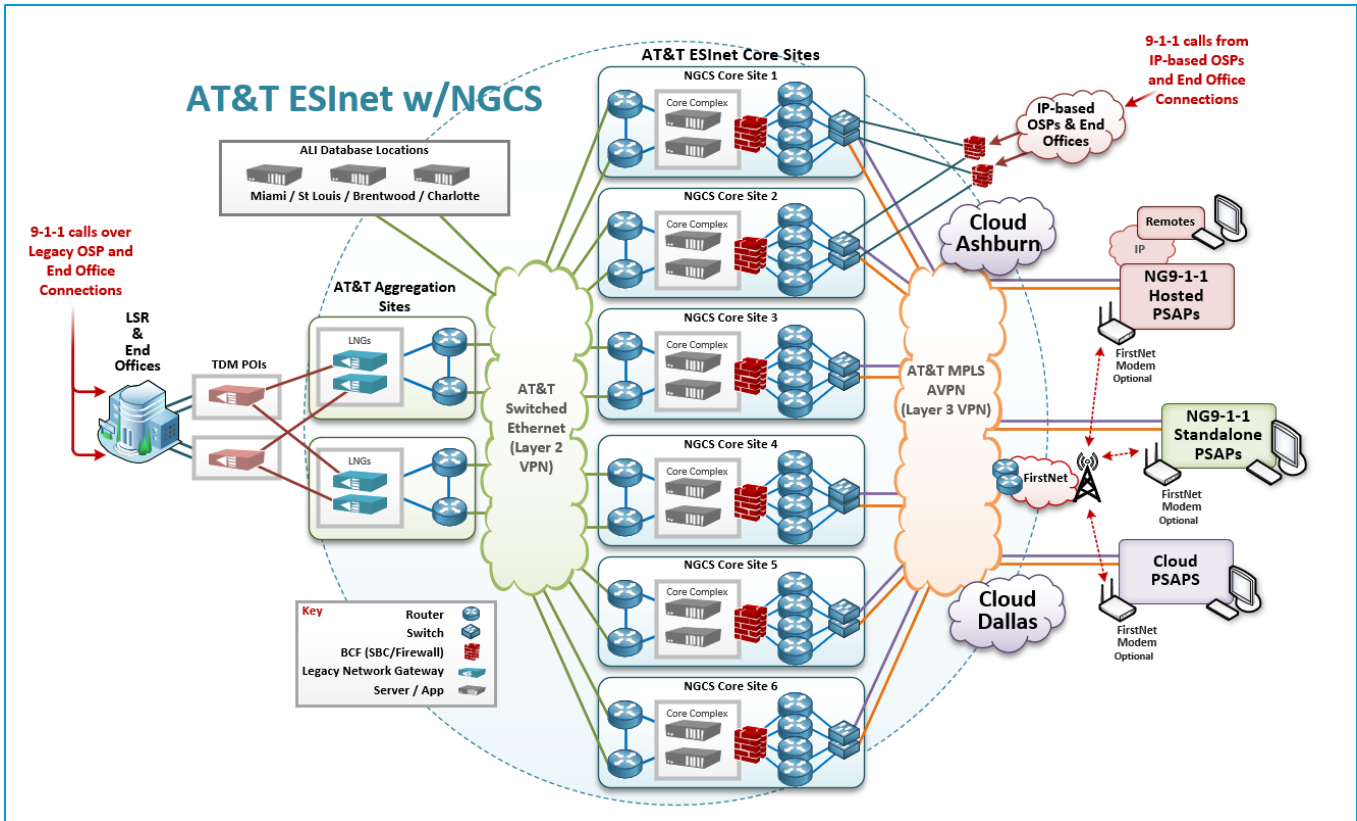


Figure 10: AT&T ESInet NGCS Architecture

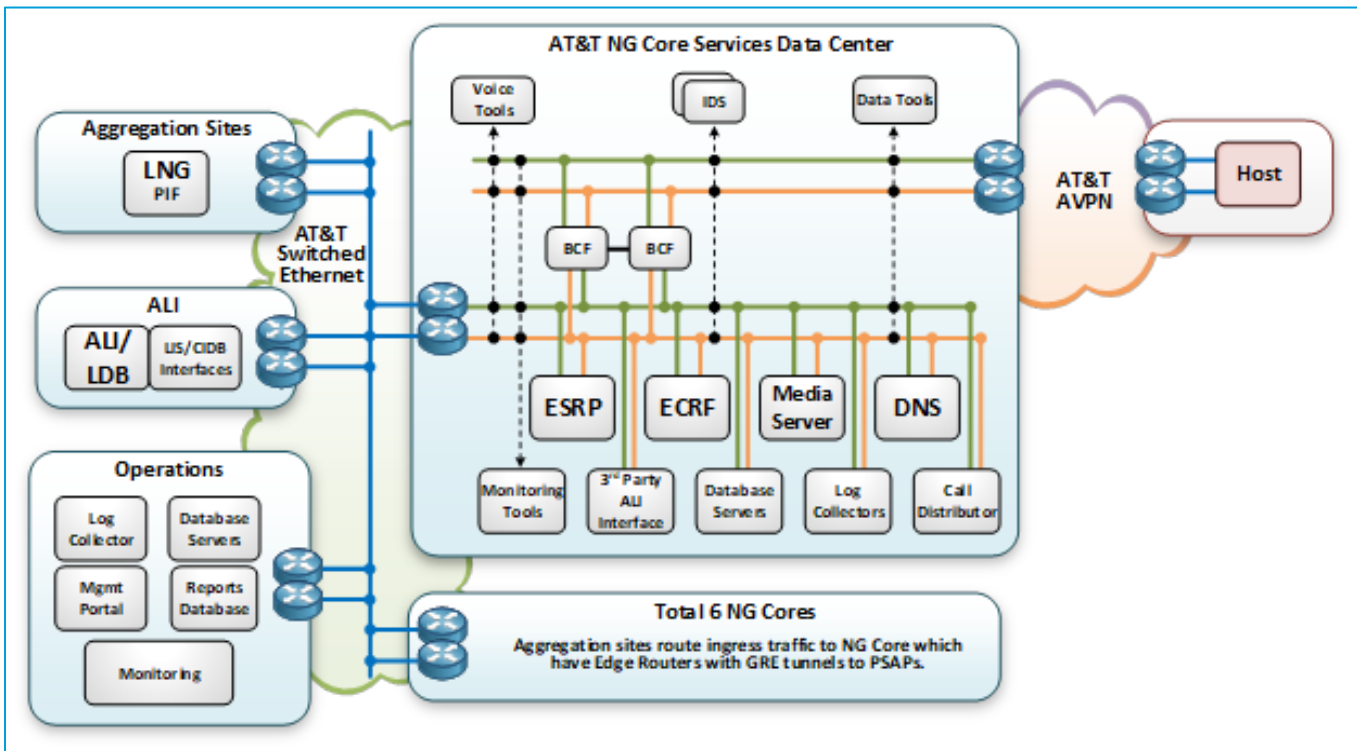


Figure 9: AT&T ESInet Functional Elements

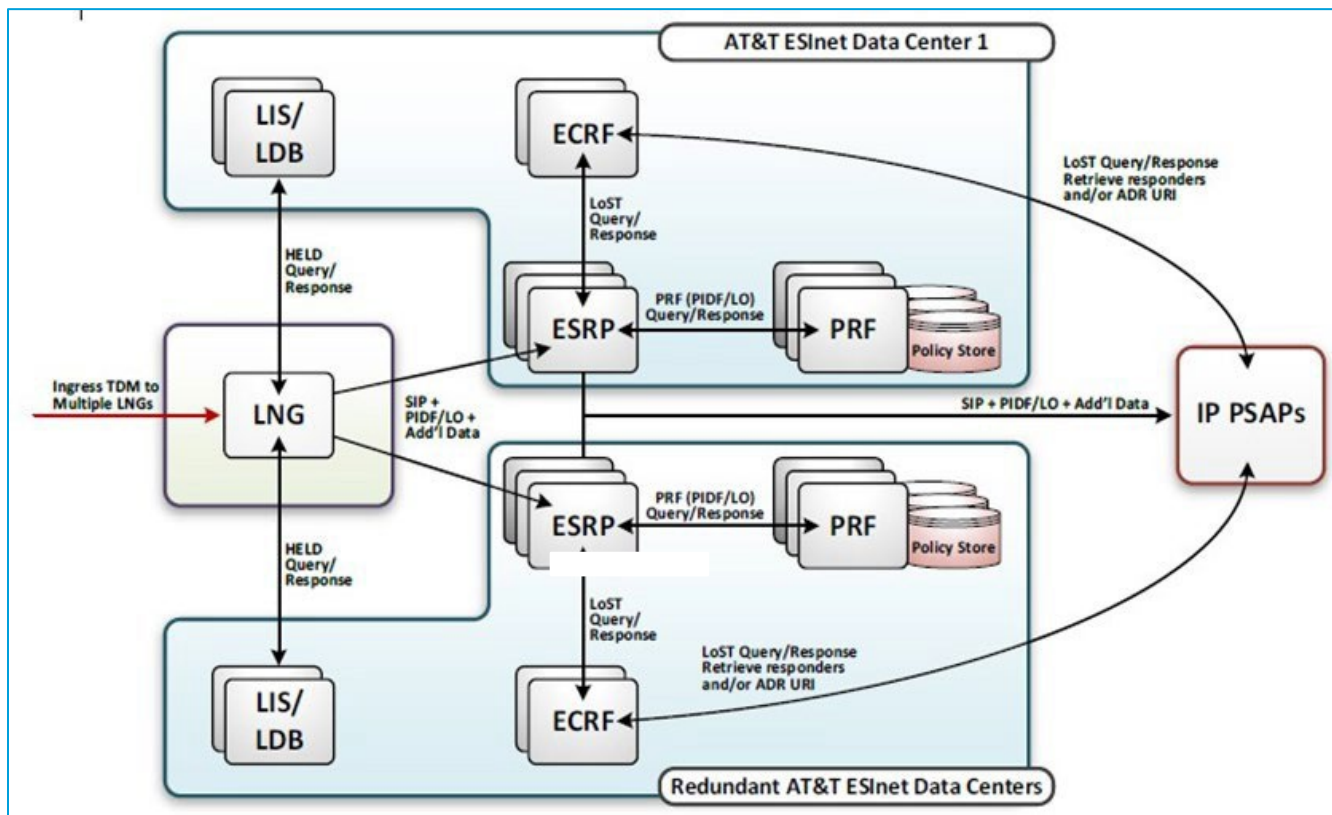


Figure 11: AT&T ESInet Redundancy by Design

AT&T ESInet™ – Component Description

AT&T ESInet™ is AT&T's managed, standards-based Emergency Services IP Network (ESInet) platform built to support NG911 call routing and delivery in accordance with NENA i3. The solution uses geographically diverse, redundant processing cores, regional aggregation sites, and secure interconnection points to provide end-to-end diversity from the caller (via OSP networks) to the call taker (PSAP). For the State deployment, AT&T maintains an authoritative inventory of all ESInet components (sites, nodes, circuits, interfaces, IP addressing/routing, and associated configuration items) and the corresponding logical and physical diagrams in a controlled repository/CMDB that is updated following approved changes.

Nebraska-specific deployment view (proposed):

For the State of Nebraska, the ESInet architecture will be documented as a statewide topology consisting of (1) **geo-diverse NGCS core sites** (national AT&T ESInet™ core locations), (2) **Nebraska interconnection/aggregation** locations (e.g., POIs and any required LNG/LSRG sites to support legacy ingress during transition), and (3) **PSAP egress/access** connections to each Nebraska PSAP (including host/remote configurations as applicable). AT&T will provide Nebraska-specific logical and physical diagrams that identify



each Nebraska POI, each PSAP demarcation, and the transport/capacity between them, and will maintain those as-built artifacts in the CMDB throughout the contract term.

- **Minimum two POIs for Nebraska:** AT&T will work with the State to identify at least two mutually agreed, geographically separated interconnection locations in Nebraska (or regionally proximate facilities) for OSP and/or peer ESInet connectivity, where practical.
- **PSAP diversity design:** For each PSAP, the design will document primary and secondary access (where feasible), including diverse POP entry and diverse last-mile routing when available, with clear identification of any single-carrier or single-route limitations.
- **Rural last-mile constraints and risk register:** Where Nebraska geography or local access constraints limit physical diversity, AT&T will document the span-of-control limitation, record it in the project risk register/CMDB, and present mitigation options (e.g., alternate provider access, alternate facility entry, microwave/FirstNet tertiary diversity where appropriate, or operational contingency routing).
- **Neighboring state connectivity:** Nebraska ESInet interconnections to neighboring ESInets/providers will be documented with boundary elements (BCF/SBC), routing policy (BGP), and tested failover behaviors.
- **Core processing sites (NGCS cores):** Geo-diverse data centers hosting NGCS application components (e.g., ESRP, ECRF, LVF, PRF, logging, databases) in a high-availability architecture.
- **ESInet IP transport (backbone):** A private IP transport layer (typically MPLS and/or Ethernet-based services) engineered with logical separation, QoS, and resilient routing between sites and to external connections.
- **Regional aggregation and legacy gateways:** Aggregation locations (e.g., LNG/LSRG sites and Points of Interconnection (POIs)) that accept legacy and/or IP ingress from OSPs and provide protocol interworking during migration.
- **PSAP connectivity layer:** Diverse access circuits to PSAPs (and host/remote PSAP architectures) supporting SIP signaling/media, text, and data connectivity as required.
- **Interconnection boundaries:** Secure boundary elements (BCF/SBC) and defined NNIs for peering with OSPs, neighboring ESInets, and external interfaces.
- **Operations, monitoring, and security:** 24x7 monitoring via NOC/SOC, logging/records, configuration management, and cybersecurity controls aligned to NG911 requirements.



Nebraska ESInet item (to be finalized during design)	Planned locations / identifiers	Transport / interface	Port speed / committed capacity	Diversity notes / constraints
NGCS Core Sites (AT&T ESInet™ cores)	(List core site names/regions used for Nebraska)	Inter-site transport (MPLS/Ethernet)	(e.g., 10G/1G links as applicable)	Geo-diverse cores; active-active processing
Nebraska POIs (OSP / peer ESInet interconnect)	POI #1: (City/Facility) POI #2: (City/Facility)	SIP over IP (TLS/SRTP where used); BGP	(Port speed per NNI; sized to 200% peak as required)	Separate facilities/paths where feasible
Legacy ingress gateways (LNG/LSRG) (if required)	(List LNG/LSRG sites serving Nebraska legacy ingress)	CAMA/SS7/ISUP interworking to SIP i3	(Trunk group sizing / DS1s / equivalent)	Transitional; retirement plan in CMDB
PSAP egress connectivity (per PSAP)	(PSAP name / address / demarc)	MPLS/Ethernet access; optional tertiary diversity	(Port speed and bandwidth per PSAP)	Primary/secondary diversity and constraints noted
External interfaces (ADR, GIS/SI, analytics, etc.)	(List systems and hosting locations)	REST/SIP/other NENA i3 interfaces	(As required)	Security boundary via BCF/SBC

Component details

- **ESInet IP transport (MPLS/Ethernet):** Provides the private, QoS-enabled IP connectivity between core sites, aggregation locations, PSAPs, and interconnection points. The transport is engineered with redundant routing and diverse paths where available, supports IPv4/IPv6, and uses QoS marking (e.g., DiffServ/DSCP) to prioritize emergency signaling and media. Port speeds and circuit types (e.g., Ethernet handoffs, 1G/10G where applicable, MPLS access) are defined per site and documented in the CMDB and topology diagrams.
- **Core processing sites (NGCS cores / data centers):** AT&T ESInet™ leverages a multi-site, geographically diverse core architecture where NGCS functions are deployed in redundant instances. Any emergency transaction can be processed by available core resources, supporting continuity of operations if a site or component becomes unavailable. Core sites host the NGCS application components listed below, along with supporting compute, storage, and database services sized to meet throughput and availability requirements. Core-site locations, roles, and inter-site connectivity are shown on the logical and physical topology diagrams maintained in the CMDB.
- **Aggregation sites and Points of Interconnection (POIs):** Aggregation locations provide the physical demarcation points where OSPs and other external parties interconnect to the ESInet. Depending on the OSP's capabilities and the migration phase, ingress may be delivered as legacy trunks (e.g.,



CAMA/SS7) into an LNG/LSRG, or as SIP over IP at an IP POI through the BCF/SBC. AT&T designs for at least two geographically diverse interconnect locations where practical and documents all ingress/egress points (facility address, circuit IDs, handoff type, and routing policy) in the CMDB.

- **PSAP connectivity (egress) and PSAP interconnects:** PSAPs connect to the ESInet using diverse access where feasible (e.g., primary and secondary circuits with physically diverse routing and/or diverse POP entry). Each PSAP connection is provisioned with bandwidth aligned to the State's requirements and sized for peak operations with resiliency under failure conditions. Connectivity supports SIP signaling and media (TLS/SRTP where used), as well as NG911 data exchanges and optional non-911 public safety data transport as authorized. PSAP connectivity details (transport type, port speed, addressing, and routing) are captured in the CMDB and reflected in the physical topology diagrams.
- **Border Control Function (BCF) / Session Border Controller (SBC):** The BCF/SBC protects ESInet boundaries and enforces trust relationships for interconnection with OSPs, PSAPs, and peer ESInets. It provides SIP security (e.g., TLS), media security (e.g., SRTP where applicable), topology hiding/policy enforcement, protocol normalization, and controlled admission of traffic into the NGCS cores. BCF/SBC instances are deployed redundantly and are documented as boundary elements on both logical and physical diagrams.

NGCS and related functional components (what each does)

- **Emergency Services Routing Proxy (ESRP):** The call routing signaling function that receives emergency call signaling (SIP), applies policy and routing logic, performs necessary lookups (directly or via other services), and routes calls toward the appropriate destination PSAP or alternate route. ESRP supports call transfers and maintains required SIP header/context handling as defined by NENA i3.
- **Policy Routing Function (PRF):** Provides policy-based routing decisions (Policy Routing Rules) used by the ESRP and related functions to determine call handling behavior (e.g., normal, alternate, overflow, contingency routing) based on conditions such as PSAP status/queue, time of day, incident conditions, or other policy inputs.
- **Emergency Call Routing Function (ECRF):** Uses authoritative GIS data to perform location-to-service translation (LoST) and returns the appropriate service URI and/or routing information needed to deliver the call to the correct PSAP and/or responder agency for the caller's location.
- **Location Validation Function (LVF):** Validates civic and/or geodetic location information against authoritative GIS/addressing data and supports returning validation results (including match/degraded match indicators) used to improve routing accuracy and data quality.
- **Spatial Interface (SI):** The standardized interface used to provision and synchronize GIS features and related spatial datasets that support ECRF/LVF and related spatial functions.
- **Location Database (LDB):** Stores location records used for NG911 call processing and legacy-to-NG transitions. It supports ingestion, normalization, and management of location data and provides interfaces for authorized provisioning and audit/history tracking as applicable.



- **Legacy Network Gateway (LNG):** Accepts legacy 9-1-1 call ingress (e.g., CAMA/MF/SS7) and converts legacy signaling and location into i3-compliant SIP, including creation of a PIDF-LO. LNG supports continued service for legacy-originating networks during transition to native i3 origination.
- **Legacy Selective Router Gateway (LSRG):** Provides selective-router-related interworking during transition where required (e.g., inter-tandem SS7/ISUP termination and signaling interworking), supporting continuity while OSPs migrate to direct ESInet ingress. Any LSRG is treated as a transitional element with a documented retirement plan.
- **Legacy PSAP Gateway (LPG):** Provides interworking for PSAPs that require legacy interfaces during migration, enabling phased transition while maintaining service continuity.
- **Additional Data Repository (ADR) / Identity Searchable ADR (IS-ADR):** Stores and provides access to additional call-associated data and supports standards-based query/dereference mechanisms so that authorized systems (including PSAP applications) can retrieve supplemental data linked to an emergency transaction.
- **Incident Data Exchange (IDX):** Supports standardized data exchange related to incidents between NG911 systems and other authorized public safety applications where applicable.
- **Logging Service / Logger:** Generates end-to-end i3 logging events and supports retrieval for troubleshooting, auditing, reporting, and incident analysis. Logs are correlated across components using identifiers/correlation methods as supported by the platform.
- **Media Server / Bridging:** Supports media services such as conferencing/bridging used for call transfers, multi-party communications, and related NG911 media handling scenarios consistent with NENA call flows.
- **Network Time Protocol (NTP) time source:** Provides a consistent time reference across ESInet components to support accurate logging timestamps, correlation, and operational troubleshooting.

Redundancy and path diversity (logical and physical)

- **Physical diversity:** AT&T designs for diverse access where feasible (e.g., separate entrances, diverse last-mile routing, and diverse POP entry) for PSAP and critical aggregation locations. Where full physical diversity cannot be achieved due to local limitations, AT&T documents the constraint, identifies the associated risk, and works with the State/PSAP/OSP to evaluate mitigation options.
- **Logical diversity:** Redundant routing and failover behaviors are implemented through resilient IP routing and policy-driven call routing (ESRP/PRF), allowing calls to be routed to alternates (alternate PSAP, overflow, last resort) based on availability and configured policy.
- **Interconnection diversity:** Interconnects with OSPs and peer ESInets are designed to use multiple points of interconnection where practical, with documented primary/alternate routing and tested failover procedures.



- **Validation:** Diversity assumptions and failover behaviors are validated during testing (including ORT and cutover readiness activities) and are revalidated when significant topology or routing changes occur.

One-time and transitional network elements

AT&T recognizes that NG911 deployments commonly require temporary or transitional elements during migration (for example, LSRG connectivity to legacy selective routers, temporary inter-tandem SS7/ISUP trunking, temporary IP POIs, dual provisioning between legacy ALI and NG LDB, and interim routing configurations). AT&T documents these one-time and transitional elements in the CMDB with (1) purpose and dependency, (2) planned duration/exit criteria, and (3) retirement/decommissioning steps. When a transitional element is removed, AT&T updates the CMDB and diagrams to reflect the as-built state.

Ingress/egress points, transport types, and capacity documentation

- **Ingress:** OSP ingress connection methods (legacy and IP) and their physical handoff locations (POIs/LNG sites) are documented, including circuit/port characteristics, interface type, and routing policy.
- **Core:** Core-site connectivity, inter-site transport, and core application capacity planning assumptions are documented, including how capacity and performance are monitored and when scaling actions are triggered.
- **Egress:** PSAP access transport type and port speeds (e.g., Ethernet handoff) and committed capacity are documented per PSAP, including primary/secondary circuit diversity and any known limitations.
- **Transport types and port speeds:** The State's ESInet design package identifies the transport type used per connection segment (e.g., MPLS, Ethernet access) and the port speeds/hand-off specifications at each demarcation point, as applicable.
- **Interconnection locations:** The CMDB and diagrams enumerate interconnection nodes (core data centers, aggregation sites, POIs, LNG/LSRG/LPG locations, and any external NNI handoff points) and identify associated technologies and interfaces used at each location.

Operations, monitoring, and CMDB/diagram governance

- **24x7 monitoring and support:** AT&T provides continuous monitoring through operational support organizations (e.g., NOC/SOC and 9-1-1 operations resources) to detect faults, performance degradation, and security events across transport, gateways, and NGCS components.
- **Configuration management:** Network and application configuration items (including routing, interconnects, addressing, security boundaries, and PSAP/OSP provisioning artifacts) are controlled through change management. Approved changes trigger updates to associated diagrams and CMDB records so that the State can validate the current deployment.



Access and currency: The State and the 9-1-1 Advisory Committee are provided access to the current, approved versions of ESInet topology diagrams and related configuration records throughout the contract term, subject to agreed security and access controls.

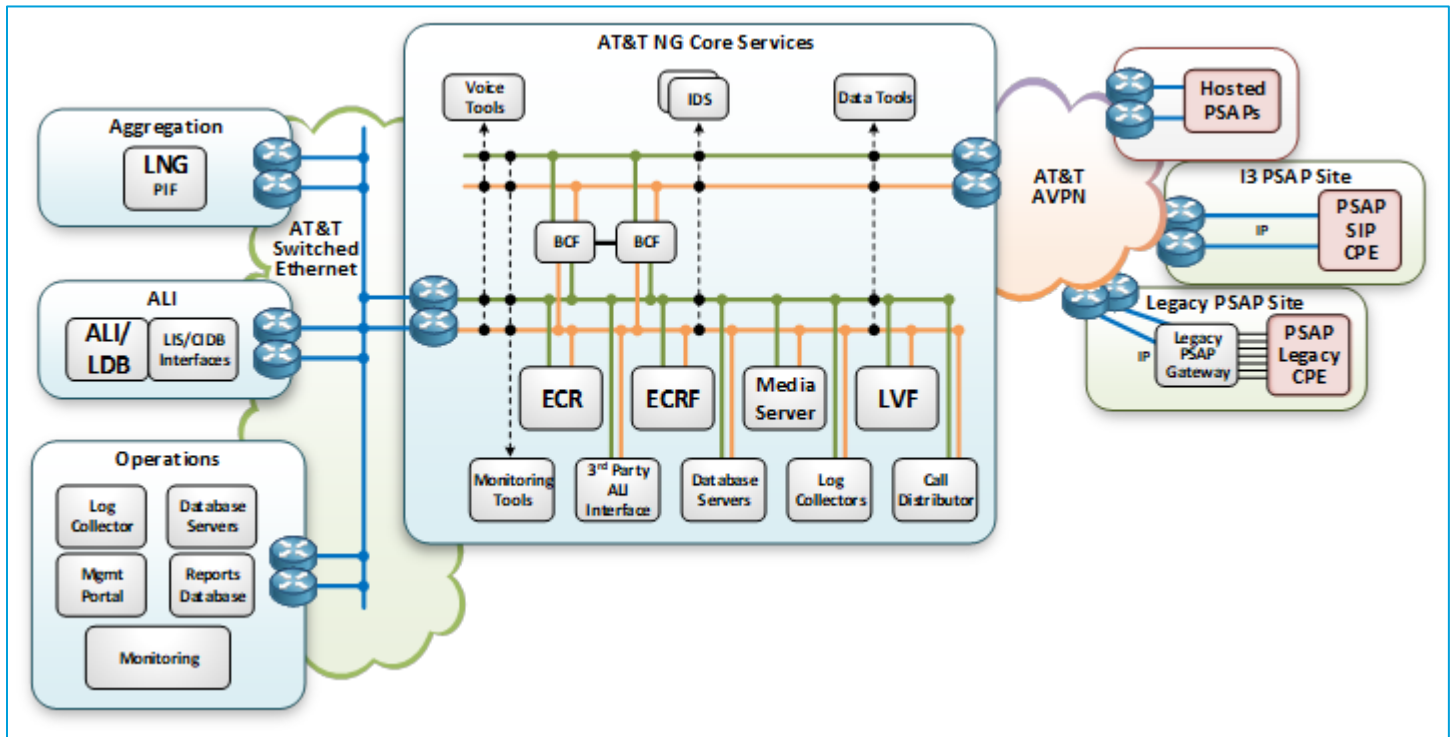


Figure 12: AT&T ESInet NGCS Functional Elements

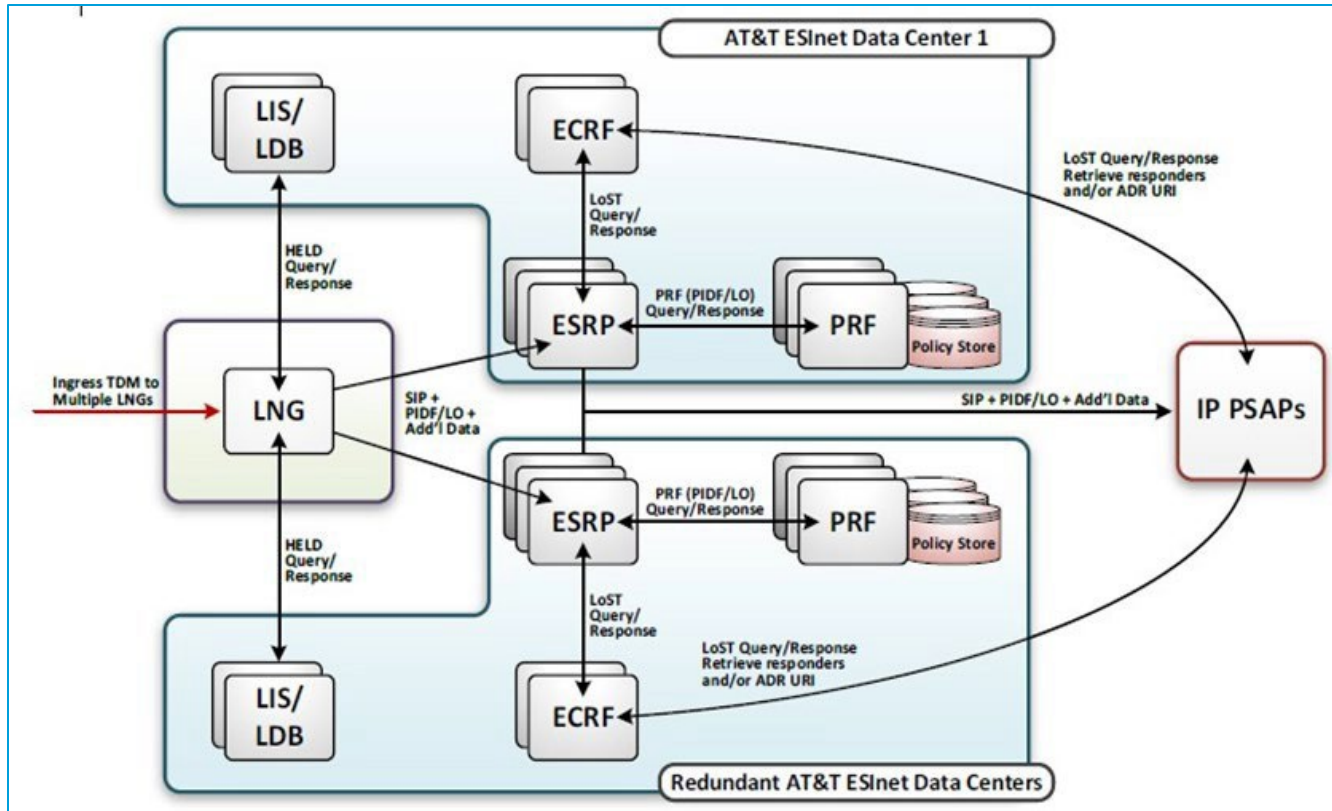


Figure 13: AT&T ESInet Redundancy by Design

1.1.2. ESInet Interconnection

The ESInet must facilitate seamless interconnections with neighboring states or regions upon deployment. The ESInet shall use the **Border Gateway Protocol (BGP)** as the sole **Exterior Gateway Protocol (EGP)**.

Newly established ESInets in cooperating states must be able to connect to the State ESInet within a designated timeframe. To ensure robustness and resilience:

- Interconnection should occur at a minimum of two mutually agreed-upon points to guarantee redundancy.
- Bandwidth provisioning must cater to **at least 200% of anticipated peak call volume**, ensuring ample capacity and robustness.
- Interconnecting methods and locations should be balanced equitably to manage costs effectively among partners.
- If neighboring ESInets do not adhere to the State's Differentiated Services Code Point (DSCP) specifications, the state's routers will remap DSCPs as deemed appropriate.
- The establishment of BGP between the State ESInet and neighboring networks is recommended.



All additional networks integrated with the ESInet must meet the specified minimum qualifications for interconnection to uphold security and performance standards. The State's security must be collaboratively protected by all involved network providers.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Seamless interconnections with neighboring states/regions upon deployment.
- Connection capability for new ESInets within designated timeframe.
- Minimum two interconnection points for redundancy.
- Bandwidth provisioning for 200% of peak call volume.
- Equitable interconnecting methods/locations for cost management.
- DSCP remapping if neighboring ESInets differ.
- Recommendation for BGP between networks.
- Minimum qualifications for additional integrated networks; and collaborative security protection by providers.

AT&T Response:

Comply.

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 highly secure and highly available facilities.

The AT&T ESInet™ supports IP ingress at geographically distributed POIs. The AT&T ESInet™ supports basic SIP or i3 protocol interfaces to external ESInets for call hand-off and call transfers. Given pre-established connectivity capability, PSAPs on the AT&T ESInet™ have the ability to transfer calls to PSAPs on other ESInets or PSAPs that have not yet transitioned off legacy selective routers. Legacy Network Gateways reside in Aggregation Site locations and convert local legacy TDM 9-1-1 calls to IP.

AT&T has executed nationwide agreements with the majority of ESInet providers offering NG 9-1-1 services and Legacy 9-1-1 service providers. AT&T will utilize its executed nationwide interconnection agreements to exchange 9-1-1 traffic with cooperating neighbor states. Neighboring states that have yet to select their NG 9-1-1 Service Provider will benefit from the existing agreement with legacy providers. If a neighboring state selects an NG 9-1-1 Service Provider without an existing interconnection agreement, AT&T will work to execute an agreement as quickly as possible. Typically, such agreements take 3-4 months to complete.



Before implementation AT&T works with other ESInets and legacy 9-1-1 service providers to arrange interconnection if an existing connection is not in place. Existing connections may be used to implement new PSAP or add new transfer capabilities. The NNI circuits in production with other ESInet providers are 1G circuits that can support 200% of the expected call volume. Connections required to handoff and/or transfer with a neighboring PSAP will be in place before an AT&T ESInet™ goes live provided the PSAP arrangement is known before implementation.

NNI connections that are required for transfers only between neighboring ESInet providers may be implemented within 90 days provided the NNI connections are in place. If new NNI connections need to be ordered the implementation could exceed 90 days due to circuit ordering intervals. These interconnection arrangements will also allow legacy PSAPs served by legacy selective routers to serve as the abandonment route for PSAPs served by the AT&T ESInet solution.

As required, AT&T will work directly with neighboring ESInets to determine appropriate interconnection points and routing configurations with the AT&T ESInet. Thorough non-live interoperability testing will be completed before live emergency calls are supported.

1.2. External and PSAP Connectivity

1.2.1. Originating Service Provider (OSP) Connection

Contractors are responsible for facilitating all necessary connectivity to allow traffic to flow from OSPs into the ESInet.

- Upon acceptance, sufficient bandwidth must be provisioned to support OSP traffic irrespective of connection method (CAMA, SS7, IP, etc.).
- Points of Interconnection (POI) must be deployed with the greatest extent of diversity possible. This means that the contractor **shall be required** to identify any situations where OSPs lack diverse connections to the POI(s).
- Where diversity is limited from an OSP to the POI, and/or from the egress gateway to the PSAP, or restricted for any reason, **the contractor must identify this as a risk to their NG911 service and discuss options with the PSC for limiting or eliminating the exposure of an OSP or PSAP if a lack of diversity may cause a disruption.**
- Careful design should ensure **redundancy and diversity from the caller to the call-taker** to ensure that the system is as diverse and redundant as possible from end-to-end.
- Communications must enable smooth migration to the ESInet once operational, including aggregation of legacy 911 traffic into the core network.
- Contractors must continuously monitor the bandwidth at aggregation points to efficiently manage and increase bandwidth as required.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Facilitation of diverse and redundant connectivity for OSP traffic flow into the ESInet.
- Provisioning of sufficient bandwidth for OSP traffic (CAMA, SS7, IP, etc.) upon acceptance.
- Smooth migration to ESInet with aggregation of legacy traffic.
- Redundant and diverse design for disruptions, interfacing with network gateways based on OSP capabilities.
- Identification of any risks to their system due to lack of diversity or redundancy from caller to call-taker.
- Identification of risks from limited diversity and options to mitigate exposure for OSPs or PSAPs.
- Continuous monitoring/increase of bandwidth at aggregation points.

AT&T Response:

Comply.

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. AT&T utilizes the TDM POI/LNG, IP POI/BCF, and LSRG. The LSRG is only used as a transitional method until the Originating Service Providers (OSPs) can rehome their traffic to either the TDM POI or IP POI.

AT&T ESInet has completed OSP interconnection with the nations wireless service providers AT&T, Verizon and T-Mobile; each of these providers is delivering SIP/IP traffic that accounts for approximately 85% of all 9-1-1 calls. Similarly, AT&T has fully integrated with other OSPs such as Lumen, Comcast, Windstream, etc. AT&T has completed intercarrier agreements with all major OSPs.

For those OSPs not yet integrated with AT&T ESInet, AT&T will work with the State to jointly manage the transition and develop communication to each OSP 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 will facilitate the establishment of OSP communication guidelines with the State and adhere to these guidelines for the project implementation and service duration. 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. AT&T will escalate to the State as appropriate regarding OSP initiatives and will request State intervention if necessary.



There are multiple design considerations associated with OSP ingress into the AT&T ESInet. The following considerations are critical for a successful OSP migration into the network. AT&T supports voice ingress (TDM or IP) and data ingress (legacy or i3) as described below to give OSPs the best option to efficiently transition to the AT&T ESInet.

1.2.2. PSAP Connection

At the point of system acceptance, the ESInet must guarantee sufficient bandwidth to support:

- **2 Mbps per PSAP + 2 Mbps per position** during standard operational conditions.
- **1 Mbps per PSAP + 1 Mbps per position** under conditions where network disruptions occur, which may include simultaneous failures of the largest link or comprehensive outages affecting all networks of a single ISP.

The contractor must commit to ongoing bandwidth monitoring throughout the contract duration and promptly increase capacity as necessary, including an annual growth factor of 10%.

The design must also facilitate interconnections with PSAP systems (like CAD and logging recorders), as well as with criminal justice networks and other secure public safety technologies, ensuring uninterrupted SIP traffic flow for 911 calls.

The ESInet shall allow for all egress connectivity, including gateways, and be configured to establish the capability for traffic to flow from the ESInet into the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Guaranteed bandwidth of 2 Mbps per PSAP + 2 Mbps per position under standard conditions and 1 Mbps per PSAP/position under disruptions (e.g., largest link failure or ISP outage).
- Commitment to ongoing bandwidth monitoring and increases with 10% annual growth factor.
- Facilitation of interconnections with PSAP systems (CAD, logging recorders), criminal justice networks, and secure public safety technologies.
- Ensuring uninterrupted SIP traffic for 911 calls.

AT&T Response:

AT&T is providing bandwidth in accordance with the requirements of the State and will provide 2M per PSAP and 2M per position. Our solution implements twice as much bandwidth as is required to serve the total number of simultaneous calls that traverse the network. If a single router or IP instance fails, enough bandwidth will still be available to support simultaneous calls to all the PSAP's provisioned dispatch seats. The IP network is designed in a 100% capacity and 100% redundancy configuration, so that if one IP carrier's



network goes down, the redundant bandwidth can manage 100% of the PSAP's capacity. The end result is a network that is truly public safety grade in terms of capacity, reliability, and redundancy. AT&T's PSAP connection supports transmission of non-emergency third-party data, including but not limited to CAD, logging recorders, and criminal justice networks.

AT&T ESInet utilizes multiple reporting tools to monitor, log and notify/alert of any bandwidth issues that arise between the NGCS and PSAP. This includes bandwidth utilization and server resource utilization. If any threshold is met, alarms trigger trained technical resources from the network engineering and NOC teams to begin to investigate possible issues and coordinate any necessary testing with OSPs. AT&T is committed to a 10% annual growth factor.

AT&T ESInet is capable of supporting non-9-1-1 call traffic such as CAD, logging recorders, criminal justice networks, and secure public safety technologies. AT&T will work with the State of Nebraska to determine any additional traffic that requires the ESInet for transport and determine if any bandwidth and capacity models need to be updated to accommodate such traffic.

AT&T ESInet utilizes multiple reporting tools to monitor, log and notify/alert of any bandwidth issues that arise between the OSP and ESInet ingress as well as the PSAP via the ESInet egress. This includes bandwidth utilization, server resource utilization, as well as network aggregation site capacity reports. If any threshold is met, alarms trigger trained technical resources from the network engineering and NOC teams to begin to investigate possible issues and coordinate any necessary testing with OSPs.

1.3. Legacy Interoperability

1.3.1. Legacy Network Gateway (LNG)

The Respondent must provide a Legacy Network Gateway (LNG) solution to serve as the ingress point for calls originating from legacy networks (e.g., wireline, wireless, VoIP) that have not yet transitioned to native i3 SIP origination. The LNG is responsible for converting legacy signaling to i3-compliant SIP and querying legacy ALI databases to obtain location information.

LNGs and/or LSRGs must conform to NENA-STA-010.3 and provide termination for all existing legacy OSPs until they migrate to i3 origination. The current solution utilizes an LSRG combining LNG and LSRG functions.

- **Interface Compatibility:** o The LNG must maintain interface compatibility with existing Selective Routers, allowing for minimal disruption and cost implications.
- **Geographical Redundancy:** o Legacy OSPs must have access to connections at two geographically diverse LNGs to enhance resilience.
- **Legacy Support:** o The LNG must be configured to manage legacy PSALI records, including migration processes outlined in the documentation provided.



LNG Connectivity to ESInet

The LNG must securely connect to the ESInet, receive calls from legacy network trunks (e.g., CAMA, MF), and interface with the ESInet's Border Control Function (BCF) to forward calls into the NG911 core.

Protocol Conversion (Legacy to SIP)

The LNG must convert legacy in-band signaling (e.g., CAMA wink-start, MF tones) and associated trunk supervision into i3-compliant SIP (RFC 3261) for processing by the ESInet.

ALI Query and Location Formatting

The LNG must use the Automatic Number Identification (ANI) received from the legacy call to perform a query against the appropriate legacy ALI database. It **MUST** then format the retrieved ALI data into a NENA-compliant Presence Information Data Format - Location Object (PIDF-LO) for inclusion in the outbound SIP INVITE.

Security, Logging, Monitoring, and Redundancy

The LNG, as a critical ESInet functional element, must adhere to the same stringent requirements for security, logging, monitoring, and redundancy as other core components to ensure system integrity and high availability. **If separate LNGs are proposed, they must:**

- Maintain interfaces similar to current systems
- Support TTY to RTT conversion
- Provide E2 connections to all MLCs, GMLCs, and VPCs
- Be positioned outside the ESInet, before the BCF
- Support ElementState and ServiceState functionality

Each component has specific requirements for capacity, performance, integration, and conformance with NENA standards.

The solution must maintain appropriate spare parts at various locations to ensure immediate system restoration when needed, with specific requirements for inventory management, replacement schedules, and on-site spares at data centers.

The LNG must support the Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS. **The LNG shall support:**

- Error checking
- GIS-based MSAG (for legacy OSP use)



- The Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS
- Service Order Address Validation
- Service Order Error checking
- Service Order history available/viewable for every telephone number
- Coordination with Telecommunications providers:
 - OSPs will be able to manage/make updates to their records directly in the database without having to submit SOI
 - OSPs will be able to run performance/statistical reports on their No Record Found (NRF)/Discrepancy and SOI processing
 - OSPs will be able to view discrepancies and NRFs directly from the web interface real time
- Data import / export
- Data integrity and availability
- ALI updates
 - OSP's have the ability to manually update their own records
 - OSP's have the ability to lock and unlock their own records
 - All manual updates be tracked in history
- Customer access to data
- Telco access to data
- Bulk modifications
- PSALI functionality
- Database reports
- NRF process o ALI discrepancies
- Tracking, reporting and timestamp for discrepancies and NRFs.
- Service Order exceptions
- ALI database audit
- MSAG database audit

The State expects the LNG to maintain connections to Text Control Centers (TCCs) so that NG PSAPs maintain a complete standard (NENA-STA-010.3) connection for Short Message Service (SMS) calls to 911 from legacy OSPs via the LNG.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LNG conformance to NENA-STA-010.3 for legacy OSPs until i3 migration.
- Interface compatibility with existing Selective Routers.
- Geographically diverse connections for legacy OSPs.
- Management of legacy PSALI records with migration processes.
- TTY to RTT conversion.
- E2 connections to MLCs/GMLCs/VPCs.
- Positioning outside ESInet before BCF.
- ElementState/ServiceState support.

AT&T Response:

Comply.

The solution provides a fully NENA compliant Legacy Network Gateway (LNG) and Legacy Selective Router Gateway (LSRG) architecture that ingests calls from legacy wireline, wireless, and VoIP networks, converts their CAMA/SS7 signaling into i3compliant SIP, and performs all required legacy ALI/location queries. It maintains compatibility with existing selective routers to minimize disruption and cost, provides geographically diverse LNG connection points so legacy OSPs can interconnect redundantly, and supports PSALI record management and migration workflows while ensuring secure, reliable, and seamless transitions to native i3 call delivery.

The LNG securely connects to the ESInet by terminating legacy CAMA, MF, and SS7 trunks, converting their signaling into i3compliant SIP, and performing necessary legacy location queries before forwarding traffic. Once converted, all SIP sessions pass through the ESInet's Border Control Function, which enforces security and protocol normalization, ensuring that only validated and properly formatted calls enter the NG911 core for further routing.

The LNG terminates legacy in-band signaling such as CAMA wink-start, MF tones, and SS7/ISUP, converting all associated signaling and trunk supervision into i3 compliant SIP (RFC 3261) for processing within the ESInet. This TDM-to-IP conversion ensures that calls originating from any legacy network can be properly translated, routed, and delivered through the NG911 core in full alignment with NENA i3 functional requirements.

The LNG uses the ANI received from the legacy call to perform a real-time query against the appropriate legacy ALI database through established E2 location interfaces. Once the ALI record is returned, the LNG reformats the location data into a NENA compliant PIDFLO and inserts it into the outbound SIP INVITE. This



ensures that calls originating from legacy networks are delivered into the ESInet with fully standards compliant i3 location information for accurate NG911 routing.

As a critical ESInet component, the LNG is held to the same rigorous standards for security, logging, monitoring, and redundancy as all other NG911 core elements. It is integrated into the system's defense in depth architecture, ensuring all LNG originated traffic is authenticated and screened through the BCF, while redundant, geographically diverse LNG nodes provide high availability and eliminate single points of failure. The LNG is continuously monitored by the NOC, with full logging, alarm generation, and system health tracking aligned with the same requirements enforced across the NGCS, maintaining system integrity and ensuring uninterrupted ESInet operation.

Multiple LNGs are deployed throughout AT&T ESInet and they will maintain interfaces consistent with existing selective router systems to minimize disruption for legacy OSPs. The LNGs support TTY and RTT handling, provide full E2 connectivity to all MLCs, GMLCs, and VPCs for legacy location retrieval, and are positioned outside the ESInet so that all LNG originated traffic is securely processed through the BCF before entering the NG911 core. They also support—or will support in updated releases—ElementState and ServiceState functionality in alignment with NENASTA010.3. Each LNG component meets the same capacity, performance, integration, and standards compliance requirements as all other NGCS elements.

The solution maintains appropriate spare parts across multiple locations, including onsite spares at core data centers and additional inventory strategically positioned to ensure rapid restoration when equipment fails. Inventory levels, replacement schedules, and replenishment cycles are managed through a formal sparing program that tracks usage, failure trends, and lifecycle requirements. Critical components—such as servers, routers, switches, power supplies, and gateways—are held in immediate deployment inventory so that replacements can be installed quickly and consistently meet uptime and restoration objectives. Regular reviews and trend analysis ensure that spare inventories remain aligned with system performance needs throughout the life of the contract.

The LNG supports the Service Order Activation interface used by legacy OSPs by receiving and processing service-order inputs and updating location records accordingly. Using the Master Control System (MCS), the solution converts legacy service-order and ALI/PSALI data into LVF-valid form, stores it in the Location Database, and supports bi-directional translation between legacy formats and NENA-compliant NG911 formats. This ensures that all location information entering the ESInet is validated, geospatially aligned, and fully compatible with i3 routing requirements while still supporting existing OSP provisioning workflows.

The LNG solution conforms to NENA-STA-010.3 and supports legacy OSPs until their full migration to i3 by converting legacy signaling into SIP, performing ALI queries, and routing calls according to i3 standards. It maintains full interface compatibility with existing selective routers, allowing legacy ISUP connections to continue operating without disruption. Legacy OSPs may connect through geographically diverse POIs feeding redundant LNG sites, ensuring resiliency and avoiding single points of failure. The solution also manages PSALI data through MCS workflows that validate and convert legacy records into LVF-valid format for storage in the Location Database.



TTY support is provided, with RTT compatibility enabled through interoperable components. The LNG provides E2 interfaces to all required MLCs, GMLCs, and VPCs for legacy ALI retrieval and reformats this data into PIDFLO for SIP delivery. In accordance with NENA standards, the LNG is positioned outside the ESInet so all traffic passes through the BCF before entering the NG911 core. ElementState and ServiceState capabilities are implemented in the solution to meet NENA-STA-010.3 requirements.

1.3.2. Legacy Selective Router Gateway (LSRG)

A Legacy Selective Router Gateway (LSRG) must serve as the interface for legacy selective routers to terminate ISUP SS7 trunks utilizing an inter-tandem trunk group method of termination.

The LSRG must convert the call signaling to SIP/RTP, query the existing ALI data management system to retrieve location information for the call and then route the call to the next nominal “hop” based on a LoST query to an ECRF.

Additionally, the LSRG must be able to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

If Respondents utilize an LSRG for their proposed solution, they must include a timeline and plan for removing the LSRG during the contract period. The LSRG is to be only a temporary solution that can be used to initially gateway OSP traffic.

Any LSRG implemented as part of the Contractor’s solution must conform to the NENA Legacy Selective Router Gateway (LSRG) Standard (NENA-STA-034.1-2022), and should be deployed to align with the relevant sections of the NENA NG9-1-1 Transition Plan Considerations Information Document (NENA-INF-008.2-2013).

LSRG Connectivity to ESInet and Legacy SR

The LSRG must provide a secure interface to the ESInet to receive routing queries from the ECRF and a separate, secure interface compatible with the legacy Selective Router's query/response protocol.

Routing Protocol Conversion (LoST to Legacy)

The core function of the LSRG is to receive a standards-based Location-to-Service Translation (LoST) protocol query (RFC 5222) from the ECRF, translate it into a format the legacy SR can process (often a proprietary format or a simplified query containing an ESN), and translate the SR's response back into a LoST response for the ECRF.

Security, Logging, Monitoring, and Redundancy

The LSRG must meet the same core requirements for security, logging, monitoring, and geo-diverse redundancy as other critical ESInet functional elements to ensure the integrity and availability of call routing.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Interface for legacy Selective Routers via ISUP SS7 trunks.
- Conversion to SIP/RTP.
- ALI query and LoST-based routing.
- Bi-directional communications for voice/data (star codes).
- Timeline/plan for LSRG removal as temporary solution for OSP traffic.
- Deployed LSRG (where applicable) in conformance with NENA LSRG Standard (STA-034.1)

AT&T Response:

Comply.

The Legacy Selective Router Gateway (LSRG) is a signaling and media interconnection point between callers in the legacy originating networks and AT&T ESInet. The LSRG converts calls from SIP to TDM signaling for egress from the ESInet to the Legacy Selective Routers. AT&T ESInet provides redundant, resilient Legacy Network Gateways (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 the NGCS and vice versa. Legacy Network Gateways reside in Aggregation Site locations and convert Local Legacy TDM 9-1-1 calls to IP.

The LSRG is a temporary network element that will be removed once remaining legacy OSPs have transitioned from TDM to IP. Per the FCC NG911 OSP mandate, carriers must deliver IP traffic within six months of receiving notification of PSAP readiness. AT&T will manage the OSP transition on behalf of the State.

1.3.3. Legacy PSAP Gateway (LPG)

The State requires **Legacy PSAP Gateways (LPGs)** that conform to NENA-STA-010.3. LPGs shall provide **origination for all legacy PSAPs until those PSAPs migrate to i3 termination. LPGs must allow PSAPs to continue to use existing equipment and processes except where NENA-STA-010.3 requires change** (for example, use of PseudoAutomatic Number Identification [pANI]). Each LPG shall connect legacy PSAPs to the ESInet using SIP and legacy interfaces such as CAMA and ALI and shall convert NG911 SIP signaling and media to legacy protocols such as TDM and ISDN to maintain compatibility.

Protocol Conversion (SIP to Legacy)

The LPG must convert the SIP-based signaling and media from the ESInet into legacy circuit-switched formats (e.g., CAMA, ISDN PRI) that are compatible with the legacy PSAP's CHE.



Location and ALI Integration

The LPG must extract location information (PIDF-LO) from the incoming SIP signaling and convert it into a legacy Automatic Location Identification (ALI) format for delivery to the PSAP's ALI database/controller.

Text Support (TTY to RTT Conversion)

The LPG must support interworking between Real-time Text (RTT) on the ESInet, and legacy Baudot-based Teletypewriter (TTY) devices used in the PSAP, ensuring seamless communication for hearing-impaired users.

Call Transfer Support

The LPG must support call transfer scenarios, including the ability to relay transfer requests from the legacy PSAP back into the ESInet to enable transfers to other NG911-capable agencies or PSAPs.

Logging and Reporting

The LPG must generate detailed logs for all call processing events, alarms, and system activities and forward them to a central logging service in a standard format (e.g., Syslog) as defined by NENA standards.

Security Mechanisms

The LPG must implement robust security measures, including access control, authentication, and encryption, to protect the interface between the ESInet and the legacy PSAP network, adhering to NG911 security standards.

Monitoring and Maintenance

The LPG must be capable of being monitored for operational status, performance, and alarms. It must support standard monitoring protocols (e.g., SNMP) and provide mechanisms for remote administration and maintenance.

Geo-Diversity and Redundancy

The LPG must be deployed in a geographically diverse and redundant configuration to ensure high availability and failover capabilities, preventing a single point of failure from isolating a legacy PSAP.

Discrepancy Reporting

The LPG must support a mechanism for reporting discrepancies, such as call routing errors or ALI data problems, from the legacy PSAP environment back to the NG911 systems Discrepancy Report service.

The Respondent must provide a description and/or documentation that supports the requirements in this section:



- The LPG must be able to maintain the PSAP's existing ALI format.
- The LPG must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3.
- The State must be able to subscribe to ServiceState and receive the standard state change • LPG connections shall allow for PSAPs to directly connect systems (cable IP) to the ESInet

AT&T Response:

Comply.

Trouble handling / trouble ticket tracking (AT&T ESInet™): AT&T provides 24x7x365 fault and trouble management for AT&T ESInet™ through AT&T's Network Operations Center (NOC) and dedicated 9-1-1 support organizations (including the AT&T 9-1-1 Resolution Center and NG911/ESInet Service Management). Incidents may be opened by Customer-authorized personnel via phone/email/portal as provided at service turn-up, or may be generated proactively through continuous monitoring and alarm correlation of ESInet, NGCS, and associated interconnection/access components under AT&T's operational control.

AT&T's trouble ticketing process provides end-to-end tracking from intake through restoration and closure, including (as applicable): incident categorization (e.g., service outage, degradation, security/event, provisioning/routing/GIS impacts), assignment to the appropriate technical support tier, time-stamped activity history, communications log, and disposition. Tickets are prioritized by severity/impact and urgency (e.g., Sev1 critical outage; Sev2 major impairment; Sev3 limited impact; Sev4 informational/request), with response and restoration targets governed by the contract Service Level Agreement (SLA). Customer-visible status updates are provided per severity and at key milestones (acknowledgement, triage, mitigation/restoration, and closure).

Escalation guideline document / procedure: AT&T will develop, maintain, and review with the State an Escalation Guideline that documents roles, contacts, and escalation thresholds for NG911 service-affecting incidents and time-sensitive issues. The guideline will define: (1) how Customer initiates an escalation; (2) severity definitions and required notification cadence; (3) escalation triggers (e.g., unresolved within defined intervals, material service impact, repeated recurrence, cross-provider dependency with an OSP/third-party access provider, or elevated risk); and (4) the stepwise escalation path within AT&T.

- **Level 1 – Operations Intake / NOC:** Ticket opened/acknowledged; initial triage; alarm correlation; immediate mitigation actions; coordination of maintenance bridges as needed.
- **Level 2 – 9-1-1 Resolution Center / Tier 2 Engineering:** Advanced diagnostics, call-flow/log review, routing/GIS/NGCS functional element analysis, and coordinated troubleshooting with PSAP/OSP stakeholders where appropriate.
- **Level 3 – Tier 3 / Vendor & Platform Engineering (as applicable):** Engagement of specialized engineering and supplier support (including NGCS application support) for defect isolation, patches/workarounds, or complex interoperability issues.



- **Service Management Escalation:** The assigned Service Manager provides customer communications, ensures SLA adherence, drives cross-team coordination, and elevates to AT&T management for priority handling when thresholds are exceeded.
- **Executive Escalation (as needed):** For prolonged/critical events, AT&T will engage senior operations and program leadership to prioritize resources and provide executive-level status to the State.

Following restoration, AT&T will validate service stability, confirm resolution with Customer (when applicable), and close the ticket with documented actions taken. For major incidents, AT&T will provide a post-incident summary and, where appropriate, a root cause analysis (RCA) and corrective action plan (CAP) consistent with SLA and operational governance. When troubles involve third-party networks or Originating Service Providers outside of AT&T's direct span of control, AT&T will coordinate troubleshooting and escalation with the responsible party, keep the State informed, and document the dependency and risk in the ticket record and operational reporting.

- LPG queries ALI databases and maps NG911 location data to legacy formats.
- Converts TTY to RTT for text-to-911 in legacy PSAPs.
- Supports call transfers to/from legacy PSAPs, mapping i3 transfers to legacy systems.
- Logs call events, protocol conversions, and errors; supports discrepancy reporting.
- Implements TLS and authentication for secure connectivity.
- Monitors LPG performance; supports maintenance with minimal disruption.
- LPG deployed with geo-redundancy to ensure high availability.
- Reports errors in call delivery, location, or protocol conversion.

AT&T Response:

Comply.

The Legacy PSAP Gateway (LPG) is deployed to support existing PSAPs that are operating with legacy 9-1-1 services to connect to and use ESInet services. In the AT&T solution, the Legacy PSAP Gateway (LPG) is only used at the interconnection point between the ESInet and a PSAP that is not yet capable of i3 call handling.

- The LPG is deployed to support existing PSAPs that are operating with legacy 9-1-1 services to connect to and use the ESInet services.
- The LPG provides a SIP interface towards the ESInet and a selective router-based ALI interface towards the PSAP.
- The LPG does not require the PSAP to upgrade to i3 NG 9-1-1 and does not require the PSAP to be GIS compatible with i3 NG 9-1-1 service.



- LPG deployment may be considered a temporary measure until selective routing is discontinued and the PSAP modifies its infrastructure to accommodate NG 9-1-1.

1.4. Network Behavior and Performance

1.4.1. ESInet IP Routing

The ESInet must follow the NENA standards to ensure that IP routing across the ESInet can handle all traffic effectively under varying conditions. **Ongoing bandwidth assessments, risk assessments, diversity, and redundancy testing must be documented and updated in a configuration management database as the ESInet evolves.** Proactive measures to trace IP routing within the diverse and redundant paths is required. Any change to the system must include testing of IP routing failover mechanisms prior to acceptance of a change.

No specific link shall be provisioned with **more than 50% of the physical limit** of that link to allow for expansion without physical changes to the link, router, or switch to which it connects. As changes in the network are completed, the IP address plan shall be updated and remain accessible to the State or designee.

- Every element proposed supports both IPv4 and IPv6 (dual stack).
- All elements in the network have globally routable IP IPv4 and IPv6 addresses.
- The network shall use one Interior Gateway Protocol (IGP) throughout, and no routers use Routing Information Protocol (RIP).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance with NENA standards for handling traffic under varying conditions.
- Documentation of ongoing bandwidth assessments, risk assessments, diversity and redundancy testing in a configuration management database.
- Proactive measures to trace IP routing in diverse and redundant paths.
- Testing of IP routing failover mechanisms prior to any system change acceptance.

AT&T Response:

Comply.

AT&T ESInet uses an MPLS/GRE/IPSEC overlay between the PSAPs and core sites, abstracting the underlying transport and enabling the ESInet to control routing convergence. This enables many things, including multi-tenancy and sub-second network reconvergence.



AT&T utilizes at least two physical circuits per PSAP (or CHE host) in the deployment of AT&T ESInet. These two circuits have logical connections to at least 3 of the AT&T data centers. This provides additional redundancy to allow any of the 3 data centers to reach the PSAP. AT&T monitors all circuits for both up/down state and degradation. The network automatically reroutes away from down or impaired circuits. Alarms are generated in our monitoring system and at our NOC, where the team investigates and takes whatever corrective action is required.

AT&T does not use static routes within the managed network environment. The only exception is if a particular PSAP insists on static routes, and this can only be supported in extremely limited scenarios. We use BGP and ISIS for all internal routing functions, and BGP is our only supported routing protocol when peering to PSAP networks. AT&T maintains IP configurations in an internal database and network diagrams can be provided for each PSAP deployment to show routing configurations.

AT&T uses QoS on each path. We ask CPE vendors to mark their traffic appropriately, but have found that many cannot or do not, so we also attempt to identify and mark traffic appropriately at our edge. Once marked, as each packet moves through the network, it is queued according to its role. Circuits have queues sized based on their expected traffic distribution, with voice traffic always receiving a large amount of extra capacity. All ESInet traffic is marked either at the generation point or at ingress into the network.

The proposed ESInet is a Quality of Service (QoS)-managed IP network which can prioritize any type of IP traffic; voice, data, and multimedia, based on Differentiated Services Code Point (DSCP) markings. The solution uses QoS and VLANs between data centers and PSAPs to prioritize and protect the data/traffic. The network equipment supports Quality of Service (QoS) marking for prioritizing traffic in the network using the 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 used within the solution are configured in such a way as to not change DSCP values set by originating functional elements. Additionally, QoS within the ESInet meets the NENA standards.

1.4.2. ESInet Bandwidth

The ESInet is expected to deliver sufficient end-to-end bandwidth to accommodate traffic to and from PSAPs effectively.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Adequate sizing must consider 911 voice and video calls, text communications, data transmissions, and a calculated surge factor based upon the State of Nebraska PSAPs.
- An **annual growth factor of 10%** must be incorporated into capacity planning.



- Bandwidth sharing with other networks within the State of Nebraska is encouraged, **especially for secondary routes, provided the contractor implements provisions to ensure that using these networks does not impact the primary ESInet performance.**
- The ESInet should be structured for future expansion, allowing scalable growth throughout the duration of the contract without impeding current services. A detailed plan should outline how the ESInet will readily accommodate increases in bandwidth, as necessary.
- A detailed plan for scalable expansion throughout the contract without impeding services.

AT&T Response:

Comply.

AT&T ESInet is designed to handle more than twice the nationwide call volume for 9-1-1 (NENA estimated at 240M calls annually). 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 configurations distribute transactions across a set of processors in an active/active configuration and any Core can handle and process any given call. Bandwidth is expandable in a short timeframe with no need for a forklift upgrade.

As per the requirements stated in this RFP, AT&T incorporates a 10% annual growth factor in all capacity planning, and complies with the bandwidth requirement of 2Mbps per PSAP + 2Mbps per position to be delivered to each PSAP. IP network transport used by the AT&T ESInet will initially be sized to comply with specified network bandwidth requirements to each PSAP. The AT&T ESInet IP network is monitored for capacity trends that indicate the need for proactive growth of the ESInet. As the needs of the State of Nebraska ESInet 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 if any contracted PSAP exceeds projected growth.

Bandwidth expansion to a PSAP will follow the pre-established AVPN Move-Add-Change (MACD) internal process. Each of the AVPN links to a PSAP will be provisioned with physical access media that is capable of supporting an increase of the MPLS/AVPN logical port speed. The MACD process for this scenario has a target completion of 30 days from change order placement to completion. In the unlikely event that a PSAP projects bandwidth growth needs larger than the physical access media can support, new access, port service and CIR changes will be required. The target time frame for completion of this process can vary depending on the availability of physical access media feeding the PSAP location. Participation from the State is requested to follow the change order process. The assigned Program Manager should be contacted to request bandwidth changes after initial deployment.

The concept of “bandwidth sharing” to PSAPs within the AT&T ESInet to support desired third-party applications can be supported. AT&T allows for third party and non-traditional connections to the ESInet. These connections are examined on a case-by-case basis to determine the traffic type, best connection type, and appropriate security protocols to be put in place. Any future services that require connection from the



ESInet to the Internet are pre-vetted and secured. Only specific content types are allowed from those connections and the connections from those sites are restricted to specific destinations within the ESInet.

The Program Manager will work with the State through a change order management structure to begin the discussions for the introduction of any third-party applications to be supported across the ESInet. When agreements are reached on the introduction of third-party applications across the ESInet, the change order management process will document the steps required to implement the desired changes. A Project Manager will be assigned and will follow the afore stated project management model to document the process through implementation and into production. The ESInet monitoring and reporting tools will be leveraged as this IP traffic traverses the ESInet.

1.4.3. Quality of Service (QoS)

The ESInet must provide Quality of Service (QoS) features at all ingress, core, and egress points.

The ESInet must employ DiffServ throughout, adhering to packet marking specifications per NENA-STA-010.3. A commitment to maintaining packet loss below 0.5%, jitter under 15 milliseconds, and (one-way) latency below 25 milliseconds is required during standard operational periods.

- Performance metrics for these characteristics should be established on a standby measurement basis, with the State stakeholders allowed to initiate specific measurements as required.
- Regular reporting must provide comprehensive insights into network performance metrics, including averages and worst-case scenarios.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Employment of DiffServ throughout with packet marking per NENA-STA-010.3.
- Commitment to packet loss below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during operations.
- Standby measurement basis for performance metrics with State-initiated measurements.
- Regular reporting on network performance including averages and worst-case scenarios.

AT&T Response:

Comply.

AT&T understands and complies with QoS requirements.

Packet loss, latency, and jitter are measured at each core site. We engineer our ESInet to keep the packet loss budget under 2.5 percent. Our ESInets are also designed without oversubscription. Packet loss of less than 1



percent is expected. AT&T ESInet currently uses a 40 ms jitter buffer for all voice calls. This means that all voice packets have been treated such that minimal end point jitter buffering would be needed (typically much less than 20 ms). Network latency is a monthly network-wide average round-trip transmission of fifty (50) milliseconds or less between the core processing sites and the PSAP end points under full load conditions.

The Service will monitor the IP 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 Daily PSAP PMOS value will be based on an average of the per call PMOS scores over a 24-hour calendar day.

1.4.4. Traffic Flow Requirements

Respondents must describe how traffic will flow from end to end across the network in a fashion that is compliant with applicable standards. ESInet and NG Core Services functions be described to allow the evaluator to clearly identify where specific operations on the traffic occur. If necessary, diagrams may be used to assist the visualization of traffic flow through the proposed solution.

The ESInet and NGCS must operate in concert with one another to establish the flow of traffic from the caller to the call-taker. This flow of traffic utilizes physical and logical connections to the resources required for call delivery. Traffic flow shall include a description of traffic flow under **NORMAL** operating conditions and traffic flow under **ABNORMAL** operating conditions.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- End-to-end traffic flow description compliant with standards.
- Identification of operations on traffic in ESInet and NGCS.
- Diagrams for visualization if necessary; traffic flow under normal and abnormal conditions.
- Handling of use cases such as legacy OSP to NG PSAP, NG OSP to NG PSAP, Internet to NG PSAP, text/ALI/GIS traffic, virtual PSAPs, BCF to ECRF, ECRF to SI/ESRP/PSAP/LPG, LSRG to OSP, OSP to LNG, logging/recording, and monitoring/management. Additional or modified use cases specific to the solution should be expanded upon.

AT&T Response:

Comply.

AT&T's i3-compliant network and Next Generation Core Services seamlessly work in sync from end-to-end across our ESInet solution to deliver emergency communications from a caller in distress to the appropriate PSAP. AT&T has provided use cases with numbered steps to demonstrate how traffic flows from one element of the system to another.

The following diagrams provide details on traffic flow for several call flows.

Wireless OSP not using FG

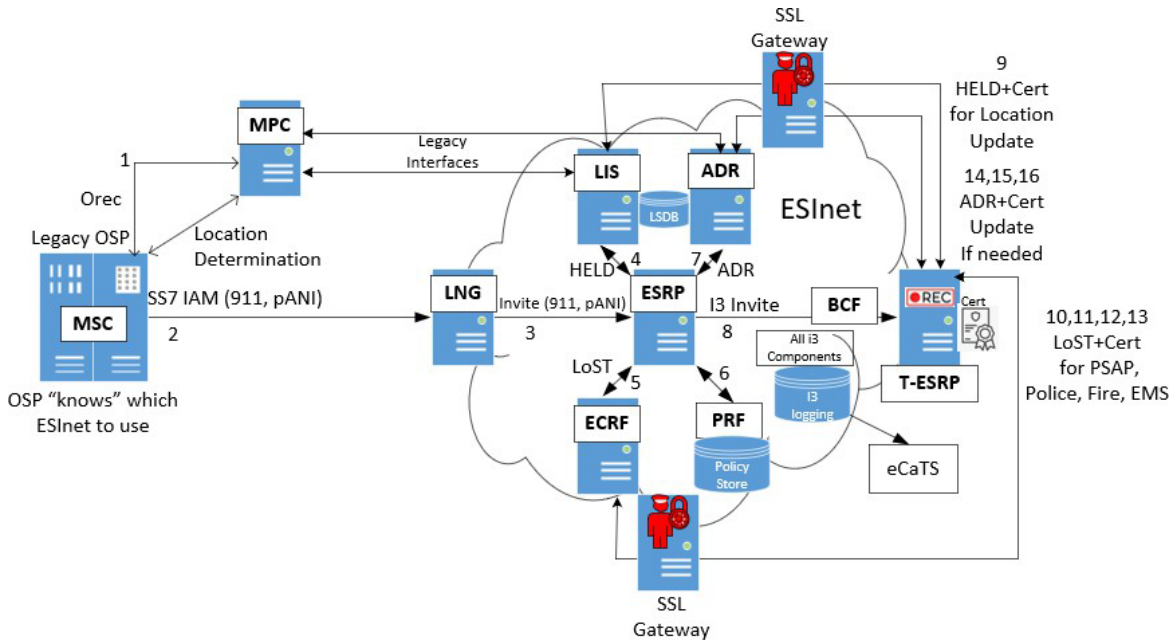


Figure 14: Wireless OSP not using FG

1. Query to MPC for routing instructions (ESRK retrieval)
2. SS7 invite message to LNG
3. Authenticated message, converted to IP sent to ESRP
4. Query to ATT LIS to retrieve location (LIS provides the LIF)
5. LoST query to ECRF to identify PSAP
6. Query to PRF to identify policy routing rules from PSAP returned in ECRF query
7. Query to ADR to provide additional data such as ProviderInfo, ServiceInfo, SubscriberInfo
8. Invite sent to PSAP via BCF.
9. HELD request with digital cert to get updated location
10. LoST Request with digital cert to get PSAP from ECRF
11. LoST Request with digital cert to get Police from ECR
12. LoST Request with digital cert to get Fire from ECR
13. LoST Request with digital cert to get EMS from ECR
14. ADR query with digital cert to get ProviderInfo



7. Query to ADR to provide additional data such as ProviderInfo, ServiceInfo, SubscriberInfo
8. Invite sent to PSAP via BCF.
9. HELD request with digital cert to get updated location
10. LoST Request with digital cert to get PSAP from ECRF
11. LoST Request with digital cert to get Police from ECR
12. LoST Request with digital cert to get Fire from ECR
13. LoST Request with digital cert to get EMS from ECR
14. ADR query with digital cert to get ProviderInfo
15. ADR query with digital cert to get ServiceInfo
16. ADR query with digital cert to get SubscriberInfo

* Assumes legacy OSP knows how to reach ESInet

NG OSP

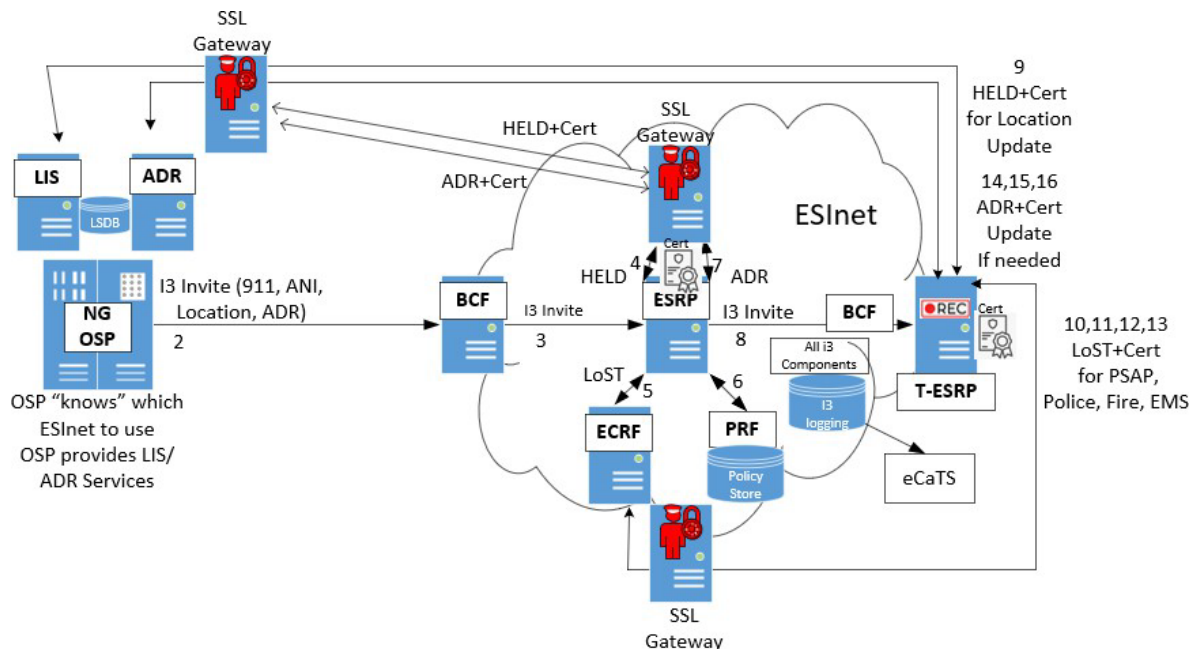


Figure 17: NG OSP

1. Internal query to identify correct ESInet.
2. i3 invite with LIS and ADR reference
3. Authenticated message, converted to IP sent to ESRP



4. HELD query using LIS reference and digital cert to OSPs LIS.
5. LoST query to ECRF to identify PSAP
6. Query to PRF to identify policy routing rules from PSAP returned in ECRF query
7. Query to OSPs ADR with digital cert to provide additional data such as ProviderInfo, ServiceInfo, SubscriberInfo
8. Invite sent to PSAP via BCF.
9. HELD request with digital cert to get updated location
10. LoST Request with digital cert to get PSAP from ECRF
11. LoST Request with digital cert to get Police from ECR
12. LoST Request with digital cert to get Fire from ECR
13. LoST Request with digital cert to get EMS from ECR
14. ADR query with digital cert to get ProviderInfo
15. ADR query with digital cert to get ServiceInfo
16. ADR query with digital cert to get SubscriberInfo

Assumes i3 OSP knows how to reach ESInet

**SSL Gateways are used for authentication

***This call flow assumes the OSP has already successfully done an LVF query

NG OSP using AT&T LIS/ADR

1. Internal query to identify correct ESInet.

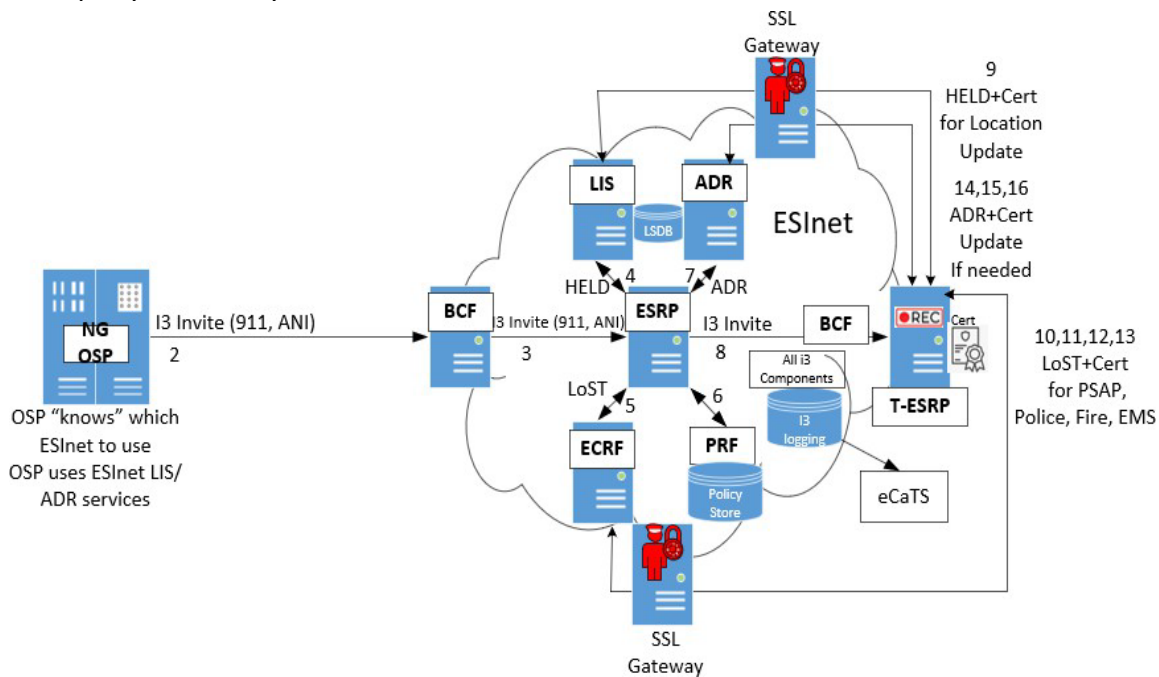


Figure 18: NG OSP using AT&T LIS/ADR

2. i3 invite with LIS and ADR reference
3. Authenticated message, converted to IP sent to ESRP
4. HELD query using LIS reference to AT&T LIS.
5. LoST query to ECRF to identify PSAP
6. Query to PRF to identify policy routing rules from PSAP returned in ECRF query
7. Query to OSPs ADR with digital cert to provide additional data such as ProviderInfo, ServiceInfo, SubscriberInfo
8. Invite sent to PSAP via BCF.
9. HELD request with digital cert to get updated location
10. LoST Request with digital cert to get PSAP from ECRF
11. LoST Request with digital cert to get Police from ECR
12. LoST Request with digital cert to get Fire from ECR
13. LoST Request with digital cert to get EMS from ECR
14. ADR query with digital cert to get ProviderInfo
15. ADR query with digital cert to get ServiceInfo

16. ADR query with digital cert to get SubscriberInfo

*Not Shown is the pre-provisioning to the AT&T LIS/LDB done by the OSP

** Assumes legacy OSP knows how to reach ESInet

***SSL Gateways are used for authentication

****This call flow assumes the OSP has already successfully done an LVF query

NG OSP using FG

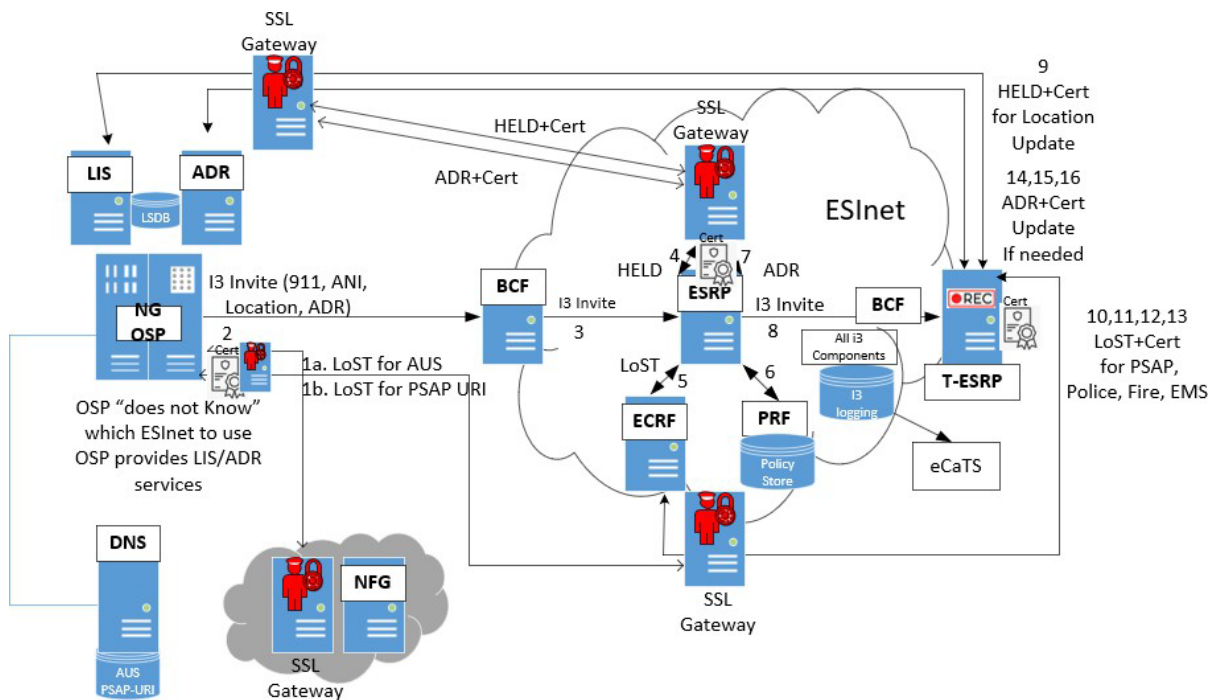


Figure 19: NG OSP using FG

1. Query to FG and DNS lookup to identify ESInet
2. i3 invite with LIS and ADR reference
3. Authenticated message, converted to IP sent to ESRP
4. HELD query using LIS reference and digital cert to OSPs LIS.
5. LoST query to ECRF to identify PSAP
6. Query to PRF to identify policy routing rules from PSAP returned in ECRF query
7. Query to OSPs ADR with digital cert to provide additional data such as ProviderInfo, ServiceInfo, SubscriberInfo



8. Invite sent to PSAP via BCF.
9. HELD request with digital cert to get updated location
10. LoST Request with digital cert to get PSAP from ECRF
11. LoST Request with digital cert to get Police from ECR
12. LoST Request with digital cert to get Fire from ECR
13. LoST Request with digital cert to get EMS from ECR
14. ADR query with digital cert to get ProviderInfo
15. ADR query with digital cert to get ServiceInfo
16. ADR query with digital cert to get SubscriberInfo

*SSL Gateways are used for authentication

***This call flow assumes the OSP has already successfully done an LVF query

ESInet to ESInet Transfer/Handoff

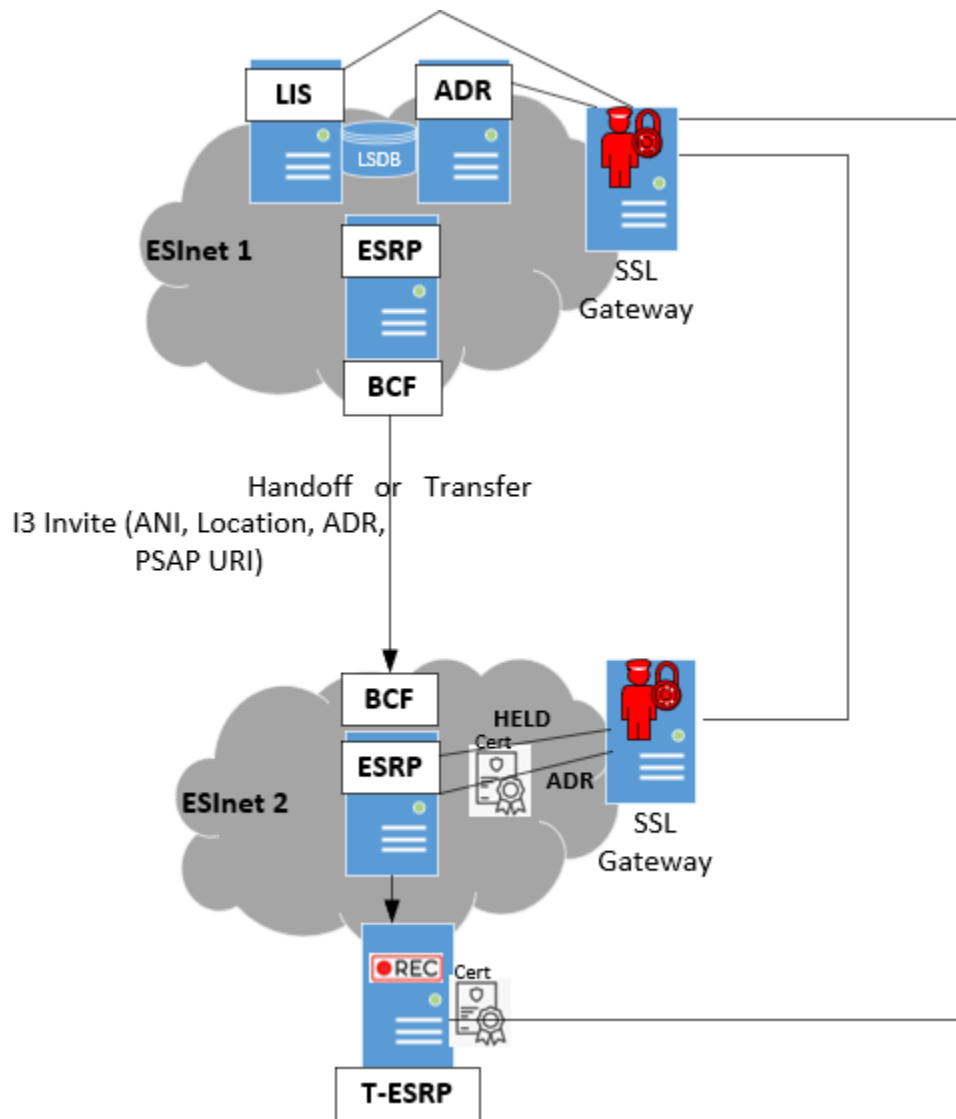


Figure 20: ESInet to ESInet Transfer/Handoff

1. i3 invite with ANI, Location, and ADR references, PSAP URI for destination PSAP
2. Queries with digital certs from ESInet 2 to ESInet 1 for Location information and ADR information (ProviderInfo, ServiceInfo, SubscriberInfo)

*Both invite and LIS/ADR queries use the same IP connection between ESInets.



Text Traffic Flow

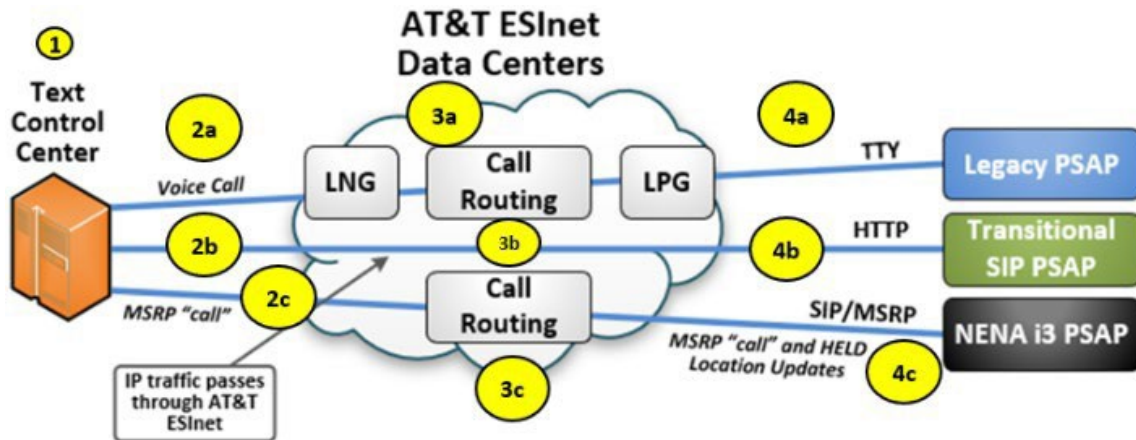


Figure 21: Text Traffic Flow

1. After a caller initiates Text to 9-1-1, the TCC determines the capability of the PSAP. This is based on the configuration that's been done prior to the call and is based on the PSAP's Request for Service indicating to the carriers if they support integrated Text to 9-1-1 or require it to be sent TTY.
- 2a. TCC converts the SMS text messages to TTY. A TTY voice call is presented to the ESInet with tones that can be converted by the PSAP's CHE to text.
- 3a. The LNG receives a Voice Call with tones and converts this to IP. The same call routing policies used for a voice call are applied.
- 4a. The LPG converts the call back to TDM with tones present.
- 2b. In this scenario, the ESInet is a passthrough. The BCF receives the "text call" and it is passed through the system.
- 3b. No call routing policies are applied as the ESInet facilitates the transport of traffic. 4b. The egress BCF sends the "text call" to the PSAP's CHE.
- 2c. The TCC sends the call to the ESInet's BCF as an MSRP "call".
- 3c. In this scenario, AT&T ESInet can apply call routing policies to the MSRP call, allowing PSAPs to reroute calls via the ESInet instead of at the TCC.
- 4c. MSRP "calls" are delivered to the PSAP's CHE.

**Scenario "a" assumes the PSAP has requested SMS to TTY conversion.



GIS Provisioning Traffic Flow

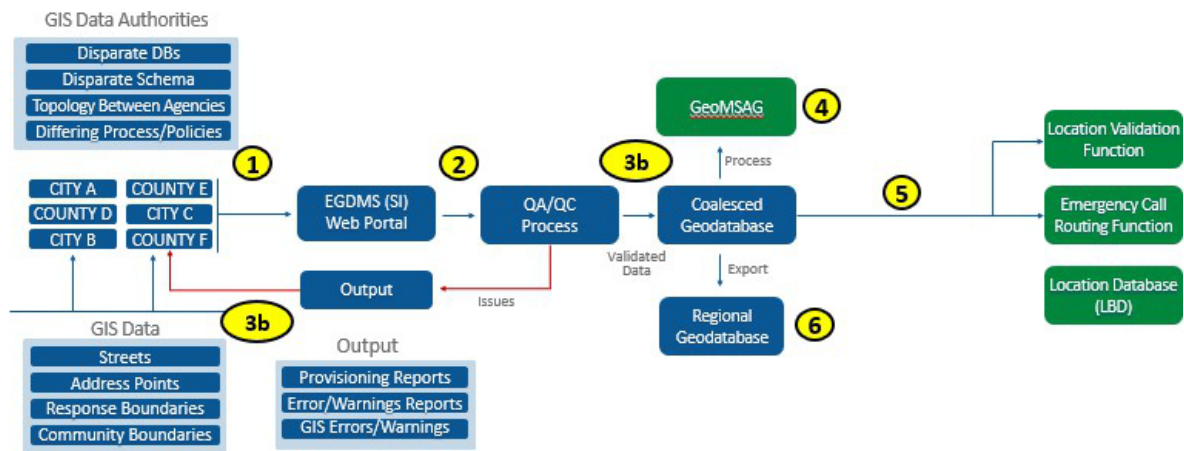


Figure 22: GIS Provisioning Traffic Flow

1. The GIS Authority submits data to AT&T's Spatial Interface (aka EGDMS). This can be done via the web portal or via an sFTP equivalent site to drop files off. Both options are offered to PSAPs.
2. The QA/QC process ensures the data meets all mandatory requirements, has no critical errors, and there are no gaps/overlaps.
- 3a. If data passes the QA/QC process, it is uploaded into EGDMS's coalesced geodatabase.
- 3b. If the submitted GIS does not pass QA/QC, the file is not processed. The GIS Authority receives notification of the failure of the QA/QC process and is provided reports to assist them in identification and correction of the GIS data. The GIS Authority will resubmit data to the Spatial Interface upon correction of the errors.
4. The error free GIS data is used to create a geoMSAG. This GIS-derived MSAG assists with the MSAG Conversion Service and provides a conversion between PIDF-LO and MSAG data as necessary for i3.
5. The error free data is pushed to the LVF, ECRF.
6. Optional and allows the coalesced database to be used for other GIS databases, such as a regional database.

*The LDB (essentially a LIS until OSPs manage their own LIS) uses the State provided GIS data to geocode static records in LDB.

1.4.5. Traffic Shaping



Respondents must include a description of where traffic shaping will be employed, detailing the techniques used and their intended benefits. A formal **traffic shaping policy document** must be created, ensuring transparency and regular updates are made available to State personnel.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Description of where traffic shaping is employed, the techniques used, and their intended benefits.
- Creation of a formal traffic shaping policy document with transparency, regular updates, and availability to State personnel.

AT&T Response:

Comply.

AT&T ESInet supports traffic shaping and traffic policing. Traffic shaping functions on the connection between the core locations and the PSAP edge to ensure flows to a PSAP are appropriately sized. Queueing mechanisms are in place throughout the entire ESInet to ensure critical traffic is delivered. AT&T ESInet follows the network performance requirements as defined in NENA-INF-016.2-2018.

System/application availability is safeguarded with clustering and load balancing techniques. The system can be configured to distribute calls between PSAPs.

AT&T ESInet utilizes multiple techniques to ensure a reliable traffic delivery. These include:

- Limiting the IPs that the PSAP-managed routers communicate to specifically designated sources.
- Shaping the traffic throughput to match the bandwidth of each circuit.
- Sizing the circuit to match the needs of each PSAP location.
- Using QoS to classify, mark, and queue voice, critical 911 application, and other traffic as needed.

AT&T will develop a formal policy post-award with State collaboration. AT&T will also share network diagrams for PSAP deployments and discuss any updates to the traffic shaping with the State.

1.4.6. ESInet Network Time

Network Time Protocol servers must be provided. The NTP servers must provide service to all elements in the ESInet including all PSAPs and other agencies on the ESInet. Time service must permit every system and every agency to maintain time within 1 millisecond of absolute time with 4 nines (99.99%) availability. The network shall have a hardware clock. However, in no circumstances, including failure of the hardware clock, must time as maintained by the time server(s) vary by more than 20 milliseconds from absolute time.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Provision of NTP servers serving all ESInet elements (NGCS FEs, PSAPs, agencies) within 1 millisecond of absolute time with 4 nines (99.99%) availability.
- Preference for hardware clock but ensuring no more than 20 millisecond variances even on failure.
- Descriptions of NTP service provision, confirmation of 1 millisecond accuracy with 4 nines availability, and meeting 20 millisecond variance threshold.

AT&T Response:

Comply.

PSAPs and NGCS processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the NG9-1-1 domain. The clock is self-contained within the ESInet and managed as part of the overall infrastructure. Time stamps are included in logs, system traces, and user reports. Network backbone equipment and internal applications form client relationships directly with NTP servers. Site-specific anycast virtual IP addresses are provisioned on backbone edge routers to facilitate the creation of an “NTP Service”. Customer access to this service is controlled through routing policy. In this model, DoS attacks sourced outside of backbone do not put NTP servers at risk. This model allows stratum-2 NTP service to be offered to external networks, and stratum-3 NTP service to be offered to local PSAP equipment (in cases where AT&T has delivered a managed network service to the PSAP).

Our solution using stratum-2 and stratum-3 for AT&T managed devices will allow every agency to maintain time within 1ms of absolute time.

External sources such as PSAPs are deployed using our time servers. AT&T will work with the PSAPs and the PSC to ensure the 20ms variance threshold is met.

1.5. Resilience and Service Levels

1.5.1. ESInet Availability

The ESInet must maintain the integrity of emergency call processes, ensuring availability of 99.999% at all network points (Ingress, Core, Egress). Key provisions include:

- The entire call path must be resilient and monitored for compliance with the availability standard.
- Support services not related to call handling should achieve an availability of 99.9%.

The Respondent must provide a description and/or documentation that supports the requirements in this section:



- Resilience and monitoring of the entire call path for 99.999% availability at ingress, core, and egress with clear identification of any boundaries that are outside of the span of control of the contractor which may be a risk to achieving five nines (e.g., OSP ingress, PSAP egress). 99.9% availability is acceptable for noncall-handling support services.
- Uptime calculations assessing physical device MTBF for critical equipment in serial/parallel configurations.
- A comprehensive sparing plan for all sites with replacement strategies.
- Established technician response times for outages.
- Calculated MTTR based on spares and response times.
- A consolidated overview of overall availability combining MTBF and MTTR data.

AT&T Response:

Comply.

The 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), see figure below. The Service Availability is calculated from the time an issue is reported that impacts Call Processing ability, until such time that the Service Call Processing ability is restored. The Service Availability downtime will not exceed 26.3 seconds per month. Customers are eligible for remedies and service credits when the Service Availability SLA is not achieved.

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 through 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.

AT&T provides a Service Level Agreement and credits should the service not be available 100 percent of the time. The performance objective for the Site Availability/Time to Restore SLA is for the Service Site Availability to be 100 percent. Time to Restore is measured from when a trouble ticket is opened by AT&T Customer Care and Customer releases the affected Service Component(s) to AT&T (in cases where it is necessary for AT&T to diagnose and/or restore a Service Component into use) until the time AT&T Customer Care makes its first attempt to notify Customer that the issue has been resolved and the Service Components are restored and available for Customer to use.

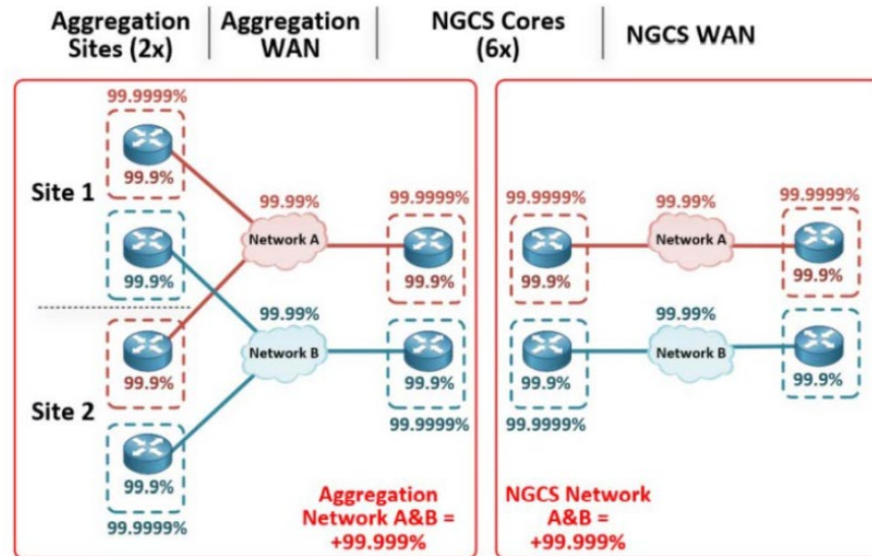


Figure 23: Service Availability

1.5.2. ESInet Reliability

The design of the ESInet must emphasize reliability through strategic diversity across geographic regions, technology, and vendors. Each node within the network must utilize **at least two routers from different manufacturers** to deliver redundancy. If this is unfeasible, a rationale for maintaining reliability under specific failure conditions must be provided. **No segment of the network should hinge on a single point of potential failure, such as a "backhoe incident."**

The reliability design must conform to guidelines specified in the FCC Report and Order 13-158 aimed at enhancing 911 reliability across all communication networks.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Strategic diversity across geographic regions, technology, and vendors.
- Use of at least two routers from different manufacturers per node for redundancy (or rationale if unfeasible).
- Elimination of single points of failure (e.g., "backhoe incident").
- Conformance to FCC Report and Order FCC 13-158 for enhancing 911 reliability.

AT&T Response:

Comply.

AT&T ESInet supports diversity at every connection node from ingress through the core and egress to the PSAPs. All AT&T TDM and IP POIs within the state of Nebraska have a minimum of at least two connections to



each AGC. Each IP connected OSP has a minimum MPLS links into AT&T's core. In addition, each AT&T AGC has redundant links to each of the 6 core processing centers (ECMC) using AT&T Switched Ethernet in a mesh fabric. Each of the ECMC's has multiple ASE connections to the other ECMC's. Finally, there are a minimum of two AVPN links to each PSAP. In addition, AT&T has a tertiary AVPN connected FirstNet connection to all PSAPs included as part of our RFP response/design.

AT&T's ESInet design utilizes carrier-grade, enterprise-class Cisco routers as the standardized routing platform at the network edge to ensure consistent configuration, proven reliability, and secure, highly available operation for mission-critical NG911 traffic; while dual edge routers from different manufacturers are not deployed at individual nodes, AT&T achieves vendor diversity and resiliency across the broader network architecture, where emergency traffic traverses aggregation, core, and interconnection layers that employ network infrastructure from multiple manufacturers, combined with geographic diversity, carrier-diverse facilities, redundant paths, and automated failover mechanisms, ensuring no single device, facility, or vendor dependency can impair the delivery of emergency services while maintaining operational simplicity and supportability at the ESInet edge.

Recognizing that cost is a significant inhibitor to such diversity, AT&T will indicate those PSAP address where obtaining such diversity may be limited and in those cases AT&T can offer additional network resiliency using our AT&T ESInet integration with FirstNet Wireless backhaul. With the FirstNet Wireless backup solution AT&T ESInet can provide automatic failover to FirstNet in the event of failure in the wireline connectivity e.g., fiber cut in last mile. AT&T ESInet will automatically deliver NG911 calls to the PSAP that take full advantage of FirstPriority where every SIP packet is prioritized and cannot be preempted.

AT&T ESInet's proven network implementation provides diversity within multiple layers e.g., physical, network, etc.) with different manufacturers and multiple network connections that enable automatic rerouting and failover. AT&T ESInet network diversity design and implementation ensure that in no circumstances can any node or nodes in the network (Ingress, Core, Egress) be severed from the network by a single "backhoe incident."

Furthermore, AT&T ESInet network reliability design and implementation are guided by several public safety and industry best practices (e.g., NENA, FCC CSRIC, TFOPA, DHS, etc.) and is consistent with the FCC Report and Order FCC 13-158 – Improving 911 Reliability and Reliability and Continuity of Communications Networks, Including Broadband Technologies.

1.6. Operations and Management

1.6.1. ESInet Monitoring and Management

A dedicated 24/7/365 Network Operations Center (NOC) must oversee continual ESInet monitoring to ensure immediate detection of any functional disruption within the system. §E-9.3.1 contains minimum NOC requirements that must be met as part of this proposal.



- **All network links require constant congestion monitoring**, with timely mitigation strategies implemented by contractors.
- **Failure alerts should be generated within a minute for any link or component malfunction** of the ESInet.

Thresholds for triggering mitigation must be explicitly delineated, especially in response to network congestion, with proactive communication to the State regarding the mitigation plan, implementation timelines, and ongoing progress reports.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A dedicated 24/7/365 NOC for continual monitoring and immediate detection of disruptions.
- Constant congestion monitoring of links with timely mitigation.
- Failure alerts within 1 minute for malfunctions.
- Explicit thresholds for mitigation (e.g., congestion).
- Proactive communication to the State on mitigation plans, timelines, and progress.

AT&T Response:

Comply.

The Network Operations Center (NOC) operates 24x7x365 and provides proactive, real-time monitoring of all components of the AT&T solution, including both primary and secondary PSAPs. This will include all Nebraska locations that are on the AT&T network.

Remote monitoring of performance is conducted to provide statistical data on the number of alarms received and reported based on severity. The NOC uses the monitoring tools to capture the elements of a complex end-to-end service environment, such as network elements, computer systems, databases, and the applications themselves. NOC staff can monitor the complex dependencies among these managed elements and alert the appropriate group for interpretation. This provides a method to immediately notify designated personnel of any system failures.

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. Delivery of monitoring reports, including bandwidth utilization and connectivity, are provided as mutually agreed upon during contract negotiations. Traditional network management tools are complemented by active application monitoring and alerting.

We monitor and audit 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 system. This capability assists in troubleshooting and anomaly resolution, as well as providing assurance of reliable performance. Information Security personnel have devised profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

AT&T's Resolution Center has access to logging that monitors backbone network capacity, aggregation site capacity, PSAP network capacity, and per server resource utilization. Alarms and notifications are set at predetermined levels to identify potential problems. AT&T uses multiple tools to track performance and fault management activities. The NOC monitors and tracks net flow statistics and performs packet level capture and forensics at the AT&T ESInet core sites. All tools are used to collect KPIs for their respective systems/servers which in turn are forwarded to a single pane of glass to the NOC. The NOC utilizes tools from new Relic and Spectrum which monitors systems and applications using agents. Visual alerts are available 24x7x365 to the NOC. This system also provides ICMP and SNMP trending and threshold alarming.

The AT&T Resolution Center will communicate with 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 customers and participating suppliers to use for reporting and obtaining/providing status on ESInet issues. Our partner 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. Also, 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.

AT&T's network is designed to quickly detect link outages and link degradation. Routers perform IPSLA testing over all WAN links to continually check end-to-end reachability quality. Jitter, round trip delay, and packet loss are all factored in to determine an estimated MOS score over each link. Should a MOS score fall beneath threshold on any given link, routing is de-prioritized over that link. Routing will re-converge in the event of a WAN link failure within 3 seconds, and link degradation (degraded voice quality) is detected within 10 seconds. This testing methodology is leveraged on both the ingress and egress portions of the network.

Following are key highlights for the network management system (NMS):

- The five state levels from NMS are Critical, Major, Minor, Warning, and Normal.
- We provide notification to the 24x7x365 NOC.
- We provide notification by email and SMS.
- The supporting entity defines notification levels.



- We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications.
- Alarms we typically process are SNMP traps, local agents, and polling.
- A monitored system sends us a trap upon observation of a pre-defined event in a monitored service.
- Agents run local to the monitored service and do logfile analysis, process analysis, and performance analysis.
- Polling occurs to monitor for availability of service.

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.

1.6.2. ESInet Maintenance Window

The proposed ESInet **must have no scheduled down time**. If maintenance is required, which would temporarily cause the network to have lower than 99.999% availability while the maintenance activity is underway, the contractor must provide a **pre-maintenance risk register** prior to commencing the maintenance and complete the maintenance under the terms of §E-9.5.1 (Change Management Requirements) and §E-9.5.2 (Scheduled Maintenance Process) below. **No maintenance activity which, if improperly completed, which could cause an outage of any part of the network, shall be permitted outside the terms of §E-9.5.1 and §E-9.5.2.**

All maintenance activity must be preceded by a Maintenance Operation Plan (MOP) required **at least 14 days** prior to the maintenance. The MOP shall include the provisional operating configuration to ensure that performance continually meets the 99.999% service level as the maintenance is being performed.

Scheduled downtime is unacceptable under routine operations. If maintenance is essential, it must follow as stringent Scheduled Maintenance Process to maintain or exceed 99.999% availability. Any maintenance that could jeopardize network functionality **must be strictly controlled**.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- No scheduled downtime; completion of any maintenance impacting availability under specified terms (§E-9.5.1 and §E-9.5.2).
- Prohibition of maintenance causing outages outside those terms.



- Requirement for a Maintenance Operation Plan (MOP) at least 14 days prior, including provisional configurations to maintain 99.999% service level.
- Descriptions of handling no-downtime requirements, planning/conducting maintenance without impacting availability, and the MOP process for guiding activities.

AT&T Response:

Comply.

Maintenance of the AT&T ESInet™ is done with no scheduled downtime. AT&T schedules planned events for routine and preventative maintenance in ways that would not temporarily cause the network to have lower than 99.999% availability while the maintenance activity is underway.

A notification of the upcoming event will be sent to the State as applicable. MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event. The AT&T ESInet™ architecture has been designed to be extremely resilient and redundant, allowing call traffic to meet the 99.999% service level even in case of a failure at one or more pieces of hardware, software, or network infrastructure. This design also allows maintenance and repairs to take place without impacting PSAPs or call delivery.

AT&T fully staffs and manages planned events with a trained event management team, facilitating the change implementation, monitoring, and communication through the duration of the event.

How the requirement of no downtime is handled

AT&T ESInet achieves 99.999 percent 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 geo-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. The AT&T ESInet components are designed and configured for continuous operation including maintenance events.

How any ESInet maintenance activity will be planned and conducted in a manner that will not impact the 99.999% requirement

AT&T fully manages and completes these events with a trained event management team, facilitating the change implementation, monitoring, and communication through the duration of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. AT&T includes the required back-out time within the scheduled maintenance time frame. MOPs (Methods of Procedures) are written, peer reviewed and Risk



Assessed prior to scheduling any event. The processes that AT&T has in place regarding maintenance activities and a system design based on no single point of failure allows AT&T to maintain the 99.999% requirement.

Discuss the MOP process and explain how the MOP will be used to guide the maintenance activity

MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event. 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. The change requests submitted to the 911 Governance Review Board include a Risk Assessed MOP that includes a step-by-step guide of the changes being made, a clear definition of scope, any clearly stated impacts, detailed validation and back-out plans and all event resources including an escalation list must be included.

1.7. Implementation Details

1.7.1. Port Mapping

Comprehensive documentation of port block/mapping/forwarding policies must be maintained, providing access to both the State and PSAPs. This documentation should include provisions that allow stakeholders to request traffic on specific ports to be allowed from external sources into predetermined network points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive documentation of port block/mapping/forwarding policies accessible to the State and PSAPs.
- Provisions allowing stakeholders to request traffic on specific ports from external sources to predetermined network points.

AT&T Response:

Comply.

AT&T comprehensively documents port mapping policies for internal use with our Chief Security Office (CSO). AT&T ESInet does not require port forwarding. Port blocking is only done by firewalls that serve as a BCF between zones of trust. Our firewalls are configured as a "deny by default," and only authorized ports are opened up to allow traffic. Port mapping is also not part of our standard practice, though AT&T does utilize NATing within the SBCs to allow PSAPs that use common private IP space by their CHE. This NATing (similar to port mapping) is documented during the deployment.

Remainder of page intentionally blank



2. Next Generation Core Services (NGCS) Requirements

The proposal must include a **Next Generation Core Services (NGCS)** implementation deployed across **multiple redundant data centers**. The system shall use **at least three (3) data centers**, with a preference for **at least one in-state** and at least **one geographically distant** (more than 100 miles away – preferably several states away) to avoid common-cause failures such as severe weather or localized incidents. The state will permit a shared facility but prefers a **separate NGCS instance** (distinct virtual machines and management) from other tenants. Each NGCS component – physical and virtual – must be **redundantly deployed in every data center** with **no single point of failure**.

The NGCS must also be **isolated and resilient** against external threats and against faults arising elsewhere in the provider's NG911 ecosystem. Respondents must **describe and demonstrate** how their design prevents impact from incidents in another ESInet or statewide NGCS service offered by the provider, ensuring Nebraska's NG911 operations continue **without degradation**.

All NGCS elements which use policies must retrieve policies from a NENA-STA-010.3-compliant policy server and must be **provisioned with the host name of the policy server it uses**. See §E-2.2.1.1 for the NGCS Policy Store requirements.

- The State desires redundant functional elements, including **all databases to be deployed active-active such that all redundant elements are actually serving traffic at all times**.
- The Respondent must state which functional elements and databases are not actually serving traffic at all times and for each such element; the mechanism for failover that will reliably guarantee the **99.999% availability requirement of the entire system**.
 - **For active-active elements**, the Respondent must describe how the client determines an element has failed, and how it recovers (typically via retry), noting what the worst-case timing for the detection and retry is, and how the appropriate Service Level Objective within that Service Level Agreement is maintained.
 - **For each database, and each call-state data object**, the Respondent must describe how state is reliably maintained, and failover within the 99.999% availability is assured, including any retry operations required at the client.
 - **For databases that are updated at call time**, the Respondent must describe the replication strategy, specify a maximum data sync time, and describe how it is achieved. Note that the State requires the ability to update a service boundary polygon in the ECRF dynamically, and replication/data sync of that operation must be described in the proposal.
 - The State expects that the LPG, LNG, and MCS be the only element that supports legacy functions.

The contractor shall **supply or ensure interoperability with all NGCS functional elements as defined by NENA**, including but not limited to the Location Validation Function (LVF), Location Information Server (LIS), Emergency Call Routing Function (ECRF), Emergency Services Routing Proxy (ESRP), Policy Routing Function



(PRF), and Legacy Network Gateway (LNG). All elements must expose the NGCS interfaces specified in the standard, with the contractor documenting implementation details for each (e.g., integrated software modules, hosted cloud services, or third-party integrations). The system must support bridging to legacy systems via appropriate gateways.

All NGCS interfaces shall adhere to defined specifications, including SIP messaging extensions, RESTful APIs (using JSON/XML payloads), and NENA-defined ESI-net ↔ Core interfaces. Payloads and schemas must comply with NENA requirements, such as Presence Information Data Format – Location Object (PIDF-LO) for location data, with support for HTTP-Enabled Location Delivery (HELD) protocols.

NGCS components (e.g., ECRF queries, LVF validations) **must achieve performance targets**, including lookup latency SLAs of 200 millisecond median and 500 milliseconds at the 95th percentile under peak load (jurisdiction may adjust based on scale). The system must handle at least 10 queries per second per component with no degradation.

The NGCS must scale horizontally to support jurisdiction-specific peak call rates (e.g., 1,000 calls per hour per PSAP) and data volumes, with tenant isolation for multiple PSAPs via virtual instances or containers. It shall enable dynamic provisioning of PSAP service boundaries through administrative interfaces.

All NGCS transactions shall be logged comprehensively, including timestamps, full request/response payloads (redacted for privacy where necessary), originator identities, correlation IDs, and error codes, enabling end-to-end tracing across components. Logs must be stored in a searchable database with retention support.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NGCS deployment in multiple redundant data centers (preference for at least 3, with one in-state and one >100 miles away).
- Preference for separate instances (different VMs) if sharing data centers.
- Redundant deployment of all components without single points of failure; resistance to external threats and internal disruptions from other ESI-nets/NGCS.
- Description/demonstration of unimpeded operation during disruptions.
- Policy retrieval from NENA-STA-010.3-compliant policy server with host name provisioning.
- Preference for active-active redundant elements/databases serving traffic at all times.
- Statements on non-active elements with failover mechanisms guaranteeing 99.999% availability.
- Descriptions of failure detection/recovery for active-active elements (worst-case timing, SLO maintenance).
- State maintenance/failover for databases/call-state data.



- Replication strategy for call-time updated databases with max sync time.
- Dynamic ECRF service boundary updates with replication/sync description.

AT&T Response:

Comply.

The AT&T solution design includes six data centers through which the NGCS will be deployed. All components are redundantly deployed with no single point of failure. Core sites work in an active-active mode; calls are distributed across all six AT&T core sites. The architecture is more than capable of processing all the 9-1-1 calls for the State; therefore, there is no need for NGCS capacity supplementation as Nebraska's PSAPs on board to AT&T ESInet service.

AT&T, upon award, will deploy two geographically diverse SIP Point of Interconnection (POIs) to comply with the FCC NG911 OSP mandate and accommodate OSP SIP ingress traffic. Additionally, AT&T can build and operate one in-state NGCS instance for additional resiliency and redundancy to meet the State's preferred approach.

Active-Active

The AT&T solution is designed as a highly available service through an active-active processing methodology, geographically diverse and distributed components, highly available component architecture, and redundant IP transport. The AT&T solution has no single point of failure. Call traffic diverts to available components upon failure or degradation of a given functional component or a loss of a physical site. IP transport paths are redundant and designed for multipath IP packet delivery, so the failure of a given IP transport mechanism will not affect overall service availability. All redundancy mechanisms for call processing and network elements that support delivery of emergency 9-1-1 calls employ automatic fail-over procedures and do not require human intervention.

For each database within the Emergency Call Management Complex (ECMC) also referred to as the NGCS Core Sites, the architecture consists of a Primary source provisioning Common Support System (CSS) database that replicates data changes to target databases in real-time. ECMC databases consist of two node Oracle RAC clusters that provide redundant failover capabilities. Application failover between the Primary CSS and Alternate CSS databases is accomplished using Transparent Application Failover (TAF), thus achieving 99.999 percent availability. TAF is an Oracle mechanism that provides for application failover via the Oracle Transparent Network Substrate (TNS).

The Emergency Call Router (ECR) is built on Oracle Communications Converged Application Server (OCCAS) architecture that provides Session Initiation Protocol (SIP) call management and control. The Emergency Call Router provides both the IP Selective Router functions and NENA i3 functions of the ESRP and PRF. The OCCAS architecture consists of a 3-node OCCAS cluster at each of our six core sites. The OCCAS cluster uses a call-state management engine to keep each of the 3-node OCCAS SIP servers in sync in real-time; during the



progress of any single E9-1-1 request for assistance call, all 3 OCCAS Servers participate in the progress and management of the call, from setup through teardown. The ECR architecture also consists of a real-time, in-memory data management facility that serves real-time CSS provisioning data state changes, for example, PSAP facility status changes such as available, busy, abandoned states, etc.

Call-State Data Object

For each database, the architecture consists of a Primary source provisioning Common Support System (CSS) database that replicates data changes to target databases in real time. One of the targets is an alternate provisioning database (ALT-CSS) and the remaining six targets are Emergency Call Management Complex (ECMC) databases, also known as the core site databases. The ECMC databases consist of two node Oracle RAC clusters that provide redundant failover capabilities. Application failover between the Primary CSS and Alternate CSS databases is accomplished using Transparent Application Failover (TAF), thus achieving 99.999 percent availability. TAF is an Oracle mechanism that provides for application failover via the Oracle Transparent Network Substrate (TNS).

For each call-state data object, our Emergency Call Router (ECR) is built on Oracle Communications Converged Application Server (OCCAS) architecture that provides Session Initiation Protocol (SIP) call management and control. The Emergency Call Router provides both the IP Selective Router functions and NENA i3 functions of the ESRP and PRF. The OCCAS architecture consists of a 3-node OCCAS cluster at each of our six core sites. The OCCAS cluster uses a call-state management engine to keep each of the 3-node OCCAS SIP servers in sync in real-time; during the progress of any single E9-1-1 request for assistance call, all 3 OCCAS Servers participate in the progress and management of the call, from setup through teardown. The ECR architecture also consists of a real-time, in-memory data management facility that serves real-time CSS provisioning data state changes, e.g., PSAP facility status changes such as available, busy, abandoned states, etc.

Retry operations from clients, specifically ingress TDM Gateways or native IP Softswitch handoffs, rely on SIP protocol retransmit timers. Several SIP timers are invoked through the life of any given SIP call offered, from initial INVITE messages, 100 trying, 180 Ringing, 183 Session Progress messages, and 200 OK messages. Any of these timers may range from three to five second retransmission depending on the criticality of the call state at any point in the call setup. For example, shorter retransmission timers are applied in advance of a ringing event or media cut-through event, giving the caller quicker response and feedback that their call is being handled, while interim progress and routing type events may permit longer retransmit intervals.

Replication

Volatile call state data is kept in an organized in-memory data store. That data store, as it changes, is replicated to all other ESRPs via an internally developed data replication software suite. The replication time is milliseconds. Also, as routing data (any kind of routing data) is provisioned, it is also replicated from the CSS database to all the ESRPs. This is via a 3rd party software component called SharePlex. The replication time is milliseconds. Data in the ECRFs is provisioned by the SI (EGDMS). A file transfer from the SI to ECRF is used to push the data. The ECRF is notified that a new data set is pending. That data set is processed into the standby



GIS data store. If the processing succeeds, then the ECRF then transfers the data set to 3 other ECRFs (ECRFs operate in a quad). Those other three ECRFs are notified that a new data set is available. These three ECRFs process the new data into the standby GIS data store. The 3 ECRFs notify the 1st ECRF when complete. Once all 4 ECRFs have successfully processed the new GIS data, the standby GIS data store is made the active. The old active is now the standby. If the new data needs to be rolled back, the standby (the previous active) is then made active. The amount of time is dependent on data size, Typically, a county-sized data set will take less than one minute. A state-sized data set could take five to ten minutes.

AT&T has proven success in integrating our NGCS solution architecture with statewide regional deployments like the State of NE 7 region hosted call handling solutions. AT&T will design and implement our redundant, diverse network connectivity from the NGCS cores to each of the host PSAP locations, transparently to the remote telecommunicator positions.

2.1. Edge Security and Ingress

2.1.1. Border Control Function (BCF)

The BCF must conform to NENA-STA-010.3 standards, preferably constructed from a commercial Session Border Controller (SBC), Firewall, and NG911-specific capabilities.

- **Call Processing:** The BCF must handle all inbound calls from OSPs and should be configured between the ESInet and any interconnected ESInets to facilitate external connections.
- **Call Egress:** While optional, a BCF to manage outgoing communications between the ESInet and a PSAP may be necessary.
- **Security Features:** The BCF must incorporate the Bad Actor and Call Suspicion mechanisms as specified in NENA-STA-010.3. Calls directed to the ESInet should be accepted unless the source is blocklisted as a Bad Actor.
- **Media Handling:** The BCF must not anchor media unless it is necessary to do so. If the BCF does anchor media, it must implement ICE, STUN, and TURN mechanisms to navigate Network Address Translation (NAT) as applicable.
- **Logging and Monitoring:** The BCF must facilitate media logging per NENA-STA-010.3 specifications, with the ability to disable logging while retaining swift reactivation capabilities for diagnostic purposes.

The BCF must:

- Addresses on BCFs receiving traffic shall be globally routable IP addresses
- Process all calls from OSPs on the ingress side
- Support Bad Actor and Call Suspicion mechanisms
- Mitigate DDoS/TDoS attacks up to terabit capacity levels



- Accept calls directed to the ESInet regardless of source (unless marked as Bad Actor)
- Implement B2BUA if calls do not support REFER
- Avoid media anchoring where possible and implement ICE, STUN, and TURN when necessary
- Support ElementState and ServiceState SUBSCRIBE/NOTIFY

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 preferably from commercial SBC, Firewall, and NG911 capabilities.
- Handling inbound calls from OSPs and between ESInets; optional egress BCF for outgoing to PSAP.
- Bad Actor/Call Suspicion mechanisms; acceptance of calls unless blocklisted.
- No media anchoring unless necessary with ICE/STUN/TURN for NAT.
- Media logging per standard with disable/reactivate capabilities.
- DDoS/TDoS mitigation up to terabit levels.
- B2BUA for non-REFER calls.
- ElementState/ServiceState support.
- Descriptions of BCF locations, Bad Actor/Call Suspicion implementation, DDoS/TDoS capacity, B2BUA details, tromboning avoidance, ICE/STUN/TURN, media recording, and ElementState/ServiceState support.

AT&T Response:

Comply.

The AT&T solution provides a Border Control Function (BCF) to interface with any non-trusted network components. The BCF provides Session Border Control and border firewall functionality in accordance with the NENA STA-010.3 specification. The BCF inspects, modifies, and controls SIP signaling and associated media where ESInets 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 PSAPs.

AT&T ESInet has redundant BCFs at both the ingress and egress of each of the six core sites. Our BCFs offer improvements upon traditional TDoS implementations that only recognize and quarantine unwanted traffic from the call queues. Nebraska PSAPs will have the ability to uniquely configure how to triage TDoS calls based on parameters and weights on parameters using our increasing capabilities to recognize different types of events in real-time and dynamically route incident information to the PSAPs. AT&T's rule engine will allow for



many types of potentially bad or blacklisted data to be evaluated, scored, processed, and routed to the appropriate priority queues to provide the State's PSAPs with improved resource utilization.

AT&T has different mechanisms for both ingress (from OSP) and egress (to PSAPs) for TDoS/DDoS attacks.

Ingress Solution:

OSP to AT&T ingress facilities are engineered not to exceed 60% utilization under normal operating conditions. This is done with the expectation that the excess 40% capacity is available to provide on-demand network capacity in the event of spikes and bursts in demand due to either emergency events or malicious TDoS/DDoS attack. For example, a traffic study determines the busy hours for Customer's A and B requires bandwidth of 3Mbps, respectively, so AT&T plans and deploys a 10Mbps facility and configures the Call Admission Control (CAC) so the total utilization (simultaneous sessions) is limited to 5Mbps for each customer; combined, their respective busy hour demand does not exceed 60% of the facility capacity, and they can each burst traffic if demand spikes. Customer Source IPs are whitelisted in the Border Control Function (BCF), preventing untrusted, non-listed, Source IP's from attacking the network. The combination of whitelisted/trusted Source IP' and CAC ensures that an attack from any IP Source will not consume all the network resources that would result in the denial of service of all IP Sources. In the case of an attack, AT&T network administrators are prepared to adjust the CAC, in real-time, to expand a customer's bandwidth in an effort to avoid the denial of service. Once the attack has concluded, the previous CAC values are restored. Regardless of the breadth of the attack, whether it's limited to a single Customer/IP Source, or the more unlikely scenario that all IP Sources are under attack and all TDoS/DDoS contingency measures are rendered defeated and the network becomes fully consumed, AT&T will work with the serving OSP's and/or VSP's to quickly identify the bad actor attack vectors in order to block the attack before it can reach the AT&T ESInet.

Egress Solution:

There are two ways TDoS/DDoS attacks are mitigated with respect to PSAP call delivery.

- A PSAP, via the AT&T Management Portal or the Resolution Center, can manually enter a Telephone Number (TN) into a TDoS/DDoS TN list.
- TDoS/DDoS attacks are automatically detected by our software, Software Event Evaluation Program (SWEEP). This software is coded to look at various attack patterns, recognize the pattern, and automatically put the TN into the TDoS/DDoS TN list.
 - *TNs will automatically age out of the TDoS/DDoS TN list; the default is 15 minutes.

When a call with a listed TN arrives, the call is given a SIP 580-banished error code, which translates to an SS7 cause code of 20. This tells the originator of the call that the number they dialed is not in service. Our experience has been that once the originator of the call gets the "not-in-service message," the calls cease.

We continue to refine this functionality and have additional TDoS/DDoS features coming soon where we will interrogate the caller and have them interact with the interrogator service to get their call delivered. Also



coming are aids to the subsequent fraud investigation. The SWEEP software will perform a dispatch (not a routing) query for location, and an ADR query to get additional data, such as the carrier or the TN owner, that will aid in finding and identifying attackers.

The AT&T solution implements B2BUAs at the ESRP application control function and the Session Border Controller (SBC). If SIP or RTP needs to cross boundaries, the traffic will be handled by the AT&T SBCs to ensure no limitations or packet loss. The application control function performs routing of ingress traffic to PSAP destinations, accomplishes call conference/transfer functions and numerous maintenance functions. The SBC performs ESInet security functions and uses a B2BUA as an element of that security function.

The AT&T BCF supports media anchoring to provide superior call control, in addition to preventing deliberate or malicious attacks on public safety answering points. The back-to-back user agent (B2BUA) removes the need to use Network Address Translations (NAT). All devices within the network are assigned static addresses. The BCF supports transfers and N-way bridging. The BCF will then join the PSAP leg of the RTP to the BCF and conference the PSAP leg with the Caller's ingress leg. The BCF is sending RTP to the Media Server for the ingress leg of the call. At this point, the Caller and the PSAP have a two-way audio pathway. During a call transfer or bridging scenario, the BCF will create a new media leg to the additional conference party (PSAP, Poison Control, etc.). As additional participants are added, new media legs are created between the BCF and the party. When a party drops, the leg is torn down and removed from the n-way bridging.

AT&T does not currently employ ICE/TURN/STUN. AT&T ESInet uses public IPs for OSP ingress and therefore NAT traversal is not needed. AT&T does accommodate entities using private IP space in today's system. An example of this is the deployment of certain CPE vendors. In order to eliminate the need for each PSAP to acquire public IP space, AT&T ESInet employs a NAT within the B2BUA. AT&T ESInet uses a set of Header Manipulation Rules (HMR) in the SBC to NAT SIP headers in the messages. The rules are applied when the SBC receives a message, and the IP addresses in the headers are changed to correspond to the egress SBC interface and network.

When messages are returned to the ingress (caller side), the SBC will NAT the headers back to the original IP addresses that were used in the originating message. AT&T recognizes the importance of ICE/TURN/STUN to allow for NAT transversal in a more dynamic means. This will come into place when a use case such as IOT devices connecting via the public internet become a reality. AT&T will employ ICE/STUN/TURN when necessary.

AT&T ESInet's BCF supports ElementState and ServiceState.

2.1.2. STIR/SHAKEN Support

The State requires that incoming calls be validated, and the attestation results be supplied to PSAPs as specified in NENA-STA-010.3. Additionally, calls placed through the OCIF must be signed and receive A-level attestation when validated by the terminating service provider.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Validation of incoming calls with attestation to PSAPs per NENA-STA-010.3.
- Signing OCIF calls for A-level attestation.
- Explanation of STIR/SHAKEN implementation/conformance.

AT&T Response:

Comply.

AT&T ESInet supports STIR/SHAKEN today, ensuring the attestation results provided by the Originating Service Providers are delivered to the PSAPs as specified within the NENA standards. Calls originating from the PSAPs that conference or transfer calls using the upcoming Outbound Call Interface Function (OCIF) will provide the A-level attestation that can be validated and passed on to the terminating caller.

2.1.3. Security Mechanisms

Until the PCA exists, the Contractor shall provide a Certificate Authority with a certificate traceable to a Certificate Authority trusted in mainstream browsers. All NGCS components must conform to NENA-STA-010.3 and NENA-STA-040.2 security requirements:

- All transactions across the ESInet (including local area network connections at NGCS sites) shall be encrypted as required in NENA-STA-010.3.
- Every entity must have credentials traceable to the PSAP Certificate Authority (PCA) as trusted root
- All TCP transactions must use TLS with mutual authentication
- Minimum cipher suite as specified in NENA-STA-010.3, with TLS 1.3 support required
- Server Name Indication support required in all systems
- All SIP "hops" within the ESInet must use TLS with mutual authentication
- Data access must conform to owner's Data Rights Management policy
- Single Sign On (SSO) mechanism with SAML authorization required
- No sharing of credentials permitted
- Public-facing connections require additional protection against security attacks
- JWS signatures required for policies and log events
- SIP transactions from OSPs at the BCF shall have appropriately strong minimum cipher suite.



- The Contractor shall notify the State if an OSP cannot support a cipher suite minimally acceptable to the Contractor.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 security with PCA-traceable credentials as trusted root.
- Mutual TLS for TCP transactions with minimum cipher suite and TLS 1.3 support.
- Server Name Indication support; TLS with mutual authentication for SIP hops in ESInet.
- Data access per owner's DRM policy.
- SSO with SAML authorization; no credential sharing.
- Additional protection for public-facing connections.
- JWS signatures for policies/log events.
- Descriptions of PCA implementation/traceability, TLS mutual authentication, cipher suite compliance, TLS 1.3 support, Server Name Indication, and SIP hop security.

AT&T Response:

Comply.

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). AT&T has been working with NIOC to participate as one of its first subscribers to the NIOC Forest Guide as well as supporting the use of PCA. AT&T has been discussing with Eonti and Digicert for how to begin the process as a Tier-2 Hosted or Discrete Intermediate Certification Authority (ICA). At this time, Eonti has stated that the process to begin certification as an ICA is pending process finalization but is expected to be completed soon to accommodate our request. Once that moves forward, AT&T will begin providing PCA certificates through the process with Digicert and Eonti as required by NENA i3 standards and the State of Nebraska. While it is expected that using PCA certificates will begin soon and be operational for Nebraska PSAPs at the time of delivery, AT&T will continue to 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.

The following are devices and/or protocols used to restrict access.

- 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.
- AT&T verifies credentialed devices or that carriers are authorized access in the following manner:
- PCA or if unavailable, Client certificates, issued by a trusted Certificate Authority (CA), are required in order to access i3 services such as LIS, ADR, and ECRF.
- The trusted CA role is currently provided by AT&T, the role will be filled by them or an authorized NENA PCA vendor once their processes are completed and certification for Hosted ICA can begin for approval.
- The IP address of any far end SIP endpoint must be provisioned in the SBC.
- The endpoint is also required to send all traffic to a uniquely assigned IP: port combination on the SBC.
- All SIP signaling is done over direct connections or VPNs.
- IP connections to the ESInet are only allowed by vetted OSPs and/or data sources.
- Connectivity to the ESInet is only by signed and approved agreement with data encapsulated by IPSEC MPLS VPN.

PCA is traceable for every element and event based on our providing of PCA certificates for all appropriate End-Entities which are stored within the AT&T ESInet SSL Gateway tied to each NGCS functional element. The SSL Gateway will track and store these certificates for use to access untrusted elements during call processing.

Every TCP transaction on the ESInet uses TLS for non-trusted entities via the SSL Gateway certificate use capabilities.

AT&T ESInet meets the minimum acceptable cipher suite as stated in 8.5 Privacy of RSA-1024, SHA-256, and AES-256. These will be kept updated within 18 months of NENA standards being updated and ratified.

Regarding Server Name Indication, the AT&T ESInet does not have multiple domain names that require the same IP Address, so SNI has not been required.

Every SIP "hop" that occurs outside of the BCF that is considered "untrusted" will use TLS with mutual authentication and identity of the PCA certificate traceable to the trusted root as outlined in 8.1.1 and 8.3. Every SIP "hop" within the AT&T ESInet BCF that is considered "trust-worthy" does not require TLS and PCA certificates.

2.2. Core Routing and Location

2.2.1. Emergency Services Routing Proxy (ESRP)



The ESRP must conform to NENA-STA-010.3 standards and function as both originating and terminating ESRP. It shall be possible for a region or group of PSAPs to provide a terminating ESRP to which the State's ESRP must route calls to as appropriate.

The proposed solution must utilize the PRF functionality to support the ability to dynamically change the primary, alternate, and contingent routes available by the ESRP. The ESRP shall retrieve rule sets from a Policy Store using the NENA-STA-010.3 proscribed Policy Store web service. The ESRP must be capable of being provisioned to use any Policy Store conforming to NENA-STA-010.3. The ESRP shall implement the test call condition modifications described in NENA-STA-010.3 to enable automated testing of policy routing rules. **All calls must be location-routed with no ALI/MSAG-based routing. Requirements include:**

- The ESRP shall be able to query any Location Information Servers using either HELD or SIP Presence.
- The ESRP shall support the QueueState and DequeueRegistration mechanisms for all queues it operates.

It must support QueueState clients for queues for all PSAPs in the State.

- Policy Routing Rule function (PRF) supporting all NENA-STA-010.3 conditions and actions
- Policy retrieval from a Policy Store with dynamic updates (within 10 seconds)
- Handling at least 100 calls per second
- Support for admin calls
- Ability to query any compliant ECRF and Location Information Servers
- Support for call routing and EIDOs for any responder agency
- Implementation of overload and diversion mechanisms
- Additional Data mechanisms for routing based on call data
- ElementState and ServiceState support

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 as originating/terminating ESRP.
- Location-based routing only (no ALI/MSAG).
- PRF supporting all conditions/actions.
- Policy retrieval from Policy Store with <10s updates.
- Handling 100 calls/second.
- Admin call support.



- Querying compliant ECRF/LIS.
- Routing/EIDOs for responder agencies.
- Overload/diversion mechanisms.
- Additional Data routing; and ElementState/ServiceState support.

AT&T Response:

Comply.

AT&T ESInet's Emergency Service Routing Proxy (ESRP) supports i3-compliant routing functionality, including full integration with geographically determined routing, carrier grade voice quality, and demonstrated reliability.

The ESRPs in the AT&T Routing solution are in private domains protected by the Border Control Function. Only authorized traffic is allowed to access the core call processing sites. Core elements are consistently scanned for malware vulnerabilities and operating systems are kept current with updates that protect against known vulnerabilities. Physical and administrative access is limited to authorized and vetted employees of AT&T and Intrado Life & Safety.

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 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. This fallback routing is only used as an alternative method to route the calls and prevents 9-1-1 calls from failing when location data is not presented for proper ECRF routing.

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.

Policy route determination includes evaluation of the PSAP-configured routing policy, the time of day, the caller's location (for geospatially determined alternate routing policies), the PSAP operational state, and the ring-no-answer timer configuration.

The i3 SIP INVITE delivered to the PSAP (terminating ESRP) includes both geodetic/civic location, as available, and additional data conveyed by value and/or reference from the LIS and ADR interface responses.

In addition to call delivery to i3-compliant PSAPs, the ESRP supports call delivery to legacy PSAPs. A sub-set of i3 routing policies can be provisioned for legacy PSAPs along with a 10-digit telephone number for delivery.



AT&T ESInet's ESRP function supports 100 calls per second with no degradation of service.

AT&T ESInet's ESRP is capable of handling admin calls. The ESRP can transfer calls via the PSTN for default routing purposes or transferring of calls. There is no current use case that PSAPs send admin calls over the ESInet. While technically possible, AT&T would need to discuss specific use cases. As admin calls are not deemed Emergency Calls, there are some concerns about mixing the use cases. A popular use case for calls routed to a PSAPs administrative line includes using this line during call handling upgrades that impact the PSAP's ability to use their CHE. In these scenarios, PSAPs enable backup routing to send the calls to their administrative lines. If their administrative calls are delivered via the ESInet and not the PSTN, they would be delivered via ESInet to the PSAPs CHE. This would therefore eliminate the PSAP from receiving calls because their admin lines only route through ESInet to a disabled CHE. AT&T is happy to work with the State of Nebraska to determine use cases and deploy the best solution to satisfy the requirements.

AT&T ESInet's ESRP supports querying of any ECRF that supports NENA-STA-010.3. Geospatially routed calls within the AT&T ESInet are using the AT&T ECRF today for over 1,900 PSAPs in production. AT&T ESInet's ESRP can get location data via HELD or SIP presence. Today, only HELD is used as no OSP is currently supporting SIP presence.

Support for routing EIDO is available. AT&T is actively involved with EIDO testing in lab environments today, which will allow for a more efficient rollout and better compatibility testing with CPE vendors.

AT&T ESInet uses other methods to handle queue congestion. These are implemented today and feature Ring No Answer (RNA) timers with retry settings as well as failover from different core locations and the ability to fail over to alternate PSAPs. This method does not require PSAPs to support QueueState and is used today by all PSAPs deployed on AT&T ESInet. QueueState and Dequeue Registration will be included in the upgrade plan and reviewed with the State of Nebraska on at least a quarterly basis.

The ESRP will invoke the alternating routing policy if the terminating ESRP call handling system does not accept the SIP invite, a ring-no-answer timeout occurs, or if call queues become congested. The user can prioritize an alternate destination via the management portal and create a PSTN back-up route on-the-fly. Additionally, AT&T supports diverting calls to other PSAPs on AT&T ESInet, a foreign ESInet, PSAPs on a legacy selective router, or even via admin lines. AT&T ESInet's ESRP also allows for volume distribution routing, allowing larger PSAPs such as City of Lincoln (Lancaster County) to choose more than one PSAP as destinations when alternately routing calls. This feature provides the ability to "load balance" alternately routed calls to multiple PSAPs so no one PSAP is overwhelmed by a larger PSAP's call volume.

AT&T ESInet's ESRP is currently using data from the AT&T ADR. This is live in production for over 800 PSAPs. AT&T is currently working to enable an IS-ADR with Intrado's Emergency Data Broker (EDB). AT&T will support additional OSP-provided ADRs when available and will work with the State of Nebraska on determining any IS-ADRs that should be implemented.



The AT&T ESInet's ESRPs support ElementState and ServiceState. AT&T will work with the State of Nebraska and the PSAPs to implement the SUBSCRIBE/NOTIFY feature to receive ServiceState and ElementState.

2.2.1.1. Policy Store

The State requires a Policy Store conforming to NENA-STA-010.3. The Policy Store must be capable of being the sole source of policies for the NGCS.

- The State **desires a flexible policy editor** that can create and modify policies conforming to NENA-STA-010.3 with an easy-to-use Graphical User Interface.
- The Policy Store **must have the capacity to support policies for all PSAPs and all elements in the NGCS** at the peak call rates specified in this RFS.
- Storage and retrieval of policies must be limited by the NENA-STA-010.3 Data Rights Management mechanism.
- The Policy Store must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy Store per NENA-STA-010.3 as sole policy source.
- Flexible GUI policy editor.
- Capacity for all PSAPs/elements at peak rates.
- DRM-limited storage/retrieval.
- ElementState/ServiceState support with State subscription.
- Detailed Policy Store description.

AT&T Response:

Comply.

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.

Using the location-determined URI retrieved from the ECRF via the LoST protocol, the ESRP interacts with the Policy Routing Function to determine what if any policies are in place that will impact call routing.



The PRF accounts for the operational status of any downstream ESRP in the evaluation of any policy. This ensures that an ESRP is in an operational state before any message is sent to that ESRP.

AT&T i3 policy routing will provide the State's PSAPs with extensive flexibility to define and update standard and alternate routing policies. PSAPs can modify routing policies, set priorities, and modify their operational state. Routing policies can be defined as recurring or onetime. The rules-based routing proxy includes the following elements:

A repository of PSAP-defined routing policies.

Customer Management Portal (CMP)—A feature-rich web tool that allows PSAPs to view their routing policies and operational status (normal, abandoned, back-up). All routing policy changes are automatically verified for syntactical and logical accuracy prior to activation in production. Secure user access is provided via the AT&T Customer portal.

Access to CMP and the policy repository is managed by a Data Rights Management policy with levels of access that follow the NENA standards.

The following routing policies are supported:

Abandonment/Night Service Routing—The abandonment policy is engaged whenever the terminating ESRP (PSAP) operational state is defined as 'Abandoned'. The PSAP operational state may be modified by contacting the Intrado NOC, triggered via a device installed at the PSAP, or modified online.

Overflow Routing—The overflow routing policy is applied during overflow scenarios when a PSAP is receiving more calls than its occupied 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 Intrado NOC or online.

Special Event Routing—Special event routing is a special type of diversion routing policy that is applied during a scheduled time window. If a PSAP jurisdiction contains venues that host events that may warrant dedicated call handling (mobile command center or dedicated resources at the PSAP), special event polygons can be pre-provisioned.

AT&T will provide a feature-rich management portal for the PSAPs to view their policies. Policies have attributes such as active/inactive, one-time or recurring time window, priority, or a set of destination(s) to send the call to, and call distribution method as examples.



Abandonment, Overflow, and Diversion policies can be configured to use any of the following policies.

Geographically—The system can be configured to send abandonment calls to different alternate PSAPs based on the geographic location of the calling party within the primary PSAP's jurisdiction. Geographic abandonment or alternate routing polygons can be pre-provisioned via the SI or submitted dynamically.

Hierarchically—The system can be configured to cascade a call to up to nine consecutive, alternate PSAPs.

Load-balanced—The system can be configured to distribute calls between PSAPs.

All policies loaded by the customer are held in a test state (non-active) until the customer confirms that all test calls using the policies perform as expected.

AT&T ESInet offers two ways to manage the PRF. AT&T's advanced policy routing can be managed through the Customer Management Portal to provide authorized users with an easy graphical interface to manage their policies. AT&T ESInet also supports a policy store that conforms to the NENA-STA-010.3 standards. This option allows PSAP to manage the policies via the web store but requires the PSAP or their CHE to support NENA-STA-010.3's methods for managing the policies.

The current policy store has the capability of supporting every PSAP in Nebraska even at peak call rates.

The i3 policy store supports the Data Rights Management group.

The Policy Store supports ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3 standards so that the State can subscribe to ServiceState and receive the standard state changes.

2.2.2. Location Information Server (LIS)

The State utilizes a Location Information Server (LIS) provided by the existing service provider. Respondents must provide a description of their LIS solution in conformance with NENA-STA-010.3.

- The LIS must supply location in the form of a PIDF-LO (location by value) or a location URI (location by reference).
- The LIS must also provide a dereference service for a location URI it supplies given the URI, the LIS provides the location value as a PIDF-LO.
- A LIS may be a database, or may be a protocol interworking function to an access network-specific protocol.
- If the LIS supply's location by reference, it must also provide dereferencing service for that location URI.
- Elements in the ESInet, including the ESRP, and the PSAP may dereference a location URI as part of processing a call.



- The LIS must support HELD, HELD Dereferencing and/or SIP Presence Event Package.
- The SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing, especially when tracking of the caller is needed. However, HELD is acceptable on any location URI.
- The LIS must support location filters and event rate control.

The LIS may support SIP Presence to provide location-by-reference as defined by RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package at the location URI provided containing a PIDF (Presence Information Data Format) document that will include the location in the Location Object (LO) part, forming the PIDF-LO.

- The LIS may validate locations prior to entering them into the LIS using the LVF.
- The LIS may support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes¹.
- The LIS must accept credentials traceable to the PCA for authenticating queries for a location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely on any other credential source to authorize location dereferencing.
- Storage and Retrieval of location data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism

When location is provided by reference there is a need for the reference to be valid, at least for the length of the call. Since the call may be transferred to a transfer-to PSAP for handling, the transfer-to PSAP must have the ability to dereference the location reference provided with the call. It is therefore critical that the location URI does not expire before the transfer-to PSAP has the opportunity to dereference it.

Any LIS that provides a dereferencing service for a location must provide an expiration time associated with that URI set at a minimum of 30 minutes, with a maximum of 24 hours.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LIS per NENA-STA-010.3 providing PIDF-LO or location URI with dereference service.
- As database or protocol interworking.
- HELD/dereferencing/SIP Presence support.
- Location filters/event rate control.
- SIP Presence for location-by-reference per RFC.

¹ <https://datatracker.ietf.org/doc/html/draft-ecrit-lost-planned-changes-00>



- Validation via LVF; support for planned changes draft.
- PCA-traceable credentials for dereferencing.
- DRM-controlled storage/retrieval; and minimum 30-min/max 24-hour URI expiration.

AT&T Response:

Comply.

AT&T ESInet supports connections to OSP provided Location Information Servers (as prescribed by NENA-STA-010.3) but does not supply a LIS itself as this is the responsibility of the i3 OSPs. Until such time, AT&T provides a Location Database (described in Section 2.2.3 below) to accommodate all legacy OSPs. The following information describes AT&T's Location Database which meets the requirements above.

AT&T's LDB provides location by value (PIDF-LO) and location by reference (Location URI). Upon successful query to the LDB, AT&T's ESRP will provide by location by value and location by reference in the SIP invite. This allows a PSAP to receive location via PIDF-LO within the SIP invite and query for location updates by dereferencing the Location URI within the SIP invite.

AT&T's LDB includes a dereference service for the location URI. PSAPs query the LDB using digital certificates to ensure a secure transaction for each location update.

AT&T's LDB is both a database and a PIF. Static records can be stored in the LDB's database. For OSPs that provide mobility such as wireless, the LDB is used as the PIF to acquire updated location information from the OSPs MPC/GMLC.

AT&T's LDB includes a dereference service for the location URI. PSAPs query the LIS using digital certificates to ensure a secure transaction for each location update.

AT&T's ESRP and PSAPs are currently using the AT&T LDB to dereference the location. AT&T's ESRP uses this location to perform call routing with the ECRF. PSAPs are actively using this for updated location requests using the Location URI provided in the SIP invite.

The LDB currently supports HELD and HELD dereferencing.

The LIS supports location filters and allows certain data to be provided per call type. The LIS also supports rate limiting.

The LDB validates data using the PSAPs GIS prior to inserting it into the production database. Only records that pass validation will be inserted.



The LDB only allows authorized queries. Today, the PSAPs utilize AT&T provided digital certs to authenticate queries to the LDB. AT&T will replace the AT&T provided certs with the PCA provided certs once all operational procedures between AT&T and NIOC's PCA provider have been completed.

AT&T's storage and retrieval of location data are secured by different means than the Data Rights Management mechanism.

2.2.3. Location Database (LDB)

The State requires a Location Database (LDB) solution as a core component of the Emergency Services IP Network (ESInet). Respondents must provide a detailed description of their LDB solution that is conformant with NENA standards, primarily the NENA Next Generation 911 GIS Data Model (NENA-STA-005.2). The LDB serves as the authoritative geospatial database for the Location Validation Function (LVF) and the Emergency Call Routing Function (ECRF).

- The LDB must store and manage all mandatory and conditional geospatial data layers as specified in NENA-STA-005.2, including but not limited to:
 - Public Safety Answering Point (PSAP) Boundaries
 - Emergency Service Boundaries (Law, Fire, EMS)
 - Road Centerlines
 - Site / Structure Address Points
- The LDB must interface directly with the LVF to enable validation of civic location information against the authoritative GIS data contained within it.
- The LDB must interface with the ECRF to provide the necessary geospatial data for determining the appropriate PSAP and emergency service agencies for a given dispatchable location. This location-to-service mapping MUST utilize a standard protocol, such as the Location-to-Service Translation (LoST) protocol.
- The solution must provide a secure and robust mechanism for the provisioning, aggregation, and ongoing maintenance of GIS data from various authoritative local sources (e.g., county, and municipal GIS departments). This includes tools for data normalization, quality control, and discrepancy resolution.
- The LDB must be architected for high availability and geographic redundancy to ensure uninterrupted location validation and call routing services. The system must meet stringent performance requirements for real-time query processing during emergency call handling.
- The LDB must control access for data provisioning and system queries through secure authentication and authorization mechanisms, protecting data from unauthorized access, modification, or deletion.



- Storage, management, and retrieval of location data MUST be controlled by policies consistent with NENA data security and privacy standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LDB conformance with the NENA-STA-005.2 GIS Data Model.
- Standard-based interfaces with the LVF and ECRF (e.g., LoST).
- Support for all required NENA GIS data layers and their lifecycle management.
- A detailed process for GIS data provisioning, aggregation, updates, and quality control.
- Description of the high-availability and redundant architecture.
- Mechanisms for secure access control for both data management and system queries.
- Tools and processes for managing data quality and resolving discrepancies from multiple sources.

AT&T Response:

Comply.

AT&T ESInet includes the Location Database as defined by NENA ([https://kb.nena.org/wiki/LDB_\(Location_Database\)](https://kb.nena.org/wiki/LDB_(Location_Database))) that retains all of the current information, functionality, and interfaces of today's ALI and can utilize the new protocols required in an NG9-1-1 deployment. The remainder of this response will focus on AT&T's Location Database and the functionality it provides, which may contradict with the requirements above as they are not the responsibility of the Location Database.

The AT&T LDB retains all 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, 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.

The AT&T Location Database 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 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 and the LNG are secured within the ESInet. Interactions with external LIS systems will use digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA), once available. Until that time, Credentialing and the issuance of digital certificates will be managed by AT&T to ensure protection and security. This mechanism will also be used for PSAP access to systems within the AT&T ESInet, including access to the LIS interface, ADR interface, and ECRF.

During carrier transition to NENA i3 compliance, AT&T will maintain the HELD interface into the LDB 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 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.

2.2.4. Emergency Call Routing Function / Location Validation Function (ECRF/LVF)

The implementation requires two independent, redundant ECRFs and LVFs (one inside, one outside the ESInet) with identical data. The ECRF/LVF must support the extensions to LoST defined in NENA-STA-010.3 and the similar location and planned-changes extensions defined in draft-ietf-ecrit-similar-location¹ and draft-ietf-ecrit-lost-planned-changes² (or RFCs issued based on those drafts).

¹ <https://datatracker.ietf.org/doc/draft-ietf-ecrit-similar-location/19/>

² <https://datatracker.ietf.org/doc/draft-ietf-ecrit-lost-planned-changes/>



Query Capability:

The external ECRF/LVF must be queryable from the public internet and by any i3 OSP, supporting both iterative and recursive queries.

Responder Types:

The system must handle up to 20 responder types and various service URNs as specified.

Data Synchronization:

Both the internal ECRF and LVF must achieve 99.999% availability, while the external ECRF must meet the same 99.999% availability SLA, and the external LVF must maintain 99.9% availability.

Performance Metrics:

The internal ECRF/LVF must handle 500 queries per second effectively, ensuring that combined services meet the specified thresholds for external queries. **Key requirements:**

- External ECRF/LVF accessible from the public Internet and i3 OSPs
- Support for iterative and recursive queries
- Support for up to 20 responder and all service URNs
- LoST sync interface to National Forest Guide and interconnected ESInets
- The ECRFs and LVFs must be capable of being provisioned from an SI conforming to NENA-STA 010.3.
- Routing/validation must change within eight (8) seconds of an update via the SI.
- The internal ECRF/LVF shall be capable of handling 100 queries per second for any valid Location Information shape as specified in OGC 06-142r1.
- The external ECRF/LVF shall be capable of handling an aggregate of 5000 queries per second with any mix of civic or geo points.
- The external ECRF/LVF shall be capable of handling an aggregate 500 queries per second.
- The external ECRF/LVF shall limit transactions from the same querier to, at most, 10 per second and fewer, if it is under a sustained excessive load. If the ECRF and LVFs are combined, the combination must meet the 5000/500 rate (not twice the rate of a single service).
- 99.999% availability for internal ECRF/LVF and external ECRF
- 99.9% availability for external LVF
- Support for Spatial Interface (SI) with routing/validation updates within seconds
- Capacity to handle specified query volumes



- ElementState and ServiceState support

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Two independents are redundant ECRFs/LVFs (internal/external) with identical data.
- External queryable from public Internet/i3 OSPs with iterative/recursive support.
- Handling up to 20 responder /service URNs; LoST sync to National Forest Guide/interconnected ESInets.
- 99.999% availability for internal/external ECRF and internal LVF, 99.9% for external LVF.
- SI support with seconds-level updates.
- Capacity for 500 queries/second internal; and ElementState/ServiceState support.

AT&T Response:

Comply.

The AT&T ECRF/LVFs can be queried by any external entity appropriately credentialed to do so.

The ECRF interfaces with the Location to Service Translation (LoST) protocol (RFC5222) and supports LoST queries via the ESRP, PSAP customer premise equipment (CPE), or any other permitted IP host such as an i3 OSP.

Interactions by external parties to the ECRFs or LVFs will use digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA) process once the remaining process details are finalized for availability. Until that time, AT&T will manage credentialing and the issuance of digital certificates to help ensure protection and security.

If the ECRF receives a request for a location outside its coverage area, it will send a recursive or iterative query to a parent/state ECRF or the NIOC Forest Guide, once available. Absent a parent ECRF or the NIOC Forest Guide, the ECRF is capable of supporting 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 AT&T ECRF/LFV functions can support recursive queries for up to 5 ECRF/LVFs from interconnected ESInets.

Support for up to 20 responder types and Service URNs.



The AT&T ECRF/LVF function is capable of supporting up to 20 responder types and all the service urns in the urn:service:sos and urn:nena:service urns.

Current implementation

- Common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire, 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, for example, urn:service:sos. When there is only a civic location element available in the PIDF-LO, the ECRF will follow the LoST protocol to locate a matching address point feature or, if one cannot be determined from the address point layer, the ECRF will attempt to locate a matching Road Centerline feature. If either is located, the ECRF will return the URI associated with the URN also specified in the LoST request.
- The ECRF supports provisioning of separate boundary layers for first responder service types - 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.

The AT&T ECRF/LVF will support the LoST sync interface to the NIOC Forest Guide when available. It will also support the LoST sync interface to / from any connected i3 compliant ESInet.

The AT&T ECRF/LVF will support LoST extensions as defined in NENA-STA-010.3 and similar-location and planned-changes extensions defined in draft-ietf-ecrit-similar-location and draft-ietf-ecrit-lost-planned-changes (or RFCs issued based on those drafts).

The Internal ECRF and upcoming external ECRF complies with 99.999% availability and the external LVF complies with 99.9% availability. All redundancy mechanisms for core applications and network elements that support delivery of emergency 9-1-1 calls across the solution (, ESRP, ESInet components, LIS, ECRF, LVF ADR,) employ “failover” procedures which are automatic and do not require human intervention.

The AT&T ESInet solution implements a design strategy of redundancy upon redundancy. Individual processing elements, including the ECRF, are redundant at each of the six Core Sites, and Core Sites are redundant to each other. Each processing element at a core site incorporates a high availability design. The failure of any component will not prevent that Core Site from processing 9-1-1 calls. If a dual failure occurs at a Core Site, or a Core Site somehow becomes unavailable, calls are processed at another Core Site. Any Core Site can process any 9-1-1 call. A geographic disaster will not remove the ability for the ESInet to process 9-1-1 calls assuming telecommunication transport services for the impacted region are operable. LVFs are provisioned with the common support services (CSS) with two deployed instances that use the same design principles.



The ECRF and LVF are not combined into one element but are implemented independently of each other, 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. The ECRF and LVF internally support 99.999% availability. Both are updated from the SI and kept in sync with updates that post within a few milliseconds. The ECRF and LVF may be combined in the future but currently are separate.

The ECRF and LVF are provisioned using the NENA compliant AT&T ESInet Spatial Interface (SI). 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.

The AT&T ECRF/LVF are capable of being provisioned from an SI conforming to NENA-STA-010.3. Additional interface specifications specific to the State of Nebraska design may be required to confirm seamless interoperability.

Routing/validation can change within a few seconds of an update via the SI as long as all data fully passes a rigorous data compliance review. This check protects the ESInet from ingesting routing information that is not accurate. Characteristics of the update process are listed below.

- Boundary updates from the SI occur in near real-time with no degradation of LoST services. The update must be error free.
- When time is critical, it is recommended that boundary updates are submitted independently of Site Structure/Address Point and Road Centerline updates as the validation process on these can take longer, depending on the number of changes that have been made since the previous data update.
- Each ECRF and LVF 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 and LVF computing elements (two per geographically diverse location), the ECRF and LVF system will notify the Spatial Interface that the load was successful and make the inactive map layer active. If the load was unsuccessful, alarm notifications are sent to relevant operations teams. If this occurs, the previously active map layer will remain active.
- ECRF prescribed functions that are not directly related to call-time activities (e.g., gap/overlap detection) are performed on separate servers to prevent any “administrative” oriented ECRF functions from interfering with the call-time functions.

At this time alternative provisioning methods are not used. AT&T would be happy to discuss alternative methods with the State as needed.

Queries / second



The internal ECRF and LVF are capable of handling 500+ queries per second with any mix of civic or geo points. The internal ECRF and LVF are capable of handling 100 queries per second for any valid Location Information shape as specified in OGC 06-142r1.

Aggregate Queries per second

The external ECRF and LVF, once deployed, will be capable of handling an aggregate of 5000 queries per second with any mix of civic or geo points. The external ECRF and LVF shall be capable of handling an aggregate 500 queries per second. The external ECRF and LVF will limit transactions from the same querier to, at most, ten per second, and fewer if it is under a sustained excessive load. As OSPs request a local ECRF and/or LVF, one will be provided and updated from the same SI that is currently used. The ECRF and LVF will support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3, allowing the State of Nebraska to subscribe to ServiceState and receive the standard state changes.

In addition, the ECRF supports the following:

- 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.

2.2.5. Forest Guide

The NGCS must handle calls transferred between interconnected ESInets, maintaining Forest Guide entries for the State's ECRF and LVF, and support recursive queries for locations outside the state's service area.

If a National Forest Guide is available, the contractor must ensure the State's ECRF and LVF entries are entered promptly.

Fallback Procedures:

In scenarios where queries fall outside the State's service area, the ECRF/LVF must initiate recursive queries to the Forest Guide.

Commercial Relationships:

Frequent and excessive queries from the same entity may not be accommodated unless a reasonable commercial relationship exists.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Handling transfers between ESInets with Forest Guide entries for State's ECRF/LVF.



- Recursive queries for out-of-area locations.
- Prompt entry into National Forest Guide if available.
- Fallback recursive queries to Forest Guide for non-State areas.
- Limitations on excessive queries without commercial relationships.

AT&T Response:

Comply.

AT&T ESInet will support the integration with NIOC's Forest Guide. 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 support coverage areas for other ECRFs. Interactions with external ECRFs will use 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.

AT&T's subcontractor, Intrado, was selected as the vendor to provide NIOC's Forest Guide. AT&T will use this knowledge of NIOC's Forest Guide to integrate it with the AT&T ESInet solution once it is available.

2.2.6. Service/Agency Locator (SAL)

The State requires a Service/Agency Locator function as described in NENA-STA-010.3.

- The S/AL must support at least 1000 entries.
- The S/AL must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.
- The proposal must describe how agency entries are provisioned in the S/AL.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Service/Agency Locator per NENA-STA-010.3 supporting 1000+ entries.
- ElementState/ServiceState support with State subscription.
- Descriptions of agency entry provisioning and detailed S/AL.

AT&T Response:

Comply.



AT&T ESInet supports the S/A Locator functionality and will allow the State of Nebraska to both populate the S/A Locator as well as query it via their PSAP's Call Handling Equipment. The S/A Locator will be able to support at least 1000 entries. The S/A Locator supports ElementState and ServiceState and AT&T will work with the State of Nebraska to ensure they can subscribe to the S/AL. AT&T will provide additional detail on provisioning of agency entries into the S/AL during the implementation of the service.

2.3. Data and Enrichment

2.3.1. Additional Data Repository (ADR)

The State requires an Additional Data Repository (ADR) database function.

URIs pointing to the ADR may be passed in a call, in an EIDO, or by other mechanisms. The ADR shall return an XML data structure in response to an HTTPS GET of the URI. The ADR provided by the contractor must:

- Supply Provider Info and Service Info for all calls handled by the LNG, and any OSP that does not provide its own ADR or AdditionalData by value when it sends a call to the ESInet
- Supply any of the valid AdditionalData blocks for any location, where the URI for the AdditionalData blocks would be returned from the ECRF when searched with an urn of "urn:emergency:service:AdditionalData"

The proposal must detail how ADR records are provisioned into the repository. Storage and retrieval of S/AL records must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.

A call-stateful ADR may limit the length of time that it will serve data after the end of the associated emergency call. Such a time limit shall be at least five minutes. ADRs may not have the data themselves but may know where the data can be found. The response to a dereference request can be redirected to another ADR with an HTTPS 303 response (Iterative Refer).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- ADR returning XML via HTTPS GET.
- Supplying Provider/Service Info for LNG/OSPs without own ADR.
- Valid Additional Data blocks via ECRF URI.
- Provisioning details.
- DRM-controlled storage/retrieval.
- Minimum 5-minute time limit for call-stateful ADR.
- Redirect capability via HTTPS 303.



AT&T Response:

Comply.

The ESInet solution supports integration with ADR, Identity-Searchable Additional Data Repositories (IS-ADR) and as described in NENA STA-010.3. AT&T's solution today provides an LDB to allow legacy OSPs to provision both location and additional data and allow the PSAPs to query this via i3 protocols. In addition to our LDB, AT&T ESInet supports queries to i3 OSPs ADRs. In addition, the AT&T ADR can do iterative query to another ADR to support additional data stored with an OSPs ADR. Today there are over 1,270 PSAPs using i3 protocols that are live on the AT&T ESInet. These PSAPs use a digital certificate for authorization to query the AT&T ADR.

PSAPs use HTTPS GET to query for ProviderInfo, ServiceInfo, and SubscriberInfo. This is done for over 1,200 PSAPs today that are part of the AT&T ESInet. Additional Data blocks will be supplied should ECRF return the URI of the Additional Data blocks.

2.4. Call Flow and Media Handling

2.4.1. Call Flow and Session Handling Requirements

The Contractor shall implement call-flow behaviors consistent with the NENA i3 call model, including processing SIP INVITE requests from access networks into the ESInet, interactions with the ESRP, location queries to LIS, LVF, and ECRF, and routing to the appropriate PSAP through gateways or Call Handling Equipment (CHE). The system must support call queuing, overflow routing, and abandonment handling.

SIP signaling and location:

Headers such as P-Asserted-Identity, Diversion, History-Info, and Geolocation shall be correctly handled, and PIDFLO location information shall be preserved during retargeting, bridging, and transfers.

Media and additional data:

The system shall handle voice, Real-Time Text (RTT), real-time video, and additional data (for example, messaging and sensor or biometric data from caller applications) per NENA definitions, with SDP negotiation, fallback to voiceonly, and transcoding as needed.

Transfers:

Support is required for warm (attended) transfers, blind transfers, and inter-PSAP transfers, preserving all call metadata, location, timestamps, and media sessions without interruption.

Identity and trust:



The system shall enforce SIP identity assertions, correctly process P-Asserted-Identity and related headers, differentiate and display validated versus unvalidated identities at the PSAP, and integrate with STIR/SHAKEN for caller authenticity.

End-to-end conformance:

The ESInet and NGCS shall manage end-to-end call flows in conformance with applicable NENA and IETF standards, including origination, routing, delivery to the appropriate PSAP, transfers, and termination, while ensuring reliable session handling for all supported media.

AT&T Response:

Comply.

The ESInet and NGCS manage end-to-end call flows in full alignment with NENA i3 and relevant IETF standards, beginning with call origination from access networks and proceeding through location acquisition, policy-based routing, and delivery to the appropriate PSAP via CHE or gateways. The system maintains standards-compliant handling of voice, RTT, video, and additional data, and supports transfers and terminations while preserving metadata, location objects, and media continuity. These call-flow behaviors conform to NENA-STA-010.3 and the associated IETF SIP and emergency-services protocols.

2.4.2. Media Quality of Service (QoS)

2.4.2.1. Audio

The proposed solution shall support high-quality, reliable audio for all emergency calls. The solution must be conformant with NENA and IETF standards for audio codecs and media transport to ensure interoperability between originating networks, the ESInet, and PSAPs.

- MOS-equivalent POLQA score of 4 minimum, 4.5 average from OSP edge to PSAP edge
- Continuous sampling of >1% of calls randomly distributed
- Capability to monitor 100% of calls between any two points for up to 5 days upon request

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- High call quality with audio MOS-equivalent POLQA score of 4 minimum/4.5 average from OSP to PSAP edge.
- Continuous sampling >1% of calls; capability to monitor 100% of calls between points for up to 5 days.
- Descriptions of end-to-end media path measurement, POLQA monitoring/measurement, and logging/reporting procedures.



AT&T Response:

Comply.

The AT&T approach to voice quality uses practical and actionable metrics on every call. The intent is to focus on key parameters that we have control over. Since the AT&T ESInet has no control over the quality of the media entering the network, parameters such as voice volumes, echo sources outside our network, and other end-to-end listener and conversational voice quality affecting parameters are not included in the evaluation criteria. AT&T monitors voice quality parameters such as dropped packets, jitter, and other packet statistics for every call, and each leg of the call. This approach provides a more comprehensive view of voice quality than could be achieved through the sampling of a subset of calls.

Due to the nature of G.711 uLaw Codec, there is less concern with the Listening Quality and Conversational Quality MOS parameters of the E-model. There is not a significant difference between any of the derived MOS scores. So, PSQM, PESQ, POLQA, or proprietary MOS scores are generally similar and any one of these methods would be able to flag voice quality problems.

AT&T supports a 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 3.5 threshold 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:

- 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

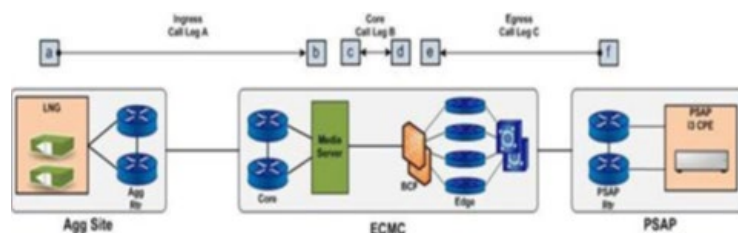


Figure 24: MOS Score Measurement

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).



2.4.2.2. Video

For video services, the proposed service must utilize MOS-equivalent PEVQ score of 4 minimum, 4.5 average from OSP edge to PSAP edge, and have continuous sampling of >1% of calls randomly distributed. They should also have the capability to monitor 100% of video calls between any two points for up to 5 days upon request.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Video MOS-equivalent PEVQ score of 4 minimum/4.5 average from OSP to PSAP edge.
- Continuous sampling >1% of calls.
- Capability to monitor 100% of video calls between points for up to 5 days; and descriptions of end-to-end video path measurement, PEVQ monitoring/measurement, and logging/reporting procedures.

AT&T Response:

Comply.

The AT&T approach to video quality uses practical and actionable metrics on every call. The intent is to focus on key parameters that we have control over. Since the AT&T ESInet has no control over the quality of the video entering the network, parameters such as voice volumes, echo sources outside our network, and other end-to-end listener and conversational voice quality affecting parameters are not included in the evaluation criteria. AT&T monitors any media quality including video parameters such as dropped packets, jitter, and other packet statistics for every call, and each leg of the call. This approach provides a more comprehensive view of voice quality than could be achieved through the sampling of a subset of calls.

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:

- 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



Figure 25: MOS Score Measurement

Media 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).

2.4.2.3. Text

The State requires that text to 911 and text from 911 be supported for both legacy and NG PSAPs and OSPs.

- For NG911, text to 911 shall be provided via Message Session Relay Protocol (MSRP) using standard NENA-STA-010.3 interfaces.
- For text from 911, Contractor shall maintain an interface to a commercial text gateway.
- For Legacy PSAPs, MSRP or web interfaces to the outgoing text service are required.

Text from NG PSAPs shall be able to send MSRP to an element in the NGCS which will send SMS text using the text gateway.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 100% correct text delivery 99.99% of the time.
- Foreign language translation for all texts; and descriptions of end-to-end text path measurement, translation delivery/display, monitoring for 99.99% availability, and logging/reporting procedures.

AT&T Response:

Comply.

The combination of the Intrado Text Control Center (TCC) with AT&T ESInet complies with the need for uptime +99.99% of the time. This is measured through internal reporting systems. If an issue occurs in text delivery, these reports are used to investigate root cause.

Language translation is handled different ways depending on whether the PSAP is using the integrated solution (MSRP delivered directly to the PSAPs CPE) or via the TXT29-1-1 Web Portal. Integrated text relies on



the PSAPs CPE to complete the translation. This allows the PSAP to manually turn on translation or not. A similar mechanism is available for the TXT29-1-1 Web Portal.

To use this feature, the call taker can enable Language Assistance for this chat anytime they realize the incoming message is not English. The most recent two inbound messages received from the wireless user will then be analyzed to auto detect the incoming language. Once the incoming language is determined, recent messages are translated, and the result is displayed in green italics under the original message. From this point on, as long as language assistance is turned on for this chat, all messages sent and received will show a translated string below the original message. Although an automatic detection of language is performed, the call taker may override the detected language and select the source and destination languages.

The mobile device will receive the original and translated message in the following format:

Original message [Translated message].

For example, if "Hello. How are you" is translated from English to Spanish, the end user will receive "Hello. How are you? [Hola. ??Como estas?].

The call taker continues to see all original messages as expected along with the translated messages in green. Note that some language special characters are not sent as they may not be delivered accurately to all devices. Suitable standard characters are substituted in certain cases.

AT&T uses two primary sources to accurately monitor and measure the text path. MSRP texts delivered to PSAP via the integrated method are measure at both the TCC as well as the AT&T ESInet. Should either the TCC or AT&T ESInet detect a failure in the text messaging service, troubleshooting begins. The web-based text model is not delivered via MSRP, so this model depends on logging and reporting that are done by both the TCC as well as the TXT29-1-1 Web Portal. Similar processes for troubleshooting and resolution of the issues are taken anytime an issue is detected.

TCC has both internal and external logging/reporting. The internal logging is done at the TCC as well as the AT&T ESInet (for MSRP delivered text).

2.4.3. Interactive Multimedia Response Service (IMRS)

The Respondent must provide a description and/or documentation that supports the requirements in this section, including IMR conforming to NENA-STA-010.3.

AT&T Response:

Comply.



In a typical 9-1-1 infrastructure, IMR is handled by the terminating ESRP (PSAP CPE). This CPE-provided IMR plays announcements, and the caller responds via Dual-Tone Multi-Frequency (DTMF). The AT&T ESInet does not contain an IMR but is fully capable of passing both tones (DTMF) to/from the caller to relay messages back to the PSAP's IMR.

2.4.4. Bridge

The State requires a multimedia bridge conforming to NENA-STA-010.3. The State expressly requires the bridge to handle audio, video, MSRP and RTT.

- The State has no preference on which model (ad hoc or answer all calls at a conference aware UA), but the bridge must be able to transfer calls to and from ESInets using either model as specified in NENA-STA-010.3.
- The bridge must have capacity to maintain 20 simultaneous 3-way video calls or 100 simultaneous 3-way audio calls or a mix thereof.
- The bridge must be capable of supporting up to 6 parties (caller, call taker and up to four other parties) in any conference, with any mix of media.
- The bridge must have a mechanism to support RTT mixing when the end points do not support multiple RTT streams conforming to RFC 9071, as specified in NENA-STA-010.3.
- The bridge must support logging of media using the NENA-STA-010.3 specified mechanisms.
- The bridge must support the RFC 4575 Conference Event Package.
- The bridge must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3. The State must be able to subscribe to ServiceState and receive the standard state changes. The proposal must describe the bridge in detail.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Multimedia bridge conforming to NENA-STA-010.3 handling audio/video/MSRP/RTT.
- Support for ad hoc or answer-all models with transfers using either.
- Capacity for 20 simultaneous 3-way video or 100 audio calls (mix).
- Up to 6 parties per conference with media mix.

RTT mixing per RFC 9071.

- Media logging per standard; RFC 4575 Conference Event Package.
- ElementState/ServiceState support.



- Detailed bridge description.

AT&T Response:

Comply.

AT&T ESInet bridge handles audio, video, MSRP and RTT. AT&T ESInet uses conference aware UA bridging per the NENA-STA-010.3 standard. The ESRP supports N-way bridging and call transfers using i3 SIP REFER and subscribe/notify messaging. i3 PSAPs can transfer calls to both i3 and non-i3 PSAPs. Subscribe/notify messaging allows the PSAP or secondary PSAP to take control over the call bridge once a call is transferred.

AT&T ESInet's bridge can currently support up to 800 simultaneous 3-way audio calls today per data center. AT&T ESInet is engineered to assume 50% of calls will be bridged between three parties. After deployment of the AT&T ESInet, it was determined that the actual percentage of bridged calls is much lower, but AT&T continues the over-engineering of the solution to account for higher rates during peak periods. Video bridging is implemented however no OSPs currently support video for 9-1-1 calls without over the top applications. AT&T will support 20 simultaneous 3-way video calls when video bridging is implemented with OSPs. The bridge can support up to ten parties in any conference with any mix of media.

AT&T ESInet's bridge supports logging of media using NENA i3v3 mechanisms.

The bridge function supports RFC 4575 that allows other parties to subscribe. AT&T's bridge will provide notify messages noting the conference status of the parties.

The bridge function supports ElementState and ServiceState to allow the State to subscribe and received notify messages that provide status of state changes. AT&T is deploying this in a phased approach, as current market capabilities have shown that most are not capable of consuming this data via the Subscribe/Notify method.

2.5. Egress and External Interfaces

2.5.1. Outgoing Call Interface Function (OCIF)

The State requires an OCIF conforming to NENA-STA-010.3. The OCIF must be capable of directing a call back of an emergency call to the OSP that originated the emergency call, offering at least the same media streams negotiated in the emergency call. The contractor must obtain appropriate identities (for example, telephone numbers) for calls sent to other service providers. Use of those identities must be controlled by the Data Rights Management system specified in NENA-STA-010.3.

The Respondent must provide a description and/or documentation that supports the requirements in this section:



- OCIF per NENA-STA-010.3 for call backs to OSP with same media streams.
- Obtaining identities for other providers controlled by DRM.
- Description of OCIF utilization for call backs with implementation/integration details.

AT&T Response:

Comply.

AT&T ESInet provides the NENA-STA-010.3 prescribed OCIF. AT&T ESInet's OCIF supports call backs to the OSP via the same media streams and is controlled by the same DRM used throughout the ESInet. OCIF is available for any PSAPs to use but has not been implemented for any PSAPs today.

Remainder of page intentionally blank



3. GIS and Database Services Requirements

The Contractor shall implement location-based routing and ECRF/LVF functions using GIS data that conforms to the NENA GIS Data Model (NENA-STA-006.2), including civic address points, road centerlines, PSAP boundaries, emergency service polygons, and other required layers. The GIS repository must support spatial indexing for efficient queries.

Operations and Administration:

Location information is handled by the PSAPs while the State handles the PSAP boundaries and provisioning boundaries. The proposal shall include measures to maintain the PSAP interaction and where the PSAP utilizes a vendor must not interfere or materially change the contract a PSAP currently has for GIS support.

Location conveyance:

Location data shall be transported using PIDF-LO per RFC 4119 and RFC 5139 with applicable NENA extensions. The system shall deliver location information to PSAP CHE and mapping clients via standardized NG911 interfaces, supporting both push and pull mechanisms.

Validation and determination:

Integrate LVF/LIS to validate caller-provided locations, supporting geodetic coordinates (for example, WGS84) and civic addresses, including complex scenarios such as multi-line enterprises and multi-tenant buildings with address reformatting.

The ECRF shall use authoritative GIS to determine the correct ESN/PSAP, with defined fallback to default routing.

Data governance and provisioning:

The GIS system shall provide change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning formats (for example, GML and GeoJSON). Provide a GIS data-provisioning API and a comprehensive audit log of changes, including user, timestamp, and deltas.

Rules-based routing (RBR):

Support RBR features, including time-of-day routing, temporary boundary adjustments, alternate routing logic, and attribute driven decisions derived from GIS layers or an integrated rules engine.

3.1. Data Management and Interfaces

3.1.1. GIS and Database Management Functionality



The contractor will utilize the PSAP and State provided data for geospatial routing from the caller to the PSAP. Management of the data will be the responsibility of the State.

The contractor will have a web interface and/or automated method to provision data and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system. The contractor will ensure that an update to the system will be reflected in a change in routes (where the change does affect routes) within 5 minutes of such a change, assuming no errors are detected (online, real time update capability).

All data associated with call routing and plotting will be provided in conformance with NENA Data Model standards – NENA-STA-015.10 for remaining Legacy/Enhanced 911 systems and NENA-STA-006.2 for NG911 systems.

Originating call network operators will verify civic address location information against the NG911 GIS data using the LVF provisioned as required.

The preferred data exchange will be in Environmental System Research Institute's (ESRI) Structured Query Language (SQL) Spatial Database Engine (SDE).

The managed GIS map data will replace the traditional MSAG database as the primary database for location-based call routing and location validation (ECRF/LVF) functions within the NG911 system.

The maintenance of this GIS dataset will be completed by PSAP staff or designee. It is a requirement that the discrepancy reports of the data are delivered for remediation.

The contractor will be utilizing all existing and available source data and the management and coordination necessary.

The PSAP will be responsible for providing all GIS data used in the location routing, validation, mapping services, and maintenance of such data that are part of the contractor's system.

- The data from the PSAP will include the road centerline and address range data, address structure points, PSAP boundaries, municipal boundaries, police, fire, EMS, and medical transport boundaries and many additional GIS layers useful for display in the PSAPs. GIS data used for call routing and call locations will be provided in a NENA NG911 standard format.
- The contractor will be required to establish a working relationship with the State and to work out mutually acceptable procedures for the maintenance of these databases.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Use of PSAP GIS data for geospatial routing.
- Web interface or automated method for provisioning and retrieving post-QA data for maps.



- Reflection of PSAP updates in routes within 5 mins (online real-time).
- Data structures organized in conformance to NENA Data Model Standards – NENA-STA-015.10 and NENA-STA-006.2.
- LVF for OSP civic address verification.
- Preferred ESRI SQL SDE exchange.
- Replacement of MSAG with GIS for routing/validation.
- PSAP maintenance with contractor discrepancy reports.
- Use of existing source data.
- Responsibility for all GIS data maintenance.
- Inclusion of road centerline, address points, PSAP emergency boundaries, and additional layers.
- Mutually acceptable maintenance procedures with State.

AT&T Response:

Comply.

The Enterprise Geospatial Database Management System (“EGDMS”) is the system's GIS Data validation and integration system serving as the nexus for all GIS data processing and fulfills the NENA Spatial Interface (SI) functionality. The EGDMS is a secure service used by local, regional, and state-level GIS data sources for ongoing quality assurance/quality control (QA/QC) validation and reporting, coalescing and provisioning of GIS data.

The EGDMS system provides automated GIS data NENA format standardization and data aggregation between regional or state-level individual participating agencies. Validations at the site structure address point level will occur prior to data being loaded for geospatial routing by performing ALI to road centerline and ALI to address point comparisons, among other validations. Post QA/QC data extracts will be made available upon request for use in call and incident mapping applications.

When using the NG9-1-1 core services, the EGDMS serves as the NENA Spatial Interface (SI), a web-based tool, provisioning the Emergency Services Network (“ESInet”) functional elements including the Emergency Call Routing Function (ECRF) and the Location Validation Function (LVF).

GIS updates are provisioned through the SI which has the additional ability to perform GIS validations, including validations to ensure geospatial call 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.



The following QA/QC processes and validations are performed within the 9-1-1 EGDMS:

- Validations for all layers
- Compare the schema and data structure and properties of the source dataset with the schema and properties of the master database and report discrepancies in the EGDMS Field Mapping Tool
- Database Field Constraint
- All Features fall within the Authoritative Boundary
- Duplicate Feature Detection
- Unique ID Validation (if provided)
- Values are present for required attributes
- Remove features with NULL geometry
- Repair features with bad geometry
- Note: Any arc or ellipse feature types will be transformed into line and polygon features during processing
- Boundary-Layer (Authoritative Boundary, PSAP, Fire, Law, EMS)
- Polygon gap/overlap validation (For errors involving multiple agencies, participants must work with neighbor agencies to resolve issues. All polygon gap/overlap issues must be correct prior to provisioning data to the ECRF/LVF.)
- Routing URI populated and valid
- Street Centerlines
- Address Range Overlap Issues

During the transitional period when carriers do not have the capability to manage their own Location Information Server (LIS), AT&T will continue to maintain location data on behalf of the carriers. The data integrity unit at AT&T will continue to work with the OSPs to resolve any errors when submitting new addresses to be provisioned in the AT&T ESInet. OSP data will be validated using the State's GIS data. Processes and procedures, as well as web applications, work to facilitate the communications between the address coordinators and the Intrado data analysts.

Included in this section, please find the AT&T ESInet EGDMS User Guide. This user guide is provided prior to a PSAPs training on using the EGDMS web portal to submit data. It outlines the critical errors, mandatory fields, and process to update the PSAPs complete GIS data. AT&T also provides an i3 GIS coach as part of the GIS onboarding services. This i3 GIS coach will assist the State in uploading their data to the EDGMS platform.

Please see separate attachment EGDMS_User_Guide.pdf.



3.1.2. Spatial Interface (SI) Functionality

The contractor will implement a Spatial Interface and ensure following capabilities are implemented:

- GIS data provisioned by the spatial interface (SI) will undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA-STA-006.2-2022, NENA-02-014 and NENA-STA-010.3-2021 while maintaining the online, real time update capability.
- The SI will convert the GIS data meeting these requirements into the format (data structure and projection) used by the ECRF and LVF, in real-time or near-real-time, using a Web feature service.
- The SI will be able to provision and perform incremental updates, in near-real-time, to the ECRF, LVF, the map viewer service, the PSAP map display and similar applications that consume GIS data.
- Validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of online real-time provisioning of updates to the GIS data provisioned to the ECRF and LVF.
- The SI operation will align with the data maintenance processes with minimal impact to existing operations.
- The SI will receive and incorporate the SI datasets that have been prepared by the PSAP as previously described.
- Web interface tool for viewing and submitting incidents and change tickets.
- Web interface tool for viewing policy-routing plans.

The contractor will be able to test and then apply updates to the operating ECRF by a secure and reliable method that does not create operational problems.

The contractor's GIS functions will be able to perform database audits for common problems and errors, such as gaps, overlaps or number range conflicts, which if encountered, will be referred back to the PSAP for resolution.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SI implementation with data-quality and integrity checks per NENA standards while maintaining real-time updates.
- Conversion to ECRF/LVF format via Web feature service.
- Incremental near real-time updates to ECRF/LVF, map viewer, and PSAP displays.
- Validation prior to provisioning with online real-time updates.
- Alignment with PSAP processes.



- Incorporation of PSAP prepared datasets.
- Web tools for incidents, change tickets and policy-routing views.
- Secure reliable update and testing application without problems.
- Database audits for gaps/overlaps/conflicts referred to PSAP.

AT&T Response:

Comply.

The Spatial Interface (SI) is responsible for provisioning and updating authoritative GIS data to the ECRF and LVF. The NENA Spatial Interface (SI) functionality is fulfilled as a function of the Enterprise Geospatial Database Management System (EGDMS). The SI/EGDMS is a fully hosted, managed service that encompasses all necessary processes to receive GIS data from a single source. Data can be submitted through the web interface in a GIS database managed by a vendor, the PSAPs, or the State as a regional authority. 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).

Data provisioned to the SI undergoes data quality and data integrity checks that ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA 02-014, and STA-010.3-2021. Where these requirements conflict with STA-010.3 and the NG9-1-1 GIS Data Model (draft), the newer requirements will be used. The SI will normalize the GIS data, converting it into a consistent format, which will meet the STA-010.3 standard.

The SI will normalize the GIS data, converting it into a consistent format, which will meet the STA-010.3 standard. This format and content meet the ECRF/LVF LoST protocol requirements.

The SI provides:

- NG9-1-1 GIS data compliancy checks
- Ongoing GIS data accuracy validation (QA/QC)
- GIS data error reporting

Provisioning to i3 systems (ECRF/LVF) and other systems specified by the State of Nebraska that consumes GIS information, e.g., PSAP Map Display.

Data provisioned to the SI undergoes data quality and data integrity checks that ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA 02-014, and STA-010.3-2021. Where these requirements conflict with STA-010.3 and the NG9-1-1 GIS Data Model, the newer requirements will be used. The SI will normalize the GIS data, converting it into a consistent format, which will meet the STA-010.3 standard. This format and content meet the ECRF/LVF LoST protocol requirements. Validation of polygon feature sets occurs very quickly and subsequent provisioning to the ECRF/LVF system is near real-time. 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.

Incident and change tickets related to GIS data are 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 AT&T Spatial Interface is a GIS agnostic tool that can be used regardless of the GIS editing software the PSAPs and their GIS authorities use. AT&T ESInet's SI will align with the PSAP's existing data maintenance processes without impact to existing processes.

AT&T ESInet's SI will receive and incorporate SI datasets that were used in the current NGCS environment. AT&T ESInet uses a similar Spatial Interface that is used throughout the State of Nebraska today so the PSAP's GIS authorities can rest assure of a smooth and efficient transition.

The AT&T Spatial Interface can be used to add special event layers to be used during by the PRF. AT&T's PRF and Policy Store are not provided within the SI but can be accessed through the secure, web-based AT&T Customer Management Portal. CMP provides PSAPs and authorized personnel with extensive flexibility to view, define, and update standard and alternate routing policies. AT&T's SI and CMP are both part of the AT&T ESInet Portal, which provides a single entry into multiple applications.

Policies have attributes such as active/inactive, onetime, or recurring time window, priority, or a set of destination(s) to send the call to, and call distribution method as examples.

Abandonment, Overflow, and Diversion policies can be configured to use any of the following policies.

- Geographically – The system can be configured to send abandonment calls to different alternate PSAPs based on the geographic location of the calling party within the primary PSAP's jurisdiction. Geographic abandonment or alternate routing polygons can be pre-provisioned via the SI or submitted dynamically.
- Hierarchically – The system can be configured to cascade a call to up to nine consecutive, alternate PSAPs.
- Load-balanced – The system can be configured to distribute calls between PSAPs.

All policies loaded by the customer are held in a test state (non-active) until the customer confirms that all test calls using the policies perform as expected.

3.2. Core Data Services

3.2.1. Mapping Data Service

A Mapping Data Service conforming to NENA-STA-010.3 will be provided. This must be available within 18 months. The MDS will be capable of providing maps for all calls for all entities inside the ESInet and for calls handled out of area in other ESInets.



- The MDS must support both images and features as described in NENA-STA-010.3
- The MDS must support all layers defined in NENA-STA-006.2. Additional layers may be supported, and the proposal will describe what additional layers the MDS will support.
- Retrieval of map data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.
- The MDS must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- MDS per NENA-STA-010.3 available within 18 months for all calls/entities.
- Support for images/features.
- All layers per NENA-STA-006.2.
- Additional layers described; DRM-controlled retrieval; ElementState/ServiceState support with State subscription.

AT&T Response:

Comply.

MDS is part of the Enterprise Geospatial Database Management System (EGDMS) and has been implemented and available to PSAPs on day one. EGDMS is the system's GIS Data validation and integration system serving as the nexus for all of our GIS data processing. The EGDMS is a secure, cloud-based service used by local, regional, and state-level GIS data sources for ongoing quality assurance/quality control (QA/QC) validation and reporting, coalescing, and provisioning of GIS data.

EGDMS will publish a Web Mapping Service (WMS) or a Web Feature Service (WFS), which are standard protocols developed by the Open Geospatial Consortium (OGC) for serving geo-referenced map images and features over the Internet. These services can be consumed by any third-party mapping application that conforms to the protocol.

The WMS will serve the map in a bitmap format, PNG, GIF, or JPEG. In addition, vector graphics can be included, such as points, lines, curves, and text, expressed in SVG or WebCGM format. The WFS allows for discovery, query, or data transformation operations. The WFS allows the client to interact with the source data behind the WMS.

EGDMS also acts as the Spatial Interface (SI), where GIS data layers are provisioned or published to other functional elements, such as ECRF, LVF, as well as Geocode Conversion Service (GCS) and Mapping Data Service (MDS).



AT&T ESInet's supports Data Rights Management per NENA-STA-010.3 as well as the ElementState and ServiceState requirements.

3.2.2. MSAG Conversion Service (MCS)

The MSAG Conversion Service (MCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The State expects the LNG to support the SOA interface towards the legacy OSP, store the data in the Location Database in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The State expects the LPG to support the MF/ALI interface towards the legacy PSAP, retrieve the location from a Location Information Server in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An MSAG Conversion Service (MCS) conforming to NENA-STA-010.3 will be implemented.
- The MCS must support Element State and Service State SUBSCRIBE/NOTIFY per NENA-STA 010.3.
- The State must be able to subscribe to Service State and receive the standard state changes.

AT&T Response:

Comply.

AT&T provides a MSAG Conversion Service that provides the capabilities as described in NENA-STA-010.3 but in a slightly different manner. We allow the OSPs to validate their data using geoMSAGs but still allow the calls to geospatially route via the PSAP-provided GIS data. As part of the implementation, we will train the State on how to use our systems and solutions to validate, load, and maintain the GIS Database systems. We have provided our GIS Data Roles and Expectations Confidential document, which details how, in what format, and what data should be included in order to transition from an ESN/tabular-based deployment into the geospatial i3 routing solution.

AT&T also provides the NENA i3 compliant MCS. The AT&T ESInet MCS supports ElementState and ServiceState per NENA-STA-010.3. AT&T will work with the State to allow them to subscribe for updates to ElementState and ServiceState.

3.2.3. Geocode Conversion Service (GCS)



The Geocode Conversion Service (GCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- GCS per NENA-STA-010.3 with SI provisioning (additional options for PSAP GIS upgrades).
- Return of ECRF routing location for civic addresses.
- ElementState/ServiceState support.
- ServiceState and receive the standard state changes.
- The GCS must return the same location that the ECRF uses for routing when given a civic address.

AT&T Response:

Comply.

AT&T ESInet provides the NENA i3 compliant GCS for outside entities to convert a civic location to geodetic and vice versa. GCS is provided via a web service (as prescribed by NENA-STA-010.3). The AT&T ESInet GCS supports ElementState and ServiceState and allows the State and/or PSAPs to subscribe for updates. AT&T ESInet's GCS uses the same GIS data as ECRF and will return the location (civic or geodetic) that matches what is loaded in the ECRF. AT&T will work with the State to allow them to subscribe for updates to ElementState and ServiceState.

3.3. PSAP-Facing Services

3.3.1. PSAP Mapping Service

The State requires a Mapping Data Service (MDS) conforming to NENA-STA-010.3.

The services required must enable the PSAP mapping system and ECRF/LVF system to support multiple methods for reporting location errors. They include:

- ECRF civic location geocoding errors are automatically captured by the data management application utilized by the PSAP.
- LVF failures are automatically captured by the LVF and forwarded to the data management application utilized by the PSAP.
- 911 call mapping failures (calls that could not be mapped automatically) are captured by the system and forwarded to the data management application utilized by the PSAP.



- 911 telecommunicators and dispatchers may manually generate a discrepancy report, and the system can automatically forward the reports to the data management application utilized by the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PSAP mapping using PSAP geospatial info.
- Support for error reporting methods (ECRF geocoding errors captured.
- LVF failures forwarded; unmapped calls captured; manual discrepancy reports forwarded.

AT&T Response:

Comply.

The Enterprise Geospatial Database Management System (EGDMS) is the system's GIS Data validation and integration system serving as the nexus for all of our GIS data processing. The EGDMS is a secure, cloud-based service used by local, regional, and state-level GIS data sources for ongoing quality assurance/quality control (QA/QC) validation and reporting, coalescing, and provisioning of GIS data.

EGDMS will publish a Web Mapping Service (WMS) or a Web Feature Service (WFS), which are standard protocols developed by the Open Geospatial Consortium (OGC) for serving geo-referenced map images and features over the Internet. These services can be consumed by any third-party mapping application that conforms to the protocol.

The WMS will serve the map in a bitmap format, PNG, GIF, or JPEG. In addition, vector graphics can be included, such as points, lines, curves, and text, expressed in SVG or WebCGM format. The WFS allows for discovery, query, or data transformation operations. The WFS allows the client to interact with the source data behind the WMS.

EGDMS also acts as the Spatial Interface (SI), where GIS data layers are provisioned or published to other functional elements, such as ECRF, LVF, as well as Geocode Conversion Service (GCS) and Mapping Data Service (MDS).

AT&T ESInet's supports Data Rights Management per NENA-STA-010.3 as well as the ElementState and ServiceState requirements.

3.3.2. Map Discrepancy Reporting

The Respondent must provide a description and/or documentation that supports the requirements in this section for referral of all geospatial discrepancies to the State for remediation.

AT&T Response:



Comply.

The Enterprise Geospatial Database Management System (“EGDMS”) is the system's GIS Data validation and integration system serving as the nexus for all GIS data processing and fulfills the NENA Spatial Interface (SI) functionality. The EGDMS is a secure service used by local, regional, and state-level GIS data sources for ongoing quality assurance/quality control (QA/QC) validation and reporting, coalescing and provisioning of GIS data.

The EGDMS system provides automated GIS data NENA format standardization and data aggregation between regional or state-level individual participating agencies. Validations at the site structure address point level will occur prior to data being loaded for geospatial routing by performing ALI to road centerline and ALI to address point comparisons, among other validations. Post QA/QC data extracts will be made available upon request for use in call and incident mapping applications.

GIS updates are provisioned through the SI which has the additional ability to perform GIS validations, including validations to ensure geospatial call 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. Authorized GIS users can view errors and fallout from the QA/QC process via EGDMS.

The following QA/QC processes and validations are performed within the 9-1-1 EGDMS:

- Validations for all layers
- Compare the schema and data structure and properties of the source dataset with the schema and properties of the master database and report discrepancies in the EGDMS Field Mapping Tool
- Database Field Constraint
- All Features fall within the Authoritative Boundary
- Duplicate Feature Detection
- Unique ID Validation (if provided)
- Values are present for required attributes
- Remove features with NULL geometry
- Repair features with bad geometry
- Note: Any arc or ellipse feature types will be transformed into line and polygon features during processing
- Boundary-Layer (Authoritative Boundary, PSAP, Fire, Law, EMS)



- Polygon gap/overlap validation (For errors involving multiple agencies, participants must work with neighbor agencies to resolve issues. All polygon gap/overlap issues must be correct prior to provisioning data to the ECRF/LVF.)
- Routing URI populated and valid
- Street Centerlines
- Address Range Overlap Issues

Please see separate attachment **Appendix E - AT&T 9-1-1 EGDMS User Guide**.

Note:

GIS-related discrepancy reporting technical requirements are detailed in §E-6.7.2, et seq. of this document.

3.4. External Integrations

The Respondent must provide a description and/or documentation that supports the integration with additional vendors as required to provide functionality to all PSAPs as currently utilized.

AT&T Response:

Comply.

Integration with additional vendors is supported through the system's open, standards based NG911 architecture, enabling PSAPs to continue using the same third-party tools and platforms they use today without workflow or contract changes. The system supports interoperability with a variety of existing PSAP vendors—such as CAD and mapping systems, commercial text gateways, logging/recording platforms, and supplemental location services—all connected through NENA compliant interfaces (e.g., SIP, LoST, HELD, MSRP, WFS/WMS).

The Spatial Interface (SI) also supports multiple GIS vendor environments, allowing PSAPs to submit data from any GIS toolset and ensuring it is validated and provisioned consistently regardless of the originating vendor. This standards based, multivendor approach ensures seamless functionality across all PSAPs and preserves existing integrations while enabling future expansion.

Remainder of page intentionally blank



4. Security Requirements

The contractor shall implement the NENA NG-SEC security and trust model, featuring strong authentication and authorization for all interfaces, mutual TLS for inter-service communications, edge security via SBCs and Back-to-Back User Agents (B2BUAs), network segmentation, and secure management planes. Threat mitigations must address Denial of Service (DoS), Distributed DoS (DDoS), Telephony Denial of Service (TDoS), SIP flooding, spoofing, and injection attacks through rate limiting, anomaly detection, and firewalls.

Implement Role-Based Access Control (RBAC) with granular permissions, multifactor authentication (MFA) for all administrative access, least privilege enforcement, and auditing of service accounts. Integration with external identity providers (e.g., SAML/OAuth) must be supported.

All location data, call content, and PII must be encrypted in transit (TLS 1.3) and at rest (AES-256 or stronger), with data minimization, pseudonymization, and compliance with laws like HIPAA and CJIS where applicable. Access to sensitive data shall require explicit consent logging.

Provide Public Key Infrastructure (PKI) processes for certificate issuance/rotation, Certificate Revocation List (CRL)/Online Certificate Status Protocol (OCSP) validation, and secure key storage using Hardware Security Modules (HSMs) or compliant vaults. Automated alerts for expiring certificates must be included.

The contractor shall supply an incident response plan aligned with NENA, including vulnerability disclosure protocols, regular patch schedules (e.g., critical patches within 30 days), and forwarding of security event logs to the jurisdiction's Security Information and Event Management (SIEM) system via secure channels (e.g., Syslog over TLS).

Provide results from independent penetration testing (conducted within the last 12 months), SSAE 18/SOC 2 audit reports, and support for jurisdiction-led security acceptance testing, including network scans, application fuzzing, and red-team exercises.

AT&T Response:

Comply.

AT&T ESInet's architecture aligns with the NENA NG SEC security and trust model and implements layered security controls, including strong authentication and authorization, network segmentation, firewalls, and edge security components. Traffic is protected using secure connections and is monitored for DoS, DDoS, TDoS, SIP flooding, spoofing, and injection attacks through rate limiting, anomaly detection, and firewall protections.

AT&T enforces role based access control (RBAC), least privilege access, multifactor authentication for administrative access, and centralized auditing of privileged and service accounts. Integration with external identity providers is supported where applicable.



Sensitive data is protected through encryption in transit and at rest, data minimization practices, and access logging in accordance with applicable laws and contractual requirements.

AT&T maintains formal certificate management processes, including certificate issuance, rotation, revocation checking, and secure key storage using enterprise grade vaulting solutions, with monitoring and alerting for certificate lifecycle events.

AT&T maintains a documented incident response program, vulnerability management and patching processes, and security event logging. Security logs can be forwarded to customer or jurisdiction SIEM platforms via secure channels, as required.

AT&T undergoes regular independent security assessments, including penetration testing and SOC 2 audits, and supports jurisdiction led security acceptance testing in coordination with operational requirements.

4.1. Management and Process Control

4.1.1. Personnel Roles and Responsibilities

Safeguarding NG911 assets – across **NGCS platforms** and the **ESInet** – is a shared duty. The contractor must **define, assign, and document** minimum security roles and responsibilities, whether performed internally or by external providers. At a minimum, the following roles must be covered by **named, accountable** individuals. Where third parties perform duties (carriers, cloud, managed services, subcontractors), the contractor remains responsible for assignment and verification.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An organizational roles matrix (e.g., org chart and/or RACI) identifying named individuals (or positions) for: Security Manager, Security Administrator, Data Owner(s), Data Custodian(s), Data User populations, and Security Audit Manager. Note any shared/combined roles and the accountable individual for each responsibility. Map these to NGCS components and ESInet segments.
- Documented role definitions aligned to the duties above, including authorities (e.g., the Security Manager's authority to set security policy for all NGCS/ESInet components; Security Administrator authority to implement and enforce controls across applications, network, cloud).
- Evidence that personnel are informed of their roles and responsibilities (e.g., acknowledgement forms, training records, onboarding materials, policy attestations).
- A data ownership register mapping every NG911 data set (local and remote) to a Data Owner; include classification and handling responsibilities.



- A data custodianship register mapping every NG911 data set (at rest and in transit, local and remote) to a Data Custodian; include the operational security measures they manage (encryption, key management touchpoints, access administration, backup/restore).
- Security administration procedures showing how the Security Administrator implements and maintains security controls in accordance with NG911 policies – for NGCS applications, the ESInet, edge devices, and management portals).

An audit governance plan for the Security Audit Manager covering periodic audit cadence (internal/external), scope, reporting, and risk rating of findings, and tracking to closure.

Role coverage procedures (e.g., delegation during absence) ensuring continuity while preserving single point accountability for each required responsibility.

- If external parties are involved, contractual or policy evidence assigning role responsibilities to vendors/contractors/subcontractors and showing how the prime provider verifies fulfillment (e.g., attestations, SLAs, right-to-audit).

AT&T Response:

Comply.

AT&T recognizes that safeguarding NG9 1 1 assets across NGCS platforms and the ESInet is a shared responsibility and maintains a defined governance model that assigns and documents minimum security roles and responsibilities. AT&T designates accountable roles for security management, security administration, data ownership, data custodianship, data users, and security audit oversight. Where roles are shared or combined, a single accountable individual is identified for each responsibility.

AT&T maintains documented role definitions that establish authority and responsibility for setting security policy, implementing and enforcing technical and administrative controls, managing access, and overseeing security monitoring and audits across NGCS components and ESInet segments. Personnel are informed of their responsibilities through onboarding, role-based training, and policy acknowledgements.

NG9 1 1 data sets are assigned to designated Data Owners and Data Custodians, with responsibilities defined for classification, handling, access control, encryption, key management touchpoints, and backup and recovery. Security administration procedures govern the implementation and ongoing maintenance of controls across NGCS applications, the ESInet, edge components, and management portals.

AT&T maintains audit governance processes that define audit scope, cadence, reporting, risk rating, and tracking of findings to closure. Role coverage and delegation procedures are in place to ensure continuity of operations while preserving clear accountability.



Where third parties (e.g., carriers, cloud providers, managed service providers, or subcontractors) perform security related duties, Intrado contractually assigns responsibilities and retains accountability for verification through governance processes, contractual requirements, and oversight mechanisms.

4.1.2. Identity Management

The contractor must operate a standards-based **Public Key Infrastructure (PKI)** to uniquely identify and authenticate every participating **agency** and **agent** across all NGCS and ESInet interfaces. An agency's identity must be a globally unique **FQDN** (e.g., erie.psap.ny.us) encoded in the X.509 SubjectAltName (**SAN**). An agent's identity must use the user@agencyfqdn format (e.g., nancy@erie.psap.ny.us) and be encoded in the SAN of the agent certificate.

For PSAPs and 911 Authorities, the **PSAP Credentialing Agency (PCA)** is the **root of trust** for agency and agent certificates. The trust chain may include **national → state → agency/PSAP CAs**. Issuance may be performed directly by the PCA or by approved subordinate CAs under that chain. Any issuing authority must operate under a formal **Certificate Policy/Certification Practice Statement (CP/CPS)** with documented identity proofing and issuance controls. If an agency cannot meet those controls, it must use a **managed CA** that enforces the CP/CPS.

Private keys must be safeguarded in **FIPS 140-2** validated cryptographic modules at these minimum levels: **Level 2** for agency private keys (**Level 3 preferred**), **Level 3** for agency CA keys, and **Level 4** for state/national CA keys. **Certificate-based authentication (e.g., mTLS)** must be enforced so that valid identities and credentials are required for access to **all** NGCS/ESInet services and data (e.g., SIP signaling, APIs, management portals, interconnects).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An identity and certificate schema showing agency FQDN conventions and agent identifier format ([user@agencyfqdn](#)), with confirmation these identifiers appear in X.509 SAN fields for agency and agent certificates.
- A PCA/PKI trust architecture (diagram & narrative) showing the PCA root, any national → state → agency CA tiers, and permitted subordinate issuing models (e.g., PSAP/Authority issuing agent certs).
- A current CP/CPS (or binding reference) for each issuing authority, defining identity proofing, issuance, renewal, revocation, auditing, and key management; state who operates each CA (Respondent, State, third party) and how compliance is enforced.
- Key protection evidence demonstrating FIPS 140-2 validation and deployment at required levels:
 - Agency private keys: Level 2 minimum (note if Level 3 is implemented).
 - Agency CA keys: Level 3
 - State/National CA keys: Level 4



- Key protection evidence should include device inventories, validation certificates, hosting locations, and any escrow arrangements.
- Access control enforcement description confirming certificate-based authentication (e.g., mTLS) is required for all NGCS/ESInet services and data, where enforcement occurs (interfaces, APIs, signaling paths), and how failed, expired, or revoked certificates are detected and blocked.
- Certificate profiles and samples (agency and agent): SAN contents, Key Usage/EKU, validity periods, revocation mechanisms (CRL/OCSP), and sample chains validating to the PCA.
- Operational lifecycle procedures for issuance, renewal, suspension/revocation, replacement, and compromise response; include joiner/mover/leaver workflows for agents and rollover plans for CA keys.
- Contingency approach if an entity cannot securely operate a CA (e.g., use of a managed CA aligned to the CP/CPS), including contractual controls, SLAs/SLOs, and audit rights.

AT&T Response:

Comply.

AT&T implements a comprehensive, standards based Identity Management framework aligned with NENA i3 and the PSAP Credentialing Agency (PCA) model to uniquely identify, authenticate, and authorize agencies, systems, and individual users across all NGCS and ESInet interfaces.

Agency identities are established using globally unique Fully Qualified Domain Names (FQDNs) (for example, psap.lincoln.county.ne.us), and individual agent identities use the required user@agencyfqdn format (for example, jane.doe@psap.lincoln.county.ne.us), with these identifiers encoded in X.509 certificate Subject Alternative Name (SAN) fields.

Identity lifecycle management is enforced through formal Identity Management (IDM) processes that govern user and agency onboarding, modification, and de provisioning. User identities are provisioned through controlled workflows with appropriate approvals, role assignment, and periodic review. Authentication mechanisms integrate Single Sign On (SSO) and multi factor authentication, where applicable, and are used to unlock private keys associated with agent certificates for secure session establishment.

For PSAPs and 911 Authorities, the PCA serves as the root of trust for agency and agent credentials. The Contractor supports a hierarchical PKI trust model consistent with NENA guidance, including national, state, and agency tiers. PCA compliant certificates are issued and managed using an approved Certificate Authority operating under the PCA Certificate Policy and Certification Practice Statement (CP/CPS). The Contractor supports the use of DigiCert as a PCA approved Certificate Authority for issuing and managing agency and agent certificates, providing a managed CA capability for entities that do not operate their own CA infrastructure.

The PCA trust hierarchy and certificate issuance model is illustrated in Figure 1.

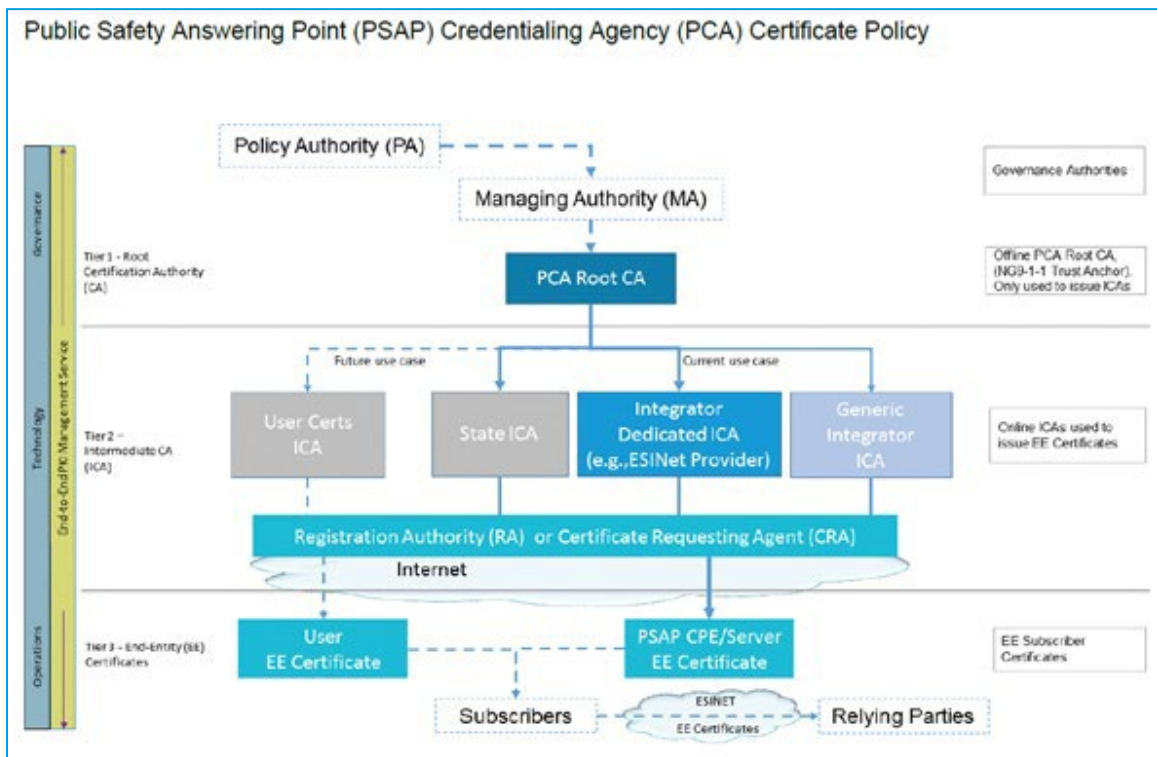


Figure 26: PCA PKI Policy

Certificate based authentication is enforced for access to NGCS and ESInet services and data. Mutual TLS (mTLS) is required for service to service, agency to service, and agent to service communications, including SIP signaling, data interfaces, APIs, and administrative access points. Certificates are validated against the PCA trust chain, and expired, revoked, or non-compliant credentials are automatically denied access.

Authorization decisions are enforced independently of authentication and are based on identity attributes, assigned roles, and applicable access policies. This ensures that authenticated entities are permitted to access only those services and data required to perform their authorized functions, supporting the principle of least privilege across the system.

All cryptographic keys are protected in accordance with FIPS 140 2 requirements. Data is encrypted in transit using industry standard cryptographic protocols and strong cipher suites, and encryption controls are enforced at network, application, and interconnection boundaries to protect sensitive operational and emergency services data.

This integrated Identity Management approach ensures secure, auditable, and policy driven control of identities, credentials, and access across the Nebraska NG911 environment while maintaining alignment with nationally recognized NG911 security and credentialing standards.



4.1.2.1. Roles

Every **agency** and **agent** must authenticate with an X.509 certificate that asserts one or more roles used for authorization.

- **Agency roles** define organizational authority, optionally constrained by **scope**.
- **Agent roles** define individual privileges and may include **modifiers** as identified in NENA-STA-010.3 §5.3.

Role assignment for any agency or agent must be **approved and limited by the immediately superior agency's policy**. Solutions may support local roles, but **full functionality must work with baseline roles and scopes** for mutual aid and roaming. Roles must be **encoded in certificates** (role OIDs/attributes per profile) and **enforced at NGCS/ESInet interfaces**.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A role model and governance describing agency role, agent roles, and allowed scopes, including how the immediately superior agency approves/limits assignments and how those policies are enforced.
- Role encoding specification for X.509 showing exactly how roles/modifiers/scopes are carried (e.g., OIDs or SAN/subject attributes) with minimal sample certs limited to the role fields and a description of validation during authentication.
- An authorization design that consumes certificate-asserted roles to make access decisions across NGCS/ESInet services, with least-privilege mappings from each role (and modifier) to permissions.
- Evidence of baseline role coverage showing agencies exist that assume all baseline agency roles and that no custom roles are required for full system functionality.
- A role registry integration plan (reference NENA-STA-010.3 §10.27 & §10.28) describing how the solution references the Agency and Agent Role registries, maps them to authorization objects, and process registry updates.
- Role lifecycle controls: request to and approval by the superior agency, assignment changes, revocation, and timely de-provisioning; include joiner/mover/leaver workflows for agents' roles.
- Operational procedures for modifiers showing how modifiers adjust privileges without creating new base roles.
- Monitoring and audit showing how role use is logged, reviewed, and tied back to the approving superior agency; include alerts for unauthorized role elevation.
- Exception handling for temporary/emergency role increases: approval, time bounds, logging, and revocation; include how conflicts between local custom roles and baseline roles are resolved while keeping services available.



AT&T Response:

Comply.

Jurisdictions have not historically required agency or agent roles to be explicitly asserted and enforced via X.509 certificates, and most do not presently specify agent level role models. AT&T ESInet currently uses certificates as the authoritative source of identity for secure access to NGCS and ESInet services. The solution architecture supports role-based authorization per NENA-STA-010.3, including certificate-encoded roles, scopes, and modifiers as required by state or local authorities. AT&T will work collaboratively with jurisdictions to define, implement, and enforce role based requirements as they are specified.

AT&T ESInet enforces mutual authentication using X.509 certificates as the authoritative mechanism for establishing trusted identity for agencies and agents accessing NGCS and ESInet services. While X.509 certificates are capable of asserting role information for authorization purposes, jurisdictions have not historically required certificate level assertions of specific agency or agent roles, and most do not presently specify agent level role models. Accordingly, certificates are used to establish identity, with authorization decisions derived from jurisdiction approved policy and system configuration.

AT&T ESInet's architecture is capable of supporting role based authorization models, including agency roles, agent roles, scopes, and modifiers as defined in NENA STA 010.3, should a jurisdiction require role assertions to be encoded and enforced via X.509 certificates. The solution is designed to accommodate both current deployment patterns and future jurisdictional requirements.

Agency roles represent organizational authority and responsibility within the NG911 environment and may be constrained by scope (e.g., jurisdictional, functional, or operational). Agent roles represent the privileges of individual users acting on behalf of an agency and may include modifiers as defined in NENA STA 010.3 §5.3 to refine privileges without introducing new base roles. Where requested, these constructs can be incorporated into certificate based authorization workflows.

Role assignment and governance are defined by the policy of the immediately superior agency. AT&T ESInet supports governance models in which superior agencies approve, limit, and revoke role assignments in accordance with local policy. While local or custom roles may be supported for jurisdiction specific use cases, the solution aligns with baseline NENA role definitions to preserve interoperability, mutual aid, and roaming when such roles are asserted.

When required by a jurisdiction, roles, modifiers, and scopes may be encoded within X.509 certificates using defined attributes and object identifiers aligned with applicable NENA profiles. During authentication, certificates are validated and role assertions may be consumed by NGCS and ESInet services to enforce least privilege access decisions. AT&T will work with states and authorities having jurisdiction to define appropriate role encoding and validation approaches consistent with their policies.



Authorization within the AT&T ESInet is designed to consume identity and, where applicable, certificate asserted role information to make access decisions across signaling, data, and management services. Role to permission mappings follow least privilege principles and can be aligned with NENA baseline roles and modifiers when such models are implemented.

Baseline role coverage is achievable without reliance on custom roles. Agencies may assume baseline agency roles sufficient to access all required system functionality, ensuring interoperability and continuity of service. Custom or local roles, if used, do not replace baseline roles and are not required for mutual aid or roaming operations.

Integration with Agency and Agent Role Registries as defined in NENA STA 010.3 §§10.27 and 10.28 has not been currently required by jurisdictions but is supported by the solution architecture. Where requested, registry definitions can be referenced, mapped to authorization objects, and incorporated into role validation and enforcement processes, with updates managed through defined governance procedures.

Role lifecycle management—including request, approval by the superior agency, modification, revocation, and de provisioning—is supported when role based authorization is implemented. Joiner, mover, and leaver workflows can be aligned with jurisdictional policy to ensure timely and appropriate access control.

Operational support for role modifiers allows temporary or contextual privilege adjustments without creating new base roles. Modifiers are applied in accordance with policy, constrained by scope and duration where appropriate, and enforced through authorization controls.

Authorization activity may be logged and audited to provide traceability to the approving superior agency. Monitoring capabilities support detection of unauthorized role use or attempted privilege elevation where role based enforcement is enabled.

Exception handling mechanisms can support temporary or emergency role elevation when required, including approval, time bound enforcement, logging, and revocation. In cases where local custom roles coexist with baseline roles, baseline role enforcement is preserved to maintain interoperability and service availability.

4.1.3. Policies and Procedures

The contractor must maintain a comprehensive cybersecurity policy framework for **NGCS platforms** and the **ESInet**. Policies may be separate or consolidated, but each required area must have clear **purpose, scope, roles, approval, version control, distribution, and compliance expectations**. Policies must be **approved, communicated to personnel, and reviewed and/or updated on a defined cadence** (at least annually or upon material change) to reflect new and emerging technologies, threats, and processes.



Policies must **flow down** to vendors/contractors/subcontractors and be backed by **Standard Operating Procedures (SOPs)** that turn policy into repeatable tasks. (e.g., user onboarding, vendor remote access, incident handling, recovery). SOPs must be created, kept current, and used in daily operations.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy governance covering ownership, approval authority, versioning, distribution/acknowledgement, training, and review/update cadence.
- A policy inventory (or consolidated policy) including, at minimum, the policies identified in NENA-STA-040.2 §4.1.2.

Contractual flow-down language proving applicable policies bind all vendors, contractors, and subcontractors supporting NGCS/ESInet.

A complete SOP catalog mapped to the above policies.

- SOP governance describing authorship, approval, version control, authoritative storage, and periodic update cycle; include triggers for out-of-band updates (e.g., new technology implementation or threat vectors)
- Training and attestation evidence showing personnel have been informed of relevant policies and procedures.
- Compliance and exception processes describing how adherence is monitored; how exceptions/waivers are requested, risk-assessed, time-bounded, approved; and how they are revisited/closed.
- Cross-references showing how policies and SOPs align with the Risk Management program and Incident Response, ensuring non-compliance items route to corrective action and/or formal risk acceptance.

AT&T Response:

Comply.

AT&T maintains a comprehensive cybersecurity policy and procedures framework governing NGCS platforms and the ESInet. Policies may be consolidated or standalone, but each includes defined purpose, scope, roles and responsibilities, approval authority, version control, distribution, and compliance expectations. Policies are formally approved, communicated to personnel, and reviewed on a defined cadence, at least annually or upon material change, to address evolving technologies, threats, and operational requirements.

AT&T's security policies are supported by documented Standard Operating Procedures (SOPs) that translate policy requirements into repeatable operational tasks, including user onboarding, vendor and remote access, incident handling, and recovery activities. SOPs are maintained under formal governance, including



authorship, approval, version control, authoritative storage, and periodic review, with defined triggers for out of cycle updates.

Applicable security policies and requirements are flowed down contractually to vendors, contractors, and subcontractors supporting NGCS and ESInet services. Compliance is reinforced through contractual obligations, governance processes, and oversight mechanisms.

Personnel receive role appropriate security training and are required to acknowledge applicable policies and procedures. Intrado maintains compliance monitoring and exception management processes to track adherence, evaluate and approve time bound exceptions based on risk, and ensure findings are remediated or formally accepted.

Security policies and SOPs are aligned with Intrado's risk management and incident response programs to ensure non compliance is routed through corrective action processes or formal risk acceptance, as appropriate.

4.1.3.1. Incident Response Plans

Early detection and disciplined response are essential to protect NG911 operations. Detection should use tooling (e.g., SIEM, IDS/IPS) and informed personnel, with trained staff triaging scope and impact. The contractor must maintain a formal, written **Cybersecurity Incident Response Plan (CIRP)** that is adaptable, periodically evaluated and tested, and staffed by trained responders. The CIRP should follow **Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity** and define when and how to engage external resources.

Because NG911 must continue answering calls and dispatching responders even under attack, recovery planning must be rigorous. The contractor must maintain **Business Continuity (BC)** and **Disaster Recovery (DR)** plans (separate or combined; separate recommended), store all plans offline yet accessible to recovery teams, and review/test at least annually, updating plans as needed.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A CIRP aligned to Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post Incident Activity, with incident declaration/classification criteria and communications/notification procedures.
- Detection capabilities and processes showing how SIEM, IDS/IPS, and staff reports enable early detection; include triage workflows, severity classification, and criteria to escalate to incident status.
- Training and exercise evidence for personnel with plan duties and proof the CIRP is tested (tabletop/live); include after-action reviews and documented improvements.



- A Business Continuity (BC) Plan for maintaining critical services during and after disruption.
- A Disaster Recovery (DR) Plan detailing IT restoration and coordination with ongoing mission-critical operations.
- Plan maintenance & accessibility controls proving CIRP/BC/DR are maintained offline yet readily accessible to recovery teams, with clear ownership, version control, and distribution.
- Review and test cadence showing at least annual reviews/tests of CIRP/BC/DR, with triggers for interim updates and documented results.
- Containment and recovery playbooks/SOPs translating plans into actionable steps for common scenarios (malware/ransomware, denial of service, critical service outage), including initial containment, eradication, service restoration, and lessons learned.
- External assistance procedures specifying when/how outside help is engaged, required approvals, and current contact lists/resources.

AT&T Response:

Comply.

AT&T maintains a formal, written Cybersecurity Incident Response Plan (CIRP) that defines roles, responsibilities, and procedures aligned to Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post Incident Activity. The CIRP includes incident classification criteria, escalation thresholds, and internal and external communication and notification procedures.

AT&T utilizes centralized security monitoring capabilities, including SIEM and network security tooling, supported by trained personnel to enable early detection, triage, severity classification, and escalation of security events to incident status when warranted. Incident response personnel receive role-based training, and the CIRP is periodically exercised through tabletop and/or operational testing, with after action reviews and documented improvements.

AT&T maintains Business Continuity (BC) and Disaster Recovery (DR) plans to ensure the continued operation and restoration of mission critical NG9 1 1 services during and after disruptive events. These plans are reviewed and tested at least annually, stored offline yet accessible to authorized recovery teams, and updated based on test results, technology changes, or emerging threats.

Containment and recovery procedures are supported by documented playbooks and SOPs for common scenarios, including denial of service events, malware, and critical service outages. Procedures define containment, eradication, service restoration, and lessons learned activities.

AT&T maintains defined processes for engaging external resources, including security vendors and service providers, when required, with appropriate approvals and maintained contact information.



4.1.4. Authorization and Data Rights Management

The contractor must enforce **XACML 2.0-based authorization** for all NG911 interfaces and protected data. Policies must evaluate **subject, resource, action, and context attributes**; be stored in a **Policy Store** (§E-2.2.1.1); decided by a **Policy Decision Point (PDP)**; and enforced at a **Policy Enforcement Point (PEP)**. Interfaces and data must use consistent names (NENA-STA-010.3 §10, et seq.). Actions must be explicit – **Read, Create, Update, Delete, Execute** – with **permit/deny rules** and an **explicit default rule** for every policy set.

Provisioning data is owned by the agency that operates the element and must be governed by **data rights management**. Each XACML policy must be **packaged as a JWS** and **signed by the policy owner**, including the **signing certificate and full chain** for validation.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Authorization architecture showing XACML 2.0 components, PDP placement, and how authorization is invoked on all NGCS/ESInet interfaces and protected data paths.
- Policy naming conventions & registries usage, including:
 - Interface policy names derived from ServiceID, and an interface keyword (NENA-STA-010.3 §10.30) formatted ServiceID~keyword (e.g., [LoST~ecrf.state.pa.us](https://www.lostecrf.state.pa.us))
 - Data item names derived from OpenAPI JSON object names and optional element tags, using dot notation (e.g., `civicAddr.A3`, or `<eido.AgencyDataComponent.AgencyName>`)
 - Mapping to the Policy Type Registry (NENA-STA-010.3 §10.33)
- Action model defining Read, Create, Update, Delete, Execute, with examples showing how each applies to representative Interfaces and data structures.
- Example XACML policy sets for:
 - One or more interfaces
 - One or more data structures
 - Each example policy set provided must include permit/deny rules, an explicit default rule, and attribute conditions (subject/resource/action/date/time as applicable).
- JWS packaging & validation: how the policy owner signs policies; how the certificate and chain are included (by value or reference); how PEP/PDP validate signatures (CRL/OCSP) and how key rotation and revocation are handled.
- Data rights management procedures establishing ownership of provisioning data and how ownership is enforced in policy.



- Policy lifecycle controls: authoring, peer review, change management, pre-production testing/evaluation, promotion, versioning, rollback, archival; include who is authorized to sign and publish policies.
- Logging & auditability: decision logs at PEP/PDP, retention, and procedures for reviewing denied/exception events.
- Performance & availability targets: PDP availability/latency, decision/policy caching (TTL/invalidations), and fail-secure behavior if policies or validators are unavailable.

AT&T Response:

Comply.

AT&T ESInet fully complies with the requirement to enforce XACML 2.0–based authorization across all NG911 interfaces and protected data. Authorization is implemented using an attribute-based access control (ABAC) model that evaluates subject, resource, action, and contextual attributes for every access request.

Authorization enforcement is implemented using standard XACML components:

- Policy Enforcement Points (PEPs) embedded within NGCS services and data access paths intercept all access requests.
- A centralized Policy Decision Point (PDP) evaluates authorization requests against applicable XACML policies.
- A Policy Store persists and retrieves XACML policies used for evaluation.
- Policy administration and attribute resolution functions support policy authoring, validation, and evaluation.

Authorization is invoked on all NGCS/ESInet interfaces and protected data paths. The PDP may be deployed within the same security domain as the enforcing service or as a dedicated service, consistent with NENA i3 guidance.

AT&T enforces consistent resource naming aligned with NENA STA 010.3 registries:

- Interface policies are named using the ServiceID and Interface Keyword registry, formatted as ServiceID~InterfaceKeyword (e.g., LoST~ecrf.state.ne.us).
- Data resources are named using OpenAPI JSON object names and optional element tags with dot notation (e.g., civicAddr.A3 or <eido.AgencyDataComponent.AgencyName>).
- All policies map to defined Policy Types from the Policy Type Registry, ensuring consistent identification and enforcement.

The AT&T solution implements the complete explicit action model required by i3:



- Read
- Create
- Update
- Delete
- Execute

Each authorization request explicitly declares the action being attempted. XACML policy sets include permit and deny rules for applicable actions and require an explicit default rule to ensure deterministic enforcement.

AT&T supports XACML policy sets for both interfaces and data structures, including:

- Interface level policies governing NG911 service access
- Data level policies governing entire data structures or specific elements
- Attribute based conditions evaluating subject identity, agency, role, agency type, resource identifiers, actions, and context

Each policy set includes explicit permit and deny rules and a mandatory default rule.

All XACML policies are packaged as JSON Web Signatures (JWS) and:

- Are signed by the policy owner
- Include the signing certificate and full certificate chain, provided by value or by reference
- Are validated by enforcing and decision components prior to use

This ensures policy integrity, authenticity, and non-repudiation.

Provisioning data is owned by the agency operating the element, or by the agency contracting for that operation. Data ownership is enforced directly in XACML policies using subject and resource attributes. Only the owning agency, or explicitly authorized delegates, may create, update, or delete provisioning data.

AT&T enforces controlled policy lifecycle management, including:

- Policy authoring by authorized entities
- Validation and integrity checks prior to acceptance
- Controlled publishing to the Policy Store
- Versioning, change management, rollback, and archival

Only authorized policy owners may sign and publish policies, enforced through certificate-based identity and ownership controls.



Authorization decisions are logged at both the Policy Enforcement Point and the Policy Decision Point, supporting auditability and compliance. Logged events include permit, deny, and exception outcomes. Logging behavior, signing requirements, and retention are governed by agency policy. AT&T supports configurable log retention by jurisdiction, with a default of seven years.

The authorization architecture is designed for high availability and low latency, including:

- A dedicated PDP service with configurable timeouts
- Support for policy and decision caching
- Granular enablement of authorization per interface
- Fail secure behavior, ensuring access is not granted when policies, validators, or trust chains are unavailable unless explicitly configured otherwise

4.2. Information System Infrastructure and Management

4.2.1. Device Inventory

The contractor must maintain a **continuously updated inventory** of all **devices, software/applications, software libraries, data sets, and cloud/third-party services** that support the NGCS platform and the ESInet. Use automated discovery and reconciliation where possible to keep records accurate, quickly identify unauthorized items, verify patch/firmware levels, and support zoning/segmentation. If full visibility is limited by span of control or contracts, clearly define what is in scope, assumptions, and responsibilities. Inventory outputs must inform critical impact analysis (BC/DR inputs) and drive trusted vs. untrusted zone design and controls at all ingress/egress points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Inventory management approach describing data sources, automated discovery tools/processes (where used), manual reconciliation, update frequency, and how unauthorized/unknown items are identified and removed or quarantined.
- Scope and span-of-control statement clarifying which assets/services fall under the Provider vs. the Customer or other vendors; include contractual boundaries, dependencies, and any blind spots.
- Comprehensive inventory documentation should identify sufficient detail – at minimum, documenting inventory elements identified in NENA-STA-040.2 §5.4 – for all aspects of NGCS and ESInet infrastructure.

Classification linkage showing how inventories map to the provider's data classification policy and define required protections.



Impact analysis methodology showing how the inventory feeds critical impact analysis and integrates with Business Continuity and Disaster Recovery planning

- Zoning/segmentation mapping that uses the inventory to define trusted vs. untrusted zones and sets control placement and rule scope at all ingress/egress points.
- Governance & lifecycle controls for the inventory: ownership, update cadence, audit/attestation of accuracy, change triggers, reconciliation with change management processes, and evidence of periodic cleanup of stale records.

AT&T Response:

Comply.

AT&T maintains a continuously updated, authoritative inventory of all assets that support the NGCS platform and the ESInet. The inventory encompasses devices, software/applications, software libraries, data sets, and cloud or third party services and is designed to support security monitoring, patch and firmware verification, zoning/segmentation, and critical impact analysis for Business Continuity (BC) and Disaster Recovery (DR). Where full visibility is constrained by contractual or operational boundaries, AT&T clearly defines scope, assumptions, responsibilities, and residual risks.

4.2.2. Patching and Update Management

The contractor must implement a disciplined, **change-managed patching program** covering **firmware, hardware drivers, operating systems, applications, and middleware**. The program must take in vendor, CERT, or other security advisories, use a common severity scale (e.g., Common Vulnerability Scoring System [CVSS]) to set priority, and check the environment for indicators of compromise (IoC) when a vulnerability is disclosed. Patching must be timely and paired with post-patch verification. The program should align with timelines and processes defined in NENA-STA-040.2 §5.5.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A process to validate – at least monthly – that all required patches are installed across in-scope hardware and software (plus event-driven checks upon major vulnerability disclosures).
- A change-managed deployment workflow ensuring approved and appropriately tested mitigations/patches are applied as soon as possible, with defined rollback steps.
- Post-patch verification to confirm remediation and to check for exploitation and/or other IoCs across the ESInet and NGCS.
- A CVSS-based timeline policy that sets SLAs by severity/criticality (e.g., critical expedited; target ≤ 48 hours from disclosure or patch availability), and an emergency change path.



- Evidence of advisory intake and triage, including how severity, affected scope, available mitigations, and permanent vs. temporary fixes are evaluated and tracked.
- Exception handling with compensating controls when patches cannot be applied immediately, with documented risk acceptance under the Entity's risk management process.
- Reporting and metrics showing patch compliance, age of open findings by CVSS band, time-to-patch, and reconciliation with the inventory/CMDB to ensure complete coverage.

AT&T Response:

Comply.

AT&T maintains a disciplined, security driven patching and update management program for all NGCS and ESInet components that aligns with NENA STA 040.2 §5.5. The program incorporates continuous advisory intake, CVSS based prioritization, change managed deployment, post patch verification, and enterprise level reporting to ensure vulnerabilities are remediated quickly without compromising NG911 availability. Patching activities are fully integrated with AT&T's inventory, change management, incident response, and risk management processes.

Patch Validation and Coverage Assurance

AT&T validates patch compliance across all in scope hardware and software at least monthly, supplemented by event driven validation when major vulnerabilities are disclosed.

- Automated checks compare deployed versions against approved baselines.
- Validation includes firmware, drivers, operating systems, applications, and middleware.
- Results are reconciled with the asset inventory/CMDB to ensure full coverage and identify gaps.

Change Managed Deployment Workflow

All patch and mitigation deployments follow AT&T's formal change management process.

- Patches are tested in non production environments prior to deployment.
- Deployment plans include impact assessment, scheduling, and communication.
- Rollback procedures are defined and approved before implementation.
- Emergency changes are supported when required to address active or high risk threats.

Post Patch Verification and IoC Checks

Following deployment, AT&T performs post patch verification to confirm:

- The patch or mitigation was successfully applied.



- The vulnerability has been remediated.
- The environment is checked for indicators of compromise (IoCs) related to the disclosed vulnerability.

Verification results are documented and retained for audit and compliance purposes.

CVSS Based Timeline Policy and Emergency Path

AT&T uses a CVSS aligned severity model to prioritize remediation and establish response timelines.

- Critical vulnerabilities are expedited, with a target of ≤ 48 hours from disclosure or patch availability where operationally feasible.
- High, medium, and low vulnerabilities follow defined remediation SLAs.
- An emergency change path allows accelerated action when risk to NG911 operations is elevated.

Advisory Intake and Triage

AT&T continuously monitors and ingests advisories from:

- Vendors and manufacturers
- CERT and other trusted security organizations
- Threat intelligence and vulnerability feeds

Each advisory is triaged to assess:

- Severity and CVSS score
- Affected scope within the NGCS/ESInet
- Availability of mitigations or workarounds
- Permanent versus temporary remediation options

Tracking continues until remediation or formal risk acceptance is complete.

Exception Handling and Compensating Controls

When a patch cannot be applied immediately (e.g., vendor dependency, operational constraint):

- The risk is documented and evaluated through AT&T's risk management process.
- Compensating controls (e.g., segmentation, access restrictions, monitoring) are implemented.
- Risk acceptance is formally approved, time bounded, and reviewed until the patch can be applied.

Reporting and Metrics



AT&T provides reporting and metrics to demonstrate patching effectiveness and compliance.

- Patch compliance status by asset class
- Age of open vulnerabilities by CVSS severity band
- Mean time to patch (MTTP)
- Reconciliation results against inventory/CMDB records

These metrics support operational oversight, audits, and continuous improvement.

4.2.3. Segmentation and Traffic Separation

The contractor must implement **domain-level network segmentation** to contain incidents, reduce lateral movement, and improve resiliency. Segmentation may be physical or logical (e.g., firewall-enforced choke points) and should extend to **zero-trust/micro-segmentation** at the endpoint or workload wherever feasible. Production and non-production (test/training) must be strictly separated so non-production activity cannot affect production services. **Development tools are prohibited in the production environment.** Within each environment, distinct traffic classes (e.g., call/signaling, management/monitoring, administrative) must be segregated and filtered (VLANs and/or dedicated equipment) with explicit allow-lists and firewall policy. Management/monitoring traffic must be out-of-band, normal traffic must not use the default VLAN, and configuration access to traffic-handling devices must use administrator-level accounts under appropriate controls.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A segmentation architecture showing production vs. non-production separation, inter-segment demarcation points, and isolation/containment controls.
- A traffic separation design identifying major traffic classes and how they are segregated and filtered.
- Evidence that production is protected from non-production, including controls preventing any nonproduction impact on production systems, and an explicit statement that no development tools exist in the production environment.
- Out-of-band management/monitoring implementation details and confirmation that normal traffic is not on the default VLAN.
- Administrative access controls for traffic-handling devices: administrator-level account use, authorization model, MFA, logging, and audit.
- Operational procedures/SOPs for change, testing, and validation of segmentation and filtering rules, including onboarding of new services without weakening isolation.



- Monitoring & alerting for policy violation and lateral movement detection within/across segments, with procedures for rapid containment.

AT&T Response:

Comply.

AT&T implements a layered, domain level network segmentation strategy across the NGCS platform and the ESInet to contain incidents, reduce lateral movement, and enhance resiliency. Segmentation is enforced using a combination of physical separation, logical controls, firewall enforced choke points, and workload level isolation.

Segmentation extends across environments (production vs. non production) and traffic classes within each environment, with explicit allow lists and deny by default controls. Production systems are strictly protected from non production activity, and development tools are prohibited from production environments.

Segmentation Architecture

AT&T's segmentation architecture establishes clear boundaries with controlled interconnections.

- Environment Separation
 - Production, test, training, and development environments are strictly segregated.
 - No direct network paths exist that allow non production traffic to affect production services.
- Demarcation Points
 - Inter segment communication occurs only at defined, firewall protected demarcation points.
 - Each demarcation enforces protocol, port, source, destination, and direction controls.
- Containment Controls
 - Segments are designed to localize faults or security events.
 - Compromise in one segment does not permit lateral movement into protected segments.

Traffic Separation Design

Within each environment, AT&T separates and filters major traffic classes.

- Primary Traffic Classes
 - Call processing and signaling traffic
 - Management and monitoring traffic
 - Administrative and support traffic
- Segregation Mechanisms



- VLANs and/or dedicated network equipment
- Firewall policies with explicit allow lists
- Role based access and protocol restrictions
- Filtering
- Deny by default posture between traffic classes
- Only explicitly authorized flows are permitted

Protection of Production from Non Production

AT&T enforces strict controls to ensure production integrity.

- Production systems cannot be accessed or influenced by non production environments.
- Test, training, and development activities are isolated and use separate tooling and infrastructure.
- No development tools exist in the production environment, and deployment pipelines prevent unauthorized tooling from entering production.

Out of Band Management and VLAN Controls

- Out of Band (OOB) Management
 - Management and monitoring traffic is carried on dedicated OOB networks.
 - OOB access is restricted to authorized management systems and personnel.
- VLAN Usage
 - Normal traffic is not permitted on the default VLAN.
 - Each traffic class uses explicitly defined VLANs or equivalent segmentation constructs.

Administrative Access Controls

AT&T applies strict administrative access controls to all traffic handling devices.

- Account Model
 - Administrator level accounts are used only for authorized management tasks.
- Authorization
 - Access is role based and aligned with least privilege principles.
- Authentication
 - Multi factor authentication (MFA) is required for administrative access
- Logging and Audit



- All administrative actions are logged and retained.
- Logs are reviewed to detect unauthorized or anomalous activity.

Operational Procedures and SOPs

AT&T maintains SOPs governing segmentation and traffic separation.

- Change Management
 - Segmentation and filtering rules follow formal change control.
- Testing and Validation
 - Changes are tested in non production prior to production deployment.
- Onboarding New Services
 - New services are introduced through controlled processes that preserve isolation.
 - Segmentation rules are reviewed to ensure no weakening of boundaries.

Monitoring and Alerting

AT&T continuously monitors segmentation effectiveness.

- Monitoring
 - Network monitoring tools observe traffic flows within and across segments.
- Policy Violation Detection
 - Alerts trigger on unauthorized traffic or attempted lateral movement.
- Rapid Containment
 - Defined procedures enable swift isolation of affected segments to protect NG911 operations.

4.2.4. Network Boundary Protection

Firewalls and Next Generation Firewalls (NGFWs) are key perimeter and inter-segment controls, but they are not the only defense. Internal systems must also be secure. The contractor must deploy a NENA-standard Border Control Function (BCF) or other boundary protections at all ESInet ingress/egress points and each segment entry/exit using explicit allow-lists that document required traffic and block all else. Specific BCF behaviors and requirements are identified in §E-2.1.1 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:



- A boundary architecture showing boundary controls (BCF or NGFW) at all ESInet ingress and segment entry/exit. The BCF must conform to requirements in §E-2.1.1 of this document.
- A traffic matrix for each firewall listing required services, ports, and protocols, with explicit allow rules; unnecessary traffic must be blocked by default.
- Performance & availability: high availability (HA) and/or failover capability, and traffic inspection features must be configured so boundary protections do not degrade service delivery capabilities.

AT&T Response:

Comply.

AT&T implements layered network boundary protections to secure all NGCS platforms and the ESInet. Boundary controls are deployed at every ESInet ingress and egress point and at each inter segment entry and exit to enforce strict traffic control, limit attack surfaces, and prevent lateral movement. While firewalls and Next Generation Firewalls (NGFWs) provide critical perimeter and segmentation enforcement, AT&T's approach recognizes that boundary protection must be complemented by internal controls and NENA standard functions to protect mission critical NG911 services.

AT&T deploys a NENA standard Border Control Function (BCF) or equivalent boundary protections at all required locations. These controls enforce explicit allow lists for required traffic and block all other traffic by default.

Boundary Architecture

AT&T's boundary architecture establishes controlled trust boundaries throughout the NG911 environment.

- ESInet Ingress/Egress
 - A BCF or NGFW based boundary protection is deployed at every point where traffic enters or exits the ESInet.
 - These boundaries protect interfaces with:
 - Originating Service Providers (OSPs)
 - Interconnected ESInets
 - External networks and services
- Inter Segment Boundaries
 - Boundary controls are also placed at each segment entry/exit within the ESInet and NGCS environments.
 - Segments are isolated using firewall enforced choke points to prevent unauthorized lateral movement.



- BCF Conformance
 - Where deployed, the BCF conforms to the requirements specified in §E 2.1.1 of this solicitation, including protocol normalization, security enforcement, and controlled session handling.

This architecture ensures that no traffic traverses a boundary without passing through an explicitly defined and monitored control point.

Traffic Allow Listing and Firewall Rules

AT&T enforces a deny by default posture at all network boundaries.

- Traffic Matrices
 - For each firewall or BCF instance, AT&T maintains a documented traffic matrix identifying:
 - Required services
 - Ports
 - Protocols
 - Source and destination zones
- Explicit Allow Rules
 - Only traffic required for NG911 operations is explicitly permitted.
 - All unnecessary or undocumented traffic is blocked.
- Change Control
 - Traffic matrices and allow lists are reviewed and updated through formal change management processes to ensure accuracy and continued alignment with operational needs.

Performance and Availability

Boundary protections are designed to preserve NG911 service quality and resiliency.

- High Availability and Failover
 - BCFs and NGFWs are deployed in high availability configurations with automatic failover.
 - Failure of a single boundary device does not interrupt call handling or signaling.
- Traffic Inspection
 - Security inspection features are configured to balance protection with performance.
 - Inspection does not introduce latency or degradation that would affect emergency call delivery.
- Resiliency Alignment
 - Boundary protections are integrated with ESInet redundancy and failover designs to maintain continuous service availability.



4.2.4.1. External Connections

NG911 relies on external connections; with these links often traversing the public internet, they must follow a zero-trust approach (NENA-STA-040.2 Appendix A & NIST Special Publication 800-207) and use layered protections. At minimum, each external connection must be protected by a boundary protection device conforming to requirements identified in §E-5.2.4 above, and any connection transporting sensitive information must use an encryption that conforms with the requirements identified in NENA-STA-040.2 §4.2.2.6 (Safeguarding Sensitive Electronic Information).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An external connectivity architecture listing counterparties, paths, and media, and how zero-trust principles are applied.
- Evidence that all external links are protected by a firewall with placement, explicit allow-lists, and default-deny posture per §E-5.2.4.
- An encryption approach for links carrying sensitive information, conforming to requirements of NENA-STA-040.2 §4.2.2.6, indicating where encryption is enforced.
- Operational controls for onboarding/approval, continuous monitoring, periodic review, and change/termination of external connections – consistent with zero-trust and boundary protection requirements.

AT&T Response:

Comply.

AT&T ESInet does not currently use any internet connectivity to support outside entities accessing the ESInet. This includes both OSPs, PSAPs, and third-party data providers. AT&T ESInet's external connectivity model follows a zero-trust architecture, with every connection to outside entities—such as OSPs, peer ESInets, or permitted Internet-facing interfaces—protected by a NENA compliant Border Control Function (BCF) deployed at all ESInet ingress/egress points. These boundary devices, built from SBC and firewall components, enforce a deny by default security posture with explicit allowlists, ensuring only vetted, PCA credentialed counterparties and documented services/ports are permitted.

Sensitive traffic—such as SIP signaling, LoST/HTTPS, LIS/ADR queries, and management interfaces—is encrypted end-to-end using TLS with mutual authentication. These boundary protections operate in active-active high availability configurations so that traffic inspection and security enforcement do not degrade call delivery or ESInet performance.



Operational governance of external links includes formal onboarding and approval, continuous monitoring via SIEM and IDS/IPS, periodic review of allowlists and boundary rules, and structured change/termination procedures under the system's ITIL based change management process.

4.2.4.2. Demilitarized Zones (DMZ)

Some NG911 services must be reachable from untrusted networks. Any externally accessible resource not otherwise protected by equivalent controls must reside in a Demilitarized Zone (DMZ) that is segments from internal NGCS/ESInet segments and mediated by a boundary protection device per §E-5.2.4 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DMZ architecture showing externally accessible resources, segmentation from internal networks, and firewall/SBC/BCF demarcation points.
- A traffic controls strategy for the DMZ: default-deny posture, explicit allow lists, tightly limited ingress/egress, and no lateral access to internal segments.
- Hardening & monitoring for DMZ assets: patch cadence, configuration baselines, centralized logging, telemetry, and alerting.
- Operational procedures for onboarding and retiring DMZ-hosted services, plus periodic reviews to confirm resources that require external access remain correctly isolated in the DMZ.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirements for the use of Demilitarized Zones (DMZs) to protect NG911 services that must be accessible from untrusted networks. AT&T isolates externally reachable resources in dedicated DMZs that are strictly segmented from internal NGCS and ESInet networks and mediated by boundary protection devices. This approach limits exposure, prevents lateral movement, and ensures that external access does not compromise core NG911 operations.

DMZ Architecture and Segmentation

AT&T implements a clearly defined DMZ architecture for all NG911 services that require external reachability and are not otherwise protected by equivalent controls.

- Externally accessible resources are deployed in a designated DMZ network zone.
- The DMZ is logically and/or physically segmented from internal NGCS and ESInet segments.



- All communication between the DMZ and other network segments is mediated through approved boundary protection devices, such as firewalls, SBCs, or NENA compliant BCFs, deployed in accordance with §E 5.2.4.
- Network demarcation points are documented to support visibility, troubleshooting, and audit.

DMZ Traffic Controls Strategy

AT&T enforces strict traffic controls for the DMZ to reduce attack surface and prevent unauthorized access.

- A default deny posture is enforced for all DMZ traffic.
- Explicit allow lists define permitted protocols, ports, source/destination pairs, and directionality.
- Ingress and egress traffic is tightly limited to only what is required for NG911 service delivery.
- No lateral access from the DMZ to internal NGCS or ESInet segments is permitted unless explicitly authorized and protected by boundary controls.

These measures ensure that compromise of a DMZ hosted asset does not provide a path to internal systems.

Hardening and Monitoring of DMZ Assets

All assets deployed in the DMZ are subject to enhanced hardening and continuous monitoring.

- Systems are built and maintained using approved secure configuration baselines.
- DMZ assets follow AT&T's disciplined patching and update cadence, consistent with NG SEC requirements.
- Logs and security telemetry from DMZ components are forwarded to centralized logging and monitoring platforms.
- Alerts are generated for anomalous behavior, policy violations, or suspected compromise, enabling rapid response.

Operational Procedures for DMZ Services

AT&T governs DMZ hosted services through defined operational procedures.

- Onboarding procedures validate the business need for external access and confirm that resources are correctly placed in the DMZ prior to activation.
- Retirement procedures ensure that decommissioned services are promptly removed and access paths closed.
- Periodic reviews confirm that only services requiring external access remain in the DMZ and that isolation controls remain effective.



These lifecycle controls ensure ongoing compliance with zero trust and boundary protection principles.

4.2.4.3. Defense in Depth

The contractor must apply Defense in Depth (DiD) – layered, overlapping controls that protect confidentiality, integrity, and availability across physical access, endpoints, data protection, boundary defenses, network and traffic separation, system monitoring, and (where applicable) vendor diversity. DiD ensures that if one control fails, others maintain security. Critical systems and sensitive information shall utilize Defense in Depth with deliberate redundancy and no single points of failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DiD architecture showing layered controls across the stack: physical access, endpoints, identity/authorization/authentication, boundary protections, and segmentation/traffic separation.
- A control-to-risk mapping for critical systems and sensitive data identifying how multiple independent controls address key threats, with no single-control dependencies.
- Failure mode and fallback analysis demonstrating how security is maintained if a layer is bypassed or fails.
- Operational integration with related sections (e.g., IAM/roles, segmentation, boundary protections, incident response, logging/monitoring), including runbooks for escalation between layers.
- Validation and review evidence and metrics showing layered control effectiveness over time.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska’s Defense in Depth (DiD) requirements for protecting NGCS and ESInet environments. AT&T applies overlapping, independent controls across physical, logical, and operational layers to protect the confidentiality, integrity, and availability of NG911 systems and data. This deliberate, multi layered approach ensures that no single control failure can compromise critical services or sensitive information.

Defense in Depth Architecture

AT&T implements a documented Defense in Depth architecture that applies layered controls across the full NG911 technology stack, including:

- Physical access controls for facilities and equipment supporting NGCS and ESInet services
- Endpoint and platform protections, including secure configuration baselines and patching



- Identity, authentication, and authorization controls, including role based access, least privilege, and MFA
- Boundary protections, such as firewalls, SBCs, and NENA compliant BCFs at ingress/egress points
- Segmentation and traffic separation, including internal zoning, DMZs, and monitoring planes

These layers operate together to prevent, detect, and contain threats while supporting uninterrupted emergency operations.

Control to Risk Mapping for Critical Systems and Data

For critical NG911 systems and sensitive information, AT&T applies multiple independent controls mapped to key risk scenarios.

- Risks such as unauthorized access, data exfiltration, service disruption, and lateral movement are addressed by overlapping safeguards.
- No critical function or dataset relies on a single security control for protection.
- Control mappings are documented to demonstrate how confidentiality, integrity, and availability are preserved even if one layer is degraded.

Failure Mode and Fallback Analysis

AT&T designs NGCS and ESInet environments with deliberate redundancy and resilience.

- Failure mode analysis identifies how a control could be bypassed, misconfigured, or fail.
- Compensating controls at other layers maintain security posture during such events.
- Architectures are designed to avoid single points of failure, particularly for systems supporting call routing, policy decision making, and access control.

This ensures continuity of NG911 services even during adverse conditions.

Operational Integration and Runbooks

Defense in Depth is fully integrated with AT&T's operational processes and related technical domains.

- DiD controls align with identity and access management, segmentation, boundary protection, incident response, and logging/monitoring functions.
- Operational runbooks define escalation paths and response actions between layers when anomalies or control failures are detected.
- Integration ensures rapid detection, containment, and recovery without reliance on a single security mechanism.

Validation, Review, and Metrics

AT&T validates the effectiveness of layered security controls on an ongoing basis.



- Monitoring and logging provide visibility across all layers of defense.
- Periodic reviews assess whether controls remain effective as threats, technologies, or system architectures evolve.
- Metrics and review results are used to drive continuous improvement and demonstrate sustained compliance with DiD principles.

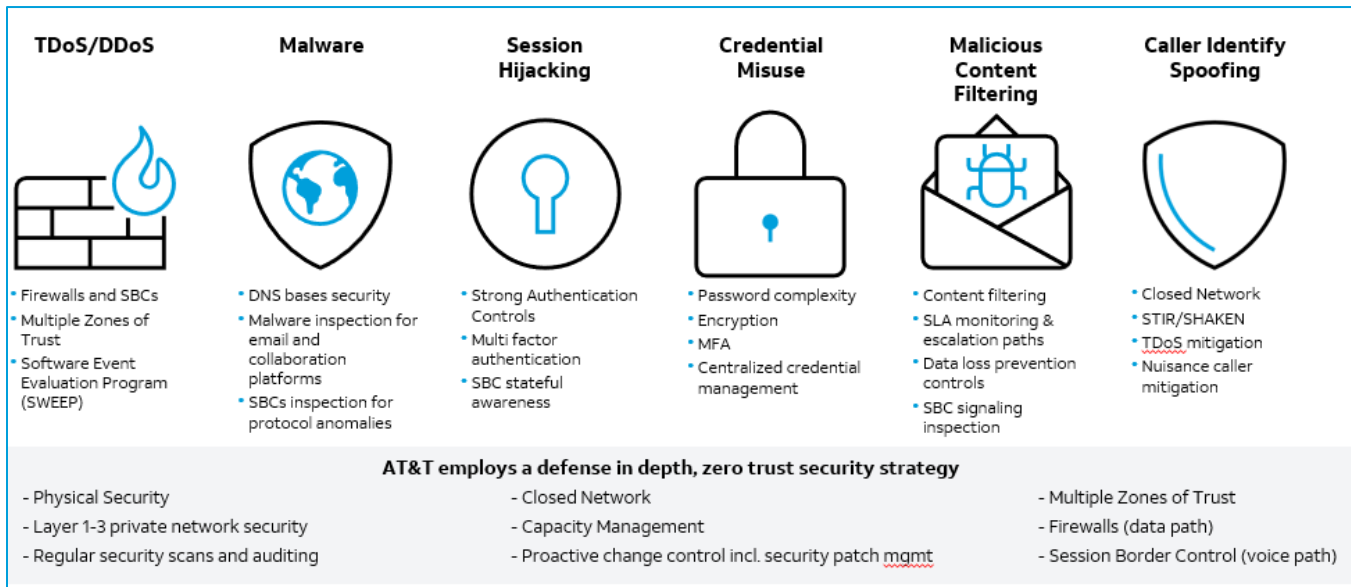


Figure 27: Security and Trust Framework

4.2.4.4. Remote Access

Remote access connects users to systems outside a physical location. External remote access carries the highest risk and must be allowed only for documented business need, routed through authorized, secured, encrypted connections (e.g., VPN aligned to NIST SP 800-77), and enforced with strong authentication and centralized logging.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Access control & eligibility: Processes ensuring external remote access is granted only for valid business need, with at least annual account reviews and timely removal when no longer required.
- Secure connectivity: Use of an authorized, encrypted connection for all external remote access. MFA must be implemented for all remote connectivity.
- Operational governance: SOPs for requesting, approving, establishing, and terminating remote access, plus periodic tests/reviews to confirm controls remain effective.
- Logging & monitoring: centralized logging for remote connectivity in conformance with minimum requirements identified in NENA-STA-040.2 §6.17.



AT&T Response:

Comply.

External remote access is tightly controlled and allowed only for documented business need that require non shared credentials, RBAC with least privilege, and periodic privilege reviews for all administrative and operational accounts. Account eligibility and continuation are evaluated through recurring access reviews, and permissions are revoked promptly when no longer required.

All remote access must occur over an authorized, encrypted connection, using TLS protected channels and mutual authentication certificates traceable to the PCA. Administrative and remote sessions require MFA, unique identities, and certificate based trust; remote connectivity is prohibited without these protections.

Operational governance—including request, approval, establishment, and termination of remote access—is handled through the ITIL aligned change management and identity management procedures. These include ticketed onboarding, authorization workflows, and the same strict identity lifecycle controls applied to all privileged accounts. Periodic reviews and tests ensure that remote access mechanisms remain secure and correctly enforced.

All remote-access activity feeds into the system’s centralized SIEM, which aggregates authentication logs, session records, and anomaly alerts in alignment with NENA STA 040.2 §6.17–style monitoring expectations. Sessions are continuously audited, with alerts generated for failed authentication, unexpected connectivity, or access outside approved roles or time windows.

4.2.5. Infrastructure Resilience

Mission-critical NG911 functions must remain available despite single-component failures and localized outages. The contractor must employ redundancy and diversity across the ESInet and NGCS, through the deployment of high availability mechanisms with supported infrastructure where appropriate. Because infrastructure failures can drop in-progress sessions, applications and signaling must gracefully recover during a path or site failure. NGCS/ESInet components must be both redundant and diverse, and ingress traffic must enter the NG911 system through diverse paths. (Additional redundancy guidance in NENA-STA-010.3 §2.9)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An end-to-end High Availability (HA) architecture showing redundant components and physically diverse ingress/egress, transport, facilities, and power; include call/signaling paths proving diverse 911 call entry.
- Component-level HA designs with health checks, failover criteria, and state synchronization.
- A diversity plan detailing route/provider diversity, facility/region separation, and power diversity.



- Application/session continuity methods that demonstrate graceful recovery during device/site failover.
- Testing & exercise evidence for failover/fallback, with measured recovery objectives and tracked corrective actions.
- Operations & monitoring for infrastructure health; maintenance procedures that avoid creating single points of failure during changes, and SOPs for failure scenarios.

AT&T Response:

Comply.

External remote access is tightly controlled and allowed only for documented business needs that require non shared credentials, RBAC with least privilege, and periodic privilege reviews for all administrative and operational accounts. Account eligibility and continuation are evaluated through recurring access reviews, and permissions are revoked promptly when no longer required.

All remote access must occur over an authorized, encrypted connection, using TLS protected channels and mutual authentication certificates traceable to the PCA. Administrative and remote sessions require MFA, unique identities, and certificate based trust; remote connectivity is prohibited without these protections.

Operational governance—including request, approval, establishment, and termination of remote access—is handled through the ITIL aligned change management and identity management procedures. These include ticketed onboarding, authorization workflows, and the same strict identity lifecycle controls applied to all privileged accounts. Periodic reviews and tests ensure that remote access mechanisms remain secure and correctly enforced.

All remote-access activity feeds into the system's centralized SIEM, which aggregates authentication logs, session records, and anomaly alerts in alignment with NENA STA 040.2 §6.17–style monitoring expectations. Sessions are continuously audited, with alerts generated for failed authentication, unexpected connectivity, or access outside approved roles or time windows.

4.3. Authentication and Federated SSO

Agent authentication across NG911 must use federated Single Sign-On (SSO) based on OASIS SAML v2.0. Identity Providers (IdPs) authenticate agents and issues assertions to Relying Parties (RPs) for authorization. For HTTP-bound apps, IdPs and RPs must support Web Browser SSO, Identity Provider Discovery, and Single Logout; ECP and Artifact

Resolution may be supported. SAML metadata should be aggregated under one `<EntitiesDescriptor>` and digitally signed by an identified administrative body using a well-known certificate to bootstrap trust.



For session establishment between agents and elements, SSO authenticates the agent and unlocks the agent's private key; the agent's X.509 certificate is then used to form the TLS session. For SIP and HTTPS, mutual TLS (mTLS) must be used with certificates traceable to the PCA for agents, agencies, and elements. RSA-2048 must be supported and accepted and accepted ESInet-wide (alternatives may be accepted only if cryptographically equivalent to, or stronger than RSA-2048). Each IdP must enforce multifactor authentication (MFA) for agents using a combination of at least two (additional factors preferred) of the following: password, token, smart card, or biometrics. Offline or other locally available backup authentication methods should be implemented for use if network access to primary authentication methods is unavailable. **The Respondent must provide a description and/or documentation that supports the requirements in this section:**

- An SSO architecture showing IdP(s), RPs, and assertion flows; conform all agent operations requiring authorization rely on SAML v2.0
- mTLS designs for SIP and HTTPS using PCA-traceable certificates for agents, agencies, and elements; include trust anchors, path validation, and revocation checks.
- A cryptographic baseline confirming RSA-2048 support and acceptance ESInet-wide and policy for accepting alternatives only if equivalent to, or stronger than RSA-2048.
- IdP MFA enforcement: supported factors, enrollment of multiple factors, and backup local authentication.
- The TLS establishment flow where SSO authentication unlocks the agent's private key used with the agent's certificate to negotiate the TLS session.
- Operational controls: onboarding/offboarding, key & certificate lifecycle, assertion & metadata signing key rotation, and monitoring/logging of authentication events.

AT&T Response:

Comply.

AT&T ESINET complies with NENA-STA-040.2-2024 NG-SEC security standard and applicable areas of the CJIS Security Policy. The solution incorporates physical, network, and application security principals. Each core site, including the associated information security infrastructure, resides in highly secure AT&T data centers, with physical access limited to only authorized personnel whose job responsibilities require interaction with the physical components of the call processing environment. 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.

Secure communications are retained through the following measures (among others)

- Rivest–Shamir–Adleman (RSA)-based public-key cryptography using 509 certificates to authenticate elements, agencies, and agents. Mutual authentication must exist between both ends of a



communication. - Intrado manages credentialing and issuing digital certificates to help ensure protection and security as defined within NENA-STA-010.

AT&T verifies credentialed devices or that carriers are authorized access in the following manner:

- Client certificates are issued by a trusted Certificate Authority (CA) are required in order to access I3 services
- AT&T validates all x.509 certificates with a trusted, key signing, CA

All systems utilize the highest capabilities of protection and authentication available, including IPsec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification. Interactions with external entities such as ECRFs, Terminating ESRPs (CPE) will utilize digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA).

Advanced Encryption Standard (AES)-based encryption to provide confidentiality - AT&T employs AES-256 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. All backups are encrypted at the hardware level during the tape writing process.

AT&T has a Cryptography Policy to ensure that appropriate cryptographic safeguards are in place to protect AT&T data against loss, unauthorized access, or disclosure.

AT&T 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 AT&T 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 AT&T systems through approved software.

Operating system and application protections are configured for segregation of duties, and strong password policies are enforced to ensure that password length and minimum change restrictions are followed, including those above. Strict auditing controls are enforced across the enterprise. Remote access to the AT&T ESINET



network is permitted providing those authorized users are authenticated, and privileges are restricted. Remote access is only permitted via a secure VPN client, via equipment which utilizes an approved firewall, anti-virus protection, up-to-date patching levels, and strong authentication using two factors for authentication. Any connections over the Internet employ a VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH). Administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform their duties. In addition, the AT&T ESInet utilizes passive vulnerability monitoring in order to detect anomalous network traffic or known signatures of known threats.

Specifically, AT&T ESInet uses Entrust to support Single Sign-On requiring two factor authentication using hardware based or application-based token generation algorithms which are validated prior to users accessing ESInet applications and especially when originating from untrusted networks using the protections previously stated above.

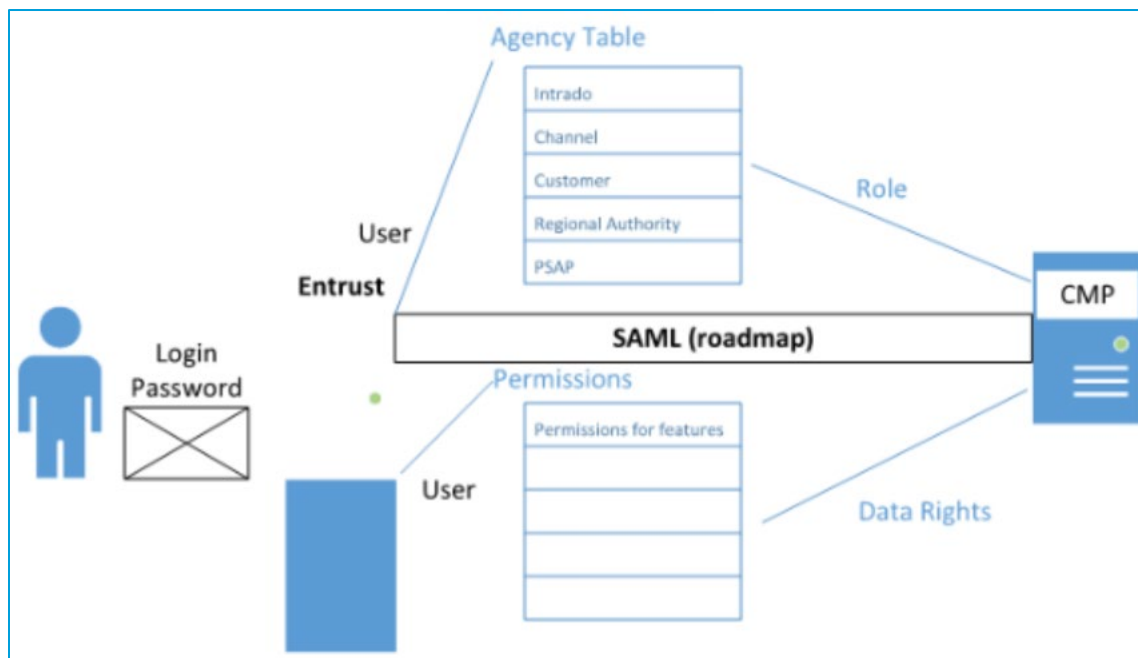


Figure 28: Single Sign-On

Regarding implementation of SAML for SSO functionality, as noted in the graphic above, AT&T will be transitioning to SAML. This will provide the Permissions and Agency Tables that will establish the proper role and data rights to AT&T Customer Management Portals or any required AT&T ESInet application.

TLS sessions are tied to SSO authentication using HTTPS access and the authentication process previously stated using Entrust Single Sign-On with two factor authorizations using hardware or application-based token generation algorithms.



The operation of Single Sign-On requires a process where authorized users are authenticated, and privileges are restricted to applications and information levels with a need to know or access as part of their job function. Remote access is only permitted via a secure VPN client, via equipment which utilizes an approved firewall, anti-virus protection, up-to-date patching levels, and strong authentication using two factors for authentication. Any connections over the Internet employ a VPN client. Remote access to perform systems administration tasks is achieved over Secure Shell (SSH). Administrators follow the principle of least privilege to ensure that all user accounts only have the necessary privileges to perform their duties. In addition, the AT&T ESInet utilizes passive vulnerability monitoring in order to detect anomalous network traffic or known signatures of known threats.

Regarding certificates that are traceable to the PCA, once the NIOC finalizes the process to allow AT&T ESInet to obtain PCA certificates, AT&T will use and begin replacing previous non-PCA certificates with PCA certificates for all relevant End-Entities (EE) requiring them.

4.4. Cryptography and Public Key Infrastructure

Cryptography in NG911 primarily secures connections and proves identity: asymmetric keys/X.509 certificates authenticate endpoints and establish sessions; symmetric ciphers then protect data in transit. The NG911 PKI is PCARooted: the PSAP Credentialing Agency (PCA) issues subordinate CA certificates to ESInet-operated Intermediate CAs (ICAs). Approved ICAs may, in turn, issue end-entity certificates to NGCS/ESInet service elements, and personnel. Full controlling specifications for the NG911 PKI are: NG911 Interoperability Oversight Commission (NIOC) PSAP Credentialing Agency Certificate Policy, and NIOC PSAP Credentialing Agency Certificate Validation Policy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PKI trust architecture showing the PCA root, Contractor-operated ICA(s), end-entity certificate issuance, and provision for subordinate ICA implementation and certificate issuance.
- Operational practices for certificate lifecycle and key management, including how asymmetric authentication bootstraps TLS/mTLS and how symmetric session keys are negotiated.
- Certificate profiles & example chains demonstrating path validation to the PCA, with revocation checking and trust-anchor management
- Conformance statements confirming acceptance of PCA-rooted RSA-compatible credentials, consistent with the controlling specifications from the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy.
- TLS alignment: where and how TLS/mTLS is enforced across NGCS/ESInet interfaces showing asymmetric establishment and symmetric protection in session.



AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's Cryptography and Public Key Infrastructure (PKI) requirements for NGCS and ESInet operations. AT&T will implement a PCA rooted PKI trust architecture that uses asymmetric X.509 certificates for identity authentication and session establishment, with symmetric cryptography protecting data in transit. All cryptographic operations align with the NIOC PSAP Credentialing Agency Certificate Policy and Certificate Validation Policy, ensuring secure, interoperable, and verifiable trust relationships across NG911 elements, agencies, and personnel.

PKI Trust Architecture

AT&T implements a documented PKI trust architecture rooted in the PSAP Credentialing Agency (PCA).

- The PCA serves as the root of trust.
- AT&T operates one or more Intermediate Certificate Authorities (ICAs) under PCA governance.
- Approved ICAs issue end entity certificates to NGCS and ESInet service elements and authorized personnel.
- The architecture supports the implementation of subordinate ICAs, if required, in accordance with PCA policy and oversight.

Certificate Lifecycle and Key Management Practices

AT&T maintains disciplined certificate lifecycle and key management practices.

- Certificates are managed through issuance, renewal, rekeying, suspension, and revocation processes aligned to PCA and NIOC requirements.
- Private keys are generated, stored, and protected using industry standard cryptographic controls.
- Asymmetric authentication (X.509 certificates) is used to bootstrap TLS and mutual TLS (mTLS) sessions.
- During TLS establishment, symmetric session keys are securely negotiated to protect NG911 data in transit.

Certificate Profiles and Validation

AT&T provides certificate profiles and example certificate chains demonstrating proper validation.

- Certificate chains validate to the PCA root through authorized ICAs.
- Trust anchors are explicitly managed and protected.
- Revocation status is verified using approved mechanisms (e.g., CRLs and/or OCSP).



- Certificate profiles conform to the controlling specifications defined by the NIOC and PCA.

Conformance to PCA and NIOC Policies

AT&T provides formal conformance statements attesting that:

- PCA rooted, RSA compatible credentials are accepted and enforced ESInet wide.
- All cryptographic and PKI operations are consistent with the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy.
- Self signed certificates are not used for NG911 communications that traverse the ESInet.

TLS and mTLS Enforcement

AT&T clearly defines where and how TLS and mTLS are enforced throughout the NGCS and ESInet.

- TLS/mTLS is applied at SIP, HTTPS, API, and management interfaces, as appropriate.
- Asymmetric cryptography is used during session establishment to authenticate endpoints.
- Symmetric encryption protects data once the secure session is established.
- This approach ensures confidentiality, integrity, and peer authentication across all NG911 communications.

4.4.1. Cryptographic Keys

Cryptographic keys underpin identity and data protection in NG911. Keys are algorithm-specific and generated by approved processes. For asymmetric key pairs, the public key is submitted to a CA for inclusion in an X.509 certificate and the private key is securely stored. Private and symmetric keys must be protected against loss, corruption, and unauthorized access, with periodic access reviews. Private keys should be classified as 'Sensitive (Most Sensitive Information)' in alignment with NENA-STA-040.2 §4.2.2.1.4, or at a comparable level that aligns with the contractor's existing data classification schema. Private keys must be revoked and reissued if compromised, or if compromised is suspected. Cryptographic key implementations must adhere to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy and align with the NENA i3 Standard (NENA-STA-010.3) and NIST SP 800-57 Part 2 Rev. 1 (Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Key generation & issuance procedures: how keys are generated, how public keys are submitted to the CA, and where/how private keys are stored.
- A classification statement designating private keys as 'Sensitive (Most Sensitive Information),' or similar, and the technical/administrative controls that enforce this classification.



- Access control & periodic review: who/what can access keys, authentication required, separation of duties, and the cadence/mechanics of access recertification.
- Key protection measures for storage/backup/restore, including protections at rest and in use, and configuration practices consistent with current TLS guidance.
- A compromise response plan detailing detection, revocation, re-issuance, distribution, and restoration steps when keys are, or suspected to be, compromised.
- Lifecycle management covering creation, distribution, rotation, archival and destruction, with logging/audit trails sufficient for compliance and forensics.
- Conformance attestations to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirements for cryptographic key management within NGCS and ESInet environments. The NIOC PCA Certificate Policy and Validation Policy, NENA STA 010.3 (i3), NENA STA 040.2, and NIST SP 800 57 Part 2 Rev. 1, AT&T employs controlled, auditable processes for cryptographic key generation, protection, access, and lifecycle management. Private keys are treated as highly sensitive assets, safeguarded against compromise, and promptly revoked and reissued when compromise is suspected, ensuring continued trust and integrity across NG911 communications.

4.4.2. Use of Self-Signed Certificates

Self-signed certificates **MUST NOT** be used for any NG911 communications that traverse an ESInet. All communications must use certificates traceable to the PCA root. External entities that are not in the PCA-traceable PKI must present certificates issued by a reputable public Certificate Authority. This ensures peer identity is validated through a recognized trust chain and prevents unauthenticated endpoints from participating in NG911 exchanges.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A certificate policy and enforcement plan affirming no self-signed certificates within or between ESInets and that NGCS/PSAP elements use PCA-anchored certificates.
- External entity onboarding requirements stating non-PCA participants must use Public CA certificates, and how this is verified during trust establishment.
- Trust store and path-validation configuration for SIP, HTTPS, APIs, and management interfaces, accepting only PCA-anchored chains (or approved public CA chains) with CRL/OSCP checks.



- An asset/certificate inventory and automated detection controls to identify and block self-signed or untrusted certs.
- An exception policy confirming there are no exceptions for self-signed certificates on ESInet-traversing communication, including test and non-production environments.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's prohibition on the use of self-signed certificates within NG911 environments. AT&T enforces a strict certificate policy that disallows self-signed certificates for any communications that traverse an ESInet. All NGCS, ESInet, and PSAP elements use certificates traceable to the PCA root, and external entities are required to present certificates issued by an approved public Certificate Authority. This approach ensures authenticated peer identity, prevents unauthorized endpoints from participating in NG911 exchanges, and maintains a consistent, trusted security posture statewide.

4.5. Integrity Protection

All NG 911 protocol operations must be integrity-protected with TLS, using SHA-256 or stronger (FIPS PUB 180-4); SHA-256 must be supported by all implementations. These controls make messages and media tamper-evident end-to-end. **The Respondent must provide a description and/or documentation that supports the requirements in this section:** • An integrity protection design confirming TLS deployment on all NGCS/ESInet protocol exchanges with SHA256, and network-wide support for SHA-256.

- Cipher/algorithm policy and configuration artifacts proving acceptance of SHA-256 and procedures to prevent/detect downgrades.
- Verification & monitoring: evidence that interfaces negotiate required integrity algorithms; ongoing checks to prevent regression.
- Exception handling for legacy interoperability (where deployed), with compensating controls and a timeline to reach full SHA-256 compliance.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirement that all NG911 protocol operations be integrity protected using TLS with SHA 256 or stronger. AT&T enforces TLS across all external NGCS and ESInet protocol exchanges to ensure end to end message and media integrity, making all signaling and data exchanges tamper evident. SHA 256 is universally supported and enforced as the minimum integrity algorithm across the environment, ensuring interoperability, regulatory compliance, and long-term cryptographic strength.



Secure communications are retained through the following measures (among others 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. - AT&T uses Intrado to manage credentialing and issuing digital certificates to help ensure protection and security as defined within NENA-STA-010.3-2021.

Intrado verifies credentialed devices or that carriers are authorized access in the following manner:

- Client certificates are issued by a trusted Certificate Authority (CA) are required in order to access I3 services
- AT&T validates all x.509 certificates with a trusted, key signing, CA

All systems utilize the highest capabilities of protection and authentication available, including IPsec and SSL VPN technology for remote access from un-trusted networks, SSH for encrypted management capability, and two-factor authentication for remote access to sensitive applications along with digital certificate verification. Interactions with external entities such as ECRFs, Terminating ESRPs (CPE) will use digital certificate-based authentication as defined by NENA and managed by the PSAP Credentialing Agency (PCA).

Advanced Encryption Standard (AES)-based encryption to provide confidentiality - AT&T employs AES-256 encryption-in-transit where possible on networks not under direct AT&T control. Encryption is achieved either using SSL/TLS or IPSEC VPN.

4.5.1. JSON Web Signatures (JWS)

The contractor must implement JWS exactly as specified in the NENA i3 Standard (NENA-STA-010.3 §5.10), including, but not limited to, serialization, algorithm, discovery, certificate/chain handling, and Logging Service provisions defined therein. This RFP does not restate i3's normative details; Respondents must conform to i3 requirements as currently defined.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to JWS requirements of NENA-STA-010.3 §5.10, plus a clause-by-clause matrix mapping the implementation to each i3 requirement.
- Operational policies reflecting i3 requirements and certificate/chain handling with long-term stability where applicable.
- Test/validation evidence showing interoperability and conformance with i3 JWS processing & verification across relevant services.

AT&T Response:



Comply.

AT&T fully complies with the State of Nebraska's requirements for the implementation of JSON Web Signatures (JWS) as defined in NENA STA 010.3 §5.10. AT&T implements JWS exactly as specified by the i3 Standard for message signing, verification, certificate and chain handling, discovery, and logging integration. JWS is applied in a standards conformant manner across relevant NGCS and ESInet services to ensure message integrity, authenticity, interoperability, and auditability without deviation from i3's normative requirements.

4.6. Information Privacy

All NG911 protocol operations must be privacy-protected in transit with TLS, and confidential data must be encrypted at rest, in conformance with the NENA i3 Standard and NG-SEC (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22). Implementations must support AES-256 (or stronger equivalent). Algorithms and key lengths must be chosen to protect data for the full retention period. Encryption keys must never be stored in plaintext; with access following a documented management policy – including strong passwords and multifactor authentication required for access. Alternative algorithms are acceptable only if cryptographically equivalent to, or stronger than, AES-256 with end-to-end interoperability support. The contractor should prepare for the ability to upgrade or replace encryption algorithms and parameters to ensure continued conformance with future updates to the NENA i3 and NG-SEC Standards. **The Respondent must provide a description and/or documentation that supports the requirements in this section:**

- A statement of conformance to NENA i3 and NG-SEC privacy & encryption requirements (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22).
- An architecture/configuration overview showing TLS everywhere in transit and encryption at rest for stored confidential data, with cipher/algorithm policies and downgrade protections.
- A cryptographic longevity rationale demonstrating algorithms and key lengths cover the full data lifecycle.
- A key management policy: generation, storage, access control, rotation, backup/restore, and revocation; identification of key custodians and audit practices.
- Operations evidence proving only approved algorithms are enabled and weaker ones disabled; include exception handling and a migration plan for any legacy endpoints.
- If proposing alternates, a strength & interoperability justification confirming parity with AES-256 and end-to-end support across all impacted components.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's Information Privacy requirements for NGCS and ESInet operations. AT&T protects all NG911 protocol operations with TLS for data in transit and strong encryption for



confidential data at rest. AT&T enforces AES 256 (or stronger equivalent) as the baseline cryptographic control, applies disciplined key management, and selects algorithms and key lengths that protect information for its full retention lifecycle. This approach ensures confidentiality, regulatory compliance, interoperability, and long term security resilience across Nebraska's NG911 environment.

Conformance to NENA i3 and NG SEC Privacy Requirements

AT&T affirms full conformance to the privacy and encryption requirements defined in:

- NENA STA 010.3 §5.8 (i3 Privacy Protection)
- NENA STA 040.2 §6.22 (NG SEC Privacy Controls)

All NG911 protocol operations and data handling practices are designed and operated in compliance with these standards across the NGCS and ESInet.

TLS in Transit and Encryption at Rest Architecture

AT&T deploys a comprehensive privacy by design architecture.

- TLS is enforced for all NG911 protocol communications in transit, including signaling, APIs, data exchanges, and management interfaces.
- Confidential data at rest is encrypted, using AES 256 or cryptographically equivalent/stronger algorithms.
- Cipher and algorithm policies explicitly permit strong encryption and disable weak or deprecated algorithms.
- Configuration standards and controls prevent cipher downgrade during protocol negotiation.

Cryptographic Longevity and Data Lifecycle Protection

AT&T selects cryptographic algorithms and key lengths to ensure protection for the full data retention period.

- AES 256 (or stronger) provides long term confidentiality assurance for stored NG911 data.
- Algorithm suitability is evaluated against projected data lifespan, regulatory requirements, and evolving threat models.
- Cryptographic policies support periodic reassessment to maintain compliance as standards evolve.

Key Management Policy and Controls

AT&T maintains a documented key management policy governing all encryption keys.

- Key generation, storage, access control, rotation, backup/restore, and revocation are formally defined.



- Encryption keys are never stored in plaintext.
- Access to keys requires strong authentication, including multifactor authentication (MFA).
- Designated key custodians are identified, and all key related actions are logged for audit and compliance purposes.

Operational Evidence and Legacy Migration

AT&T provides operational evidence demonstrating that:

- Only approved encryption algorithms are enabled across NGCS and ESInet environments.
- Weaker or deprecated algorithms are explicitly disabled.
- Any required temporary exceptions for legacy endpoints are formally documented, protected by compensating controls, and governed by a defined migration plan to reach full AES 256 compliant operation.

Alternate Algorithms (If applicable)

If alternate algorithms are proposed, AT&T provides:

- A formal justification demonstrating cryptographic equivalence to, or strength exceeding, AES 256
- Validation that end to end interoperability is maintained across all impacted NG911 components
- Confirmation that alternates align with i3 and NG SEC requirements and do not reduce privacy protections

4.7. Security Assessment and Audit

A cybersecurity assessment/audit verifies conformance/compliance with security requirements, controls, and standards. At a minimum, assessments/audits shall apply the impact categories (low, moderate, high) and security objectives (confidentiality, integrity, availability) defined in NIST FIPS 199 when assessing findings, and use those categories and objectives – together with vulnerability and threat information – to determine risk and remediation priority.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An audit methodology that applies NIST FIPS 199 impact categories and security objectives and explains how impact × likelihood (or equivalent) drives risk ratings and prioritization.
- The proposed audit scope and cadence – initial baseline and periodic re-evaluation – including coverage of ESInet segments, NGCS components, PSAP-facing interfaces, and policy/procedure controls.



- A findings lifecycle including severity assignment using FIPS 199 impacts, remediation due dates, owner assignment, tracking to closure, and verification of issue remediation.
- Integration points with the Risk Management program and with continuous monitoring for follow-up testing of high-severity items.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska’s Security Assessment and Audit requirements for NGCS and ESInet environments. AT&T conducts structured cybersecurity assessments and audits that evaluate conformance with applicable security controls, standards, and policies using NIST FIPS 199 impact categories (Low, Moderate, High) and security objectives (Confidentiality, Integrity, Availability). Assessment results are risk ranked using impact and likelihood, prioritized for remediation, and integrated with AT&T’s broader risk management and continuous monitoring programs to ensure sustained security posture over time.

Audit Methodology (NIST FIPS 199–Based Risk Scoring)

AT&T employs a formal audit and assessment methodology aligned with NIST principles.

- Findings are evaluated using FIPS 199 impact categories (Low, Moderate, High).
- Each finding is mapped to the affected security objectives (Confidentiality, Integrity, and/or Availability).
- Risk ratings are derived using impact × likelihood (or equivalent scoring), informed by vulnerability severity and threat context.
- This methodology ensures consistent, defensible prioritization of remediation actions across the NG911 environment.

Audit Scope and Cadence

AT&T defines a clear audit scope and assessment cadence.

- An initial baseline security assessment is performed to establish the security posture.
- Periodic re evaluations are conducted thereafter, or following material changes.
- Assessment scope includes:
 - ESInet core and segmented network components
 - NGCS functional elements
 - PSAP facing interfaces and interconnections
 - Relevant security policies, procedures, and operational controls



This approach ensures both technical and procedural compliance is evaluated.

Findings Lifecycle Management

AT&T manages assessment findings through a documented findings lifecycle.

- Each finding is assigned:
 - A severity rating based on FIPS 199 impact
 - A remediation owner
 - A defined remediation due date
- Findings are tracked through resolution using centralized tracking mechanisms.
- Remediation actions are validated, and closure is verified to confirm the issue has been effectively addressed.

Integration with Risk Management and Continuous Monitoring

Security assessments are integrated into AT&T's broader Risk Management and Continuous Monitoring programs.

- High severity findings trigger enhanced monitoring and follow up testing.
- Assessment results inform enterprise and program level risk registers.
- Continuous monitoring activities validate that remediation remains effective and detect regression or emerging risks.

This integration ensures assessments drive ongoing security improvements rather than one time compliance events.

4.7.1. Assessment and Audit Documentation

Security requirements and risk considerations must be built into development and delivery. Before deployment, every NG911 resource must complete a documented security assessment verifying conformance/compliance with applicable policies and/or requirements. Related components may be assessed as a group when appropriate. Assessment records must be retained as auditable evidence for future reviews.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A pre-deployment security assessment process covering all components with acceptance criteria, approvers, and required evidence.



- Templates and examples of deliverables (control test results, residual risk statements, exceptions & compensating controls, approval sign-off) mapped back to requirements.
- A documentation retention & evidence management plan supporting internal and third-party audits/assessments.
- Integration points with change management and release processes to ensure no promotion to production without a complete, approved assessment.
- A tracking mechanism linking assessment findings/exceptions to remediation or formal risk acceptance and verification of closure.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirements for security assessment and audit documentation. AT&T integrates security and risk considerations into the development, deployment, and release of all NG911 resources. Prior to promotion to production, each NGCS and ESInet component undergoes a documented security assessment verifying conformance with applicable security policies, standards, and requirements. Assessment artifacts are retained as auditable evidence and linked to remediation or formal risk acceptance to support ongoing oversight and future reviews.

4.8. Security Monitoring, Detection, and Alerting

4.8.1. Security Event Logging and Continuous Monitoring

Security event logging is essential for early detection, scoping, and investigation of cybersecurity incidents. Logging should be centralized and standardized, tuned to capture only what is necessary, and informed by a baseline of "normal" activity so anomalies can be detected. While "Security Event Logging" objects for the NG911 Logging Service are not yet defined, the contractor's proposed solution must be ready to adopt them when published and leverage current standardized log retrieval functions.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time synchronization controls proving all logging applications and device clocks align to the time server requirements from NENA-STA-040.2 §5.6.1, enabling cross-system correlation.
- A centralized logging architecture (collection, transport, storage) with coverage to trace and correlate events end-to-end across ESInet/NGCS; include any additional logging for administrative accounts.
- A review/monitoring cadence: at minimum weekly human review, plus a plan to reach near real-time visibility via automation (e.g., SIEM).



- Log integrity & access protections: controls preventing deletion/modification, role-based access, retention periods, and storage locations that satisfy retention requirements.
- Tuning & performance practices showing log scopes/levels calibrated for detection without degrading performance; include the method to establish and update behavioral baselines.
- Forward-compatibility commitment to adopt forthcoming NG911 Security Event Logging specifications on release, including mapping/schema updates for integration with the NG911 Logging Service.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirements for security event logging and continuous monitoring within the NGCS and ESInet. AT&T implements centralized, standardized, and integrity protected logging designed to support early detection, correlation, and investigation of cybersecurity events. Logging is informed by established behavioral baselines, reviewed through defined operational cadences, and integrated with automated monitoring platforms. AT&T's solution is designed to adopt forthcoming NG911 Security Event Logging specifications upon publication, ensuring long term interoperability and standards alignment.

4.8.1.1. Time Synchronization

Accurate, consistent time underpins authentication, logging/correlation, troubleshooting, and continuous monitoring across the ESInet & NGCS. All elements must implement NTP (RFC 5905) and synchronize to a common, resilient time source consistent with NENA-STA-010.3 ('Time' §2.2 & 'Time Server' §4.17). The ESInet must provide an authoritative NTP service backed by a hardware clock or synchronized to external sources with sufficient redundancy to maintain local time during isolation. Service accuracy must be $\pm 1\text{ms}$ from true time, and the absolute time difference between any two elements within the ESInet/NGCS must be ≤ 0.1 second.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time architecture showing the ESInet NTP service, upstream sources/hardware clocks, and redundancy/backup design.
- Element compliance evidence that all ESInet/NGCS elements support NTP (RFC 5905) and are configured to the designated time sources
- Accuracy & drift SLAs proving $\pm 1\text{ms}$ at the ESInet time service, and 0.1 second max element-toelement skew; include monitoring and alerting for out-of-tolerance conditions.
- Isolation resilience procedures to maintain accurate local time if upstream is unreachable.



- Operational controls: change management for time sources, certificate/time coupling checks, log/time baseline verification, and periodic audits of time-sync configuration and performance.

AT&T Response:

Comply.

PSAPs and NGCS processing elements achieve time synchronization via Network Time Protocol (NTP) from redundant and geographically distributed sources within the NG9-1-1 domain. The clock is self-contained within the ESInet and managed as part of the overall infrastructure. Time stamps are included in logs, system traces, and user reports. Network backbone equipment and internal applications form client relationships directly with NTP servers. Site-specific anycast virtual IP addresses are provisioned on backbone edge routers to facilitate the creation of an “NTP Service”. Customer access to this service is controlled through routing policy. In this model, DoS attacks sourced outside of backbone do not put NTP servers at risk. This model allows stratum-2 NTP service to be offered to external networks, and stratum-3 NTP service to be offered to local PSAP equipment (in cases where AT&T has delivered a managed network service to the PSAP).

Our solution using stratum-2 and stratum-3 for AT&T managed devices will allow every agency to maintain time within 1ms of absolute time.

External sources such as PSAPs are deployed using our time servers. AT&T will work with the PSAPs and the State to ensure the variance threshold is met.

4.8.2. Denial of Service and Telephony Denial of Service (DoS/TDoS)

A DoS/TDoS attack attempts to render resources unavailable by overwhelming capacity or impeding traffic flow. ESInet providers must have plans and procedures to mitigate and manage DoS/TDoS events. An ESInet must be able to withstand the largest feasible Distributed Denial of Service (DDoS) or TDoS attack, which, as of the current version of NENA-STA-010.3, means $\approx \geq 1$ Tbps (terabit per second) of mitigation capacity. This can be achieved via a combination of network/BCF bandwidth and mitigation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DDoS/TDoS resilience architecture demonstrating $\approx \geq 1$ Tbps (terabit per second) effective mitigation capacity across ESInet ingress, BCF/SBC, upstream carriers, and contracted mitigation services (including how capacity is measured and assured).
- Traffic re-route capability design showing how private links and any Internet-based paths can be redirected to a mitigation service during events; include activation triggers, propagation steps, and rollback.
- Plans and procedures to mitigate and manage DoS/TDoS incidents.



- Operational testing evidence of re-route/mitigation cutovers and load exercises, with results demonstrating maintained call delivery and measured restoration times.
- Monitoring & detection of volumetric and signaling-layer abuse with alert thresholds and dashboards spanning network, BCF/SBC, and application layers.
- Configuration governance for temporary blocks/rate limits and rule updates during incidents, including audit trails and post-incident reviews.

AT&T Response:

Comply.

AT&T's approach to TDoS/DDoS attacks is two-dimensional, where Ingress and Egress contingencies are solved.

Ingress Solution:

OSP to AT&T ingress facilities are engineered not to exceed 60% utilization under normal operating conditions. This is done with the expectation that the excess 40% capacity is available to provide on-demand network capacity in the event of spikes and bursts in demand due to either emergency events or malicious TDoS/DDoS attacks. For example, a traffic study determines that the busy hours for customers A and B require bandwidth of 3Mbps, respectively, so AT&T plans and deploys a 10Mbps facility, and configures the Call Admission Control (CAC) so that the total utilization (simultaneous sessions) is limited to 5Mbps for each customer; combined, their respective busy hour demand does not exceed 60% of the facility capacity, and they can each burst traffic if demand spikes. Customer Source IPs are whitelisted in the Border Control Function (BCF), preventing untrusted, non-listed, Source IPs from attacking the network. The combination of whitelisted/trusted Source IPs and CAC ensures that an attack from any IP Source will not consume all the network resources that would result in the denial of service of all IP sources. In the case of an attack, AT&T network administrators are prepared to adjust the CAC in real-time to expand a customer's bandwidth in an effort to avoid the denial of service. Once the attack has concluded, the previous CAC values are restored. Regardless of the breadth of the attack, whether it's limited to a single customer/IP source, or the more unlikely scenario that all IP sources are under attack and all TDoS/DDoS contingency measures are rendered defeated, and the network becomes fully consumed, AT&T will work with the serving OSPs and/or VSPs quickly to identify the bad actor attack vectors in order to block the attack before it can reach the AT&T ESInet.

Egress Solution:

There are two ways TDoS/DDoS attacks are mitigated with respect to PSAP call delivery.



1. A PSAP, via the AT&T Management Portal or the Resolution Center, can manually enter a Telephone Number (TN) into a TDoS/DDoS TN list.
2. TDoS/DDoS attacks are automatically detected by our software, Software Event Evaluation Program (SWEEP). This software is coded to look at various attack patterns, recognize the pattern, and automatically put the TN into the TDoS/DDoS TN list. *TNs will automatically age out of the TDoS/DDoS TN list; the default is 15 minutes.

When a call with a listed TN arrives, the call is given a SIP 580-banished error code, which translates to an SS7 cause code of 20. This tells the originator of the call that the number they dialed is not in service. Our experience has been that once the originator of the call gets the “not-in-service message,” the calls cease.

We continue to refine this functionality and have additional TDoS/DDoS features coming soon where we will interrogate the caller and have them interact with the interrogator service to get their call delivered. Also coming are aids to the subsequent fraud investigation. The SWEEP software will perform a dispatch (not a routing) query for location, and an ADR query to get additional data, such as the carrier or the TN owner, that will aid in finding and identifying attackers.

4.8.3. Intrusion Detection and Prevention Systems (IDS/IPS)

The contractor must include intrusion detection to identify known threats and suspicious behavior across endpoints and networks, with alerts routed to a central monitoring function. Intrusion prevention adds automated blocking and must be carefully deployed to avoid disrupting 911 call handling; on segments carrying live call media and signaling, IPS should be avoided unless rigorously engineered, tested, and monitored. Controls must be tuned and maintained so detections remain accurate as the environment changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Architecture and placement: where IDS is deployed, where IPS (if any) is deployed, and how alerts flow to a central SIEM; include rationale for deployed controls – ensuring no impact to legitimate media/signaling.
- Content currency & tuning: processes to update signature content at least weekly and to review/update anomaly profiles at least annually and upon material changes; including tuning and drift management.
- Monitoring cadence: procedures for at least weekly human reviews, with staffing/tools that achieve daily or near real-time monitoring; escalation paths and on-call coverage.
- Configuration governance: annual configuration reviews, change controls, test/validation before enabling prevention actions, and rollback procedures.



- Quality management: metrics and methods to track and reduce false positives/negatives, periodic effectiveness reviews, and sample investigation records.
- Integration: how IDS/IPS telemetry correlates with firewalls, endpoint security, event logs, and SIEM; storage/retention aligned to logging requirements and protected against tampering.

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's requirements for Intrusion Detection and Prevention within the NGCS and ESInet. AT&T deploys intrusion detection across network, application, and endpoint layers, with alerts routed to a centralized monitoring and analysis function. Intrusion prevention controls are applied selectively and conservatively, ensuring no disruption to legitimate 911 call signaling or media. All IDS controls are continuously tuned, governed, and integrated with AT&T's SOC and SIEM capabilities to ensure accurate detection as the NG911 environment evolves.

Architecture and Placement (IDS vs. IPS)

AT&T implements a layered IDS/IPS architecture designed for NG911 environments.

- IDS is deployed across ESInet perimeter, core network segments, NGCS infrastructure, and supporting platforms to detect known threats and anomalous behavior.
- IPS, where used, is limited to non media, non call critical segments and only enabled after rigorous testing and validation.
- Live call signaling and media paths avoid inline prevention controls unless specifically engineered to ensure zero impact.
- All alerts flow to a centralized SIEM, supporting correlation, investigation, and response.
- Placement decisions are documented with explicit rationale to protect availability and call integrity.

Content Currency and Tuning

AT&T maintains disciplined signature and anomaly management practices.

- Threat signature content is updated at least weekly, or more frequently as required.
- Anomaly detection profiles are reviewed at least annually and upon material system or traffic changes.
- Tuning processes manage drift to minimize false positives and false negatives while maintaining detection efficacy.

Monitoring Cadence and Response Coverage



AT&T establishes a defined monitoring cadence.

- IDS/IPS alerts receive at least weekly human review.
- Staffing, tools, and automation provide daily or near real time monitoring, with on call coverage for escalation.
- Escalation paths are clearly defined to ensure timely incident response and coordination across operational teams.

Configuration Governance and Change Control

IDS/IPS configurations are subject to formal governance and control.

- Configurations undergo annual review to confirm alignment with current threats and standards.
- Changes follow documented change management procedures.
- Prevention actions are tested and validated before being enabled.
- Rollback procedures exist to rapidly disable or reverse controls if unintended impacts occur.

Quality Management and Effectiveness Tracking

AT&T actively manages IDS/IPS quality and effectiveness.

- Metrics track detection accuracy, false positives, and false negatives.
- Periodic effectiveness reviews assess whether controls meet security objectives without impacting operations.
- Sample investigation records and outcomes are retained to support audits and continuous improvement.

Integration with Security Ecosystem

AT&T integrates IDS/IPS telemetry into its broader security monitoring ecosystem.

- IDS/IPS data correlates with:
 - Firewalls and BCF/SBC controls
 - Endpoint security tools
 - Centralized event logs and SIEM analytics
- Log storage, retention, and access controls align with NG911 logging requirements.
- Protections prevent unauthorized modification or deletion of IDS/IPS data.



4.9. Domain Name System (DNS)

DNS is mission-critical for NG911 service reachability and must be engineered and operated to resist tampering and disruption (e.g., spoofing, cache poisoning, DoS on resolvers). The contractor shall implement defense-in-depth protections (DNSSEC validation/signing, logging, cache-locking, response-rate limiting), and align DNS administration with privileged account, patching, and change-management controls/requirements outlined elsewhere in this RFP. **The Respondent must provide a description and/or documentation that supports the requirements in this section:** • DNSSEC is enabled on all deployed DNS servers, and clients are configured to request DNSSEC validation.

- DNS logging is enabled on all DNS servers with centralized collection and retention; describe log scopes and how performance impact is managed.
- Cache locking is enabled and set to 100% of TTL on recursive servers.
- Response rate/time limits are configured on name servers to mitigate DoS/TDoS effects.
- Administrative access controls to DNS infrastructure conform to requirements in NENA-STA-040.2 §6.2.1.3 'Administrator Accounts'.
- Patch and update compliance for all DNS components conforming to requirements in NENA-STA-040.2 §5.5 'Patching and Updating' including emergency update procedures for critical CVEs.
- Network placement & resilience: DNS architecture diagrams showing internal vs. external roles, inter-site redundancy, diverse upstream resolvers, and protections at network boundaries.
- Monitoring and alerting for DNS health and integrity (e.g., DNSSEC validation failures, abnormal NXDOMAIN spikes, RRL hits).

AT&T Response:

Comply.

AT&T recognizes that Domain Name System (DNS) services are mission critical to NG911 service reachability and must be engineered and operated to resist tampering, spoofing, cache poisoning, and denial of service conditions. DNS supporting the ESInet is designed and operated using a defense in depth security architecture aligned with NENA i3 standards and NG911 best practices to ensure availability, integrity, and resiliency under both normal and adverse operating conditions.

DNSSEC Enablement

DNS Security Extensions (DNSSEC) are deployed on authoritative DNS servers supporting ESInet services, including those resolving names for external ECRF and LVF resources. DNS resolvers used by ESInet elements support DNSSEC validation to ensure the authenticity and integrity of DNS responses and to protect against spoofing and cache poisoning attacks, thereby ensuring trusted name resolution for all NG911 dependencies.



This approach exceeds baseline requirements by consistently applying DNSSEC across authoritative services supporting both internal ESInet operations and external NG911 integrations rather than limiting DNSSEC to only select resolution paths.

DNS Logging and Centralized Collection

DNS servers operate with logging enabled and are integrated into the ESInet's centralized logging and monitoring framework. DNS related events are centrally collected and correlated with network, security, and application telemetry to support operational visibility, troubleshooting, and threat detection, with performance impacts minimized through aggregation and centralized analysis rather than localized processing.

This implementation exceeds minimum requirements by embedding DNS logging within an enterprise scale logging and SIEM ecosystem that enables real time correlation and proactive security monitoring across the entire ESInet.

Cache Integrity and Resolver Resilience

Recursive DNS resolvers within the ESInet are configured to preserve service continuity during upstream failures. When authoritative DNS servers are unreachable, resolvers reuse previously cached records in accordance with i3 referenced standards, ensuring uninterrupted DNS resolution while maintaining cache integrity and operational stability.

This behavior exceeds basic DNS availability expectations by providing standards based continuity during authoritative DNS outages rather than allowing service degradation or resolution failure.

DoS and TDoS Mitigation Controls

DNS infrastructure is protected against Distributed Denial of Service (DDoS) and Telephony Denial of Service (TDoS) attacks through layered security controls that include traffic filtering, rate limiting, access control mechanisms, and upstream DDoS mitigation services. Authoritative DNS servers supporting ESInet services are backed by mitigation capacity capable of absorbing attack volumes exceeding the largest known DNS attacks observed on the Internet.

This design exceeds the requirement by providing Internet scale DDoS protection capacity rather than relying solely on localized or best effort defensive measures.

Administrative Access Controls

Administrative access to DNS infrastructure is restricted to authorized personnel using individual credentials, least privilege role assignments, secure remote access mechanisms, and multi factor authentication. Administrative activity is audited and monitored in alignment with NG911 security standards and enterprise access control policies to ensure accountability and integrity.



This control framework exceeds baseline requirements by leveraging enterprise wide identity, authentication, and auditing systems that extend beyond DNS specific controls.

Patch and Update Management

All DNS components participate in the ESInet's formal patching and vulnerability management program. Routine updates are applied through controlled maintenance processes, and emergency update procedures are supported to rapidly remediate critical vulnerabilities and security advisories impacting DNS infrastructure.

This approach exceeds minimum patching requirements by incorporating continuous vulnerability monitoring and accelerated emergency remediation capabilities across the enterprise environment.

Network Placement, Segmentation, and Resilience

DNS services are deployed using a resilient, geographically diverse architecture with no single point of failure. Internal ESInet DNS resolution is isolated from public Internet DNS services and does not require external connectivity to function, while externally exposed authoritative DNS services are firewalled and segmented from internal DNS infrastructure. Global load balancing mechanisms return only healthy DNS endpoints, supporting rapid fault isolation and recovery.

This architecture exceeds standard redundancy expectations by combining structural Internet isolation, active active DNS design, and health aware global load balancing.

Monitoring, Alerting, and Operational Oversight

DNS health, availability, and integrity are continuously monitored through centralized network and security monitoring platforms. Alerting mechanisms support detection of abnormal traffic patterns, service degradation, and security events affecting DNS operations, with events integrated into established incident response and escalation processes.

This monitoring model exceeds basic alerting requirements by providing 24x7 operational oversight through dedicated Network Operations Centers with defined escalation and response procedures.

Summary

Across DNSSEC deployment, resilience, DDoS mitigation, architectural isolation, centralized monitoring, and operational governance, the proposed DNS solution not only meets but exceeds Nebraska RFP and NENA i3 requirements by leveraging carrier grade infrastructure, enterprise security operations, and standards driven continuity controls.

Remainder of page intentionally blank



5. Reporting Services Requirements

The contractor shall implement end-to-end logging for all call and transaction events across ESInet and NGCS components in RAW format. Logs must include ISO 8601 timestamps with time zone offset, unique correlation IDs, call identifiers, SIP message summaries (headers and SDP), PIDF-LO snapshots (privacy-redacted), routing decisions, ECRF/LVF responses, PSAP handoff timestamps, and error details. Logs shall be tamper-evident through cryptographic hashing or blockchain-like mechanisms and protected against unauthorized access.

The system shall generate CDRs for every emergency call, capturing fields such as calling line identifier, location used for routing, receiving PSAP ID, call start/answer/end timestamps, media types negotiated, disposition codes, and any transfers. CDR format and fields must align with NENA specifications, supporting export in XML/JSON.

Logs and CDRs shall be retained for a minimum of 7 years (or per jurisdictional policy), with secure storage, searchable indexing (e.g., via Elasticsearch), and export in standard formats (CSV, JSON, PDF). Access must be role-based, with audit trails for queries.

The contractor shall provide data to the PSC data analytics platform to allow for pre-built reports on call volume, average answer time, transfer metrics, location validation failures, and outage incidents, along with ad-hoc querying tools.

The system must maintain auditable trails for all configuration changes, GIS updates, and policy modifications, recording user identity, timestamps, before/after values, and rationale.

5.1. Reporting and Data Collection Requirements

The State requires enterprise-wide reporting and data collection capabilities on all aspects of the proposed NG911 system.

This capability must be agnostic to provider, system or technology and must be able to collect reportable data on the operation, configuration, and maintenance of the NG911 system. This includes both the NG911 systemwide/statewide/enterprise wide and local/PSAP specific data collection, logging and reporting necessary for the processing and documentation of 911.

AT&T Response:

Comply.

AT&T fully meets the State of Nebraska's requirements for enterprise wide reporting and data collection across the NG911 environment. AT&T provides a centralized reporting capability that captures operational, configuration, and maintenance data across the ESInet and NGCS without dependency on a specific vendor, platform, or technology. This design supports both statewide oversight and localized PSAP level visibility,



ensuring the State has comprehensive insight into NG911 system performance, usage, and change activity across its entire lifecycle.

Enterprise Wide, Provider Agnostic Data Collection

AT&T ESInet supports enterprise wide data collection that is independent of vendor, subsystem, or underlying technology.

- Data is collected uniformly across NGCS functional elements, ESInet infrastructure, and supporting services.
- The reporting framework aggregates information regardless of whether the source is state managed, vendor provided, or locally operated.
- This ensures consistent visibility across the statewide NG911 environment while avoiding vendor lock in.

Comprehensive Operational Coverage

AT&T captures reportable data spanning all major operational domains of the NG911 system, including:

- Call processing and routing activity
- System health and performance metrics
- Configuration and policy changes
- Maintenance actions and service events

Collected data supports both operational monitoring and post event analysis, enabling accurate documentation of 911 service delivery.

Statewide and PSAP Specific Reporting

AT&T's reporting approach supports multiple perspectives:

- Statewide/enterprise level visibility to support governance, trend analysis, and systemwide performance management
- Local and PSAP specific reporting to support day to day operations, troubleshooting, and compliance needs

This allows the State to maintain centralized oversight while ensuring PSAPs retain access to the data relevant to their individual operations.

Standards Aligned Logging and Reporting



AT&T's reporting capabilities align with NENA i3 logging and reporting principles, ensuring consistent event capture across NGCS functional elements and the ESInet.

- Functional element data is normalized and correlated for end to end visibility.
- Reporting supports both real time operational insight and historical analysis.
- The architecture scales to accommodate future data sources and reporting enhancements.

5.2. Logging Service

The State requires that there be a Logging Service conforming to NENA-STA-010.3. The logging service must be capable of logging all **LogEvents** defined in NENA-STA-010.3, including media, and all Functional Elements provided under the contract must generate such **LogEvents** and send them to the logging service.

The State desires that the Logging Service be made available to any PSAP that chooses to use it and implements the required i3 logging interfaces.

The Logging Service must support the query, retrieval, and log event replicator mechanisms described in NENA-STA-010.3.

The Logging Service must support **ElementState** and **ServiceState** SUBSCRIBE/NOTIFY per NENA-STA-010. The State must be able to subscribe to ServiceState and receive the standard state changes.

The proposal shall describe the Logging Service in detail.

AT&T Response:

Comply.

AT&T provides a centralized Logging Service that fully conforms to NENA STA-010.3 and supports comprehensive, end to end visibility across the ESInet and NGCS. AT&T's Logging Service ingests LogEvents from all NGCS Functional Elements, including events associated with call signaling and media, and enables correlated transaction analysis across the statewide NG911 environment. The service is designed for scalability, interoperability, and shared use — allowing PSAPs that implement i3 logging interfaces to leverage the service as part of a unified state logging framework.

NENA STA 010.3 Logging Conformance

AT&T's Logging Service conforms fully to the requirements of NENA STA-010.3.

- The service supports ingestion and processing of all LogEvents defined in the standard, including those related to media.



- Every NGCS and ESInet Functional Element provided under the contract is capable of generating LogEvents and forwarding them to the centralized Logging Service.
- LogEvents include sufficient identifiers to support end to end correlation of call processing and system activity.

NGCS and ESInet Functional Element Integration

All Functional Elements within the AT&T ESInet environment participate in logging.

- Network services, call routing components, and related NGCS functions generate standardized LogEvents.
- Events from these elements are aggregated centrally to support operational monitoring, troubleshooting, and forensic analysis.
- The logging design avoids dependence on proprietary interfaces, enabling long term interoperability.

Availability to PSAPs

AT&T's Logging Service is designed as a shared, optional service for PSAPs.

- Any PSAP that elects to use the Logging Service and supports the required i3 logging interfaces may participate.
- This approach allows the State to offer consistent logging capabilities statewide while accommodating PSAP specific operational choices.

Query, Retrieval, and Replication Capabilities

The Logging Service supports standardized log access mechanisms defined in NENA STA-010.3.

- Authorized users can query and retrieve LogEvents for analysis and reporting.
- Log event replication mechanisms are supported to enable integration with downstream systems, analytics platforms, or state repositories.
- These capabilities support both real time operational needs and historical review.

ElementState and ServiceState Subscription Support

AT&T's Logging Service supports ElementState and ServiceState subscriptions.

- The State may SUBSCRIBE to ServiceState updates and receive standard notifications as state transitions occur.
- These mechanisms provide visibility into the health and status of NGCS and ESInet services and support proactive operational management.



5.3. i3 Logging and Reporting Requirements

The proposed solution's NG911 logging and reporting system must conform to NENA-SAT-010.3 i3 logging requirements, including functional element logging, data collection, and reporting.

AT&T Response:

Comply.

AT&T's proposed NG911 logging and reporting capability is fully designed in accordance with NENA-STA-010.3 i3 logging standards and supports comprehensive visibility across the ESInet and NGCS environment. All NGCS and ESInet Functional Elements generate standardized operational and event data that is securely collected and centrally managed to support monitoring, troubleshooting, and performance analysis.

The logging architecture enables consistent capture of system activity across network, routing, and call-processing components, ensuring that operational data is available for both real-time awareness and historical reporting. AT&T's approach emphasizes interoperability and standards-based data exchange, allowing the State to leverage logging and reporting information in support of oversight, compliance, and continuous service improvement.

5.4. Functional Element Reporting

All functional elements within the ESInet (e.g., ESRP, ECRF, LVF, LIS, BCF) MUST be capable of reporting their operational status, critical events, alarms, and other relevant data. This reporting is essential for system monitoring, troubleshooting, security analysis, and performance management. Reporting mechanisms shall conform to standard protocols to ensure interoperability with a centralized logging and monitoring infrastructure.

- ESInet to PSAP Call Delivery transactions
- SIP Conference metrics
- PSAP Routing Duration Report
- Concurrent Calls
- BCF Session Reporting
- ESRP Session Reporting
- ESRP Queue State
- ECRF Session Reporting
- LVF Reporting
- LNG Session Reporting



Respondents must describe the proposed enterprise-wide NG911 logging, data collection, and reporting system and the elements provided above.

AT&T Response:

Comply.

AT&T ESInet incorporates an enterprise wide monitoring and reporting framework that enables consistent visibility into all NGCS and ESInet Functional Elements deployed under this contract. Each functional element— including the ESRP, BCF, ECRF, LVF, LIS, and associated services—publishes operational and performance information using standards based interfaces aligned with NENA STA 010.3.

Operational telemetry includes service availability, session activity, alarms, and event notifications that collectively support proactive system oversight and rapid issue resolution. These data points are centrally collected to provide meaningful insight into call routing behavior, system performance trends, and network utilization across the ESInet.

AT&T's reporting framework supports a comprehensive set of NG911 operational metrics, including call delivery transactions between the ESInet and PSAPs, SIP conference activity, routing duration, concurrent call volumes, and session level reporting for ESRP, BCF, ECRF, LVF, and LNG services. Queue state visibility and routing decision information further assist with performance management and capacity planning.

All reporting mechanisms are designed to interoperate with a centralized logging and monitoring environment, enabling the State to leverage real time status views and historical reporting to support monitoring, troubleshooting, security analysis, and service performance objectives at both the enterprise and PSAP levels.

5.5. Monitoring, Outages, Failover, Trouble Tickets, and Escalation

The State requires that there be a Network Operation Center (NOC) that monitors the ESInet, the NGCS, the gateways, and all the other elements provided under the Contract. Each element must be continuously monitored for correct operation, and any faults must cause alerts to the NOC.

Any element failure must be treated as an outage. Any service failure must be treated as a serious outage. The proposal must include a description of outage classifications with escalation processes and notification processes. A system outage must have an escalation process that escalates to the highest non-executive level within the committed SLA. For example, an outage on a service with a 5-nines (99.999% uptime) SLA must escalate to the highest non-executive level within five (5) minutes of the outage. In this context, non-executive means all the contractor and appropriate subcontractor technical staff is committed at the highest level, but not necessarily senior executives who could monitor, but not actually contribute to problem resolution. A single person must be designated the owner of such an outage, and that owner must be empowered to direct



any available resources to assess, diagnose and repair the cause or effect of the outage. The owner of the outage must be reported to the State promptly.

Any outage visible to any PSAP must be reported to that PSAP and to the State. The proposal must include the available notification methods and timing of reports of outage, progress, and restoration.

Any outage which causes an SLA failure for the month in which the outage occurred must be investigated, the root cause(s) must be determined, and corrective actions must be undertaken. The State and affected PSAPs must receive a report with the root causes, corrective actions and with committed dates. Follow-up reports noting progress against the committed dates must be provided quarterly. The State expressly reserves the right to question the root cause determination and, if it determines that the proposed corrective action plan is deficient, the contractor and the State will negotiate in good faith to amend the root cause and form a corrective action plan that is mutually agreeable.

The State requires that the contractor provide a help desk, which may be the NOC or a different group. The help desk must be staffed 24/7/365 by staff qualified to solve the most common issues encountered by PSAPs. The help desk must have a ticketing system that accepts tickets submitted by website or telephone call. The help desk must be the exclusive mechanism used to report problems by PSAPs or State staff. Every problem report must generate a ticket.

For problem reports received by telephone, the call must be answered by a qualified technician within 60 seconds 90% of the time. For website entered tickets, an initial automated email must be generated immediately, and a follow up email or telephone call must be sent within 5 minutes 99% of the time. The technician first encountering a new issue must be able to solve the problem by taking whatever actions are required to close the ticket themselves 50% of the time. This should be included in a monthly report to offer KPIs.

The help desk must take ownership of all reported problems. Sustained effort must be maintained until the problem is solved and the ticket is cleared.

The State requires that the contractor integrate or “bond” the ticketing systems of each supplier or subcontractor which may be engaged by a ticket, so that the help desk is able to have full visibility and follow up as necessary with such suppliers and subcontractors. The help desk must maintain ownership of issues even if suppliers or subcontractors must solve all or part of the reported problems. However, while the help desk must maintain ownership of the issue, it is incumbent upon the contractor to keep the State informed and fully aware of progress during the effort to restore services. The State prefers that the reporting entity be able to converse with the people who can solve the problem, so if a contractor is solving the problem, the State desires the help desk to keep abreast, but not be in the middle of solving the problem.

When sustained outages (more than 15 minutes) occur, the contractor must investigate and initiate workarounds to bring the system back to at least partial operational state. Even if the actual problem source



has been found, and repairs underway, workarounds must be devised to ameliorate the problem if the workarounds can be completed faster than the actual problem repair.

AT&T Response:

Comply.

AT&T will provide 24x7x365 monitoring and operational support for the ESInet, NGCS, gateways, and all solution elements delivered under the Contract, supported by AT&T's Network Operations Center (NOC) and dedicated 9-1-1 support organizations (including the AT&T 9-1-1 Resolution Center and NG911/ESInet Service Management).

24x7 Monitoring, Alerting, and Continuous Health Assurance

AT&T will continuously monitor all in-scope elements for correct operation using network and application monitoring, alarm correlation, and performance telemetry (e.g., link status, congestion, packet loss/jitter/latency, server/resource utilization, and functional-element health). Monitoring includes proactive detection of link outages and degradation, including automated path-quality testing and alarm thresholds that trigger immediate investigation by trained NOC/engineering resources.

AT&T's monitoring model includes severity-based alerting (e.g., Critical / Major / Minor / Warning / Normal) and supports notification to the 24x7 NOC with automated escalation triggers.

Outage Definition, Classification, and Escalation (Including "Owner" Accountability)

Outage treatment:

AT&T will treat any element failure as an outage and any service-affecting failure as a serious outage, consistent with the RFP.

Outage classification (proposed):

AT&T will classify incidents by impact and urgency, aligning to a severity model (e.g., Sev1–Sev4) that drives response targets, escalation, and customer communications.

Escalation to highest non-executive level: For any outage that threatens an SLA commitment (including "five-nines" services), AT&T will implement an escalation path that rapidly commits the highest non-executive technical leadership (Tier 2/Tier 3 and platform/vendor engineering, as appropriate). The escalation guideline will define severity triggers, escalation thresholds, and required notification cadence.

Outage owner: For each Sev1/SLA-threatening incident, AT&T will assign a single accountable Incident/Outage Owner (Incident Commander) empowered to direct resources across AT&T and subcontractors, run the



maintenance bridge, coordinate mitigation/workarounds, and drive restoration. The Outage Owner's identity will be provided to the State promptly as part of the initial incident notification/update.

Escalation structure (aligned to AT&T's operating model):

- Level 1 – NOC / Operations Intake: ticket creation, alarm correlation, initial triage, immediate mitigation steps, coordination of bridges.
- Level 2 – 9-1-1 Resolution Center / Tier 2 Engineering: advanced diagnostics, call-flow/log review, routing/GIS/NGCS functional-element analysis, coordination with PSAP/OSP stakeholders.
- Level 3 – Tier 3 / Platform & Vendor Engineering (as applicable): deep-dive troubleshooting, defect isolation, patches/hotfixes, complex interoperability remediation.
- Service Management Escalation: Service Manager ensures SLA adherence, customer comms, and cross-team coordination; escalates priority handling as thresholds are exceeded.

Failover and Restoration Approach (Including Workarounds for Sustained Outages)

AT&T's ESInet/NGCS architecture is designed for high availability and operational continuity, with automatic reroute/failover behavior and continuous monitoring for faults and degradation.

Sustained outages (>15 minutes): AT&T will investigate and implement workarounds to restore service to at least a partial operational state as quickly as possible. Where an end-to-end repair will take longer than an alternate workaround, AT&T will prioritize the workaround path to reduce PSAP-visible impact while permanent repair continues. (Examples may include alternate routing plans, controlled traffic re-homing, or temporary operational routing adjustments coordinated through the Resolution Center and the State/PSAPs.)

Outage Notification: PSAP + State Visibility, Methods, and Timing

AT&T will notify the State and any impacted PSAP(s) for any outage visible to a PSAP, including outage declaration, status, mitigation progress, and restoration confirmation. AT&T supports multi-channel notification (e.g., email and SMS) and can provide written and verbal mass notification to PSAPs for service-affecting events using established notification tooling.

AT&T will align notification cadence to incident severity and will provide updates at key milestones (acknowledgement, triage, mitigation/restoration actions, and closure).

Help Desk / Ticketing: 24x7x365, Submission Channels, and KPIs

24x7 Help Desk: AT&T will provide a 24x7x365 help desk function (may be integrated with the NOC/Resolution Center operating model) staffed by qualified personnel to resolve the most common PSAP issues and to coordinate escalation for complex incidents.



Exclusive problem-report mechanism: AT&T will require incidents to be opened via the designated help desk intake methods, and every problem report generates a ticket with end-to-end tracking from intake to closure.

Ticket submission channels: AT&T supports ticket creation via telephone and web portal, including the AT&T Express Ticketing portal for trouble tickets and change requests and status review.

Response-time performance commitments (as required by RFP): AT&T will meet the State's requirements for:

- **Phone-submitted tickets:** answered by a qualified technician within 60 seconds, 90% of the time.
- **Web-submitted tickets:** immediate automated email acknowledgement; follow-up via email/phone within 5 minutes, 99% of the time.

First-contact resolution KPI: AT&T will track and report the percentage of tickets resolved by the first technician (target $\geq 50\%$, as required), and will include these and related KPIs in monthly operational reporting to the State.

Ownership until closure: The help desk will maintain ownership of every ticket and sustain effort through restoration and closure, including coordination across internal teams and subcontractors.

"Bonded" Ticketing with Subcontractors / Suppliers (Visibility + Direct Engagement Preference)

AT&T will provide a ticketing process that supports end-to-end visibility, including interfaces/processes between AT&T and participating suppliers/subcontractors so the help desk can track status and drive follow-up as needed.

At the same time, AT&T recognizes the State's preference for direct engagement with the party best positioned to resolve the issue. AT&T will support direct technical collaboration between the State/PSAP and the resolving engineering/vendor teams as appropriate, while AT&T Service Management maintains overall accountability, SLA governance, and consolidated communications.

SLA Failures: Root Cause Analysis (RCA), Corrective Action Plans (CAP), and Quarterly Follow-Up

For any outage that causes a monthly SLA failure, AT&T will:

1. conduct an investigation,
2. determine root cause(s),
3. implement corrective actions, and
4. provide the State and affected PSAPs a written report including root cause, corrective actions, and committed dates.



AT&T will provide quarterly follow-up reports on progress against committed CAP dates until closure. AT&T will also support the State's right to question RCA conclusions and will work in good faith to adjust the corrective action plan if the State deems it deficient.

Severity Classification & Escalation / Notification Summary

Severity	Definition (Impact)	Examples (Non-exhaustive)	Ownership & Escalation Path	Notifications (State + PSAPs)
Sev1 – Critical Outage	Service-affecting outage or failure that is visible to PSAP operations and/or threatens SLA compliance.	Loss of call processing/delivery, major ESInet/NGCS element failure, widespread gateway failure, statewide or multi-PSAP impact. (Examples are illustrative; classification is impact driven.)	Single Incident/Outage Owner assigned; immediate NOC intake and triage, rapid escalation to 9-1-1 Resolution Center / Tier 2, then Tier 3 / platform & vendor engineering as needed. State requirement: escalate to highest non-executive technical level within SLA time (e.g., 5 minutes for 99.999%).	State requirement: any PSAP-visible outage must be reported to impacted PSAP(s) + State. AT&T provides customer-visible updates at key milestones (acknowledgement, triage, mitigation/restoration, closure). Notification mechanisms include email/SMS and mass notification tooling (e.g., Everbridge) as implemented for ESInet operations.
Sev2 – Major Impairment	Significant degradation/partial loss of service that impacts operations but does not represent a full outage.	Call delivery delays, intermittent failures, major packet loss/jitter issues affecting call quality, partial functional-element impairment with active failover functioning.	Ticket owned by AT&T operations; escalates from NOC to Tier 2 as needed; Tier 3 engaged if complex interoperability/defect suspected.	Updates provided based on severity with milestone-based communications (acknowledgement → mitigation → restoration). PSAP/State notification methods available include email/SMS.
Sev3 – Limited Impact	Localized issue with limited operational impact; workaround typically available.	Single-site/limited-scope alarms, isolated routing/policy/GIS issue affecting a	Owned by assigned support team; escalates to Tier 2 if unresolved or if impact increases;	Status updates at key milestones; customer-visible updates provided as appropriate.



		subset of transactions, non-critical gateway anomalies not impacting active call completion.	tracked to closure with documented actions.	
Sev4 – Informational / Service Request	Non-service-impacting request, inquiry, or planned change coordination item.	How-to requests, access changes, reporting questions, routine change requests, documentation requests.	Standard ticket workflow; routed to appropriate team; tracked and closed with disposition.	Acknowledgement and completion notifications per standard ticket workflow.

5.6. Maintenance and Configuration Reports

Respondents must provide maintenance and configuration reports once a maintenance issue has been completed or an issue requiring maintenance is resolved. This report shall include a description of the event and the corrective or preventative action taken.

- Lists events by date/time range
- Provides drill down to specific events

AT&T Response:

Comply.

AT&T provides structured maintenance and configuration reporting following the completion of any maintenance activity or the resolution of an event requiring corrective action within the NGCS or ESInet environment. Reports are generated through AT&T's formal change, incident, and maintenance management processes and are made available to the State upon completion of the activity.

Each report documents the nature of the event, the affected systems or functional elements, and the actions taken to correct or prevent recurrence. Where applicable, configuration changes and validation outcomes are summarized to confirm service integrity following maintenance completion.

Maintenance and configuration reports support chronological review through event listings organized by configurable date and time ranges. This allows the State to correlate maintenance activities with operational observations or performance metrics.

To support transparency and detailed review, reports enable drill down to individual maintenance or configuration events. Drill down views provide additional context such as impacted components, specific



changes implemented, verification steps performed, and confirmation of service restoration or stabilization. This approach ensures traceability and supports ongoing operational oversight and compliance objectives.

5.7. Discrepancy Reporting

Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The functional elements and service will support the NENA-STA-010.3 discrepancy report (DR) function. The discrepancy report function is intended to be generated by any entity that is using the data and finds a problem.

- The Discrepancy Reporting web service will be used by a reporting entity to initiate a Discrepancy Report per NENA-STA-010.3.
- Discrepancy Resolution will follow the NENA-STA-010.3 standard to request the resolution to the DR and sends the resolution to the Resolution Uri parameter in the report request.
- Entities will have access to discrepancy status updates. **The Discrepancy Report (DR) function supports a phased response like the following:**
 - The reporting entity creates the DR and submits it to the responding entity.
 - The responding entity acknowledges the DR and provides an estimate of when it will be resolved.
 - The reporting entity may request a status update and receive a response.
 - The responding entity resolves the DR and reports its resolution to the reporting agency. **All DRs MUST contain common data elements (a prolog) that include:**
 - Time Stamp of Discrepancy Submittal
 - Discrepancy Report ID (a unique value generated by the reporting entity)
 - Discrepancy reporting entity FQDN
 - Discrepancy reporting agent user ID
 - Discrepancy reporting contact info
 - Service or Instance in which the discrepancy exists.
 - Discrepancy Report type (from the list of DRs in this section)
 - Additional notes/comments
 - Reporting entity's assessment of severity

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Support for NENA-STA-010.3 DR function generated by data users.



- Discrepancy Reporting web service for initiating a DR.
- Resolution per standard to Resolution URI.
- Access to status updates.
- Phased response (create/submit, acknowledge/estimate, status update, resolve/report).
- Common prolog elements (timestamp, ID, FQDN, user ID, contact, service/instance, type, notes, severity).

AT&T Response:

Comply.

AT&T fully complies with the State of Nebraska's Discrepancy Reporting requirements by implementing the NENA STA 010.3 Discrepancy Report (DR) function across the NGCS and ESInet environment. AT&T enables authorized data users—including PSAPs, GIS operators, service providers, and other NG911 entities—to generate, submit, track, and resolve discrepancy reports using standardized interfaces and workflows. The solution supports the complete NENA defined phased DR lifecycle, ensures use of required common prolog elements, and provides transparency through acknowledgment, status updates, and documented resolution. This standards based approach ensures consistent handling of discrepancies related to data, configuration, signaling, routing, and service behavior across all NG911 functional elements.

Support for NENA STA 010.3 DR Function Generated by Data Users

AT&T supports the NENA STA 010.3 DR function allowing any authorized data user or consuming entity to initiate a Discrepancy Report when an error, inconsistency, or unexpected behavior is identified.

Discrepancy Reporting Web Service for Initiating a DR

AT&T provides a standards based Discrepancy Reporting web service that enables reporting entities to submit DRs in accordance with NENA STA 010.3. The service accepts DR submissions from authorized entities and associates each report with the appropriate NG911 functional element or service instance for processing and resolution.

Resolution per Standard Using the Resolution URI

Discrepancy resolution is performed in accordance with NENA STA 010.3, with responses communicated through the Resolution URI specified in the original DR submission. AT&T's workflow ensures that resolution information is formally returned to the reporting entity, preserving alignment with NENA defined response handling and closure expectations.

Access to Discrepancy Status Updates



AT&T provides reporting entities with access to discrepancy status updates throughout the lifecycle of the DR. Authorized users may request and receive information regarding acknowledgment, investigation progress, estimated resolution timelines, and final disposition, ensuring visibility and accountability during resolution activities.

Phased Discrepancy Response Workflow

AT&T fully supports the phased DR lifecycle defined by NENA STA 010.3, including:

- Creation and submission of the Discrepancy Report by the reporting entity
- Acknowledgment by the responding entity with an estimated resolution timeframe
- Status update requests and responses
- Final resolution and reporting of corrective action to the reporting entity

Support for Common DR Prolog Data Elements

All Discrepancy Reports processed by AT&T include the required common prolog elements, ensuring uniformity and traceability, including:

- Timestamp of discrepancy submittal
- Unique Discrepancy Report ID
- Reporting entity FQDN
- Reporting agent user ID
- Reporting contact information
- Affected service or instance
- Discrepancy report type
- Notes or comments
- Reporting entity's severity assessment

These elements are captured and preserved as part of the DR record to support investigation, correlation, and auditability in accordance with NENA STA 010.3.

5.7.1. Policy and Core Routing

5.7.1.1. Policy Store Discrepancy Report

A client of a Policy Store may report a discrepancy. This type of DR most commonly arises when a Policy Query returns an invalid Policy from the Policy Store. A Policy Owner may retrieve a policy it previously stored to



verify the query returns an exact match to the one that was stored; if not, then a DR should be filed against the Policy Store. A policy store may report a discrepancy against itself to raise an issue.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy Store DR against Policy Store

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.1.1 by supporting the NENA STA 010.3 Policy Store Discrepancy Report function within the NGCS and ESInet environment. AT&T enables authorized clients and policy owners to identify, report, and resolve discrepancies associated with Policy Store content, including cases where policy query results do not match stored or expected policy definitions. The solution supports discrepancies raised by external clients, policy owners verifying stored policies, and self reported discrepancies generated by the Policy Store itself, ensuring standardized handling, traceability, and resolution consistent with NENA i3 requirements.

NENA STA 010.3 Policy Store DR Against Policy Store

AT&T supports a Policy Store Discrepancy Report (DR) mechanism in full alignment with NENA STA 010.3. A client consuming policy data from the Policy Store may initiate a DR when a policy query returns an invalid, unexpected, or inconsistent policy. This includes scenarios where the returned policy does not exactly match the policy as originally stored and verified by the policy owner.

Authorized Policy Owners may retrieve and validate policies they previously stored and initiate a DR if discrepancies are discovered between the stored policy and the query response. In addition, the Policy Store itself may generate a self reported discrepancy when internal validation, consistency checks, or operational monitoring identifies a potential issue impacting policy integrity or availability.

All Policy Store DRs are processed using AT&T's standardized discrepancy workflow, which conforms to NENA STA 010.3 requirements and includes acknowledgment, investigation, status visibility, and documented resolution. Policy Store discrepancies are associated with the affected policy instance and relevant system context to support efficient analysis and corrective action. This approach ensures consistent, auditable management of policy related discrepancies across the NG911 ecosystem and aligns with Nebraska NG911 requirements.

5.7.1.2. Policy Discrepancy Report



A Policy Discrepancy Report function will be implemented per NENA-STA-010.3. Any entity (such as an ESRP) using a policy (such as a routing policy) will be able to report a discrepancy against the owner of the policy (e.g., a PSAP or an ESRP).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy DR against policy owner (e.g., PSAP/ESRP).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.1.2 by implementing the NENA STA 010.3 Policy Discrepancy Report function across the NGCS and ESInet environment. AT&T enables authorized entities that consume or enforce policies—including ESRPs and other NG911 functional elements—to report discrepancies directly to the policy owner when routing policies or other policy artifacts produce invalid, conflicting, or unintended results. This standards based approach ensures timely identification, visibility, and resolution of policy related issues while maintaining alignment with Nebraska NG911 requirements.

NENA STA 010.3 Policy DR Against Policy Owner (e.g., PSAP/ESRP)

AT&T supports a Policy Discrepancy Report (DR) mechanism in accordance with NENA-STA-010.3, enabling any authorized entity using a policy—such as an Emergency Services Routing Proxy (ESRP)—to report discrepancies against the owner of the policy, including a PSAP or another ESRP.

Policy DRs may be initiated when a routing or operational policy results in incorrect call handling, conflicts with other policies, produces an invalid routing outcome, or otherwise fails to behave as expected when enforced. Reporting entities submit the DR to the policy owner using the standardized NENA defined mechanism, ensuring consistent handling regardless of which NG911 functional element detects the issue.

All Policy Discrepancy Reports are managed through AT&T's standardized discrepancy reporting workflow, which includes formal acknowledgment, investigation by the policy owner, status visibility, and documented resolution consistent with NENA STA 010.3. This ensures traceability, accountability, and coordinated resolution of policy issues across the NG911 ecosystem.

5.7.1.3. Emergency Services Routing Proxy (ESRP) Discrepancy Report

An ESRP Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP or other entity will be able to report a discrepancy against an ESRP when a call is received that should not have been routed to the PSAP, or the ESRP has one or more queues whose fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally be expected. A routing problem may be the result of incorrect



data in the ECRF (GIS data). Calls are sent to PSAPs by ESRPs (Emergency Services Routing Proxy), so a PSAP should report a problem to the ESRP. The ESRP, in turn, reports any suspected GIS problems to the ECRF.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ESRP DR for misrouted calls, queue fullness, low volume; ESRP reports GIS issues to ECRF.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.1.3 by providing an ESRP Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables PSAPs and other authorized NG911 entities to report discrepancies related to ESRP call routing behavior, queue conditions, or call volume anomalies. The solution supports standardized discrepancy reporting, coordinated investigation, and resolution, including escalation of suspected GIS or ECRF data issues. This ensures transparent, traceable handling of ESRP related discrepancies consistent with Nebraska NG911 requirements.

NENA STA 010.3 ESRP DR for Misrouted Calls, Queue Fullness, Low Call Volume; ESRP Reports GIS Issues to ECRF

AT&T supports an ESRP Discrepancy Report mechanism in accordance with NENA STA 010.3, allowing a PSAP or other authorized entity to report discrepancies against an ESRP when:

- A call is received that should not have been routed to the PSAP,
- ESRP queue conditions indicate backlog, saturation, or abnormal fullness, or
- The PSAP experiences lower than expected call volume suggesting a potential routing or data issue.

When an ESRP discrepancy is reported, AT&T processes the DR using the standardized NENA discrepancy workflow, including acknowledgment, investigation, status visibility, and documented resolution. As part of the investigation, if the issue is suspected to originate from Location or GIS data, the ESRP coordinates escalation by reporting the discrepancy to the ECRF, ensuring that routing decisions remain aligned with authoritative data sources.

This approach supports closed loop resolution between PSAPs, ESRPs, and GIS data sources, providing consistent, auditable handling of routing anomalies and ensuring compliance with NENA i3 architecture requirements.



5.7.2. Location and GIS Sources

5.7.2.1. Location Information Server (LIS) Discrepancy Report

The contractor will include a LIS Discrepancy Report function per NENA-STA-010.3. Any client of a LIS will be able to report a discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 LIS DR for LIS clients.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.2.1 by providing a LIS Discrepancy Report (DR) function that conforms to NENA STA 010.3. AT&T enables any authorized LIS client—including originating service providers, network elements, ESRPs, and PSAPs—to report discrepancies related to location data, location resolution, or returned location objects. The solution supports standardized discrepancy reporting, investigation, and resolution to ensure the integrity, accuracy, and reliability of location information used throughout the NGCS and ESInet environment.

NENA STA 010.3 LIS DR for LIS Clients

AT&T supports a Location Information Server (LIS) Discrepancy Report mechanism in full alignment with NENA STA 010.3, allowing any client of a LIS to initiate a discrepancy report when issues with location information are identified. This includes, but is not limited to, cases where a client is unable to obtain its own location value or reference, where a location reference cannot be resolved, where a malformed or incorrect PIDF LO is returned, or where a PSAP determines that the civic address received does not match the caller verified location.

All LIS Discrepancy Reports are processed using AT&T's standardized discrepancy workflow, which includes acknowledgment, investigation, status visibility, and documented resolution consistent with NENA i3 requirements. LIS related discrepancies are correlated with the affected LIS service and associated provisioning or source data to support efficient root cause analysis and corrective action. This approach ensures consistent, auditable handling of location related discrepancies and aligns with Nebraska NG911 requirements.

5.7.2.2. GIS Discrepancy Report

The contractor will include a GIS Discrepancy Report function per NENA-STA-010.3. With this mechanism, the LoST server or other entity will be able to report a discrepancy report against GIS data.



Expected reports include: A gap or overlap discovered when data is coalesced.

- Incorrect information (such as the LoST server to query for information about an area)
- Bad GIS data (such as bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an address range issue on centerline, a general provisioning failure, or a malformed URI).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 GIS DR for gaps/overlaps, incorrect info, bad data (geometry, attributes, ranges, provisioning, URI).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.2.2 by providing a GIS Discrepancy Report (DR) function that conforms to NENA-STA-010.3. AT&T enables the LoST server and other authorized NG911 entities to report discrepancies related to GIS data quality, completeness, and correctness. The solution supports standardized reporting, investigation, and resolution of GIS related discrepancies to ensure that routing, location validation, and NG911 operations rely on accurate and authoritative geospatial data.

NENA-STA-010.3 GIS DR for Gaps/Overlaps, Incorrect Information, and Bad GIS Data

AT&T supports a GIS Discrepancy Report mechanism in full compliance with NENA-STA-010.3, allowing the LoST server or other authorized entities to initiate discrepancy reports against GIS data when issues are identified. Supported GIS discrepancy types include, but are not limited to:

- Gaps or overlaps identified when GIS data layers are coalesced
- Incorrect GIS information, such as an incorrect LoST server association for a given area
- Bad or malformed GIS data, including geometry errors, duplicate or conflicting attributes, missing mandatory fields, incorrect data types, address range errors on centerlines, general provisioning failures, or malformed URIs

All GIS Discrepancy Reports are processed using AT&T's standardized NENA defined discrepancy workflow, which includes acknowledgment, investigation, status visibility, and documented resolution. GIS discrepancies are correlated to the affected data layers and source systems to support efficient root cause analysis and remediation. This approach ensures transparent, auditable handling of GIS issues and supports the integrity of location validation and call routing across the NGCS and ESInet environment, consistent with Nebraska NG911 requirements.

5.7.2.3. MSAG Conversion Service Discrepancy Report



A MSAG Conversion Service (MCS) Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. An LSRG or other entity will be able to report a discrepancy against the MSAG Conversion Service (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR may also be filed when the conversion succeeded but the returned location from the MCS is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to MSAG or MSAG to PIDF-LO).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 MCS DR for failed conversions or invalid returned locations (PIDF-LO/MSAG bidirectional).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.2.3 by providing a MSAG Conversion Service (MCS) Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables LSRGs and other authorized NG911 entities to report discrepancies when location conversions fail or when returned location data is not MSAG valid or LVF valid. The solution supports standardized reporting, investigation, and resolution of MCS related discrepancies to ensure reliable, accurate location data normalization across the NGCS and ESInet environment.

NENA STA 010.3 MCS DR for Failed Conversions or Invalid Returned Locations (PIDF LO/MSAG Bidirectional)

AT&T supports an MSAG Conversion Service Discrepancy Report mechanism in full alignment with NENA STA 010.3, allowing an LSRG or other authorized entity to initiate a discrepancy report when an MCS conversion fails but is expected to succeed. In addition, discrepancy reports may be generated when a conversion completes but the returned location is not MSAG valid or LVF valid.

The MCS DR function supports bidirectional discrepancy reporting, including:

- PIDF LO to MSAG conversion failures or invalid results, and
- MSAG to PIDF LO conversion failures or invalid results.

All MCS Discrepancy Reports are handled through AT&T's standardized NENA defined discrepancy workflow, including acknowledgment, investigation, status visibility, and documented resolution. Discrepancies are correlated with the underlying source data, validation logic, and conversion context to support efficient root cause analysis and remediation. This ensures consistent, auditable handling of location conversion issues and supports the integrity of downstream location validation and call routing functions within the NG911 ecosystem.



5.7.2.4. LoST Discrepancy Report

The contractor will include a mechanism for any client of an LVF/ECRF/LoST server to report a discrepancy per NENA-STA-010.3.

The expected reports are:

- The LoST server reports a location as invalid when the client believes it is valid.
- A LIS MAY report a discrepancy against an LVF (as well as against an Originating Service Provider) if a civic address provisioned by an Originating Service Provider for a fixed device is reported invalid by an LVF.
- The LoST server returned an incorrect route in a findServiceResponse.
- The LoST server returned an incorrect error or warning regarding the location.
- The getServiceBoundaryResponse is incorrect.
- The listServicesResponse is incorrect.
- The listServicesByLocationResponse is incorrect.

Other discrepancies may be reported but are expected to be less common. These include:

- A client received an address reported as valid that it considers invalid.
- Multiple mappings were returned when only one was expected.
- Incorrect service number(s) returned.
- Expired data returned.
- An incorrect <Uri> element was returned.

A DR against a LoST server must also support the ability of the LoST server to report a discrepancy against the GIS data.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism for LVF/ECRF/LoST client to report discrepancies (invalid location, incorrect route/error/warning, incorrect responses).
- Support for LIS reports against LVF/OSP.
- LoST server reports against GIS data.

AT&T Response:

Comply.



AT&T fully complies with Nebraska RFP §5.7.2.4 by providing a LoST Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables any authorized client of the LVF, ECRF, or LoST server to report discrepancies associated with location validation, service resolution, routing responses, or returned service information. The solution also supports LIS initiated discrepancy reports against the LVF or Originating Service Providers, as well as LoST server initiated discrepancies against GIS data. This standards-based approach ensures accurate, transparent, and auditable resolution of service and routing discrepancies across the NGCS and ESInet environment.

Mechanism for LVF/ECRF/LoST Clients to Report Discrepancies

AT&T provides a NENA STA 010.3 compliant discrepancy reporting mechanism that allows any authorized LVF, ECRF, or LoST client to initiate a Discrepancy Report when anomalies are detected. Supported LoST related discrepancies include situations where:

- The LoST server reports a location as invalid when the client believes it to be valid
- The LoST server returns an incorrect route in a findServiceResponse
- The LoST server returns an incorrect error or warning related to location
- The getServiceBoundaryResponse, listServicesResponse, or listServicesByLocationResponse is incorrect

Additional supported discrepancy scenarios include incorrect service numbers, expired data, multiple mappings returned when only one is expected, incorrectly classified valid/invalid addresses, or an incorrect <Uri> element being returned.

Support for LIS Reports Against LVF and Originating Service Providers

AT&T supports LIS initiated Discrepancy Reports against an LVF or Originating Service Provider when a civic address provisioned for a fixed device is reported as invalid by the LVF but is believed by the LIS to be correct. These discrepancy reports follow the NENA STA 010.3 standardized workflow, ensuring that address validation issues are visible, traceable, and resolved in coordination with the appropriate data owners.

LoST Server Reports Against GIS Data

AT&T supports the ability for the LoST server to initiate Discrepancy Reports against GIS data when routing errors, incorrect service boundaries, or validation failures are suspected to originate from underlying geospatial data. In these cases, the LoST initiated DR is processed through the standardized NENA discrepancy lifecycle, enabling coordinated investigation, correction, and confirmation across GIS, ECRF, and LoST functions.

5.7.3. Signaling and Edge



5.7.3.1. SIP Discrepancy Report

The contractor will have a NENA-STA-010.3 SIP Discrepancy Report function. Entities that encounter an error communicating with another entity via SIP (such as a PSAP) will be able to report a discrepancy. **The expected reports are:**

- An initial INVITE request failed.
- A MESSAGE request failed.
- An OPTIONS request failed.
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.
- Required media stream (audio, text, video) failed to be accepted.
- Media problems during a dialog.
- Signaling failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 SIP DR for comm errors (failed requests, media stream failures, media problems, signaling failure).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.3.1 by providing a SIP Discrepancy Report (DR) function that conforms to NENA STA 010.3. AT&T enables PSAPs and other authorized NG911 entities to report SIP signaling or media related communication issues encountered during call setup, call handling, or in dialog operations. The solution supports standardized discrepancy reporting, investigation, and resolution to ensure reliable SIP signaling and media exchange across the NGCS and ESInet environment.

NENA STA 010.3 SIP DR for Communication Errors

AT&T supports a NENA STA 010.3 compliant SIP Discrepancy Report mechanism that allows authorized entities to initiate a DR when communication errors occur between SIP based NG911 functional elements. Supported discrepancy scenarios include, but are not limited to:

- Failure of an initial INVITE request
- Failure of a MESSAGE request
- Failure of an OPTIONS request
- Failure of a SIP request sent within an established dialog, such as a re INVITE or INFO request



- Required media streams (audio, text, or video) failing to be successfully accepted
- Media problems occurring during an active SIP dialog
- SIP signaling failures impacting call setup, maintenance, or teardown

All SIP Discrepancy Reports are processed using AT&T's standardized NENA defined discrepancy workflow, including acknowledgment, investigation, status visibility, and documented resolution. SIP DRs are correlated with SIP signaling and media telemetry to support efficient root cause analysis and corrective action, ensuring reliable inter entity communication throughout the NG911 ecosystem.

5.7.3.2. Border Control Function (BCF) Discrepancy Report

The contractor will have the BCF Discrepancy Report function as defined in NENA-STA-010.3. This function allows for an entity routing traffic through (to or from) a BCF to report a discrepancy. **The expected reports are:**

- Traffic incorrectly blocked before a dialog has been established (e.g., an INVITE, MESSAGE, or OPTIONS request, or response blocked).
- Traffic incorrectly blocked during a dialog.
- SIP signaling is inappropriately modified or dropped.
- Session Description Protocol (SDP) incorrectly regenerated during B2BUA/media anchoring.
- Media relayed with loss.
- Traffic permitted that should have been blocked because a designated bad actor generated it.
- Traffic permitted that should have been blocked for some other reason.
- QoS inconsistency.
- Invalid or improper Call Detail Recording.
- TTY to RTT transcoding errors.
- Firewall (non-SIP) errors.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 BCF DR for traffic routing issues (blocked/modified/dropped traffic, SDP regeneration, media loss, permitted bad actor traffic, QoS inconsistency, invalid CDR, TTY-RTT errors, firewall errors).

AT&T Response:

Comply.



AT&T fully complies with Nebraska RFP §5.7.3.2 by providing a BCF Discrepancy Report (DR) function that conforms to NENA STA 010.3. AT&T enables any authorized NG911 entity routing traffic through the Border Control Function to report discrepancies related to signaling behavior, media handling, security enforcement, quality of service, and session control. The solution supports standardized reporting, investigation, and resolution to ensure secure, reliable, and policy compliant traffic handling at the edge of the NGCS and ESInet.

NENA STA 010.3 BCF DR for Traffic Routing, Media, and Security Issues

AT&T supports a NENA STA 010.3 compliant Border Control Function Discrepancy Report mechanism that allows authorized entities to report discrepancies encountered when routing traffic to or from a BCF.

Supported discrepancy scenarios include, but are not limited to:

- Traffic incorrectly blocked before a dialog is established, such as INVITE, MESSAGE, or OPTIONS requests (or responses) being blocked
- Traffic incorrectly blocked during an established dialog
- SIP signaling that is inappropriately modified or dropped
- Session Description Protocol (SDP) incorrectly regenerated during B2BUA or media anchoring operations
- Media relayed with packet loss or degradation
- Traffic permitted that should have been blocked because it was generated by a designated bad actor
- Traffic permitted that should have been blocked for other policy or security reasons
- QoS inconsistencies impacting signaling or media
- Invalid or improper Call Detail Records (CDRs)
- TTY to RTT transcoding errors
- Firewall related (non SIP) errors impacting call delivery or media

All BCF Discrepancy Reports are processed through AT&T's standardized NENA discrepancy workflow, including acknowledgment, investigation, root cause analysis, status visibility, and documented resolution. BCF DRs are correlated with signaling, media, security, and QoS telemetry to support timely remediation and ensure secure and reliable edge communications across the NG911 ecosystem.

5.7.4. Network and Infrastructure

5.7.4.1. Network Discrepancy Report



A Network Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. Any entity will be able to report a general networking discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 general networking DR.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.4.1 by providing a Network Discrepancy Report mechanism that conforms to NENA STA 010.3. AT&T enables any authorized entity to report general networking discrepancies impacting ESInet or NGCS performance, availability, or behavior. The solution supports standardized reporting, investigation, and resolution, and is integrated with AT&T's continuous monitoring and operational support processes to ensure timely remediation and transparent closure.

NENA STA 010.3 General Networking Discrepancy Report

AT&T provides a NENA STA 010.3 compliant Network Discrepancy Report mechanism that allows any entity to initiate a discrepancy report for general networking issues that do not fall under a more specific functional element DR category. Network DRs may be submitted for conditions affecting network availability, connectivity, performance, or behavior across the NGCS and ESInet environment.

Reported Network Discrepancy Reports are logged, categorized, and processed through AT&T's standardized discrepancy lifecycle, including acknowledgment, investigation, status visibility, and documented resolution. Network DR handling is integrated with AT&T's 24x7 network monitoring, alarm management, and Network Operations Center (NOC) processes to support efficient diagnosis and corrective action. Resolution outcomes are communicated back to the reporting entity to ensure transparency, auditability, and closure, consistent with NENA STA 010.3 requirements.

5.7.5. Security and Trust

5.7.5.1. Permissions/Security/Authentication Discrepancy Report

The contractor will deliver a Permissions/Security/Authentication Discrepancy Report function as defined by NENA-STA-010.3. Entities that identify a security issue or a permissions or authentication error that is believed to be incorrect, will be capable of reporting a discrepancy using the DR interface of the entity or element believed to be responsible for the discrepancy. **The expected reports are:**

- Unable to authenticate.



- Unable to SUBSCRIBE to an event package.
- Permitted to SUBSCRIBE to an event package when it should have been denied.
- Unable to read a resource.
- Unable to write/modify a resource.
- Unable to delete a resource.
- Able to read a resource when it should have been denied.
- Able to write/modify a resource when it should have been denied.
- Able to delete a resource when it should have been denied.
- Unable to establish secure communication (e.g., TLS certificate is invalid or TLS failure).
- Unable to verify digital signature of a resource (e.g., a routing policy signature verification failed, or the certificate chain is invalid or contains an untrusted authority).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports for security/permissions/auth errors (unable to auth/subscribe/read/write/delete, able when denied, TLS/certificate/signature failures).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.5.1 by delivering a Permissions / Security / Authentication Discrepancy Report (DR) function that conforms to NENA STA 010.3. AT&T enables authorized NG911 entities to report discrepancies when authentication, authorization, permissions enforcement, or secure communications behave in a manner believed to be incorrect. This standards based approach ensures secure, consistent, and auditable handling of identity, trust, and access related discrepancies across the NGCS and ESInet environment.

Reports for Security, Permissions, and Authentication Errors

AT&T provides a NENA STA 010.3 compliant Permissions/Security/Authentication Discrepancy Report mechanism that allows authorized entities to initiate a discrepancy report against the functional element believed to be responsible for an incorrect security or access outcome. Supported discrepancy scenarios include, but are not limited to:

- Unable to authenticate to a NG911 functional element
- Unable to SUBSCRIBE to an event package when properly authorized



- Permitted to SUBSCRIBE to an event package when access should have been denied
- Unable to read a resource
- Unable to write or modify a resource
- Unable to delete a resource
- Able to read a resource when access should have been denied
- Able to write or modify a resource when access should have been denied
- Able to delete a resource when access should have been denied
- Unable to establish secure communication, including TLS handshake failures or invalid certificates
- Unable to verify a digital signature, such as when a routing policy signature verification fails, the certificate chain is invalid, or an untrusted authority is encountered

All Permissions/Security/Authentication Discrepancy Reports are logged and processed through AT&T's standardized NENA defined discrepancy lifecycle, including acknowledgment, investigation, root cause analysis, status visibility, and documented resolution. Security related DRs are correlated with credentialing, authorization policies, certificate validation, and trust framework data to ensure timely remediation and maintain the integrity, confidentiality, and availability of NG911 services.

5.7.5.2. Log Signature/Certificate Discrepancy Report

A Log Signature/Certificate Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the signature verification fails, it will be able to report the discrepancy to the entity that generated the LogEvent. **The expected cases for this Discrepancy Report are:**

- The certificate cannot be obtained (no "x5c" nor "x5u" field provided).
- The "x5u" field cannot be resolved or does not resolve to a valid certificate.
- The "x5u" field is present but the "x5t#256" field is missing, or the thumbprint specified does not match the certificate obtained from the "x5u" field.
- The signature of a LogEvent does not verify.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 report for certificate/signature issues (unobtainable/invalid cert, mismatched thumbprint, failed verification).



AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.5.2 by providing a Log Signature/Certificate Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables authorized entities that perform LogEvent verification — such as Logging Services or other NG911 functional elements—to report certificate and signature validation discrepancies to the entity that generated the LogEvent. This capability supports the integrity, authenticity, and non repudiation of NG911 logging and audit data across the NGCS and ESInet environment.

NENA STA 010.3 Report for Certificate and Signature Issues

AT&T provides a NENA STA 010.3 compliant Log Signature/Certificate Discrepancy Report mechanism that enables reporting of certificate and signature verification failures encountered during LogEvent validation. Supported discrepancy scenarios include, but are not limited to:

- Certificate cannot be obtained, including cases where neither an “x5c” nor an “x5u” field is provided
- “x5u” field cannot be resolved, or resolves to an invalid certificate
- “x5u” field is present but the “x5t#256” field is missing, or the thumbprint does not match the certificate retrieved from the “x5u” field
- LogEvent digital signature fails verification

When such conditions occur, authorized entities may initiate a Log Signature/Certificate DR against the LogEvent generating entity. Submitted discrepancy reports are logged, tracked, and processed through AT&T’s standardized NENA defined discrepancy lifecycle, including acknowledgment, investigation, status updates, and documented resolution. This ensures consistent, auditable handling of log integrity and trust issues and supports statewide NG911 security and compliance objectives.

5.7.6. Data and Logging

5.7.6.1. Logging Service Discrepancy Report

The contractor will have a Session Recording Client (SRC) or any entity generating logging events to, or retrieving logging records from, a Logging Service that may report a discrepancy. **The expected reports are:**

- An SRC encountered an error inviting the SRS.
- LogEvent returned an error when it should not have.
- RetrieveLogEvent returned an error when it should not have.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SRC/entity reports for errors in inviting SRS, LogEvent, or RetrieveLogEvent.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.6.1 by providing a Logging Service Discrepancy Report (DR) mechanism that conforms to NENA-STA-010.3. AT&T enables a Session Recording Client (SRC) or any authorized NG911 entity that generates logging events or retrieves logging records from the Logging Service to report discrepancies when logging service interactions do not behave as expected. This capability supports reliable logging operations, rapid identification of logging service issues, and auditable resolution of discrepancies across the NGCS and ESInet environment.

SRC / Entity Reports for Logging Service Errors

AT&T supports a NENA STA 010.3 compliant Logging Service Discrepancy Report mechanism that allows authorized entities to initiate discrepancy reports related to logging service interactions, including:

- An SRC encountered an error inviting the SRS
- LogEvent returned an error when it should not have
- RetrieveLogEvent returned an error when it should not have

When such conditions are encountered, the SRC or other authorized entity may submit a Logging Service Discrepancy Report against the affected Logging Service or associated NGCS functional element. Submitted discrepancy reports are logged, tracked, and processed through AT&T's standardized discrepancy management workflow, consistent with NENA defined practices, including acknowledgment, investigation, status visibility, and documented resolution. This ensures consistent, auditable handling of logging service issues and supports statewide operational, regulatory, and evidentiary requirements for NG911.

5.7.6.2. ADR/IS-ADR Discrepancy Report

An ADR/IS-ADR Discrepancy Report mechanism per NENA-STA-010.3 will be provided. A PSAP, ESRP, ECRF, or other entity or function will be able to report a discrepancy against an ADR or IS ADR.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ADR/IS-ADR DR by PSAP/ESRP/ECRF/etc.

AT&T Response:



Complies

AT&T fully complies with Nebraska RFP §5.7.6.2 by providing an ADR / IS ADR Discrepancy Report mechanism that conforms to NENA STA 010.3. AT&T enables a PSAP, ESRP, ECRF, or other authorized NG911 functional entity to report discrepancies against an ADR or Incident Specific ADR when issues with additional data are identified. This capability supports the reliable use of supplementary incident data within the NGCS and ESInet environment and ensures discrepancies are tracked, investigated, and resolved in a standardized, auditable manner.

NENA STA 010.3 ADR / IS ADR Discrepancy Report by PSAP / ESRP / ECRF / Etc.

AT&T supports a NENA STA 010.3 compliant ADR / IS ADR Discrepancy Report mechanism that allows authorized NG911 entities—including PSAPs, ESRPs, ECRFs, and other functional elements—to initiate discrepancy reports when issues are identified with additional data referenced or retrieved from an ADR or IS ADR.

The ADR / IS ADR DR mechanism supports reporting of discrepancies related to, but not limited to:

- Availability or accessibility of additional data
- Accuracy or integrity of incident related data
- Inconsistencies between retrieved data and expected results

Submitted ADR / IS ADR Discrepancy Reports are logged, categorized, and managed through AT&T's standardized discrepancy reporting workflow consistent with NENA STA 010.3, including acknowledgment, investigation, status visibility, and resolution reporting. Resolution outcomes are communicated back to the reporting entity, ensuring transparency and closure while supporting statewide operational, regulatory, and evidentiary requirements for NG911.

5.7.7. PSAP Operations and Treatments

5.7.7.1. PSAP Call Taker Discrepancy Report

The contractor will include the ability for a PSAP, downstream agency, or other entity to report a discrepancy against a PSAP Call Taker when a call is received that should not have been transferred to the reporting entity.

The resolution parameter in a DiscrepancyResolution report per NENA-STA-010.3 requires one of the following tokens:

- CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)
- TransferCorrect (the transfer was correct)



- NoDiscrepancy
- OtherResponse

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports against PSAP Call Taker for erroneous transfers.
- Resolution tokens (CallTakerAdvised, TransferCorrect, NoDiscrepancy, OtherResponse).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.7.1 by providing a PSAP Call Taker Discrepancy Report mechanism that conforms to NENA STA 010.3. AT&T enables a PSAP, downstream agency, or other authorized entity to report erroneous call transfers involving a PSAP Call Taker and supports standardized resolution outcomes using the required NENA defined tokens. This approach ensures accurate identification, tracking, and resolution of call handling discrepancies across the NGCS and ESInet environment.

AT&T supports a NENA STA 010.3 compliant PSAP Call Taker Discrepancy Report mechanism that allows authorized entities—including PSAPs and downstream agencies—to report discrepancies when a call is received by a PSAP Call Taker that should not have been transferred to that entity. Discrepancy reports may be initiated when analysis of call routing or transfer behavior indicates a potential call handling error. All submissions are logged and processed through AT&T’s standardized discrepancy reporting workflow, providing visibility, investigation, and documented outcome consistent with NENA i3 requirements.

Discrepancy Resolution Tokens

AT&T supports the NENA STA 010.3 Discrepancy Resolution parameters required by Nebraska RFP §5.7.7.1. Each PSAP Call Taker Discrepancy Report includes one of the following standardized resolution tokens:

- CallTakerAdvised – The call taker who transferred the call has been advised that the transfer was in error
- TransferCorrect – The transfer was determined to be correct
- NoDiscrepancy – No discrepancy was identified
- OtherResponse – The discrepancy resulted in an alternate documented disposition

Resolution outcomes are recorded and communicated back to the reporting entity, ensuring transparency, auditability, and closure in accordance with NENA STA 010.3.



5.7.7.2. Call Transfer Failure Discrepancy Report

A Call Transfer Failure Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP, LSRG, or other entity will be able to report a discrepancy against a transfer entity when a transfer fails. The notification should be made to both the entity originating the transfer and the entity receiving the transfer.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 mechanism for transfer failures, notified to originating/receiving entities.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.7.2 by providing a Call Transfer Failure Discrepancy Report mechanism that conforms to NENA-STA-010.3. AT&T enables a PSAP, LSRG, or other authorized entity to report failed call transfers and ensures that discrepancy notifications are delivered to both the entity originating the transfer and the intended receiving entity. This capability supports coordinated awareness, investigation, and resolution of transfer related issues across the NGCS and ESInet environment.

NENA STA 010.3 Mechanism for Transfer Failures, Notified to Originating / Receiving Entities

AT&T supports a NENA STA 010.3 compliant Call Transfer Failure Discrepancy Report (DR) mechanism that enables authorized entities to report instances where a call transfer does not complete successfully. A PSAP, LSRG, or other authorized entity may initiate a DR when a transfer fails at initiation, during negotiation, or at handoff.

Each Call Transfer Failure DR is associated with relevant call signaling and logging artifacts to support timely investigation and remediation. In accordance with Nebraska RFP §5.7.7.2, notification of the discrepancy is automatically communicated to both the entity originating the transfer and the entity designated to receive the transfer, ensuring shared visibility and coordinated resolution.

Call Transfer Failure Discrepancy Reports are logged, tracked, and processed through AT&T's standardized discrepancy reporting workflow consistent with NENA STA 010.3, including acknowledgment, investigation, status updates, and documented resolution.

5.7.7.3. Interactive Media Response (IMR) Discrepancy Report

An Interactive Media Response (IMR) Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. Any entity aware of a discrepancy at an Interactive Media Response (IMR) will be able to report a discrepancy at it.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 IMR DR.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.7.3 by providing an Interactive Media Response (IMR) Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables any authorized NG911 entity that becomes aware of an issue with IMR behavior to initiate a discrepancy report, supporting consistent identification, tracking, and resolution of IMR related issues across the NGCS and ESInet environment.

NENA STA 010.3 IMR Discrepancy Report

AT&T supports a NENA STA 010.3 compliant IMR Discrepancy Report mechanism that allows any authorized NG911 entity—including PSAPs, ESRPs, call takers, or other functional elements—to report discrepancies associated with Interactive Media Response behavior.

IMR Discrepancy Reports may be initiated for issues such as IMR interactions, prompts, queues, or media handling that do not perform as expected within the call flow. Submitted IMR DRs are logged, categorized, and processed through AT&T's standardized discrepancy management workflow consistent with NENA i3 practices, including acknowledgment, investigation, status updates, and documented resolution. IMR discrepancy handling is fully integrated with AT&T's broader NG911 discrepancy reporting and operational support framework to enable efficient root cause analysis and corrective action.

5.7.8. External Providers

5.7.8.1. Originating Service Provider Discrepancy Report

A mechanism for Originating Service Providers to file Discrepancy Reports will follow NENA-STA-010.3. The service allows an entity to create a discrepancy against an Originating Service Provider when a location provided by the Originating Service Provider fails validation.

- An ECRF or ESRP or PRF or PSAP may report a discrepancy when a default location is used for routing because the location is missing or not usable.
- An LNG or other entity may report a call received without ANI.
- An LNG or ESRP or other entity may report that a badly formed PIDF-LO was received, or a location query timed out without receiving a PIDF-LO.



- An LSRG or other entity may report that a call was dropped or terminated without appropriate signaling.
- A PSAP may report a discrepancy when a civic location received with a fixed (wireline) call is incorrect.
- A BCF, ESRP, PSAP, or other entity may report an incorrectly formed call (e.g., a SIP INVITE that is badly formed, lacks certain header fields or body parts, etc.).
- A BCF, ESRP, PSAP, or other entity, may report that an unusually large call volume (which might suggest a DoS or other attack) or an unusually low call volume is being generated by the Originating Service Provider.
- An Originating Service Provider may report a discrepancy against itself to raise an issue to be addressed.
- An entity may report a discrepancy when an Additional Data Reference included in the call is invalid.
- An entity may report a discrepancy when an Additional Data value is invalid.
- The Secure Telephone Identity-Verification Service (STIVS) FE may report a Secure Telephone Identity verification failure to an Originating Network.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism per NENA-STA-010.3 for OSP DRs (invalid/missing location, no ANI, bad PIDF-LO/query timeout, dropped call, incorrect civic, badly formed INVITE, unusual volume, invalid Additional Data, STIVS verification failure).
- Self-reports by OSP.

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.8.1 by providing a NENA STA 010.3 compliant Originating Service Provider Discrepancy Report (DR) mechanism. AT&T enables authorized NG911 entities to report discrepancies against an Originating Service Provider when issues are detected with call signaling, location information, identity, or additional data. The solution also supports self reported discrepancies by the Originating Service Provider, ensuring proactive identification and remediation of originating side issues across the NGCS and ESInet environment.

NENA STA 010.3 Mechanism for OSP Discrepancy Reports

AT&T supports a NENA STA 010.3 compliant Originating Service Provider Discrepancy Report mechanism that allows authorized entities to initiate discrepancy reports against an OSP under the following conditions, including but not limited to:



- Invalid or missing location information, including cases where a default location is used for routing because the provided location is missing or not usable (reported by ECRF, ESRP, PRF, or PSAP)
- Calls received without ANI (reported by LNG or other entities)
- Badly formed PIDF LO or location query timeout without receipt of a PIDF LO (reported by LNG, ESRP, or other entities)
- Calls dropped or terminated without appropriate signaling (reported by LSRG or other entities)
- Incorrect civic location received with a fixed (wireline) call (reported by a PSAP)
- Incorrectly formed calls, such as malformed SIP INVITEs, missing required headers, or missing body parts (reported by BCF, ESRP, PSAP, or other entities)
- Unusual call volume patterns, including unusually high or unusually low call volumes that may indicate misconfiguration, failure conditions, or potential security events (reported by BCF, ESRP, PSAP, or other entities)
- Invalid Additional Data References included in a call
- Invalid Additional Data values associated with a call
- Secure Telephone Identity verification failures, reported by the STIVS Functional Element to the originating network

All OSP Discrepancy Reports are logged, tracked, and processed through AT&T's standardized discrepancy management workflow consistent with NENA STA 010.3, including acknowledgment, investigation, status updates, and documented resolution.

Self Reports by Originating Service Provider

AT&T supports self initiated discrepancy reports by an Originating Service Provider in accordance with NENA STA 010.3. This capability allows an OSP to proactively raise issues related to its own call origination, signaling, location, identity, or data handling for investigation and resolution. Self reported discrepancies follow the same standardized workflow and documentation process as externally generated DRs, ensuring transparency, traceability, and timely corrective action.

5.7.9. Test and Tools

5.7.9.1. Test Call Generator Discrepancy Report

A Test Call Generator Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When a Test Call Generator encounters errors initiating or processing a test call, it reports the discrepancy to the PSAP that should have received the test call. **The expected cases for this Discrepancy Report are:**

- An initial INVITE request failed.



- A MESSAGE request failed.
- An OPTIONS request failed.
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.
- Loopback media stream (audio, text, video) failed to be accepted.
- Loopback media problems during the test dialog.
- Signaling failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Test Call Generator DR to PSAP for errors (failed requests, loopback failures, media/signaling issues).

AT&T Response:

Comply.

AT&T fully complies with Nebraska RFP §5.7.9.1 by providing a Test Call Generator Discrepancy Report (DR) mechanism that conforms to NENA STA 010.3. AT&T enables a Test Call Generator to generate and submit discrepancy reports when errors occur during test call initiation or processing and ensures those discrepancies are reported to the PSAP that should have received the test call. This capability supports effective validation, testing, and ongoing assurance of NG911 call handling and network performance.

NENA STA 010.3 Test Call Generator Discrepancy Report to PSAP

AT&T supports a NENA STA 010.3 compliant Test Call Generator Discrepancy Report mechanism that enables discrepancies to be reported when test calls fail to initiate or process correctly. When such failures occur, the Test Call Generator generates a discrepancy report and delivers it to the PSAP that should have received the test call.

The Test Call Generator DR mechanism supports reporting of the following discrepancy conditions, including but not limited to:

- Initial SIP INVITE request failures
- SIP MESSAGE request failures
- SIP OPTIONS request failures
- Failures of SIP requests within an established dialog, such as re INVITE or INFO
- Loopback media stream failures, including audio, text, or video streams not being accepted
- Media problems occurring during the test dialog



- General signaling failures encountered during test call processing

All Test Call Generator Discrepancy Reports are logged, tracked, and processed through AT&T's standardized discrepancy management workflow consistent with NENA STA 010.3, including acknowledgment, investigation, status updates, and documented resolution. This approach ensures traceability, repeatable testing, and continuous improvement of NGCS and ESInet operations.



6. Installation Requirements

Respondents are required to assume the primary project management and installation management role for their NG911 system. The State will aid and coordinate support for some aspects of the installation but will be looking for the Respondent (Contractor) to provide all installation services. **Installation as defined in this RFP includes:**

- Coordination with PSAPs
- System and service migration (i.e., logging, recording, CAD)
- Coordination with OSPs
 - Ingress
 - Core
 - Egress
- Coordination with current 911 system service provider o Ingress o Core o Egress
- Traffic migration
- Data migration
- Staging
- Testing
- Pre-cutover
- Cutover planning
- Training

The Respondent must, at a minimum, provide installation, maintenance, and support services for the duration of the contract period. Customer service support functions are identified below (§E-9, et seq.) and must be included in the Proposal to ensure that the network is fully supported.

AT&T Response:

Comply.

AT&T will serve as the primary project management and installation authority for the State's NG911 system. AT&T fully understands that while the State may assist with coordination and support for certain aspects of the implementation, the State is relying on AT&T to plan, manage, execute, and validate all installation activities required to deliver a fully operational, secure, and resilient NG911 solution. AT&T accepts full responsibility for installation management and will provide a single point of accountability throughout the project lifecycle.



AT&T will employ a structured, phased installation and migration methodology designed to minimize risk, maintain continuity of emergency services, and ensure operational readiness across all participating PSAPs. A dedicated AT&T Project Manager and specialized NG911 implementation team will lead all coordination, integration, testing, and transition activities, ensuring that the State's NG911 system is deployed efficiently, predictably, and in alignment with industry best practices and public safety operational requirements.

6.1. Installation Services

The Contractor is responsible for the installation of all requirements listed in the RFS and attachments and any other functional elements such as power and UPS as necessary to implement their NG911 solution. Devices that are installed at a PSAP may require analysis of the power and backup power supply at that PSAP. In some cases, the contractor may need to remediate issues to ensure their device has the resources needed. The State may aid coordination support for some aspects (such as approvals and scheduling) of the installation but is relying upon the Contractor to perform all installation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Methodology for installation of all NG911 system components and explain the approach to completing installation of the delivery of NG911 traffic. The methodology must include coordination with OSPs, PSAPs and other potential networks that can enhance the delivery of 911 traffic across the system.
- Coordination methodology to interconnect with all current telecommunication companies that are responsible for 911 call delivery and explain how these providers are accounted for during implementation.
- Plan to coordinate with all current 911 system service providers.
- Installation services to be provided and outline the roles and responsibilities of the Contractor and Subcontractor(s) during installation. Installation tasks as defined include, but may not be limited to:
 - Coordination with PSAPs
 - System and service migration (i.e., logging, recording, CAD)
 - UPS integration to support a minimum 3-hour backup validated with an MTTR / MTBF calculation
 - Coordination with OSPs
 - Coordination with current 911 system service provider
- Traffic migration
- Data migration
- Staging
- Acceptance testing



- Cutover planning
- Training

AT&T Response:

Comply.

The AT&T methodology for the installation of all NG911 system components is driven through the AT&T Project Management framework used universally by any and all AT&T PM individuals assigned to the State of Nebraska project. The framework is rigorous and proven through the deployment of the current State of Nebraska AT&T ESInet network. Extensive meetings and industry standard coordination tools are employed to clearly outline tasks, responsibilities, deliverable time frames, testing procedures, completion verification and exception issues process handling.

The coordination methodology to interconnect with all telecommunications companies is likewise driven through the rigorous AT&T project management framework that is proven through the deployment of statewide deployments in states including Indiana, North Carolina, Kansas, Tennessee, Connecticut and regional deployments in Texas, Florida, Georgia, Virginia. Please see the below for details.

AT&T uses an extensively employed plan to coordinate with all current 911 system providers that is comprehensive in its scope and execution. Experience in the AT&T deployed ESInets throughout the country has leveraged the strength of the AT&T project management framework. Please see the below for details.

The Project Manager will contact all telecommunication companies involved with the project to establish a dialog in order to share and gather the required data for a successful project. The PM will schedule and coordinate resources from the companies for testing and cutovers.

AT&T will manage the migration of existing legacy 9-1-1 services already in place at the PSAP(s) onto the NGCS. AT&T will manage the implementation of NG 9-1-1 services between the 9-1-1 call originating networks and the NGCS 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.

As part of implementation activities AT&T conducts a Business Practices and Call Flow Analysis with the customer's administrative, supervisor, and technical personnel and provides support in gathering the required configuration data from the customer. The analysis is a review of current and future operations, call flow, trunk lines, and integrations.

AT&T has the appropriate agreements, relationships, licenses, and interconnection agreements necessary to provide 9-1-1 services statewide. 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. There are two major parts of the migration of current telecommunication companies



onto the AT&T ESInet. Each part will be done in parallel. The first item is migration of the OSPs data from the currently ALI Database to the AT&T LDB.

AT&T works on the migration of many disparate ALI databases into the LDB. AT&T understands the complexity in Nebraska with multiple providers. Following contract award, AT&T will work with OSPs to migrate records from the existing ALI databases into the AT&T ESInet™ LDB. As part of the migration, AT&T will load or create MSAG records to support ongoing database validations and perform data validations against an initial load file of the ALI records from the various OSPs in advance the production load into the LDB.

The second part of the transition for OSPs onto the AT&T ESInet involves providing interconnection points for call ingress. AT&T will utilize connections to the Legacy Selective Routers for immediate connection to the AT&T ESInet. This allows AT&T to receive all calls from OSP regardless of whether they have migrated to direct connections to the AT&T ESInet. This process starts with an Interconnect Agreement with every OSP (or their service providers) to establish connections to the ESInet. For TDM OSPs, AT&T offers several TDM Points of Interconnect throughout the state.

AT&T will gather data about OSPs that are active in Nebraska and the associated rate centers from a multitude of data sources. 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's Program Manager will also coordinate contact with the OSPs for transition of both data and calls to AT&T ESInet.

6.2. Wiring and Cabling

All interface connections and visible cables must use standard EIA connectors secured by wall plates where exposed.

All cables must be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends. Any cables used must be plenum rated where required by local building or fire codes.

Respondents must ensure that all equipment is connected to emergency AC power and is configured to be supported by a UPS.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms must be installed in accordance with national standards and applicable local codes. **The minimum standards used in the installations shall include, but are not limited to, the following:**

- ANSI/TIA/EIA-568 – Commercial Building Telecommunications Wiring Standard
- ANSI/TIA/EIA-569 – Commercial Building Standard for Telecommunications Pathways and Spaces



- ANSI/TIA/EIA-606 – Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- ANSI/TIA/EIA-607 – Commercial Building Grounding and Bonding Requirements for Telecommunications
- Building Industry Consulting Service International, Telecommunications Distribution Methods Manual
- National Electrical Code (NFPA-70)
- FCC Rules and Regulations, Parts 68 and 15

AT&T Response:

Comply.

All interface connections and visible cables are standard EIA connectors and are secured by wall plates where exposed. All cables used are plenum-rated where required by local building or fire codes. All cables are clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends. Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms are installed in accordance with national standards and applicable local codes.

Local and remotely monitored power controls, built at least to an N+1 methodology, include diverse commercial power feeds.

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

All NGCS and network elements use dual power supplies so that a failure on the primary circuit will not disable the operation of the device. Each cabinet is fed with redundant A & B power circuit and is on redundant UPS systems conditioned by battery back-up and emergency generator back-up systems.

Minimum standards used in AT&T ESInet installations include, but are not limited to the following:

- ANSI/TIA/EIA-568 - Commercial Building Telecommunications Wiring Standard.
- ANSI/TIA/EIA-569 - Commercial Building Standard for Telecommunications Pathways and Spaces
- ANSI/TIA/EIA-606 - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- ANSI/TIA/EIA-607 - Commercial Building Grounding and Bonding Requirements for Telecommunications Building Industry Consulting Service International, Telecommunications Distribution Methods Manual



- National Electrical Code (NFPA-70)
- FCC Rules and Regulations, Parts 68 and 15

6.3. Grounding

The proposed system must provide surge and lightning protection for all connections to AC power and is required to meet the R-56 standard.

All hardware and peripheral devices must be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse.

Respondents must ground all equipment in compliance with manufacturer recommendations and applicable standards.

Respondents must furnish and install the required grounding and bonding conductors where necessary and complete the connections to the grounding system at all sites.

AT&T Response:

Comply.

AT&T understands and complies with the R-56 standard for services delivered by AT&T. AT&T complies with manufacturer recommendations for proper surge and lightning protection. All hardware and peripheral devices provided by AT&T as part of the ESInet solution will be grounded. AT&T will ground the equipment provided in compliance with manufacturer recommendations and applicable standards.

Site surveys are conducted before services are delivered and installed at each PSAP location. If remediation on the part of the PSAP is required to comply with standards, AT&T will work with local PSAP leadership to address such issues to bring the AT&T delivered services into compliance.

The Customer PSAP will provide power, ground, and environmental controls for the PSAP Network Edge

Equipment to be installed in the equipment room, as follows:

- Two (2) dedicated 110 volt/20 AMP power feeds are required with A & B feed (separate power source) and receptacle plug type NEMA L5 20R twist lock
- Any metallic component that is part of the Customer PSAP infrastructure (such as equipment, racks, ladder racks, enclosures, cable trays, etc.) must be bonded to the grounding system
- Surge/Lightning Protection



We will provide all surge and lightning protection for all connections to AC power. All hardware and peripheral devices are grounded in compliance with manufacturer recommendations and ANSI/TIA/EIA standards. We will ground hardware to rack and provide ground point off rack system. Terminating ground system to main ground bus should be completed by certified PSAP electrician under Intrado supervision. Permission to ground to main bus can be requested.

Remainder of page intentionally blank



7. Training

The Respondent shall work cooperatively with the State and designated staff to deliver training for the proposed solution. Training shall be ongoing throughout the term of the contract, with the ability to provide on-demand sessions at the State's request. The Respondent must include a description and supporting documentation for all requirements in this section.

7.1. Audiences and Scope

PSAP Operations:

- Network status reports
- Help desk usage and processes
- Text-to-911 operations
- Text- from-911 operations
- Trouble Ticketing

State-Level Operations:

- Network status reports
- Help desk processes
- Trouble ticketing
- Root-cause analysis and review

AT&T Response:

Comply.

AT&T will work cooperatively with the State and designated stakeholders to develop and deliver comprehensive training for the proposed NG911 solution. Training will be provided throughout the term of the contract and will be structured to support initial implementation, operational readiness, and ongoing system evolution. AT&T will also provide on-demand training sessions upon the State's request to address new staff onboarding, system enhancements, refresher needs, or operational changes.

AT&T's training program is designed to support both PSAP-level operations and State-level oversight functions. Training content and delivery methods will be tailored to each audience to ensure users clearly understand system functionality, operational workflows, and support processes necessary to effectively operate and maintain the NG911 environment.

PSAP Operations Training will include:



- Network status visibility and reporting
- Help desk usage, escalation paths, and support processes
- Text-to-911 operations
- Text-from-911 operations
- Trouble ticket creation, tracking, and resolution processes

State-Level Operations Training will include:

- Network status reports and system health monitoring
- Help desk processes and coordination procedures
- Trouble ticketing workflows and service management
- Root-cause analysis, incident review, and post-event reporting

7.2. Training Elements

The Respondent shall develop and deliver training to meet the following minimum requirements:

- Login and logout procedures
- Password reset
- Equipment problem reporting
- Call transfer functionality
- Call conferencing functionality
- Discrepancy reporting
- Foreign language interpretation process
- Rebid/refresh of call information
- Instant recorder/playback
- Text-to-911
- Text-from-911
- Other solution features not otherwise listed

AT&T Response:

Comply.



AT&T will develop and deliver a comprehensive NG911 training program designed to ensure PSAP personnel, supervisors, and designated support staff are fully prepared to operate and manage the AT&T ESInet™ and associated Next Generation Core Services (NGCS). Training is delivered using a structured curriculum aligned with operational workflows and real-world scenarios, and is provided prior to go-live and throughout the term of the contract as needed for refresher or new-hire training.

Training will be delivered using a combination of instructor-led sessions (in-person and virtual), hands-on exercises, recorded sessions, and electronic training materials.

Training Scope and Functional Coverage

AT&T's training program will include, at a minimum, the following operational elements:

Login and Logout Procedures

Training includes secure user access procedures, session management, and proper login/logout practices aligned with NG911 security and access control requirements.

Password Reset

Users are trained on password management processes, reset procedures, and escalation paths in accordance with AT&T security policies and NG911 system controls.

Equipment Problem Reporting

Training covers how to identify issues, initiate trouble reports, and properly engage the AT&T 9-1-1 Resolution Center, including severity classification and escalation expectations.

Call Transfer Functionality

Hands-on instruction is provided for transferring calls between PSAPs, positions, and external agencies, including intra- and inter-jurisdictional transfers over the ESInet.

Call Conferencing Functionality

Training includes initiating, managing, and terminating conference calls with other PSAPs, responders, or support agencies as supported by the call handling environment.

Discrepancy Reporting

Users are trained on identifying and reporting call-related discrepancies, data inconsistencies, or routing anomalies, including the proper channels for notification and documentation.

Foreign Language Interpretation Process



Training addresses how to access and engage language interpretation services during emergency calls, including call handling considerations and proper escalation procedures.

Rebid / Refresh of Call Information

Instruction is provided on refreshing call-associated data (ANI/ALI, location, call metadata) when updates occur during active call handling.

Instant Recorder / Playback

Users are trained on using instant replay and playback functionality to support operational review, clarification, and quality assurance during active or recently completed calls.

Text-to-911

Training includes handling inbound Text-to-911 interactions, managing message threads, and operational best practices for text-based emergency communication.

Text-from-911

Users are instructed on initiating outbound text communications from the PSAP when supported by policy, including proper usage and documentation.

Other Solution Features

Training also covers additional ESInet and NGCS features not otherwise listed, including alternate routing behaviors, overflow handling, abandonment procedures, reporting portals, and system monitoring views applicable to PSAP operations.

Training Delivery and Materials

- Training sessions may be recorded and made available for later playback, supporting refresher use and onboarding of new staff.
- Electronic training materials (user guides, reference documents, and job aids) are provided in native formats and maintained throughout the contract term.
- Training is delivered using live system or test/training environments, allowing hands-on experience without impacting production operations.
- AT&T works collaboratively with the Authority and PSAPs to tailor training content to local workflows, operational policies, and call handling configurations.

Ongoing Training Support



AT&T will provide refresher training, update training, and supplemental instruction as system features evolve, new capabilities are introduced, or operational changes occur. Training support is coordinated through AT&T's project team and ongoing service management resources.

7.3. Technical Assistance

Upon request by the State, the Contractor shall provide technical assistance to PSAP personnel during training and testing.

AT&T Response:

Comply.

AT&T will provide technical assistance to PSAP personnel during training and testing as requested by the State.

7.4. Schedule and Locations

No later than fourteen (14) calendar days before each PSAP cutover, train all PSAP personnel (including State and administrative personnel assigned to the PSAP) on the proper operation of all Contractor-supplied software and equipment. To maintain the deployment schedule and accommodate call-taker travel, the Contractor shall establish temporary training site(s) in Nebraska as needed and provide weekend and evening sessions when required.

AT&T Response:

Comply.

AT&T will ensure that all PSAP and State personnel are properly trained on the systems necessary to support the AT&T ESInet. AT&T will work with the State on exact timing of the trainings, but standard training such as (but not limited to) GIS, LIS, reporting, dashboards, and trouble ticketing are scheduled in accordance with the rollout schedule. For example, GIS training is completed early in the deployment process to allow the PSAPs or the State to load the data via the Spatial Interface at least 30 days before the PSAP cutover date. This ensures that GIS causes no roadblocks to the cutover date. Other items such as reporting, and dashboards training are generally completed more closely to the cutover in order to provide PSAP and State personnel with ample training and still allow retention of the information for the upcoming deployment.

7.5. Training Materials

Provide all training materials and a Train-the-Trainer (TtT) curriculum for State approval. Maintain up-to-date training materials at the State for the duration of the contract.



AT&T Response:**Comply.**

AT&T will provide all training materials and Train-the-Trainer curricula, subject to approval by the State, and maintain up-to-date training materials for and at the State.

7.6. Post-Deployment Training and Costs (Proposal Requirement) The Respondent shall, as part of their response:

- Provide a proposed cost for post-deployment training for up to fourteen (14) students per class
- Provide a proposed cost for the post-deployment TtT course, including the maximum class size.

AT&T Response:**Comply.**

Proposed costs for post-deployment training have been included in the price quote.

7.7. Comprehension, Testing, and Certification

Apply testing at intervals during initial and ongoing training and provide the State a final evaluation of each student's knowledge upon completion. Instructional methodologies shall include lectures, group discussions, audiovisual methods, and role-playing. Testing methodologies shall include written exams, oral exams, hands-on testing, and end of-course certification.

AT&T Response:**Comply.**

Training sessions are designed to allow trainees to understand and effectively interact with trainers and the web-based tools to maximize benefits of the system and tools. 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.

We will work with the State and PSAPs to mutually agree upon training formats and methodologies to ensure that every student has a clear grasp of the subjects.

7.8. Training Plan and Samples (Proposal Requirement) The Respondent shall, as part of their response:

- Provide a proposed training plan and sample documentation and/or materials covering the topics and audiences listed in §E-8.1 and §E-8.2, above.



AT&T Response:

Comply.

A proposed training plan and sample documentation are included. See **Appendix F - AT&T ESInet Training Plan** for a sample training plan. This plan will be customized for the State of Nebraska based on the State's input and feedback.

Remainder of page intentionally blank



8. Operations and Service Management Requirements

The Contractor shall manage all service support for the NG911 system, including integration of service and support for all partners and Subcontractors delivering components to the State.

Service levels and escalation: The Contractor shall commit to 99.999% availability for core voice paths, MTTR < 2 hours for Priority 1 incidents, and defined response times (for example, 15-minute acknowledgment). Include documented escalation paths, root-cause analysis reports, and penalty provisions for SLA breaches.

Operations enablement:

Provide comprehensive training curricula (in-person and virtual), role-based certifications, and operational runbooks for common scenarios such as failover and GIS updates. Supply full technical documentation that uses NENA functional element nomenclature and is tailored to PSAP operators, network administrators, and GIS staff.

Change management:

Establish documented change-control protocols, including scheduled maintenance windows during off-peak hours, rollback procedures, impact assessments, and at least 30 days' advance notice for changes that affect routing, GIS, or call handling.

Standards conformance and interoperability:

Demonstrate conformance to NENA i3 and NGCS standards through self-attestation and participation in multi-vendor interoperability events (for example, NENA ICE). Test plans shall include NENA-defined sequences, and the system shall interoperate with third-party equipment (for example, CHE from different vendors).

Testing program:

Execute a phased testing program covering unit tests, component integration, system integration, failover simulations, performance, and load testing (including 200% of peak capacity), and security validations using NENA test cases. Success criteria shall include 100% pass rates for critical flows.

Product documentation:

Provide thorough user manuals, API specifications (in OpenAPI format), and release notes, along with the training programs noted above, aligned with NENA terminology.

AT&T Response:

Comply.



AT&T will provide comprehensive operations and service management for the NG911 system, serving as the single accountable Contractor responsible for end-to-end service support across the AT&T ESInet™ solution. This includes full operational integration and coordination of all service partners and Subcontractors delivering components of the NG911 ecosystem, ensuring cohesive performance, accountability, and governance across the entire service lifecycle.

Service Availability and Reliability

AT&T ESInet™ is designed and operated as a mission-critical, carrier-grade platform supporting continuous NG911 operations. The ESInet architecture leverages geographically diverse core processing sites, redundant transport facilities, diverse power and environmental systems, and elimination of single points of failure. This design enables AT&T to commit to 99.999% availability for core voice paths, consistent with prior statewide ESInet deployments and AT&T’s national NG911 operating model. Continuous, real-time monitoring of all ESInet components is performed by AT&T’s dedicated 9-1-1 Network Operations and Resolution Centers, staffed 24x7x365, to proactively detect and address service conditions before they impact call handling operations.

Incident Management, Response, and Restoration

AT&T employs a formal Incident and Outage Management process specifically tailored for NG911 services. All Priority 1 (P1) incidents are treated as mission-critical events, with a target mean time to repair (MTTR) of less than two (2) hours for service-impacting conditions. Upon identification or notification of a P1 event, AT&T provides an initial acknowledgment within fifteen (15) minutes, followed by rapid engagement of the appropriate network, platform, and service management resources until service is fully restored.

Incident handling is governed by documented trouble reporting and resolution procedures, including priority assignment, coordinated incident bridge management, and ongoing communications with the State throughout the lifecycle of the event.

Escalation Management

AT&T maintains clearly defined escalation paths to ensure rapid advancement of issues when resolution thresholds are at risk. Escalation is available across multiple levels of technical, operational, and executive management, including direct access to AT&T Service Management leadership for critical or prolonged incidents. Escalation procedures are documented, consistently exercised, and fully integrated into AT&T’s incident management workflows to ensure accountability and timely decision-making during high-impact events.

Escalation Intervals	Level	Responsibility
First Escalation • SEV 1 – 1 Hour	NOC Manager	• Review Customer request and keep customer updated



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

Root Cause Analysis and Continuous Improvement

For service-impacting incidents, AT&T provides formal Root Cause Analysis (RCA) reports that document the underlying cause of the event, corrective actions taken, and preventative measures implemented to avoid recurrence. RCA reports are delivered in accordance with AT&T's standard outage management practices and support ongoing operational transparency and governance. Lessons learned are incorporated into AT&T's continuous improvement processes, including platform enhancements, operational refinements, and preventive maintenance activities across the ESInet environment.

Service Level Agreements and Accountability

AT&T's NG911 operations are governed by defined Service Level Agreements (SLAs) covering availability, incident response, restoration objectives, and service performance metrics. SLA compliance is actively monitored and reported through established service management and performance reporting mechanisms. In the event of SLA non-performance attributable to AT&T-managed components, contractual remedies and penalty provisions for SLA breaches may be applied in accordance with the terms of the final agreement. AT&T's service management framework emphasizes accountability, transparency, and continuous performance optimization in support of the State's public safety mission.

Operations Enablement

- **Comprehensive training curricula (in-person and virtual):**
AT&T provides a comprehensive NG911 training curriculum delivered through both in-person and virtual formats. Training is structured to support initial system readiness as well as ongoing operational proficiency and is available throughout the life of the contract.



- **Role-based certifications:**
Training programs are role-based and tailored to the responsibilities of PSAP operators, network administrators, and GIS staff. Where applicable, AT&T provides role-based completion validation or certification to confirm knowledge transfer and operational readiness prior to acceptance and during ongoing operations.
- **Operational runbooks for common scenarios (failover, GIS updates, etc.):**
AT&T supplies detailed operational runbooks documenting standard operating procedures and response actions for common and critical scenarios, including ESInet failover events, planned maintenance activities, GIS data updates, configuration changes, and coordinated incident response. Runbooks are designed for real-time use by operational staff during live events.
- **Full technical documentation using NENA functional element nomenclature:**
AT&T provides complete technical documentation aligned with NENA i3 standards and functional element nomenclature. Documentation references applicable functional elements and interfaces to support standards conformity, interoperability, and long-term maintainability of the NG911 system.
- **Documentation tailored to PSAP operators, network administrators, and GIS staff:**
Documentation is audience-specific and organized to address the unique operational and technical needs of PSAP personnel, network and service administrators, and GIS professionals. Materials are written to support practical, day-to-day operations as well as advanced configuration, maintenance, and governance functions.

Change Management

- **Documented change-control protocols:**
AT&T employs a formal, documented change management and change-control process governing all modifications to the ESInet environment. This process includes standardized request submission, technical review, approval, implementation, and post-change validation to ensure changes are executed in a controlled and auditable manner.
- **Scheduled maintenance windows during off-peak hours:**
Planned changes and maintenance activities are scheduled, wherever feasible, during designated off-peak maintenance windows to minimize operational impact to PSAPs and NG911 services. Maintenance scheduling is coordinated with the State and affected stakeholders in advance.
- **Rollback procedures:**
All planned changes include defined rollback procedures to enable rapid restoration to a known-good configuration in the event of unexpected impacts. Rollback plans are validated as part of the change approval process to reduce service risk.
- **Impact assessments:**
Each change undergoes an impact assessment to evaluate potential effects on ESInet operations,



routing, GIS, interfaces, and dependent systems. Risk mitigation strategies are identified and incorporated into the change plan prior to implementation.

- **At least 30 days' advance notice for changes affecting routing, GIS, or call handling:**
AT&T provides a minimum of thirty (30) days' advance notification for planned changes that may affect call routing, GIS data, or call handling services. Notifications include a description of the change, anticipated impact, proposed schedule, and coordination steps with the State and PSAP stakeholders.

Standards Conformance and Interoperability

- **Conformance to NENA i3 and NGCS standards:**
AT&T ESInet™ is designed and operated in conformance with NENA i3 and applicable NGCS standards. AT&T demonstrates conformance through formal self-attestation and by aligning system architecture, interfaces, and operational practices with NENA-defined functional elements and call flow models.
- **Participation in multi-vendor interoperability events (e.g., NENA ICE):**
AT&T actively participates in multi-vendor interoperability testing events, including NENA Industry Collaboration Events (ICE), to validate real-world interoperability across NG911 ecosystems. These activities support ongoing verification of standards compliance and interconnection readiness.
- **Test plans incorporating NENA-defined sequences:**
AT&T test plans incorporate NENA-defined call flows and test sequences to validate system behavior across ingress, routing, policy, and delivery functions. Testing aligns with NENA standards to confirm expected outcomes under normal, degraded, and failover conditions.
- **Interoperability with third-party equipment (e.g., CHE from different vendors):**
AT&T ESInet™ interoperates with third-party NG911 components, including call handling equipment (CHE) from multiple vendors, using standards-based SIP and i3 interfaces. This approach ensures vendor neutrality, flexibility, and long-term interoperability.

Testing Program

- **Phased testing approach:**
AT&T executes a phased testing program that includes unit testing, component integration testing, system integration testing, and end-to-end operational validation. Each phase is completed and validated prior to progression to the next testing stage.
- **Failover simulations:**
Testing includes planned and unplanned failover simulations to validate network, core, and application resiliency. These tests confirm continuity of service and validate operational response procedures under fault conditions.



- **Performance and load testing (including 200% of peak capacity):**
AT&T conducts performance and load testing to validate system behavior under sustained and peak load conditions, including testing at up to 200% of anticipated peak traffic levels, to ensure sufficient capacity and performance headroom.
- **Security validations using NENA test cases:**
Security testing is performed using applicable NENA-defined test cases and best practices to validate system integrity, interface security, and access controls within the NG911 environment.
- **Success criteria and critical flow validation:**
Test success criteria include 100% pass rates for defined critical call flows and service functions. Any identified issues are remediated and re-tested prior to system acceptance.

Product Documentation

- **User manuals:**
AT&T provides comprehensive user manuals tailored to PSAP operators, network administrators, and GIS staff. Manuals are written using NENA terminology and support both operational and administrative use cases.
- **API specifications (OpenAPI format):**
Where applicable, AT&T supplies API documentation in OpenAPI format to support integration, interoperability, and system extensibility. API documentation clearly defines interfaces, inputs, outputs, and error conditions.
- **Release notes:**
AT&T provides release notes for system updates and enhancements, documenting functional changes, fixes, and operational considerations. Release information supports operational awareness and change coordination.
- **Alignment with training programs and NENA terminology:**
All documentation is aligned with the associated training programs and uses NENA functional element nomenclature to ensure consistency across training, operations, and technical reference materials.

8.1. Service Management Framework

8.1.1. Service Management Plan

Oversight of the NG911 system and services post implementation/transition is required. The preferred best practice is to utilize Information Technology Infrastructure Library (ITIL) as a guideline for how NG911 services are designed, implemented, managed, maintained, and improved within the term of the contract.



ITIL integrates five stages of service delivery into a comprehensive methodology for managing the lifecycle of services.

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Within these stages are specific areas relating to Information Technology Service Management.

At a high level, these areas reference how a service maintains availability, capability, capacity, security, manageability, and operability. Respondents must describe their approach to service management for the operation of the NG911 system. The NG911 service management approach shall incorporate components of ITIL or follow industry best practices for IT service management.

Respondents must provide a narrative of how their proposed service management approach is integrated into their project management activities. Respondents must discuss their ability to maintain consistent performance and the service levels of the network

Respondents must discuss their ability to maintain consistent performance and the service levels of the network to support the following framework:

- Determination of the single point of contact
- Management of subcontracted support components
- Support personnel required and identification of Key Personnel
- Underpinning contract management
- Third-party support contracts
- Pre-emptive support
- Equipment refreshes
- Preventative maintenance
- Bug fixes
- Patching and upgrades
- Warranty
- Out of warranty items
- Service Level Agreements



AT&T Response:

Comply.

Service Management Plan

ITIL-based service management framework:

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 BMC Remedy 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. For change requests at an individual PSAP level, KY911 would follow the Move, Add, Change, and Disconnect (MACD) process described below.

- **Service Strategy:**
AT&T's service strategy establishes governance, service objectives, performance targets, and operational accountabilities for the NG911 system. Strategy activities align business requirements, public safety mission needs, and contractual obligations to ensure long-term service sustainability and performance consistency.
- **Service Design:**
Service design activities address availability, capacity, resiliency, security, manageability, and operability of the NG911 system. Design considerations include redundancy, monitoring, escalation



models, service level objectives, and maintenance strategies required to support mission-critical operations.

- **Service Transition:**
AT&T integrates service management planning into project management activities to ensure controlled transition from implementation to steady-state operations. This includes change control, documentation handover, operational readiness validation, and coordination between implementation teams and operational support resources.
- **Service Operation:**
AT&T provides 24x7x365 operational support for the NG911 system through dedicated service management and network operations teams. Service operation focuses on maintaining consistent performance and service levels through proactive monitoring, incident management, escalation handling, and coordination with internal and external stakeholders.
- **Continual Service Improvement:**
AT&T applies continual service improvement practices to evaluate service performance, incident trends, and operational effectiveness. Lessons learned, root cause analyses, and performance data are used to drive enhancements to processes, tooling, and system components over the life of the contract. Currently AT&T is on release 17 and continues to apply improvements as the service evolves.

Service Management Integration and Performance Framework

- **Single point of contact:**
AT&T provides a designated single point of contact for NG911 service management, responsible for coordination, communications, and accountability for service performance and issue resolution.
- **Management of subcontracted support components:**
AT&T assumes responsibility for coordinating and managing subcontracted support components as part of the overall NG911 service delivery model, ensuring seamless integration and consistent service quality.

Support personnel and identification of Key Personnel:

The AT&T ESInet staff and support teams currently consist of hundreds of personnel from the combined core and edge organizations. These organizations and functions are described below. AT&T shall employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with Customer's operations and use of telecommunications services, to provide and support Customer's use of the Services in accordance with the terms of AT&T's response to this RFP. The identities and titles of specific persons and their availability to provide and support Customer's needs will be separately established by authorized representatives of AT&T upon award of the RFP to AT&T. If required after contract award, AT&T will supply documentation to authenticate technical expertise, within the parameters of confidentiality limits.

Program Management



AT&T Program Management will be responsible for AT&T Customer PSAP implementation on AT&T ESInet. Program Managers are associated with each of the following ESInet functional components: OSP, Call Routing, Security, Network, ALI DB, GIS and PSAP.

The dedicated AT&T Program 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 dedicated Program Manager will allocate 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.

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:

- 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 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 AT&T Field Technicians that are geographically located throughout the Nebraska 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 data centers.

AT&T Labs

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 operates 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 answering 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.
- **Underpinning contract management:**
Service delivery is supported by structured contract management practices that align service commitments, SLAs, and operational responsibilities with contractual requirements.
- **Third party support contracts:**
AT&T manages applicable third-party support relationships to ensure alignment with service objectives and operational requirements. To that end, AT&T has Service Level Agreements in place with all sub-contractors to ensure their contributions to the AT&T ESInet offer align with our customer facing SLA's
- **Preemptive support:**
Proactive monitoring, trending, and predictive analysis are used to identify and address potential issues before they impact NG911 services. The AT&T ESInet™ service is monitored as a complete end-to-end operation via our NOCs on a 24 x 7 basis. AT&T's approach enables rapid diagnosis and resolution of potential issues before they become customer impacting.
- **Equipment refreshes:**
AT&T incorporates lifecycle management and planned refresh strategies to maintain system reliability, performance, and supportability. 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.
- **Preventative maintenance:**
Preventative maintenance activities are performed in accordance with defined maintenance schedules and industry best practices to minimize service disruption. The AT&T ESInet solution includes preventative maintenance will be provided during the contract term to enable PSAPs to operate on the most modern communications technology.



- **Bug fixes:**
Identified defects are tracked, prioritized, and remediated through controlled change and release management processes. If an issue is identified as a probable defect in the AT&T ESInet™ platform, the defect is logged and tracked by 9-1-1 Product Management and reviewed by a cross-functional team for prioritization and implementation into a future release or patch.
- **Patching and upgrades:**
Software patches and system upgrades are managed through formal change control procedures to ensure security, stability, and operational continuity. Patching and Upgrades are included with the AT&T ESInet solution. If an issue is identified as a probable defect in the AT&T ESInet™ platform, the defect is logged and tracked by 9-1-1 Product Management and reviewed by a cross-functional team for prioritization and implementation into a future release or patch.
- **Warranty management:**
AT&T manages warranty coverage for supported components to ensure timely repair or replacement when required. The AT&T ESInet™ is designed and implemented as a fully managed service offering. 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.
- **Out of warranty items:**
AT&T implements support and maintenance strategies for out of warranty components to maintain service continuity and manage operational risk. As a fully managed service offering, AT&T maintains, 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.
- **Service Level Agreements:**
AT&T maintains and monitors defined Service Level Agreements to ensure consistent performance and availability of the NG911 network and associated services. AT&T has established performance objectives for its AT&T ESInet™ Service. While AT&T does not guarantee performance, AT&T will provide credits to an eligible Customer when a performance objective is not met. The performance objectives and the associated credits shall be referred to as a Service Level Agreement or "8.1.2".

8.1.2. Service Level Agreement (SLA)

The NG911 system will utilize the requirements outlined in this RFP to negotiate a Service Level Agreement (SLA) with the selected vendor. In preparation all Respondents must provide a description of their SLA performance measures and identify how the thresholds that are not met are recovered.

The Respondent shall negotiate a comprehensive Service Level Agreement (SLA) framework that defines specific, measurable, achievable, relevant, and time-bound (SMART) metrics for the performance, availability, and reliability of the ESInet and all its functional elements. This framework must detail the processes for



monitoring, reporting, and reviewing SLA compliance. The approach should align with industry best practices for IT service management and project management to ensure consistent quality and continual improvement.

The State expects the Respondent to provide a description of how each of these components are met within their SLA.

The State recognizes the following categories as expectations for their SLA.

Critical – Network Outage

- 1st Level Support – Immediate
- Continuous problem resolution/workaround effort
- 2nd Level Support – within 15 minutes
- 3rd Level Support – within 30 minutes or upon Customer request.

Major – Service effecting

- 1st Level Support – Within 5 minutes
- 2nd Level Support – Within 30 minutes
- 3rd Level Support – Within 2 Hours or upon Customer request.

Minor – Non-service effecting

- 1st Level Support – Within 30 minutes
- 2nd Level Support – Within 2 Hours
- 3rd Level Support - Within 1 business day or upon Customer request.

The Respondent must provide a description and/or documentation that supports the requirements in this section.

AT&T Response:

Comply.

During contracting discussions, AT&T will formalize Service Level Agreements with the State. AT&T complies with the Critical, Major, and Minor categories as well as the escalation requirements listed above. As part of our standard AT&T ESInet offer, AT&T provides Service Level Agreement Performance Objectives. Below you will find an overview of AT&T's standard SLA's objectives, how they will be measured, and reported to the State of Nebraska.

SLA On-Time Provisioning - The performance objective for the On-Time Provisioning SLA relates to activating a new PSAP or Host location for the Service by the Service Activation Committed Date. The Service Activation



Committed Date is the mutually agreed upon date that a new, moved or changed Service and/or Service Component will be made available to customer. The Service Activation Date for the Service is the date AT&T provides notice that the Service is available for use by the PSAP or Host location. ("Service Activation").

If AT&T does not meet this performance objective for On-Time Provisioning SLA, Customer may be entitled to a one-time SLA credit equal to one (1) month's discounted MRCs for call routing service for the applicable Service site, after the Service Activation is completed.

Service Availability/Time to Restore SLA - The performance objective for the Site Availability/Time to Restore SLA is for the Service Site Availability to be 100%. Time to Restore is measured from when a trouble ticket is opened by AT&T Customer Care and Customer releases the affected Service Component(s) to AT&T (in cases where it is necessary for AT&T to diagnose and/or restore a Service Component into use) until the time AT&T Customer Care makes its first attempt to notify Customer that the issue has been resolved and the Service Components are restored and available for Customer to use.

If AT&T does not meet this performance objective, 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.

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	40%

PSAP Call Delivery - The performance objective for the PSAP Call Delivery SLA is for calls received into the Service in any given calendar month delivered to a Valid Destination.

The PSAP Call Delivery SLA is not met in a calendar month if AT&T fails to deliver to a Valid Destination:

- one (1) or more call(s) if fewer than 100,000 calls are presented in a calendar month, or
- more than 001% of the total calls if 100,000 or more calls are presented in a calendar month.



If AT&T does not meet this performance objective and fails to remedy the issues within one (1) month following the month AT&T did not meet its performance objective, Customer may be entitled to a one-time SLA credit equal to 5% of the discounted MRCs for call routing services for the impacted PSAP.

SLA Voice Quality - The performance objective for Voice Quality SLA is for the Daily Predicted MOS (PMOS) value per PSAP to be 3.5 or more for G.711 codec as measured by AT&T, where the ideal PMOS score for the G.711 codec is 4.3. The Service will monitor 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 Daily PSAP PMOS value will be based on an average of the per call PMOS scores over a 24-hour calendar day.

If AT&T does not meet this performance objective and the Voice Quality SLA falls below the performance objective for three consecutive days in a given calendar month and AT&T is unable to restore Service to meet the performance objective within 30 days of the failure, the Customer may be entitled to a one-time SLA credit equal to 5% of the discounted MRCs for call routing service for the impacted PSAP(s).

Remediation Details - The AT&T Service Manager that have been assigned to this specific project will work directly with the State of Nebraska and impacted PSAPs throughout the contract period addressing all Service Level Agreement issues.

8.1.3. Compliance and Risk Management

The State requires the contractor to run a documented risk management program for all NGCS components and the ESInet. The program must identify assets, threats, and vulnerabilities; rate and rank risks by **likelihood** and **impact on call delivery, location accuracy, security, availability, latency, and resilience**; and select a treatment (reduce, avoid, transfer, or accept). Any non-compliance with security requirements, standards, procedures, or practices must be documented and submitted to the State for written approval, including criticality analysis and a corrective action and/or risk acceptance path.

Each risk under the contractor's control or those outside of the contractor's span of control that will negatively impact the ESInet or NGCS must be recorded on a risk acceptance form and signed by a member of the contractor's senior leadership with the authority – and financial/legal responsibility – to accept that risk for the NGCS/ESInet scope.

All risks must be reassessed at least annually, and high/critical risks at least monthly. The method may use qualitative (very low ↔ very high) or numeric scales but must address both likelihood and impact.

Third-party risks (carriers, The cloud providers, data suppliers, managed services, subcontractors) must be tracked and visible even when control is limited. Where a third-party risk could affect service to the State, the contractor must implement compensating controls and define escalation tied to SLA/SLOs (e.g., uptime, MTTR).



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A documented Risk Management methodology covering asset identification, threat identification, vulnerability assessment, risk assessment and prioritization, and risk treatment selection (reduction, avoidance, transfer, acceptance). Include working definitions of threat, vulnerability, and risk, and show how business impact is mapped to NGCS/ESInet outcomes (call completion, routing location, latency, availability).
- A risk register template and sample entries showing fields for asset, threat, vulnerability, likelihood, impact, inherent and residual risk, selected treatment, owner, due dates, status, and verification of closure. Include examples for both NGCS applications and ESInet network elements.
- A risk acceptance form/template and completed examples that quantify or qualify likelihood and impact, reference the related non-compliance (if applicable), and record a senior leadership signature with authority to accept risk on behalf of the contractor for the NGCS/ESInet scope.
- Review cadence and triggers, showing at least annual reassessment of all risks and monthly reassessment of critical/high risks; include procedures to re-evaluate on material changes (e.g., carrier migrations, cloud region moves, software upgrades, configuration changes, new interconnections) or emerging threats.
- A third-party risk approach, including how contractor/subcontractor/carrier/cloud risks are tracked (e.g., supplier registers, attestations), how visibility is maintained when direct control is limited, required compensating controls, and escalation timelines aligned to SLAs/SLOs.
- Non-compliance linkage, showing how unresolved non-compliance (policy gaps, audit findings, penetration test results, vulnerability scans) is converted to corrective action or formal risk acceptance within the same process, with State notification/approval where required.

AT&T Response:

Comply.

AT&T operates a documented, enterprise-grade risk management program governing the AT&T ESInet™ and all NGCS components. The program is designed to continuously identify, assess, document, treat, and monitor risks that could impact NG911 operations, consistent with AT&T's best practices implemented for other statewide deployments.

Risk Management Methodology

AT&T's risk management methodology aligns with NIST RMF and ISO-based practices and includes:

- **Asset Identification:** NGCS applications, ESInet network elements, cloud infrastructure, interfaces, data repositories, facilities, and operational processes



- **Threat Identification:** Cyber threats, configuration errors, carrier outages, equipment failure, and human error
- **Vulnerability Assessment:** Results from audits, vulnerability scans, penetration testing, incident reviews, and change management
- **Risk Assessment and Prioritization:** Risks rated by likelihood and impact using qualitative or numeric scales
- **Risk Treatment Selection:** Reduce, avoid, transfer, or formally accept

Impact is explicitly mapped to NG911 outcomes, including:

- Call delivery and completion
- Routing and location accuracy
- Latency and performance
- Availability and resilience
- Security and data protection

Risk Register

AT&T maintains a centralized Risk Register for ESInet and NGCS that includes, at minimum:

- Asset
- Threat
- Vulnerability
- Likelihood and Impact
- Inherent and Residual Risk
- Selected Treatment
- Risk Owner
- Corrective Actions and Due Dates
- Status and Verification of Closure

The register includes risks associated with both NGCS applications and ESInet network elements.

- ***See Appendix G - NGCS_ESInet_Risk_Register_Template***

Risk Acceptance



When risks are accepted, whether within AT&T's control or due to third-party dependencies—they are documented on a formal Risk Acceptance Form that includes:

- Likelihood and impact justification
 - Reference to any related non-compliance (if applicable)
 - Identified compensating controls
 - Signature by AT&T senior leadership with authority to accept financial and legal responsibility for NGCS/ESInet risk
- See ***Appendix H - NGCS_ESInet_Risk_Acceptance_Form***

Where required, risk acceptance documentation and non-compliance details are submitted to the State for written approval.

Review Cadence and Triggers

- All risks are reassessed at least annually
- High and Critical risks are reassessed at least monthly

Risks are also re-evaluated upon material changes, including:

- Carrier or OSP migrations
- Cloud region or hosting changes
- Software releases or configuration changes
- New interconnections or interfaces
- Emerging cybersecurity threats

Third-Party Risk Management

AT&T tracks third-party risks associated with carriers, cloud providers, subcontractors, managed services, and data suppliers, even when direct control is limited. The program includes:

- Supplier risk tracking and attestations
- Continuous performance and SLA/SLO monitoring
- Defined compensating controls
- Escalation procedures aligned to availability, uptime, and MTTR commitments

Third-party risks remain visible throughout the contract lifecycle.



Non-Compliance Integration

Unresolved non-compliance—such as audit findings, policy gaps, penetration test results, or vulnerability scan results—is managed through the same risk management process and is converted to either:

- A Corrective Action Plan (CAP) with defined remediation steps, or
- A formal risk acceptance, approved by senior leadership

State notification and approval are provided where required.

8.1.4. Monthly Project Review and Compliance

The contractor shall meet with the PSC and any of the PSC designated resources at a minimum of monthly throughout the contract period. The frequency of these meetings may be adjusted by the PSC at any time based upon the project lifecycle. Additionally, the agenda of the meeting may be modified based upon any pressing issues that need attention.

The contractor is responsible for providing a report to the State each month that details:

- **Monthly Project review and timeline updates** to document a regular consistent path toward full implementation of the items within the contract
- **Regular Process Audits** to validate adherence to procedures, assess process maturity, and document any corrective actions.
- **Monthly System status and performance** summarizing the performance of the system with details such as utilization, packet success rate, call success rate, traffic path utilization, call transfer updates, database updates, and contract compliance
- **Monthly Service Level Agreement / and Service Level Objective** status vs the Key Performance Indicators in the SLA.
- **Monthly Risk Management Reports** providing updates to the risk register, risk response (impact and priority) to proactively communicate potential triggers that can cause the system harm.
- **Monthly Change Management Reports** summarizing all changes (planned, emergency, completed, deferred, and failed).
 - **Comprehensive Audit Trails** for all changes, retained for a minimum of three (3) years and available to the State upon request.

The contractors monthly project review process shall:

- Ensure the State is regularly informed of any roadblock or constraint in a proactive manner



- Address issues that arise before they become a barrier
- Regularly assess compliance with applicable **NENA i3** standards.
- Support compliance with **47 CFR Part 9, CJIS Security Policy, HIPAA** (where applicable), and State-level cybersecurity directives.
- Align with **PMI PMBOK** integrated principles.
- Conform to **ITIL v4** practices.
- Ensure traceability of all activities and all provisions of the contract to maintain expectations of the State of Nebraska.

AT&T Response:

Comply.

Monthly Project Review and Compliance

AT&T will conduct structured Monthly Project Review and Compliance meetings with the PSC and PSC-designated representatives throughout the contract period. These meetings are a foundational element of AT&T's service management and governance model and ensure ongoing oversight of the NG911 system and associated services following implementation and transition. Meeting frequency may be adjusted by the PSC at any time based on project lifecycle, operational priorities, or emerging issues. Meeting agendas are flexible and may be modified to address pressing concerns or time-sensitive matters.

AT&T will provide meeting agendas and supporting materials in advance and will document meeting outcomes, action items, risks, and follow-ups to ensure transparency, accountability, and traceability.

Monthly Reporting

AT&T will deliver a comprehensive monthly report to the State that consolidates project status, operational performance, risk posture, and compliance indicators. Monthly reporting will include the following components:

Monthly Project Review and Timeline Updates

AT&T will provide detailed project status reporting aligned with the approved Master Project Plan. Reports will document progress against milestones, delivery schedules, dependencies, and upcoming activities, demonstrating a consistent and controlled path toward full implementation of all contract elements.

Process Audits

AT&T will conduct regular internal process audits to validate adherence to established service management, operational, and governance procedures. Process audits assess maturity, identify gaps,



and document corrective actions to ensure continuous alignment with approved methodologies and best practices.

System Status and Performance Reporting

AT&T will provide a monthly system performance summary describing the operational health of the NG911 system. Metrics may include network utilization, packet success rates, call success rates, traffic path utilization, call transfers, database and GIS update status, and overall contract compliance indicators.

Service Level Agreement and Service Level Objective Reporting

Monthly reports will include SLA and SLO performance results measured against defined Key Performance Indicators. Performance trends, exceptions, and remediation actions will be clearly identified to support contractual accountability and continuous improvement.

Risk Management Reporting

AT&T will maintain a formal risk register and provide a monthly risk management report that documents identified risks, likelihood, impact, priority, mitigation strategies, and potential triggers. This proactive approach enables early identification of conditions that may impact system performance, schedule, or operational stability.

Change Management Reporting

AT&T will provide a consolidated monthly change management report summarizing all change activity, including planned, emergency, completed, deferred, and failed changes.

Change Audit Trails

AT&T will maintain comprehensive audit trails for all changes affecting the NG911 environment. Change records will be retained for a minimum of three (3) years and made available to the State upon request.

Monthly Project Review Governance Objectives

The monthly project review process will:

- Ensure the State is proactively informed of roadblocks, constraints, or risks before they impact performance or delivery
- Address issues early to prevent escalation into material barriers
- Regularly assess compliance with applicable NENA i3 standards
- Support compliance with 47 CFR Part 9, CJIS Security Policy, HIPAA (where applicable), and State-level cybersecurity directives
- Align with PMI PMBOK integrated project management principles



- Conform to ITIL v4 service management practices
- Ensure traceability of all project activities, operational actions, and contractual provisions to maintain alignment with State expectations throughout the term of the contract

Integrated Project and Service Management

AT&T integrates monthly project reviews with both project management and service management disciplines through dedicated Program and Service Managers, standardized reporting artifacts, and executive-level performance dashboards. This integrated approach ensures continuity from implementation through steady-state operations while maintaining consistent network performance, service levels, regulatory compliance, and contractual accountability.

8.2. Continuity and Resilience

8.2.1. Availability

The entire IP path, and call-related services, data transactions, and associated services will be available 99.999% of the time, end to end, with the appropriate caveat for PSAPs that do not have the necessary redundancy to maintain 99.999%. Provisioning services not related to call time, such as provisioning the location database in the LNG by legacy OSPs, will be available 99.9% of the time.

Availability is defined as:

$$\text{MTBF} / (\text{MTBF} + \text{MTTR})$$

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 99.999% availability for IP path/call services/data transactions end-to-end (with caveat for non-redundant PSAPs).
- 99.9% for non-call provisioning

AT&T Response:

Comply.

The 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), see figure below. The Service Availability is calculated from the time an issue is reported that impacts Call Processing ability, until such time that the Service Call Processing ability is restored. The Service Availability downtime will not exceed 26.3 seconds per



month. Customers are eligible for remedies and service credits when the Service Availability SLA is not achieved.

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.

AT&T provides a Service Level Agreement and credits should the service not be available 100 percent of the time. The performance objective for the Site Availability/Time to Restore SLA is for the Service Site Availability to be 100 percent. Time to Restore is measured from when a trouble ticket is opened by AT&T Customer Care and Customer releases the affected Service Component(s) to AT&T (in cases where it is necessary for AT&T to diagnose and/or restore a Service Component into use) until the time AT&T Customer Care makes its first attempt to notify Customer that the issue has been resolved and the Service Components are restored and available for Customer to use.

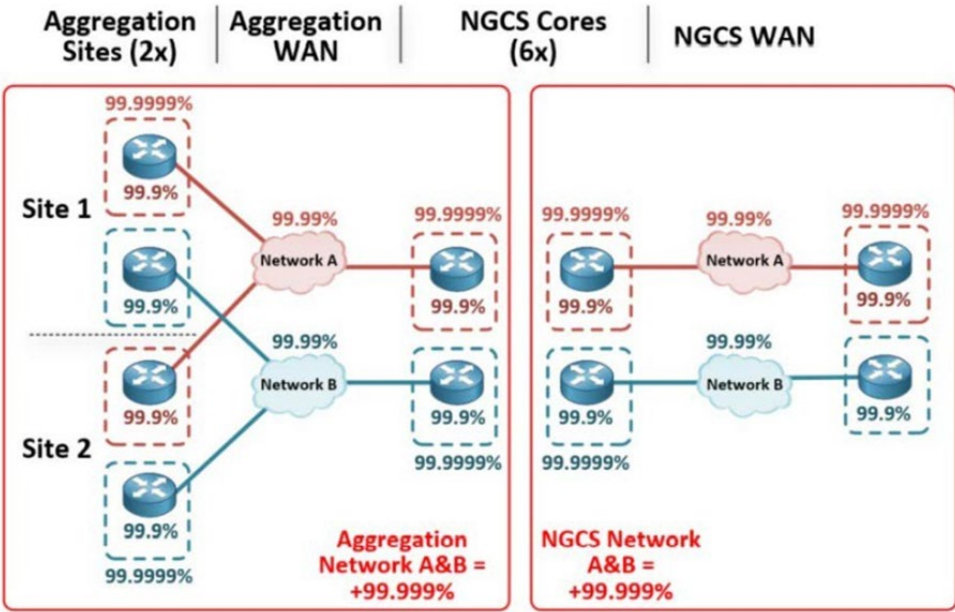


Figure 29: Resiliency Design

8.2.2. Continuity of Operations Plan (COOP)

The Continuity of Operations plan will include measures to account for common cyber security threats and “sunny day” outage vulnerabilities that could affect the normal operation of the NG911 system and cause an outage.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Measures for cyber threats/"sunny day" outages causing system disruptions.



AT&T Response:**Comply.**

The AT&T ESInet solution is backed by AT&T's business continuity/disaster recovery organization. AT&T has established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to our facilities or systems, including:

- Building emergency procedures (e.g., bomb threat, earthquake, power failure, 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

Please see attachment ***Appendix I - AT&T Business Continuity & Emergency Management***.

8.2.3. Disaster Recovery (DR) The Disaster Recovery Plan will include the procedures for:

- Activation procedures
- Recovery team identification
- Roles and responsibilities
- Recovery strategies and response
- Recovery management procedures
- Recovery cost procedures
- Recovery resources
- Recovery communications
- Stakeholder management
- Subcontractor, Supplier, Partner communication, and coordination

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- DR Plan with activation procedures, team ID/roles/responsibilities, strategies/response, management/cost/resources/communications, stakeholder/subcontractor coordination.

AT&T Response:**Comply.**



Network Disaster Recovery

In addition to the AT&T ESInet resources, AT&T's Network Disaster Recovery (NDR) team recovers voice and data service network elements in affected areas. Our NDR plan has three primary goals:

- Route non-involved communications traffic around an affected area
- Give the affected area access to worldwide communications
- Restore normal communications service as quickly as possible

To replace a completely destroyed central office, we transport equipment in specially designed technology trailers. Each trailer has self-contained or dedicated power and environmental capabilities, and each houses a component of the network technology that would normally be part of a central office. Once on site, we connect the individual components to match the unique configuration of a heavily damaged, unrecoverable or destroyed central office.

NDR provides equipment and a team in response to fires, flooding, earthquakes, gas line explosions, and train derailments. We also provide emergency communications support for humanitarian relief efforts.

Since 1993, NDR has held three or four full-scale disaster recovery exercises each year. The exercises test as many of the NDR processes as possible—from the initial call to equipment transportation and setup to technology turn-up and testing. At these exercises, team members get hands-on training on new technologies and operate recovery equipment in a variety of field conditions.

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 will 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 will provide a mutually agreed upon an action plan for the final resolution. AT&T will continue resolution activity until full service is restored. The primary objective of an incident response 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 large-scale 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, ensuring 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.

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 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 service disruptions and support rapid response to loss or impairment of crucial business functions or infrastructure. To address potential risks, AT&T uses:
- Redundant, Geographically Diverse Systems – The six-core site AT&T ESInet architecture is located in strategically geographically diverse and redundant data centers throughout the continental United States.

Incident Management

In the event of an unplanned outage, or intermittent outage of a system, network component, or application that has the potential to cause an adverse impact to production services, 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

- AT&T has established business and service continuity, disaster recovery, and emergency procedures that address potential risk situations to our facilities or systems, including:
 - Building emergency procedures (e.g. bomb threat, earthquake, power failure, and flood)
 - Data center risks (e.g. water, flood, power, electrical, and fire)
 - Security risks (e.g., information and network security, physical security)
 - Building evacuations
 - Inclement weather
 - Building disasters

Implementing Risk Reduction and Recovery Measures

- 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

- 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:
 - Essential functions and personnel
 - Employee emergency contact information
 - Building emergency procedures
 - Contractor/Vendor contact procedures



- Crisis communications 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 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.

AT&T deploys firewalls and other network security devices and software to protect against inbound threats and malicious attacks on the NGCS components. AT&T protects the IP Virtual Private Network (VPN) using continuous network monitoring and traffic analysis performed by the AT&T Security Operations Center (SOC).

The AT&T Security Operations Center (SOC) provides comprehensive security across one of the world's largest network infrastructure by deploying a pro-active defense-in-depth strategy of including additional layers of security behind the network perimeter. AT&T utilizes the same set of security tools to manage its global network that it uses for its Managed Security Services available to its customers.

The AT&T SOC is a 24x7 centralized command and control facility that includes seasoned expert staff, time-tested methodologies, and AT&T proprietary technology. The SOC can monitor and analyze traffic via the AT&T IP backbone, to provide near real-time and advance notification of different types of security events, and to produce daily company security reports, and alerts. AT&T's advanced network used by AT&T ESInet™ is one of the world's most advanced and powerful global backbone networks and carries 670 petabytes of traffic on an average business day.

Vulnerability Testing is performed by authorized personnel to verify whether controls can be bypassed to obtain any unauthorized access.

- Vulnerability tests to evaluate the level of safeguards on network components are performed on a varying frequency based on the risk of compromise, utilizing authorized leading-edge testing tools.
- Vulnerability scans are conducted on networks, computer hosts and applications owned by AT&T at regular intervals as directed by AT&T security policies using AT&T- developed tools and leading-edge scan tools from recognized commercial software providers.



Network or computer security analysis is commonly referred to as intrusion testing, penetration testing, sweeps, profiling, and vulnerability analysis. Performing security analysis of the AT&T networks or computers or applications is the responsibility of AT&T. Performance of security analysis by customers is expressly prohibited unless written approval has been obtained from AT&T global security organization management.

AT&T 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.

More information regarding our NDR program is available online. AT&T can provide the link to the AT&T disaster recovery website if requested.

Please see attachment ***Appendix I - AT&T Business Continuity & Emergency Management***.

8.3. Operations Centers and Support

8.3.1. Network Operations Center (NOC)

The NOC must operate on a 24x7x365 basis for the duration of the contract. In addition, the NOC will include the capability to perform remote maintenance and restoration of alarms, as necessary.

The NOC will be the single point that performs continuous monitoring, maintenance, and network support services of the NG911 System. The NOC will interface with the help desk and the PSAPs or designated staff. The NOC will be staffed with appropriate technical resources to aid troubleshooting, diagnosis and recovery from issues related to the operation of the NG911 system.

The NOC will perform monitoring of the entire ESInet, all connections and functional components used in the routing of 911 calls. The NOC will be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure of the NG911 system.

- The NMS will continuously monitor the performance and availability of all devices.
- The NMS will monitor network performance, including throughput, latency, jitter, packet loss, and other parameters deemed necessary by the State.
- The NMS will monitor the network for network intrusion attempts or security breaches and be capable of issuing security alerts when an event is recognized.



- The NMS will create alarms based on thresholds and parameters and distribute alarm notifications appropriately.
- The NMS will monitor the environment at all data centers or points of presence where critical network components are housed to ensure functionality.
- The NMS will monitor ancillary network components such as power utilization and backup power systems.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24x7x365 NOC with remote maintenance/restoration.
- Single point for monitoring/maintenance/support.
- Interface with help desk/PSAPs.
- Staffed for troubleshooting/recovery.
- Monitoring of ESInet/connections/functional components.
- NMS for device performance/availability, network params (throughput/latency/jitter/packet loss), intrusion/breaches with alerts, threshold-based alarms/notifications, data center environment, power utilization/backup.

AT&T Response:

Comply.

The AT&T ESInet™ solution is supported by a unified operational support model consisting of the Network Operations Center (NOC), Security Operations Center (SOC), and AT&T 9-1-1 Resolution Center, delivering continuous 24x7x365 monitoring, maintenance, and support for the NG911 ESInet and associated Next Generation Core Services (NGCS). **24x7x365 Operations and Single Point of Support.** The AT&T ESInet™ Network Operations Center (NOC) is staffed 24x7x365 to actively monitor and manage ESInet services, network connectivity, and NG911 functional components. The NOC serves as the single operational monitoring and coordination point for the NG911 system, ensuring continuous visibility, proactive incident detection, and rapid response.

When a potential or actual customer-affecting condition is detected and determined to be an incident, the NOC immediately engages the AT&T 9-1-1 Resolution Center, initiating established escalation, notification, and restoration processes. All operational activities are executed using documented, ISO 9001:2008-compliant processes for incident management, resolution, and reporting. eMonitoring of ESInet, Network Performance, and Infrastructure the AT&T NOC performs end-to-end monitoring of the entire ESInet, including all connections, interconnection points, and NG911 functional components involved in the routing and delivery of 911 communications. This includes continuous oversight of:



- Device availability and operational status
- Network performance metrics, including throughput, latency, jitter, and packet loss
- Alarm generation based on defined thresholds with prioritized notification and escalation
- Environmental conditions at data centers and points of presence housing critical ESnet components
- Power utilization, UPS systems, and backup power infrastructure supporting NG911 services

Enterprise-grade Network Management Systems (NMS) provide real-time visibility and “single-pane-of-glass” monitoring, enabling proactive identification of conditions that may affect service quality or availability.

9-1-1 Resolution Center Interface and Incident Response

The AT&T 9-1-1 Resolution Center is responsible for accepting incoming trouble reports and serves as the first line of support for PSAPs and Originating Service Providers (OSPs). The Resolution Center includes Tier 1, Tier 2, and Tier 3 technical staff responsible for rapid identification, isolation, and mitigation of incidents.

- Tier 1 support initiates incident handling and engages Tier 2 and Tier 3 resources as required for high-priority or complex conditions
- Operations are staffed from two geographically diverse facilities located in Atlanta and Chicago, ensuring survivability and continuity
- If troubleshooting requires coordination with an OSP, AT&T directly contacts the appropriate wireline, wireless, and/or VoIP carriers, providing full turn-key 24x7x365 support

Remote and On-Site Maintenance and Restoration

The AT&T NOC and Resolution Center are equipped to perform remote diagnostics, maintenance, and restoration of alarms and incidents. If on-site intervention is required, the Resolution Center dispatches appropriate technical resources as soon as possible to implement corrective actions either on-site or via secure remote access.

8.3.2. Security Operations Center (SE)

The proposed solution requires the services of a Security Operations Center (SOC). The SOC (Security Operations Center) may be combined with the NOC and shares the overall requirements. The SOC must provide support for the following items:

- 24x7x365 operation.
- Capability to perform remote maintenance and restoration of security events.



- Single point that performs continuous monitoring, maintenance, and network support services of the NG911 System and identifies security faults.
- Interfaces with the help desk and the PSAPs or designated staff.
- Staffed with appropriate technical resources to aid troubleshooting, diagnosis, and recovery from security issues.
- Perform security monitoring of the entire NG911 system, all connections and functional components used in the routing of 911 calls.
- Security compliance testing, penetration testing, vulnerability testing, etc.
- Collection and monitoring security logs, and assist with incident response
- Operational security administration such as identity & access management, key management, firewall administration, etc.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24×7×365 SOC (possibly combined with NOC) with remote maintenance/restoration of security events.
- Single point for monitoring/maintenance/support identifying security faults.
- Interface with help desk/PSAPs.
- Staffed for security troubleshooting/recovery.
- Security monitoring of system/connections/components.

AT&T Response:

Comply.

AT&T provides a robust Security Operations Center (SOC) capability that operates 24×7×365, delivering continuous cybersecurity monitoring, analysis, and incident response for the entire NG911 system. The SOC operates in close coordination with the AT&T NOC and 9-1-1 Resolution Center, forming an integrated operational and security monitoring framework for ESInet and NGCS services.

Global, 24×7×365 SOC Operations

AT&T's MPLS core network (AVPN), which underpins AT&T ESInet™, is supported by eight Security Operations Centers located across North America, Latin America, Europe, and Asia Pacific. This global SOC footprint ensures continuous follow-the-sun coverage, redundancy, and rapid response to security events.

The SOC provides centralized security monitoring and serves as the single point for identifying, analyzing, and responding to security incidents impacting the NG911 system, its connections, and associated infrastructure.



Security Monitoring, Detection, and Response

The AT&T SOC performs continuous security monitoring across the ESNet and supporting network infrastructure, including:

- Detection of security events, anomalies, intrusion attempts, and policy violations
- Collection, aggregation, and monitoring of security logs across NG911 systems and network devices
- Issuance of real-time security alerts and coordination with operational teams
- Remote investigation, containment, mitigation, and restoration following security incidents
- Integration with Security Information and Event Management (SIEM) platforms as required

The SOC also performs ongoing vulnerability assessments across AT&T's network to continually evaluate and strengthen security posture.

Security Expertise and Operational Scale

AT&T brings unmatched scale and depth in cybersecurity operations, including:

- More than 1,500 dedicated security experts supporting AT&T networks and services
- Over 9,000 AT&T-badged sales and technical personnel trained in security disciplines
- A security portfolio used to protect AT&T data centers and networks carrying more than 670 petabytes of data traffic on an average business day

These same security capabilities, processes, and tools are leveraged to protect the ESNet and NG911 operational environments.

Security Operations and Administration

In support of NG911 operations, the SOC provides or supports:

- Identity and access management controls
- Key and certificate management
- Firewall and security policy administration
- Security compliance testing, vulnerability testing, and penetration testing
- Coordinated incident response with the NOC, 9-1-1 Resolution Center, PSAPs, and designated authority staff

Security incidents are managed using documented incident response procedures with defined escalation paths and coordination to ensure continued NG911 service availability.



8.3.3. Help Desk

A help desk will be included with the NG911 system. The help desk(s) will operate on a 24x7x365 basis and be adequately staffed by resources who are trained and qualified in help desk and customer support services.

The help desk will serve as a single point of contact for all NG911 system and service matters, including without limitation, the NG911 system, all components of the NG911 system, and any additional system service providers delivering services or components for the NG911 ecosystem.

Only a fully staffed help desk will be considered. The help desk must not use an automated attendant or other automated means of answering a call.

The help desk must be accessible via various methods including voice, text, email, and other means as deemed appropriate or as directed by the State.

The help desk will have the ability to communicate directly and immediately with maintenance and support services for the NG911 system and all components of the system, including, without limitation, network troubles. This includes partner providers who are performing or supplying services within the system.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24x7x365 staffed help desk trained in support.
- Single point for all system matters/components/providers.
- No automated attendant.
- Accessible via voice/text/email/etc.
- Direct/immediate communications with maintenance/support including network troubles/partners.

AT&T Response:

Comply.

The AT&T 9-1-1 Resolution Center is the first point of contact for PSAPs and OSP's and responsible for accepting incoming trouble reports and serves as the single point of contact for all AT&T ESInet issues. The AT&T 9-1-1 Resolution Center provides support 24x7x365 and is the first line of support for PSAPs and OSPs. The AT&T 9-1-1 Resolution Center is fully staffed by AT&T Managers and has two locations (Atlanta & Chicago) that back each other up.

AT&T 9-1-1 Resolution Center Responsibilities for AT&T ESInet™ includes the following:

- Single Point of Contact for PSAP customer trouble reporting and support
- Tiered technical support providing Incident Management and follow-up



- Outage response and PSAP notifications
- Coordination with all teams in support of resolving an issue or question
- Customer contact for:
 - PSAP abandonment requests and test calls
 - Emergency Customer PSAP re-route requests
 - AT&T ESInet™ Reporting Portal password resets
 - Voice quality troubleshooting support
- Coordination of AT&T technician field dispatches for AT&T ESInet™ PSAP Network Edge Equipment Area
- Trouble Reporting
- A dedicated AT&T Toll-Free number has been established for our AT&T ESInet™ 9-1-1 customers to utilize for reporting and obtaining/providing status on issues. AT&T also provides you with our AT&T Express Ticketing Portal for creating and checking status on open trouble tickets. Historical trouble ticket information is retained in this portal for 60 days after the ticket is closed.
- AT&T does not currently offer the option of opening a 9-1-1 ticket via email, as AT&T considers email an unreliable form of communication for reporting 9-1-1 Service Troubles.

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 State to determine the appropriate contact list.

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.

AT&T has extensive experience in 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 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.



8.3.3.1. Trouble Handling and Ticketing Requirements

Trouble handling, and trouble ticket tracking services will be required for the successful operation of the NG911 system and services.

To ensure that all trouble tickets are resolved in a timely manner, The contractor will develop and maintain an escalation guideline document that describes the escalation procedure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Trouble handling/tracking.
- Escalation guideline document/procedure.

AT&T Response:

Comply.

AT&T has long established trouble handling and ticketing processes that are part of AT&T's 9-1-1 Resolution Center. These processes have been refined over the years to accommodate the evolving requirements of the Public Safety customers we support on a 24 X 7 basis across the United States. To aid the restoration of mission critical Public Safety applications and services, AT&T has a well-defined Escalation Document that outlines type of issues, time for response, time for resolution and finally an escalation chart that feeds up to Executive Leadership of the AT&T Resolution Center.

For any critical event or major outage, the dedicated AT&T Service Manager will provide the initial report within 5 days as required by the State of Nebraska or designated 9-1-1 staff

1. Reason for Outage (RFO) Reporting

In the event of an incident that meets pre-defined guidelines and requested by the customer, AT&T will prepare a preliminary RFO report within 3 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 within 28 calendar days, that describes the impact of the event, the cause, resolution, and any preventative steps that may be taken to eliminate future events.

- 2. A dedicated AT&T Toll-Free number has been established for our AT&T ESInet™ 9-1-1 customers to utilize for reporting and obtaining/providing status on issues. AT&T also provides you with our AT&T Express Ticketing Portal for creating and checking status on open trouble tickets. All trouble tickets should be opened through the 911 Resolution Center for proper tracking and timely resolution. Trouble issues should not be reported to technicians or the 911 Service Exec via phone, text message, or e-mail. Trouble tickets remain open until there is resolution of the identified issue. Historical trouble ticket information is retained in this portal for 60 days after the ticket is closed.**



AT&T's Resolution Center maintains ownership of all issues through resolution up to and including engaging vendors where appropriate. 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. Tier 1 support engages Tier 2 and Tier 3 support as required to assist in resolution of high priority tickets and complex alarms.

3. Under AT&T ESInet™, the ticket opened by the 9-1-1 NOC will automatically generate an e-Bonded ticket to the AT&T ticketing system monitored by the AT&T 9-1-1 Resolution Center. For severity level 1 issues, the 9-1-1 NOC will also place a phone call to AT&T 9-1-1 Resolution Center to notify the AT&T E9-1-1 Resolution Center of the issue. In cases where eBonding is not available, the AT&T E9-1-1 Resolution Center and 9-1-1 NOC will exchange trouble reports and request support via phone call.
4. A dedicated AT&T Toll-Free number has been established for our AT&T ESInet™ 9-1-1 customers to utilize for reporting and obtaining/providing status on issues. AT&T also provides you with our AT&T Express Ticketing Portal for creating and checking status on open trouble tickets. Historical trouble ticket information is retained in this portal for 60 days after the ticket is closed. All tickets remain open until we have concurrence from the reporting party or PSAP that the issue has been resolved. Only then do we close a ticket.

In the event of an outage, AT&T applies immediate and sustained effort, 7x24, until the service is restored. We use all reasonable efforts to restore service within an agreed upon time frame of the issue being detected. The Incident Commander and Incident Administrator will call upon whatever resources are required to identify and restore functionality. Again, all tickets remain open until we have concurrence from the reporting party or PSAP that the issue has been resolved. Only then does AT&T close a ticket

5. The AT&T Resolution Center is always the first point of contact for PSAPs and OSPs. These two fully manned support centers are located in Chicago and Atlanta. They are fully staffed by AT&T managers on a 24 x 7 x 365 basis. A dedicated AT&T Toll-Free number has been established for our AT&T ESInet™ 9-1-1 customers to utilize for reporting and obtaining/providing status on issues. AT&T also provides you with our AT&T Express Ticketing Portal for creating and checking status on open trouble tickets. Historical trouble ticket information is retained in this portal for 60 days after the ticket is closed.
6. AT&T has clearly defined processes, tools, and resources that address outages or service impacting events. As part of our AT&T 9-1-1 Resolution Center, AT&T has defined metrics and associated escalation procedures in place to ensure the appropriate level of visibility are achieved including notification of AT&T Executives ensuring rapid resolution of the identified issues. An escalation framework has been supplied as an attachment along with additional information that addresses AT&T's approach to customer care in support of AT&T ESInet.

8.3.3.2. Monitoring of Applications and Equipment



Proactive monitoring of all NG911 system components for operation, performance, and fault conditions will be provided.

The contractor will ensure that all alarms including environmental status alarms are received and monitored in a Network Operations Center (NOC).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Proactive monitoring of components for operation/performance/faults.
- Receipt/monitoring of alarms including environmental in NOC.

AT&T Response:

Comply.

The AT&T NOC uses a comprehensive set of tools for monitoring and management of the solution.

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. Delivery of monitoring reports, including bandwidth utilization and connectivity are provided as mutually agreed upon during contract negotiations. Traditional network management tools are complemented by active application monitoring and alerting. AT&T ESInet application elements will 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. Visual alerts are available 24x7x365 to the 9-1-1 NOC. These systems also provide ICMP and SNMP trending and threshold alarming.

In addition, the NOC provides continuous system support and monitoring 24x7 to each ALI node and to the database management system. The NOC also monitors all PSAP connections into the ALI nodes at the application level. Staffing in the NOC is second to none in the industry with Tier 1 through Tier 3 support staff on duty 24x7x365.

The following are key highlights for the network management system (NMS):

- The five state levels from NMS are as indicated: Critical, Major, Minor, Warning, and Normal
- We provide notification to the 24x7x365 NOC
- We provide notification by email and SMS
- Notification levels are defined by the supporting entity

We are capable of alarm suppression by time, quantity, and a combination for reducing alarm notifications. For example, we can say “no more of a certain alarm for the next 30 minutes” or we can say “send me duplicate alarms every 5 minutes”



Alarms we typically process are SNMP traps, local agents, and polling

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

All ESInet network, system and application components are monitored as outlined above. Critical and major alarms are sent to the 24x7x365 NOC for immediate investigation.

The fault management system used for monitoring and alarming retains logs for all events. The event logs are available onsite for three months, after that time these logs are move to storage and retained for three years. The fault management system in place is high availability system with geo-redundancy. The geo-redundant sites are mirrored and run in an 'active active' mode.

The system allows for dynamic configuration of notification thresholds, as well as the definition of new alarm categories.

8.3.3.3. Root Cause Analysis

The contractor is required to provide a complete Root Cause Analysis (RCA) for any trouble with the system. The RCA process will follow a process like the following:

- Following any critical event or major outage, the State/designated staff must receive a root cause analysis within five (5) business days.
- Immediately after a trouble has been identified the contractor will begin documenting the information as they complete the RCA. This documentation will be made available to the State via a shared online platform that will allow for constant tracking by the State as more information becomes available.
- The RCA format will include dates, times, and discoveries by the contractor as they investigate the trouble.
- Once the investigation has concluded the RCA must be submitted to the State for acceptance and approval that the trouble has been resolved.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- RCA for troubles (within 5 business days for critical/outages).
- Immediate documentation shared online.
- Format with dates/times/discoveries.
- Final submission for State approval.



AT&T Response:

Comply.

AT&T will perform a Root Cause Analysis (RCA) for any trouble on the system.

1. After trouble has been identified, AT&T will immediately begin documenting the information during the RCA investigation. The documentation will be made available to the State via a shared online platform and updated as the investigation unfolds.

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. 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.

2. At the time of initial notification and from that point on, the AT&T Service Manager will provide as much updated status information that is available at the time, including but not limited to: dates, times, 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.
3. 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 within 30 calendar days (or as otherwise agreed to by the State), that describes the impact of the event, the cause, resolution, and any preventative steps that may be taken to eliminate future events.

8.3.4. Customer Support Services

The Respondent must provide a description and/or documentation that supports the requirements in this section, including SLA management (performance/monitoring/delivery/reporting/review); event/incident management; diagnostics/reporting; problem resolution/trouble handling; network fault monitoring; request fulfillment; access management; remote diagnostics; environmental requirements;



capacity/change/configuration/transition management; training; commercial availability; all tied to SLOs for SLA measurement.

The contractor is required to provide monthly updates to the PSC regarding the performance of the system in the form of a Monthly Performance Review which is used to measure adherence to the contract elements, the performance measures, and Key Performance Indicators (KPIs). The KPIs are directly tied to the SLA.

Anticipated support services include:

- Service Level Agreement (SLA) management
 - Performance measurement and monitoring
 - Guaranteed delivery
 - SLA reporting and review
- Event management
- Incident management
- Diagnostics and reporting
- Problem resolution/trouble handling
- Network fault monitoring
- Request fulfillment
- Access management
- Remote diagnostics
- Environmental requirements
- Capacity management
- Change management
- Configuration management
- Transition management
- Training arrangements
- Commercial availability

Each of the items listed above are tied to Service Level Objectives (SLO) that the State measures against the Service Level Agreement (SLA).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SLA management (performance/monitoring/delivery/reporting/review) on a monthly basis to the PSC.



- Event/incident management.
- Diagnostics/reporting.
- Problem resolution/trouble handling.
- Network fault monitoring.
- Request fulfillment.
- Access management.
- Remote diagnostics.
- Environmental requirements.
- Capacity/change/configuration/transition management; training.
- Commercial availability.
- All tied to SLOs for SLA measurement.

AT&T Response:

Comply.

AT&T will provide customer support services as a component of the AT&T ESInet offer. AT&T will follow best practices such as ISO, ITIL, and PMI and other industry related standards. AT&T will provide customer support to the State of Nebraska, PSAPs, and other system service providers as necessary or as designated by the Board. The AT&T solution includes a dedicated Program Manager, dedicated Service Manager and Customer Advocate/Trainer for the life of the agreement.

AT&T has deep support provisions in place to support AT&T ESInet and utilizes industry best practices such as ISO, ITIL and PMI among other industry-related performance-based standards in the support of AT&T ESInet. Our support posture is backed by AT&T's 24x7x365 Resolution Center, the Network Operations Center, AT&T's Product Management, Service Delivery and Program Management organizations. The AT&T ESInet managed service includes a 9-1-1 Resolution Center and Network Operations Centers (NOC) /Security Operations Centers (SOC) dedicated solely to monitoring and managing 9-1-1 processes and system elements. 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 will work hand in hand with the AT&T Service Manager who is designated to the State of Nebraska ESInet project. The Service Manager will provide status updates and reports to the State of Nebraska. Shown on the following pages is the Incident Communication Plan which outlines how AT&T communicates with PSAPs, OSPs, and vendors.



AT&T has provided an overview of our industry leading Service Level Agreements (SLA's) that are included as part of the AT&T ESInet standard offer. AT&T is willing to review our standard Service Level Agreements and negotiate with the Statewide 9-1-1 Board on a final list of mutually agreed upon Service Level Agreements.

AT&T ESInet has a standard set of SLAs that come with the offer and any deviation from the AT&T ESInet's standard SLA's may require additional costs to accommodate for new processes required to develop, measure, capture, monitor and account for mutually agreed upon SLA's.

AT&T and our assigned resources (Program Manager & Service Manager) will be able to provide weekly status/reports on project specific items during the standing weekly calls that the Statewide 9-1-1 Board and its consultant holds. Service Level Agreement reports are provided monthly and will be reviewed as part of any standing calls put in place by the State of Nebraska and AT&T. Other customer reports will be delivered on a mutually agreed upon frequency that addresses the needs of the Statewide 9-1-1 Board and the consultants who support the project.

AT&T Program Manager – Dedicated resource and overall lead for the project who will address a wide range of topics ranging from contractual, project timeline, project objectives, technical/operational items, SLAs, and other activities deemed necessary to successfully implement, test, maintain AT&T ESInet within the State of Nebraska.

AT&T 9-1-1 Service Manager – Dedicated resource and overall lead within AT&T to address service impacting events within the State of Nebraska. This resource will work in unison with the AT&T Program Manager to ensure that the proper levels of communication are in place to address notification of service impacting issues, maintenance of AT&T ESInet and any contract required reporting requirements. The AT&T 9-1-1 Service Manager will also serve as the primary escalation path within AT&T to address all AT&T ESInet service impacting issues and will work hand in hand with the AT&T 9-1-1- Resolution Center.

8.4. Monitoring and Event Management

8.4.1. Alarm Categories

Alarms by event types depending on the criticality of the event (i.e., critical, major, etc.) will be provided. Dynamic configuration of notification thresholds will be utilized to allow new alarm categories to be defined, as necessary.

The system will have automatic notification of the NOC when alarm conditions are detected. Different notification and escalation procedures may apply depending on the alarm category.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Alarms by criticality (critical/major/etc.).



- Dynamic notification thresholds for new categories; automatic NOC notification.
- Varying notification/escalation per category.

AT&T Response:

Comply.

AT&T ESInet's monitoring and event management framework complies with the State's alarm categorization requirements by implementing a structured, severity based alarm model integrated with continuous, automated NOC monitoring. Alarms are classified by criticality to ensure appropriate prioritization and response, with dynamically configurable thresholds that allow new alarm categories to be introduced as operational needs evolve. Upon detection of alarm conditions, notifications are automatically generated and delivered to the 24/7/365 Network Operations Center, with escalation procedures tailored to the severity and impact of each event. This approach ensures rapid awareness, proportional response, and consistent operational oversight across the ESInet.

Alarm Categorization by Criticality

AT&T's monitoring systems classify alarms by event severity (e.g., critical, major, minor), enabling prioritized handling of incidents that may affect emergency service availability or performance.

Dynamic Notification Thresholds

Alarm thresholds are dynamically configurable, allowing AT&T to define, modify, or introduce new alarm categories as the ESInet evolves or as operational requirements change.

Automatic NOC Notification

All alarm conditions automatically generate notifications to AT&T's dedicated 24/7/365 Network Operations Center, ensuring immediate visibility and timely initiation of response actions.

Tiered Notification and Escalation Procedures

Notification and escalation workflows vary by alarm category, ensuring that higher severity events trigger expedited response, broader notification, and enhanced escalation, while lower impact events are handled through standard operational processes.

8.5. Change, Maintenance, and Release Management

8.5.1. Change Management Requirements



The Contractor shall ensure that all changes – planned or unplanned – are managed through a structured, documented, and auditable process that maintains service stability, security, and interoperability. The process shall conform to the principles of the **Project Management Institute (PMI)** and the **ITIL v4 Service Management Framework**.

Objectives

The objectives of the Contractor’s Change Management process shall be to:

- Maintain a stable and secure NG911 operational environment.
- Minimize the impact of changes on system availability, reliability, and public safety operations.
- Provide transparency and accountability for all system modifications.
- Ensure that all stakeholders are informed, consulted, and prepared for any change that affects service delivery.
- Incorporate continuous improvement through post-implementation review and process enhancement.

The Change Management process shall apply to all infrastructure, applications, systems, and interfaces under Contractor operational control, including but not limited to:

- **ESInet Infrastructure:** routers, firewalls, switches, circuits, transport paths, and interconnections.
- **NGCS Components:** ESRP, ECRF/LVF, PRF, BCF, LIS, logging, and policy routing elements.
- **Call Handling Systems:** software, hardware, operating systems, and integrations with CAD, logging, and recording systems.
- **Security Systems:** encryption, certificates, firewalls, intrusion detection/prevention, and access controls.
- **Support and Management Tools:** monitoring platforms, ticketing systems, and network management applications.

Change Classification

The Contractor shall classify all changes into the following categories:

- **Standard Change:** Pre-approved, low-risk, repeatable changes executed according to preestablished procedures (e.g., routine software patching).
- **Normal Change:** Planned changes that require full evaluation, testing, review, approval, and scheduling.
- **Emergency Change:** Unplanned changes necessary to restore service, mitigate critical vulnerabilities, or prevent imminent service degradation.



Each classification shall have documented criteria, approval authorities, and implementation procedures.

Process Requirements

The Contractor shall implement a formal Change Management process that includes the following elements:

- **Change Management Plan:** A documented process outlining governance, roles, responsibilities, and workflows aligned with PMI and ITIL best practices.
- **Change Advisory Board (CAB):** A standing review body, including State representation, responsible for evaluating and approving all Normal and Major Changes.
- **Change Request System:** A centralized, auditable tool for logging, tracking, and managing all changes from request through closure.
- **Risk and Impact Assessment:** An analysis of each proposed change to evaluate its impact on system performance, service continuity, interoperability, and cybersecurity.
- **Rollback and Contingency Plans:** Documented procedures for reverting or recovering from unsuccessful change implementations.
- **Change Scheduling and Coordination:** Change windows coordinated with the State and PSAPs to minimize service disruptions.
- **Notification Requirements:** Written notice to affected stakeholders no less than ten (10) business days prior to implementation of any planned change, unless otherwise authorized.
- **Post-Implementation Review (PIR):** A formal evaluation of significant or failed changes to identify root causes, corrective actions, and process improvements.

Emergency and Security Changes

- The Contractor shall maintain procedures for the execution of emergency changes required to restore service or address urgent security vulnerabilities.
- All emergency changes shall be documented and submitted for retrospective review by the CAB within five (5) business days.
- Security-related changes, including software updates, certificate renewals, or configuration modifications, shall comply with PMI and ITIL Change Enablement best practices.
- Security changes shall be tested in a controlled environment prior to production deployment whenever feasible.
- The Contractor shall notify the State of any emergency or security change within twenty-four (24) hours of implementation.

Integration with Other Service Management Processes



The Contractor shall integrate Change Management with the following processes:

- **Configuration Management:** Each change shall be linked to affected Configuration Items (CIs) within the Configuration Management Database (CMDB).
- **Incident Management:** Changes shall be correlated with incident and problem records to support root cause analysis and continuous improvement.
- **Release and Deployment Management:** The Contractor shall coordinate releases to ensure version control and documentation integrity across environments.

AT&T Response:

Comply.

AT&T ESInet complies with the State's Change Management requirements by implementing a structured, documented, and auditable change management process aligned with PMI principles and the ITIL v4 Service Management Framework. The process is designed to maintain a stable, secure, and interoperable NG911 environment while minimizing risk to availability, reliability, and public safety operations. AT&T's approach ensures transparency and accountability for all planned and unplanned changes, incorporates formal risk and impact assessments, provides timely stakeholder notifications, and includes post implementation review to support continuous improvement. Change management is fully integrated with configuration, incident, and release management processes to ensure controlled evolution of ESInet and NGCS services.

Change Management Scope

AT&T applies formal change management controls to all infrastructure, applications, systems, and interfaces under its operational control, including ESInet infrastructure, NGCS functional elements, call handling systems, security components, and operational support tools.

Change Management Objectives

The change management process is designed to:

- Maintain a stable and secure NG911 operating environment
- Minimize impacts to availability, reliability, and emergency operations
- Ensure transparency, accountability, and traceability for all changes
- Inform and prepare stakeholders for changes affecting service delivery
- Drive continuous improvement through post implementation review

Change Classification

AT&T classifies all changes into clearly defined categories:



- Standard Changes: Pre approved, low risk, repeatable activities executed using established procedures
- Normal Changes: Planned changes requiring evaluation, testing, approval, and scheduling
- Emergency Changes: Unplanned changes required to restore service or mitigate critical risks

Each category includes documented criteria, approval authorities, and implementation procedures.

Change Management Plan

AT&T maintains a documented Change Management Plan defining governance, roles, responsibilities, workflows, and controls aligned with PMI and ITIL v4 best practices.

Change Advisory Board (CAB)

A formal Change Advisory Board is used to review and approve Normal and Major Changes. The CAB includes State participation to ensure transparency and shared decision making.

Change Request System

All changes are logged, tracked, and managed through a centralized, auditable change request system that provides full lifecycle visibility from request through closure.

Risk and Impact Assessment

Each proposed change undergoes a documented risk and impact assessment evaluating effects on system performance, service continuity, interoperability, and cybersecurity.

Rollback and Contingency Planning

AT&T documents rollback and contingency plans for changes to ensure rapid recovery if an implementation does not proceed as expected.

Change Scheduling and Coordination

Changes are scheduled and coordinated with the State and PSAPs to minimize operational impact and avoid disruption to emergency services.

Notification Requirements

Written notification is provided to affected stakeholders at least ten (10) business days prior to implementation of planned changes, unless otherwise authorized.

Post Implementation Review (PIR)



Significant or failed changes are subject to formal post implementation review to identify root causes, corrective actions, and opportunities for process improvement.

Emergency and Security Changes

AT&T maintains procedures for emergency and security related changes, including:

- Immediate execution when required to restore service or mitigate urgent risks
- Documentation and retrospective CAB review within five (5) business days
- Notification to the State within twenty four (24) hours of implementation
- Testing in controlled environments when feasible

Integration with Other Service Management Processes

Change management is fully integrated with:

- Configuration Management through linkage to Configuration Items (CIs) in the CMDB
- Incident and Problem Management to support root cause analysis and trend resolution
- Release and Deployment Management to ensure version control and documentation integrity

8.5.1.1. Security Considerations in Change Management

In conjunction with the change management processes defined in §E-9.5.2 (Scheduled Maintenance Process) and §E-9.5.3 (Software Update and Improvements) of this document, the contractor must evaluate the **security impact** and **operational risk** for all changes to NGCS elements and the ESInet – including equipment, software, and configurations. Every change requires **policy-compliant review and approval, a documented security review, and complete records**. If timing precludes standard pre-approval (Unplanned/Emergency [timecritical issues with expedited workflows] issues), all required reviews and documentation must be completed immediately after implementation. The contractor should utilize segregation of duties, maintain configuration baselines, and coordinate maintenance windows to protect call delivery, routing, location accuracy, latency, and availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Evidence that all changes are reviewed and approved per policy with a documented security review (threat/impact, affected NGCS/ESInet elements and services, potential customer impact, required controls and monitoring).



- An Unplanned/Emergency change process that documents expedited approvals and requires retroactive completion of all “SHALL” requirements and documentation identified in NENA-STA-040.2 §4.4 (Change Management) within a defined timeframe.

AT&T Response:

Comply.

AT&T ESInet’s change management framework complies with the State’s Security Considerations requirements by integrating formal security impact assessment, policy based review, and approval into every change affecting ESInet and NGCS components. All changes undergo documented security evaluation to assess threat exposure, operational risk, and potential service impact, with complete records maintained for auditability. For unplanned or emergency changes where pre approval is not feasible, AT&T executes expedited workflows to protect service continuity, followed by prompt completion of all required reviews and documentation. Segregation of duties, configuration baseline management, and coordinated maintenance windows are employed to safeguard call delivery, routing accuracy, location integrity, latency, and overall system availability.

Security Review and Policy Compliant Approval for All Changes

AT&T ensures that every change to ESInet and NGCS elements—covering equipment, software, and configuration—receives policy compliant review and approval supported by a documented security assessment. The review addresses threat and impact analysis, affected services and components, potential customer or PSAP impact, and required security controls and monitoring.

Documented Security Impact and Risk Assessment

Each change includes a documented security review that evaluates operational risk, cybersecurity implications, and service delivery impacts, with records retained to support traceability and audit requirements.

Unplanned / Emergency Change Handling

AT&T maintains a defined Unplanned/Emergency change process that supports expedited approvals for time critical issues required to restore service or mitigate urgent risks. All emergency changes are fully documented, and all required reviews and approvals are completed retroactively within a defined timeframe.

Post Implementation Documentation and Review

For emergency changes executed without standard pre approval, AT&T completes all required documentation and review activities immediately following implementation, ensuring compliance with established change management and security requirements.



Segregation of Duties and Configuration Baselines

AT&T applies segregation of duties and maintains configuration baselines to reduce risk and prevent unauthorized or unsafe changes. Baseline adherence is verified as part of the change and security review process.

Coordination of Maintenance Windows

Maintenance windows are coordinated to minimize risk to call delivery, routing, location accuracy, latency, and availability, ensuring that security related changes do not adversely impact NG911 operations.

8.5.2. Scheduled Maintenance Process

A scheduled maintenance process document will be developed and maintained. The process must include a methodology for coordinating and scheduling preventative maintenance activities and how those events are executed as may be necessary during the operation of the NG911 system.

During scheduled maintenance activities the ESInet and NG911 system must maintain 99.999% availability. There must not be a substantial degradation or disruption caused by the maintenance activity. However, individual components may be taken down for maintenance if an alternate route or redundant system is used to maintain the 99.999% threshold.

If a partial or total outage occurs within hours of a maintenance activity, Contractor shall issue a report within 30 days to the State detailing:

- What occurred during the outage, including system elements that were impacted
- Whether the outage was caused by, or influenced by, the maintenance activity
- What corrective actions, specifically corrective actions to the change control process, will be implemented to avoid recurrence, not just to the specific problem but to similar problems

Following any scheduled maintenance, a maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What are the results of the scheduled maintenance
- What was done during the scheduled maintenance
- How will such scheduled maintenance impact the services in operation

Following any emergency maintenance, an emergency maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What caused the emergency maintenance



- What was done during the emergency maintenance
- How will such emergency maintenance be avoided in the future

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Developed/maintained process document for coordinating/scheduling preventative maintenance.
- No degradation/disruption during activities.
- Allowance for individual component downtime with alternates/redundancy.

AT&T Response:

Comply.

AT&T's Service Management Organization will provide advanced notice of maintenance events via email, 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.

In addition, the dedicated AT&T Program Manager will work with AT&T's Service Management organization to keep the State of Nebraska informed of significant events.

AT&T will communicate to State and PSAP staff 48 hours prior to scheduled maintenance events. 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 duration of the event. Event team personnel will keep the customer informed of event progress. We adhere to stringent, internal event plan processes and procedures to include step-by-step execution procedures with the associated time frames, back-out procedures, and baseline and validation testing. AT&T includes the required back-out time within the scheduled maintenance time frame. MOPs (Methods of Procedures) are written, peer reviewed and Risk Assessed prior to scheduling any event.

The AT&T ESInet™ architecture has been designed to be extremely resilient and redundant, allowing call traffic to continue in case of a failure at one or more pieces of hardware, software or network infrastructure. This design also allows maintenance and repairs to take place without impacting PSAPs or call delivery.

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.

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.

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	• Pre-planned maintenance events or upgrades • Normal changes are categorized according to risk and impact	• AT&T shall notify customers in advance when there are potential impacts identified to the service

Change Event Definitions and Notifications Matrix

Event Type	Definition	Notification
Emergency	• Typically, unplanned events • Issues that have a potential for an immediate threat to the production environment or 9-1-1 service.	• 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 / Maintenance Plan

AT&T broadly classifies Change Management into 2 categories:

- Global Change Management Process for AT&T ESInet™ (“Change Management”) o 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”) o 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 is the process that 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 BMC Remedy 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.

Change Management Tools

AT&T utilizes both the Incident / Problem Management module and the Change Management module of Remedy 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.

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**

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.

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.

8.5.3. Software Development Process

The Contractor and all Subcontractors shall use a documented, modern software development lifecycle (SDLC) that produces high-quality code with minimal delay. At a minimum, the SDLC shall include secure coding standards, peer/code reviews, automated testing, version control, and controlled release management (CI/CD or equivalent).

For all software components directly in the NG911 call path, the Contractor and all Subcontractors shall have a process to evaluate, release, and deploy critical security patches within 72 hours of the patch's public availability. This process shall be rehearsed on a regular cadence, and rehearsal results shall be shared with the State.

When a trouble ticket or outage results in a software bug, a discrepancy report, or a required system change to prevent recurrence, the Contractor shall maintain an online, State-accessible log showing each item, severity, affected components, current status, workaround (if any), and the target fix version and release date. This log shall also include items required to bring the system into conformance with standards such as NENA-STA-010.3(including the Discrepancy Reporting function).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Modern processes for high-quality code with minimal delay.
- 72-hour release/install for critical security patches with rehearsal/results shared.
- Log of bugs/changes/estimated fixes available online.
- Updates for standards conformance.

AT&T Response:

Comply.



For our Software Development Life Cycle (SDLC) methodology, AT&T and Intrado follow the Agile model. Agile focuses on building solutions incrementally and iteratively. In Agile, self-empowered teams produce rapid and frequent deliverables of partial solutions that can be evaluated and used to determine next steps. Many Agile methodologies exist, for example Scrum, XP, Kanban, Crystal, and FDD. Intrado uses Scrum, following the Scaled Agile Framework (SAFe).

Scrum Framework

In the Scrum framework, a team produces a potentially shippable product, incrementally within a time-boxed period called an Iteration (also known as a Sprint).

1. **Iteration Planning Meeting**—At the Iteration planning meeting, the team determines the amount of work that can be accomplished within the timeframe— two weeks (or as determined by the train)—of the Iteration and selects the specific work tasks from the product backlog. The set of tasks committed to the Iteration constitute the Iteration backlog.
2. **Daily Scrum**—Each day during an Iteration, the team—including a Scrum Master who leads the meeting and a Product Owner who translates the customer needs into product features—meets in a very brief daily scrum meeting to discuss any progress and impediments to completing the assigned work for the Iteration. The purpose of the daily scrum is to inform the team on what you are working on and, if needed, to solicit team help to overcome difficulties.
3. **Iteration Review Meeting**—At the end of an Iteration, the team presents accomplishments and demonstrates working software to the stakeholders in an Iteration Review meeting. Ideally, the team demonstrates “working software”—and often, potentially shippable software. However, this is not always possible. In some cases, the team can demonstrate results of their research: slides, tables, and metrics, for instance.
4. **Team Backlog Refinement (formerly known as Grooming)**—Backlog refinement is an activity that is performed on a regular basis. The person designated as the Product Owner, and some, or all of the rest of the team review items on the backlog to ensure the backlog contains the appropriate items, items are prioritized, and the items at the top of the backlog are ready for the next Iteration Planning Meeting
5. **Iteration Retrospective**—Finally, during the Iteration Retrospective, the team discusses what did—and did not—go well during the Iteration and creates an action plan to improve the next Iteration.

Following is a description of our SAFe implementation.

Alignment

Alignment occurs before the PI Planning and is owned primarily by the Product Manager and Product Owner.

- Product Manager creates Epics or identifies Epics and reviews them with Engineering to ensure they are ready for the upcoming PI.



- Product Manager adds the Field Fix Version(s) for the PI version to the Jira Epic.
- Product Manager adds the Business Value to the Epic after working with the Stakeholders.
- Product Owner works closely with the Product Manager to ensure alignment and the Epics are clear and begins to break the Epics down into Stories.
- Epic status is set to Ready in JIRA by the Product Manager or Product Owner when the Epic is ready to be a candidate feature for the next PI Planning.
- Product Manager determines what features under development will be part of the next release.

Program Increment (PI) Planning

The PI Planning is a quarterly planning that takes place with all teams on a train. During the PI Planning, dependencies are determined, risks are identified and reviewed, and teams provide their plan for the next 12 weeks (or as defined by the train).

- The Product Manager provides the vision for the Product for the upcoming PI.
- Architectural changes are presented.
- The Agile team plans for the upcoming PI using the Epics created by the Product Manager and stories created by the Product Owner.

Agile Scrum and Software Release Process

During Agile Execution, the Agile team selects items from the product backlog to develop. This is an iterative and incremental process. Multiple Agile iterations occur during the Execution. The last iteration is reserved for innovation and planning for the next PI. The Agile team also meets in daily Scrums for the required Iterations.

- The Product Owner continually evaluates and, if necessary, adjusts product backlog priorities.
- Scrum team members pull items from the team backlog.
- Early in this phase, the Scrum Master, working with the Product Manager and Product Owner, may set a preliminary release date that may be adjusted.
- Scrum Master and team commit to deliver the release according to their iteration schedule.
- All new and existing features must pass regression testing prior to the release.
 - All regression test cycles are created by the team.
 - Third-party software and systems are upgraded to the latest version (or to the latest tested and verifiably acceptable version).
 - Regression test cases are executed by the team.
 - Bugs found during regression are analyzed during the team backlog refinement to decide whether they are fixed in the current release cycle or postponed to a future release



- Software Developers continue to fix all bugs from the release backlog until it is empty. System Team completes system level testing as needed (primarily Government Solutions [CHE] teams)
- The release training date is scheduled and communicated, if applicable. (Responsibility for this task differs and is determined by the team.)
- Product Manager determines when the release can occur. Once the Product Manager determines the release can occur, no scope can be added.

Inspect and Adapt

At the end of each quarterly Program Increment (PI), the train meets to reflect upon what went well during the PI and what can be improved. The feedback collected is turned into action items and added to the train's backlog.

Key Process Indicators (KPIs)

Generating KPI charts and reports on a regular basis provides the following value:

- Provides more visibility into an Agile Release Train (ART)
- Ensures consistency of practice across Safety Services
- Continually drives better outcomes

KPIs are generated as part of the Agile process.

Release Cycle

The following is a description of the Intrado Safety Services product release cycle. The Agile Scrum process itself does not provide recommendations on how to release software. That is, Agile does not define an organizational process nor does it define software release milestones. The following information describes our product release cycle, outside of the Agile Scrum process.

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.

At General Availability:

- User documentation, APIs, and release notes are uploaded to the tool or site where customer-facing documents are published or made available (which varies by product).
- The Official Confluence release page is updated (Scrum Master).
- An Official Release communication is sent to all groups (Scrum Master).

Bug Reporting and Resolution

The defect resolution process is tightly integrated with Intrado's SAFe software development practice. Whether the defect is found in SQA testing, in the normal cadence of Development and Testing, or found in Production by the customer, the defect, or Bug, is described in a Jira ticket. The details of how the defect was encountered, and the steps to reproduce it, are documented in the Bug Jira. The Bug Jira is then assigned to a developer responsible for the software that delivers the function, and that developer assesses the nature of the defect and estimates the scope, or size in terms of duration, it will take to correct the defect. Per the SAFe process, the development team meet bi-weekly in a SAFe ceremony known as "Refinement" to review the backlog of development work, it is during this ceremony that priority is determined for the Bug Jira and its resolution is assigned to a release. The urgency of the defect fix will determine whether the resolution will make it into the current release under development or whether it will be resolved in a future release. In the case that the defect is determined to be exceedingly urgent the defect may also be addressed outside the SAFe process and given the highest priority and deemed a software patch that will need to be deployed immediately under the Change Management process. A reporting, or log, of Bugs is available from our Jira systems and may be provided per the contract.

Change Management

All changes are requested through strict adherence to Service Now (SNOW) ticketing process. Changes are submitted in SNOW with detailed description of the proposed change, including Method of Procedure (MOP) documents describing the Change implementation and backout procedures. A Change Approval Board (CAB) is assembled on a weekly basis to review SNOW requests, identify organizational responsibility, and subject



matter experts (SME) required for work, review the thoroughness of MOP's, the Key Performance Indicators (KPI) of success versus failure of change, and schedule the Change Event to implement the requested change (frequency of CAB meetings vary based on volume of SNOW tickets in the queue and their urgency). All approved changes and MOPs are exercised in pre-production labs to validate the change procedure and backout processes in advance of Change Event execution. Immediately following Change Event execution, the systems enter a high visibility "soak period" (soak periods vary in duration based on system access/usage volumes) where Network Operations and Organizational owners monitor the operation and performance of changed systems to ensure the systems are performing optimally, e.g., KPI's are being met, before final Change Event completion is declared. A reporting, or log, of SNOW change activity is available and may be provided per the contract.

Security Patches

Security Patches are given the utmost priority and are immediately remediated within 72hrs of Security Advisory and/or Patch availability. The process follows our Change Management intake process, initiated by SNOW ticket submission, but the invocation of CAB and SAFe/Jira Development processes are accelerated, where Executive and Operational Organization sponsors shepherd the CAB process, on an as-needed/adhoc basis outside the normal weekly CAB cadence, to assess scope and risk of remediation, while ensuring that critical staff are available to implement and test remediation patches in pre-production labs, as well as test deployment process and backout plans in advance of production patch deployment. Likewise, a reporting, or log, of SNOW change activity is available and may be provided per the contract.

8.5.4. Software Updates and Improvements

Updates, bug fixes, and patches must be classified by the contractor as normal or emergency. When any normal hardware or software changes are made to a site, there will be a minimum of 30 days before any hardware or software changes can be made to any other site. Where more than one instance of a function or service is provided on a site, only one instance can be changed at a time. Where there are both multiple sites and redundant instances per site, one instance may be changed at the first site, at least 30 days must elapse, one instance on another site can be made, at least two weeks must elapse, another instance can be updated, after which at least one week must elapse before the next change.

Emergency bug fixes/patches are not required to meet these minimum times. However, if the contractor determines that an emergency bug fix/patch is necessary, it will transmit a report to the State within 48 hours of such a determination, detailing the problem, the necessary fix, and a valid reason the fix could not be completed in regular software update or bug fix processes.

A prescheduled maintenance window will be negotiated between the contractor and the State. All normal maintenance will take place within that window. Extra-ordinary maintenance processes that require additional time may be scheduled with a minimum of 30 days' notice.



Emergency maintenance can be scheduled with no prior notice, but the State must be notified immediately that such an emergency maintenance is needed, what the estimated duration is and why the emergency maintenance is necessary.

The Respondent must provide a detailed methodology for managing all system updates, including software patches, security updates, configuration changes, and data updates (e.g., GIS data). The process must be structured to minimize service disruption, ensure system integrity, and maintain security. The update process must include procedures for testing, scheduling, deployment, and verification of all changes in the production environment.

A formal process for releasing software updates, bug fixes and improvements, and any changes to the process will be communicated to the State within 30 days of the change being put into practice.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Formal process for updates/fixes/improvements with 30-day notice of changes.
- Classification as normal/emergency.
- Minimum 30-day spacing for normal changes across sites/instances.
- No minimum times for emergency but 48-hour report to State.
- Negotiated maintenance window.
- Extra-ordinary with 30-day notice.
- Immediate notification for emergency with duration/reason.

AT&T Response:

Comply.

AT&T has developed a proven, mature, formal process for change management used in releasing software updates, bug fixes and improvements, summarized in the paragraphs below. Although AT&T does not anticipate major changes to the proven methodology, any modifications or improvements to the process shall be shared with the Board within 30 days of implementation.

The AT&T 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. Maintenance activities on the AT&T ESInet™ solution are designed to be completed with no scheduled downtime for the customer.

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 make 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.

8.6. Spares and Inventory

8.6.1. Spares

Respondents must describe their spares program, including stocking levels, storage locations, and the time required for an on-site field technician to obtain a spare. If the State has any role in spare stocking or access, explain that role.

A sufficient supply of spare parts shall be maintained at locations that enable immediate restoration of service. This requirement is tied to the Mean Time to Repair (MTTR) specified in §E-9 of this document. Where there are multiple connections, the Contractor shall provide multiple spare units staged in multiple locations.

Within the proposal response, explain how sparing strategies maintain both Mean Time Between Failures (MTBF) and MTTR at levels necessary to achieve 99.999% availability.

If malfunctions or failures recur, the State may require the Contractor to increase spare inventory to ensure adequate parts are available to address the repeated issue.



The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Describe the spares program, including stocking levels, locations, and technician access time
- Explain any State role in spare stocking or access
- Show how sparing maintains required MTBF/MTTR to achieve 99.999% availability

Operational Obligations (Post-Award):

- Maintain spare inventory at levels consistent with MTTR needs.
- Refresh replacement stock within twenty-four (24) hours after use
- Retain sole responsibility for restocking spare parts
- Track and report monthly on equipment failures requiring use of spare inventory
- Adjust inventory as needed and provide documentation to the State upon request
- Identify where spares are located and maintained
- Use spare inventory to support the entire proposed system, adjusting as needed
- Replenish remote parts depots when their stock is depleted • Increase spare inventory if repeated malfunctions occur.

AT&T Response:

Comply.

AT&T ESInet maintains an inventory of network components to ensure expeditious replacement of failed equipment. These include the redundant routers co-located with PSAP call handling equipment.

More importantly, the AT&T ESInet employs a six-core platform for geographic and system redundancy. Further, each core is comprised of redundant, high-availability (HA) systems with automatic failover capabilities. These multiple layers of redundancy allow for the seamless operation of the AT&T ESInet without suffering downtime while replacement equipment is being secured.

8.6.2. Spare Inventory at Data Centers

In addition to the spare inventory maintained at Contractor locations, the Contractor must maintain critical spare inventory on-site at each data center location. The Contractor must:

- Identify and provide documentation of critical spare inventory maintained on-site at each data center
- Add equipment to this list based on frequency and type of repair to ensure critical spare inventory is maintained on-site at all times



- Replenish spare parts inventory if required by the State in case of repeated malfunction or failure

This on-site inventory ensures immediate access to critical components needed to maintain the required system availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- On-site critical spare inventory at each data center.
- Identification/documentation of inventory.
- Additions based on repair frequency/type.
- Replenishment for repeated malfunctions/failures.

AT&T Response:

Comply.

The AT&T ESInet employs a six-core platform for geographic and system redundancy. Further, each core is comprised of redundant, high-availability (HA) systems with automatic failover capabilities. These multiple layers of redundancy not only provide spare resources they allow for the seamless operation of the AT&T ESInet without suffering downtime while replacement equipment is being secured. To that end, component failures with the NGCS and ESInet will be replaced without impact to the State of Nebraska PSAPs.

Additionally, AT&T manages spare equipment deployed at the NGCS and PSAPs at nearby AT&T depots and employs an advanced vendor replacement strategy. Should a device go out of service, an AT&T technician will be dispatched with a preconfigured spare to replace the faulty equipment from the depot. This allows AT&T to maintain the proper number of spares and more importantly to ensure the spares are up to date in terms of both hardware and software rev levels required as part of the AT&T ESInet solution.

Remainder of page intentionally blank



9. Value Add and Optional Services

Respondents will describe any optional services that may enhance their product or the delivery of NG911 to the State. Particularly, this may mean the ability to deliver a hosted call handling system after the ESInet has been deployed and NG911 routing is being provided.

9.1. Call Handling Equipment (CHE) Services

The PSC would like to have insight into the options a vendor may provide for CHE. PSAPs in the State may want to move to a hosted solution or an approved solution at some point during the contract period. In order to determine the viability proposers may offer a CHE solution as an option, but it is not a firm requirement at this time.

Hosted CHE is preferred; to allow PSAPs an option of moving from an on-prem call handling system into the hosted CHE platform over time.

The Respondent may provide a Call Handling Equipment (CHE) solution that serves as the primary user interface for PSAP call takers and dispatchers. The CHE must be capable of receiving and managing emergency calls from the ESInet, including support for various media types such as voice, real-time text (RTT), and video. The solution must provide an intuitive graphical user interface (GUI) that displays all pertinent call information, including caller location on a map, and integrates seamlessly with other PSAP systems like Computer Aided Dispatch (CAD) and logging recorders.

Also, the signaling and media interface at the demarcation between the ESInet infrastructure and the PSAP will comply with standards-based NG911 requirements as stated in the NG911 services section and elsewhere within the technical and operational requirements. Solutions that utilize proprietary signaling and/or media across the Access Network to End Site demarcation point, or that otherwise do not comply with the technical or operational requirements specified for this demarcation point, will not be acceptable.

AT&T Response:

AT&T understands the State of Nebraska Public Service Commission's (PSC) desire to evaluate Call Handling Equipment (CHE) options that may be required by PSAPs during the contract term, while recognizing that CHE is not a firm requirement at this time. AT&T's approach is intentionally flexible to support PSAPs at varying stages of their NG911 maturity while minimizing risk and preserving local choice.

CHE-Agnostic ESInet Architecture

AT&T's ESInet solution is **CHE-agnostic by design**, allowing PSAPs to select, retain, or transition between approved NG911-compliant CHE solutions without requiring changes to the underlying ESInet. This architecture enables PSAPs to:

- Maintain existing on-premise CHE solutions



- Transition to a hosted CHE solution over time
- Adopt future CHE solutions as operational or funding needs change

AT&T's ESInet supports CHE solutions that comply with **NENA i3 standards**, including SIP-based call signaling and RTP/SRTP media delivery, ensuring interoperability and long-term vendor flexibility. AT&T does **not** require or utilize proprietary signaling or media protocols across the Access Network to End Site demarcation point. [\[Intrado Re... v2 9.5.25 | Word\]](#)

Hosted CHE Options

Consistent with the PSC's stated preference, AT&T can support hosted CHE solutions through its established partner ecosystem. Hosted CHE offerings provide PSAPs a migration path from on-premise systems to a centrally managed, resilient call handling platform, reducing local hardware dependencies while improving scalability and disaster recovery capabilities.

Hosted CHE solutions supported by AT&T are capable of:

- Receiving and managing NG911 voice calls delivered via the ESInet
- Supporting next-generation media, including Real-Time Text (RTT) and video (where enabled by the CHE provider)
- Operating in geo-redundant, high-availability configurations

CHE Functional Capabilities

When provided, CHE solutions supported by AT&T serve as the **primary user interface** for call takers and dispatchers and include:

- An intuitive graphical user interface (GUI)
- Display of call detail and location information, including map-based visualization
- Call control, queuing, transfer, conference, and call history functions
- Integration with external PSAP systems such as:
 - Computer Aided Dispatch (CAD)
 - Logging recorders
 - Mapping/GIS platforms

Integration is achieved using standards based interfaces and established APIs, allowing PSAPs to preserve existing workflows while enhancing NG911 capabilities.

Cloud-Based Hosted CHE Solutions



In support of the PSC's preference for hosted Call Handling Equipment (CHE) solutions, AT&T's ESInet is fully compatible with leading cloud-based NG911 call handling platforms, enabling PSAPs to transition from on-premise environments to hosted CHE solutions over time without disruption to ESInet services.

AT&T's CHE-agnostic ESInet currently interoperates with, and supports, multiple production-deployed, standards-based cloud CHE platforms, including:

Motorola VESTA NXT (Cloud)

Motorola VESTA® NXT is a cloud-based evolution of the widely deployed VESTA NG911 call handling platform. When deployed in a hosted configuration, VESTA NXT provides:

- NG911 i3-compliant call processing
- Geo-redundant, high-availability architecture
- Support for voice, Real-Time Text (RTT), and multimedia services (where enabled)
- A modern, intuitive call taker interface with integrated mapping and call data display
- Standards-based integration with ESInet, CAD, and logging recorders

AT&T has extensive experience supporting ESInet connectivity to Motorola VESTA platforms across both hosted and hybrid deployments.

Intrado VIPER NextGen (Cloud)

Intrado VIPER® NextGen is a cloud-hosted NG911 call handling solution designed specifically for i3-compliant ESInet environments. VIPER NextGen supports:

- SIP based call signaling and standards based media delivery
- Voice, RTT, and multimedia handling capabilities
- Geo-diverse core infrastructure for resilience and survivability
- Browser based and workstation based user interfaces
- Seamless integration with CAD, logging recorders, and GIS systems

AT&T and Intrado maintain a long-standing interoperability relationship, and AT&T's ESInet is deployed in live production environments supporting VIPER NextGen for both centralized and distributed PSAP operations.

Carbyne APEX (Cloud-Native CHE)

Carbyne APEX is a cloud-native, NG911-aligned call handling platform designed to enhance emergency call intake through advanced user interfaces and real-time data sharing. When used in conjunction with AT&T's ESInet, Carbyne APEX can support:



- Standards-based call and data exchange over the ESInet
- Enhanced call visualization and situational awareness tools
- Integration with CAD, mapping, and external emergency data sources
- Flexible deployment models supporting primary or supplemental CHE use cases

Carbyne APEX can be leveraged by PSAPs seeking a modern, cloud-first call handling experience while remaining compliant with NG911 standards and PSC demarcation requirements.

Standards-Based Demarcation Compliance

AT&T confirms that all signaling and media interfaces at the demarcation between the ESInet and the PSAP comply with NG911 standards as defined in the NG911 Services and Technical Requirements sections of this RFP. Specifically:

- SIP signaling and media delivery are standards-based
- No proprietary protocols are required or permitted across the ESInet-to-PSAP demarcation point
- CHE solutions that rely on proprietary signaling or non-compliant media handling would not be supported
- This ensures interoperability, reduces vendor lock-in, and aligns with long-term NG911 evolution strategies.

Operational Flexibility and Future Readiness

By decoupling CHE from the ESInet infrastructure, AT&T provides the PSC and PSAPs with a future-proof model that supports:

- Incremental onboarding of PSAPs
- Phased migration from legacy or on-prem systems
- Introduction of new CHE technologies as standards mature

This approach has been successfully deployed across thousands of PSAPs nationwide and is consistent with AT&T's national NG911 architecture strategy.

9.2. ESInet and NGCS backup system

The PSC would also like to understand the options a vendor may provide to increase the diversity and redundancy of the system. This may be a tertiary alternative that could be utilized in the event of the primary system or transport failure.



AT&T Response:

In addition to the active/active twelve core NGCS, redundant and geographically diverse architecture, AT&T can provide additional ESInet value added backup services to help increase the diversity and redundancy of the end-to-end system. These disaster recovery systems include: a) cloud-based call handling continuity and disaster recovery; b) AT&T's National Disaster Response Team (NDRT) and Response Operations Group (ROG); and c) FirstNet® Wireless Backup – Tertiary Redundancy for Standalone PSAPs. These valued added services are further described in the paragraphs below.

Disaster Recovery System/Solutions

AT&T proposes a layered disaster recovery (DR) and continuity solution designed to maintain NG9-1-1 call-taking and operational capability during events that impair or disable traditional terrestrial telecommunications infrastructure, including but not limited to fiber cuts, central office outages, power failures, flooding, and wildfires.

The proposed approach combines cloud-based continuity, wireless network independence, and operational response support to ensure PSAPs retain access to critical 9-1-1 services even when primary facilities or networks are unavailable. The solution is intentionally designed to operate independently of the existing wired telecommunications infrastructure.

APEX Continuity – Cloud-Based Call Handling Continuity and Disaster Recovery

Purpose

APEX Continuity provides a cloud-hosted continuity environment that enables NG9-1-1 call-taking and operational workflows to continue when primary call handling systems, PSAP facilities, or terrestrial connectivity are unavailable or compromised.

Key Capabilities

- Cloud-hosted continuity environment capable of supporting NG9-1-1 call-taking functions during outage scenarios.
- Rapid activation and elastic scaling to accommodate sudden call volume surges during large-scale incidents.
- Remote and alternate-site call-taking support, allowing call takers to operate from secondary locations or approved remote environments (subject to Authority policy, security requirements, and integration scope).
- Public-safety-appropriate security controls, including role-based access and secure connectivity, finalized during solution design.
- Independence from Existing Telecommunications Infrastructure



Because APEX Continuity is cloud-based, it is not dependent on local PSAP facilities, central offices, or fixed terrestrial transport. The continuity environment can be accessed over any available IP path, including wireless broadband connectivity as described below, providing true operational independence during infrastructure-impacting events.

To further ensure independence from terrestrial telecommunications infrastructure, AT&T provides FirstNet wireless broadband connectivity options that allow PSAPs or remote call-taking locations to access APEX Continuity when wired connectivity is unavailable. This further enables the APEX Continuity solution to:

- Utilize wireless failover connectivity using FirstNet's nationwide wireless network.
- Provide support for temporary or mobile call-taking locations.
- Rapidly deploy a solution to support emergency response and recovery operations.

AT&T National Disaster Response Team (NDRT) and Response Operations Group (ROG)

Purpose

AT&T's National Disaster Response Team (NDRT), supported by AT&T's Response Operations Group, provides deployable, on-the-ground incident response to help re-establish and sustain communications during declared disasters or major emergency events. This service is provided at **no additional cost** to customers and is activated in coordination with public safety agencies during large-scale incidents.

Key Capabilities

- Rapid deployment of trained personnel and specialized assets to disaster-affected areas.
- Restoration and support of telecommunications infrastructure, including temporary and emergency connectivity solutions where feasible.
- Coordination with incident command, emergency management, and public safety stakeholders to prioritize communications restoration.
- Support for emergency communications needs during events such as hurricanes, flooding, wildfires, and other infrastructure-impacting disasters.

AT&T has deployed NDRT resources during major events, including hurricane responses and regional flooding incidents such as those that impacted Kerrville, Texas or Hurricane Helene in North Carolina, to assist with restoring communications and supporting public safety operations.

Independence from Existing Telecommunications Infrastructure

NDRT assets are mobile and deployable, enabling AT&T to support communications even when local wired infrastructure, facilities, or commercial power are impaired or unavailable. This capability complements cloud-based continuity and wireless access solutions by providing physical, field-based restoration and support during prolonged or severe incidents.



FirstNet® Wireless Backup – Tertiary Redundancy for Standalone PSAPs

Purpose

FirstNet Wireless Backup provides a tertiary, independent connectivity path for standalone PSAPs, enabling fast and seamless failover to maintain access to NG9-1-1 continuity and disaster recovery services when primary and secondary circuits are unavailable.

Key Capabilities

- Dedicated wireless broadband failover using the FirstNet network (Band 14).
- Priority and preemption are inherent with FirstNet, ensuring PSAP traffic receives preferential access during emergencies and network congestion.
- Supports automatic or manual failover configurations based on Authority requirements and network design.
- Enables continued access to cloud-based continuity services, remote operations, and other critical PSAP applications during outages.

Proven Public Safety Solution

FirstNet is a nationwide, public-safety-grade network purpose-built for first responders and emergency communications. Its use as a backup and failover solution is well-established across public safety environments and complements AT&T's ESInet, APEX Continuity, and disaster response capabilities.

Independence from Existing Telecommunications Infrastructure

FirstNet wireless connectivity operates independently of traditional wireline "last-mile" infrastructure, providing an alternate access path when fiber, copper, or local facilities are impaired. This makes it an effective tertiary redundancy option for PSAPs requiring high resiliency.

How the Pieces Work Together — Independent, Layered Disaster Recovery

AT&T's disaster recovery solution is intentionally designed as a layered, independent resiliency architecture that maintains NG9-1-1 operations even when traditional terrestrial telecommunications infrastructure is unavailable.

At the core of the solution, **APEX Continuity** provides a cloud-based call-taking and operational environment that is not dependent on PSAP facilities, central offices, or fixed wireline transport. When primary systems or locations are impaired, PSAP operations can rapidly transition to this continuity environment.

FirstNet® Wireless Backup serves as a tertiary, independent access path, enabling fast and seamless failover to APEX Continuity using Band 14 with inherent priority and preemption. This ensures PSAP connectivity



during congestion or infrastructure outages and eliminates reliance on the same terrestrial “last mile” as primary circuits.

In parallel, **AT&T’s National Disaster Response Team (NDRT) and Response Operations Group** provide deployable, on-the-ground support during declared disasters. These teams assist with restoring communications, establishing temporary connectivity, and supporting prolonged recovery efforts—at **no additional cost** to the State—when physical infrastructure is damaged or inaccessible.

Together, these components deliver a comprehensive disaster recovery system that is cloud-enabled, wireless-independent, and operationally reinforced, firmly addressing the requirement for a DR solution independent of existing telecommunications infrastructure, while providing Nebraska PSAPs with proven, real-world resiliency.

Remainder of page intentionally blank

10. Use Case Examples for Use with Response

10.1. Instructions

The following diagrams depict the NG911 system from a functional view. These Use Case scenarios provide Respondents the opportunity to demonstrate the traffic flow and performance perspectives of their proposed system. The Use Cases are designed to present a basis for validation of responses to the requirements of the RFP and will be used as a basis for evaluation of the delivery of traffic from caller to PSAP.

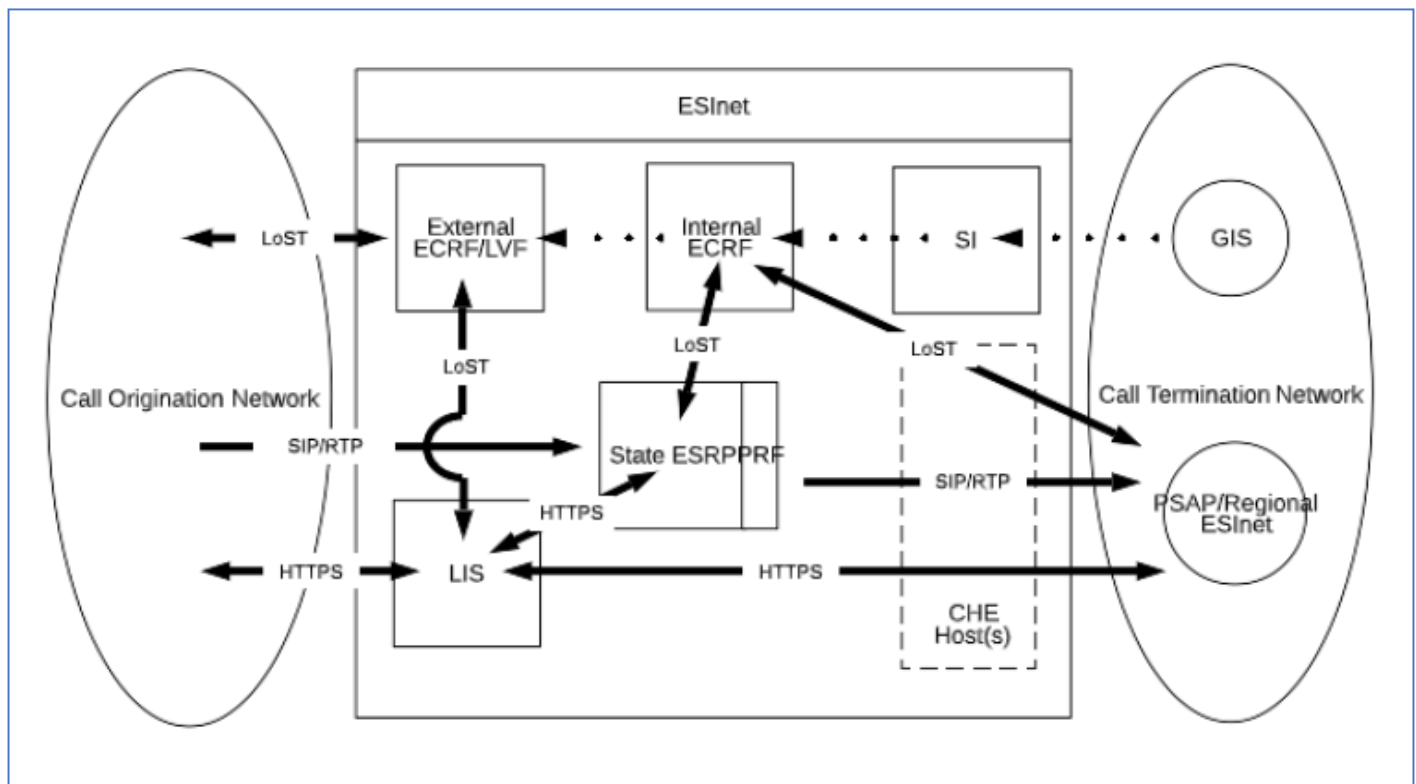


Figure 3: High-level NENA i3v3 Architecture

Remainder of page intentionally blank



High-Level Use Case and Overall Expectation

The first expectation is for the Respondent to offer a narrative of how their proposed solution will meet the functionality depicted in the above diagram.

Respondents must:

- Describe how traffic flows from the call origination network, through the core to the PSAP in step-by-step fashion.
 - At each functional element, a description shall be provided to discuss how the traffic flow is being modified or adjusted due to additional data between functional elements.
 - At each functional element, a description shall be provided to identify how the system is managed and how alerts of disruptions or incidents will automatically notify the NOC.
 - At each functional element, a description of how the interface between the functional elements will be utilized.
 - Demonstrate how the system will handle the use case presented and discuss the operation, including which partner(s) (Prime or Subcontractor) would be responsible for ingress, core, and egress.
 - Identify the bandwidth available and options to manage and monitor bandwidth between functional elements and for the entire platform.
- Describe the performance expectations of the system and explain how performance is guaranteed for legacy 911 across the entire system to egress to a legacy PSAP.
 - Identify how systems operate in a “normal” state.
 - Identify how systems operate in an “abnormal” condition.
 - Demonstrate how the platform will operate in a “fail” condition.
- Describe how security is implemented across the system while maintaining the performance guarantees expected to egress to a legacy PSAP.
 - Identify how DDoS and TDoS events are mitigated.
 - Identify how security events are mitigated at each component throughout the system, including incidents that derive from the OSP, the PSAP and other ESInets.
- Describe how 911 data is delivered to the logging and reporting system to be accessed by a PSAP.
 - Identify how databases operate.
 - Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.
 - Explain how logging is collected and accessed for legacy CDR and i3 logging.
- Describe how calls may be transferred between NG PSAPs.



- Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on the same NG911 system.
- Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on a different NG911 system.
- Describe how transfers are logged and how the data is logged. ○ Discuss the data that is transferred to the receiving PSAP. ○ Explain how logging is collected and accessed for legacy CDR and i3 logging

Describe any areas where the “span of control” on enforcement of diversity, redundancy, policies, procedures or any other automated or manual function that would limit the overall success of a call reaching a call taker is within the system.

- Explain the limitations with the proposed system in a clear manner so that the evaluation team, and the State have a clear understanding of what is being proposed.
- Gaps and limitations do not disqualify or eliminate a proposal; on the contrary an open and honest response will allow these types of issues to be documented and will lead to a collaborative plan to remediate.

AT&T Response:

Comply.

The diagram provided in the description alludes to an i3 OSP sending a call destined for a Terminating ESRP/PSAP that is also i3. The four diagrams below provide a high-level overview of the call flow and the GIS provisioning via the SI. In addition, AT&T has included a detailed document providing full call flow scenarios in ***Appendix J - AT&T ESInet Call Flow Scenarios***.

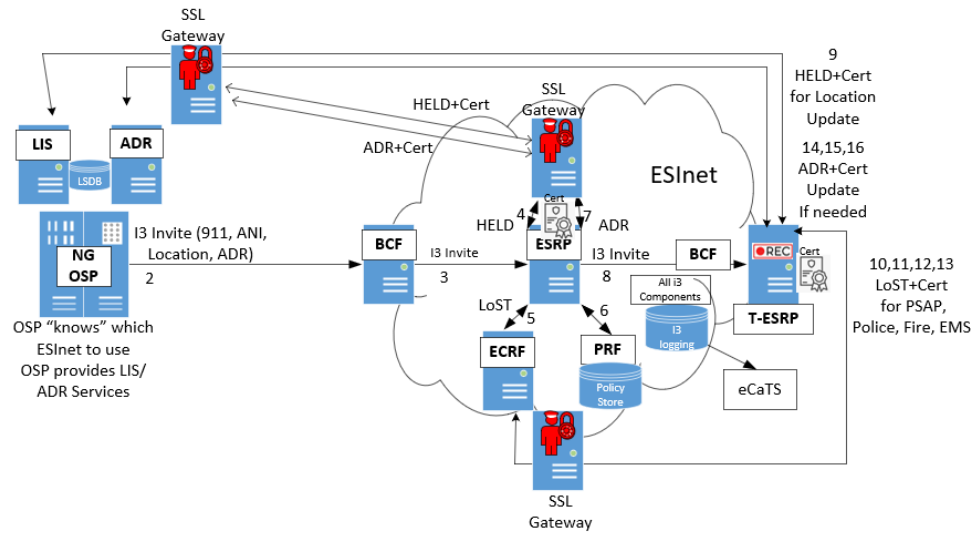


Figure 30: i3 OSP w/LIS/ADR not using NFG

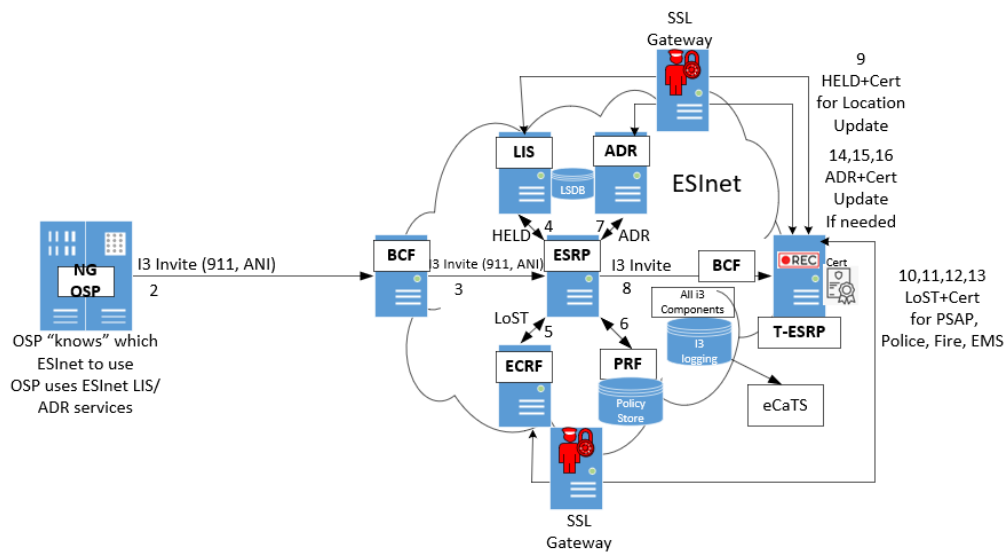


Figure 31: i3 OSP not using NFG using AT&T LIS/ADR

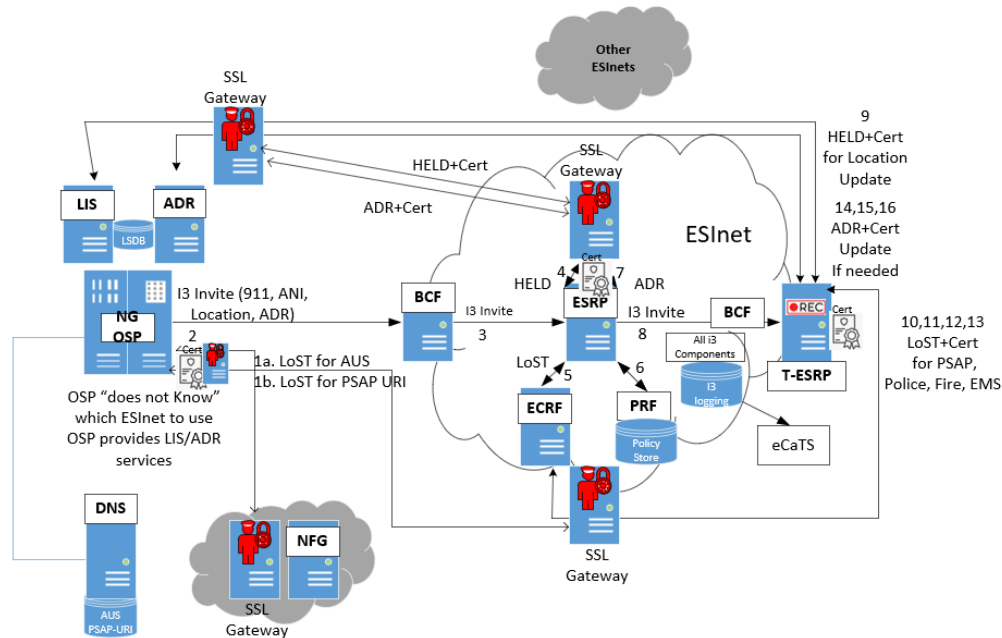


Figure 32: i3 OSP using NFG

Appendix J - AT&T ESInet Call Flow Scenarios provides detailed information on each functional element. This document shows ladder diagrams for ease of reading. For this use case, section 4 of the document provides details on the i3 ingress.

Remote monitoring of network and computer performance is conducted to provide statistical data on the number of alarms received and reported based on severity. Monitoring tools to capture the elements of a complex end-to-end service environment include New Relic and Spectrum for monitoring all network elements, data communications, computer systems, databases, remote facility environments, and the applications themselves. Multiple network management components monitor IP paths, packet rates, packet loss, retransmission, and other IP network metrics. These components generate alarms to system operators if the reliable delivery of calls or data is threatened. NOC staff can monitor the complex dependencies among these managed elements and alert the appropriate group for interpretation. This provides a method to immediately notify designated personnel of any system failures or performance degradations. Monitoring and alarming are created for each FE throughout the call flow.

The Call Scenarios document provides detailed information about how the interface between the functional elements will be utilized.

AT&T has engineered the system to support 2x the nationwide busy hour call volume. To support this, the following bandwidth is provided today.

- Intra-Core networking uses components with dual 1Gbs NICs to redundant Gigabit switches. Switches are cross connected with 10Gbs switch to switch links.



- Intra-Agg site networking uses components with dual 1Gbs NICs to redundant Gigabit switches. Switches are cross connected with 10Gbs switch to switch links.
- The aggregation sites operate with redundancy at each location and are configured at 20-40mb on 100mb Ethernet circuits or 40mb on 45mb DS-3 based circuits.
- Each core site has redundant 1 G connections to AT&T's MPLS core network (AVPN)

AT&T activity monitors both network utilization and server resource utilization. AT&T's NOC actively monitors utilization and will begin troubleshooting processes if utilization is above preset thresholds. AT&T also has internal reporting that includes the following reports:

- Backbone Network Capacity Management
- Network Aggregation Site Capacity Management
- PSAP Network Capacity Management
- Server Resource Utilization Capacity Management

AT&T uses these reports for trending purposes and augments the network or server capacities as needed.

The attached Call Scenarios document provides detailed information about normal state (sunny day) and abnormal/fail conditions. Section 2.2 describes a legacy OSP sending the call to a legacy PSAP. This includes both normal and abnormal. The Loss of RTP described in section 4 of the Call Scenarios document also includes additional details for an abnormal/fail condition.

AT&T's approach to TDoS/DDoS attacks is two-dimensional, where Ingress and Egress contingencies are solved independently.

Ingress Solution:

OSP to AT&T ingress facilities are engineered not to exceed 60% utilization under normal operating conditions. This is done with the expectation that the excess 40% capacity is available to provide on-demand network capacity in the event of spikes and bursts in demand due to either emergency events or malicious TDoS/DDoS attacks. For example, a traffic study determines the busy hours for Customers A and B requires bandwidth of 3Mbps, respectively, so AT&T plans and deploys a 10Mbps facility, and configures the Call Admission Control (CAC) so the total utilization (simultaneous sessions) is limited to 5Mbps for each customer. Combined, their respective busy hour demand does not exceed 60% of the facility capacity, and they can each burst traffic if demand spikes. Customer Source IPs are whitelisted in the Border Control Function (BCF), preventing untrusted, non-listed, Source IPs from attacking the network. The combination of whitelisted/trusted Source IPs and CAC ensures that an attack from any IP Source will not consume all the network resources that would result in the denial of service of all IP Sources. In the case of an attack, Intrado network administrators are prepared to adjust the CAC, in real-time, to expand a Customer's bandwidth in an effort to avoid the denial of service. Once the attack has concluded, the previous CAC values are restored. Regardless of the breadth of the



attack, whether it's limited to a single Customer/IP Source, or the more unlikely scenario that all IP Sources are under attack and all TDoS/DDoS contingency measures are rendered defeated and the network becomes fully consumed, Intrado will work with the serving OSPs and/or VSPs to quickly identify the bad actor attack vectors in order to block the attack before it can reach the AT&T ESInet.

Egress Solution:

There are two ways TDoS/DDoS attacks are mitigated with respect to PSAP call delivery;

1. A PSAP, via the AT&T Management Portal or the Resolution Center, can manually enter a Telephone Number (TN) into a TDoS/DDoS TN list.
2. TDoS/DDoS attacks are automatically detected by our software, SoftWare Event Evaluation Program (SWEEP). This software is coded to look at various attack patterns, recognize the pattern, and automatically put the TN into the TDoS/DDoS TN list.

*TNs will automatically age out of the TDoS/DDoS TN list; the default is 15 minutes.

When a call with a listed TN arrives, the call is given a SIP 580-banished error code, which translates to an SS7 cause code of 20. This tells the originator of the call that the number they dialed is not in service. Our experience has been that once the originator of the call gets the "not-in-service message," the calls cease.

We continue to refine this functionality and have additional TDoS/DDoS features coming soon where we will interrogate the caller and have them interact with the interrogator service to get their call delivered. Also coming are aids to the subsequent fraud investigation. The SWEEP software will perform a dispatch (not a routing) query for location, and an ADR query to get additional data, such as the carrier or the TN owner, that will aid in finding and identifying attackers.

In addition to the TDoS/DDoS approach, each functional element has security policies applied to it. Continuous monitoring and threat analytics are provided through the implementation of a centralized security incident and event management solution (SIEM), allowing for real-time visibility and event correlation across the entire security and network infrastructure. Alerts provided through the SIEM are monitored and would trigger an investigation with Security Incident Response capability activated, as needed.

For each database within the Emergency Call Management Complex (ECMC), also referred to as the NGCS Core Sites, the architecture consists of a Primary source provisioning Common Support System (CSS) database that replicates data changes to target databases in real-time. ECMC databases consist of two-node Oracle RAC clusters that provide redundant failover capabilities. Application failover between the Primary CSS and Alternate CSS databases is accomplished using Transparent Application Failover (TAF), thus achieving 99.999 percent availability. TAF is an Oracle mechanism that provides for application failover via the Oracle Transparent Network Substrate (TNS).



AT&T ESInet records media and allows authorized users to access recordings within the AT&T Customer Management Portal. This recording is primarily used to facilitate troubleshooting. AT&T will also work with PSAPs to determine if they have audio recording. This responsibility is outside of the scope of ESInet, but AT&T can use its experience to help facilitate a successful transition from analog recording to digital recording of RTP at the PSAP.

i3 loggers collect logs from each functional element. These logs are aggregated and stored at within the Common Support Services (CSS) sites. CSS sites are not part of the 9-1-1 call flow and, in addition to storage of i3 logs, they are also used for Spatial Interface, monitoring, and management portals for configuration of the system. AT&T offers ECATS to compile i3 logs and present them to authorized users in their reporting tool. Call Detail Records (CDRs) are stored within the CSS sites. CDRs can be viewed within the Customer Management Portal.

For an i3 PSAP, a transfer is triggered by SIP REFER message from the PSAP's CHE, unlike a legacy PSAP that relies on star codes. This message includes the PSAP URI for the destination PSAP within the Refer-To header. Based on the SIP URI, AT&T ESInet identifies this as an on-net PSAP. AT&T ESInet creates a SIP invite to the transfer PSAP. This SIP invite contains the LIS/ADR references so the PSAP receiving the call can query for updated location information. The invite also contains an updated History-Info header. This header is used by the PSAP's CHE to indicate the call transfer and not a 9-1-1 origination. If the PSAP's CHE supports History-Info, the call can be identified as a transfer, and the PSAP should not try to transfer the call back to the original PSAP. Section 3.1 in the attached Call Flow Scenarios document describes in detail the transfer mechanism between PSAPs.

For a NG PSAP transferring to a PSAP off-net (on a different ESInet), the transfer is triggered using the same REFER functionality from the PSAP CHE. During this request for a transfer, AT&T recognizes the PSAP URI for an off-net PSAP (not on AT&T ESInet). The AT&T ESInet then identifies the correct ESInet to send the call to based off configurations. AT&T has deployed ESInet-to-ESInet transfers/handoffs and provides the Network-to-Network Interface (NNI) specifications to provide detailed requirements to these call scenarios. Please see ***Appendix K - AT&T ESInet-to-ESInet Interface Specification SIP Basic_v3.4.1*** for additional NNI specification information.

All transfers are logged in the ESRP i3 logs and in the CDR. Call transfers can be identified in the Customer Management Portal via the CDR screen indicated by the "Bridge Field = true".

There are multiple options to allow PSAPs to receive data. In an i3 call, the exchange of data should follow the NENA i3 standards, and the PSAP receiving the call should use the LIS/ADR references. The PSAP's CHE queries the LIS/ADR using digital certs for authentication to retrieve the data. This can become more problematic between different ESInet systems depending on the capability of the foreign ESInet. AT&T has implemented different options to allow PSAPs on ESInets that don't support an i3 transfer. These include dual provisioning of LDB/LIS and No Record Found Steering. These options are not preferred, but do allow the PSAPs to receive data for the calls.



i3 loggers collect logs from each functional element. These logs are aggregated and stored within the Common Support Services (CSS) sites. CSS sites are not part of the 9-1-1 call flow and, in addition to storage of i3 logs, they are also used for Spatial Interface, monitoring, and management portals for configuration of the system. AT&T offers ECaTS to compile i3 logs and present them to authorized users in their reporting tool. Call Detail Records (CDRs) are stored within the CSS sites. CDRs can be viewed within the Customer Management Portal (CMP).

AT&T provides diversity, redundancy for all NGCS elements provided as part of the AT&T ESInet service. AT&T does not have the ability to monitor or enforce diversity and redundancy within non-AT&T systems. This limitation includes both OSPs and PSAPs portion of the 9-1-1 call flow. These are outside of the AT&T span of control. AT&T can assist in notifying the State if there are areas that would limit the overall success of a call reaching a call taker but as the State of Nebraska is purchasing ESInet and NGCS, this would be limited to services that AT&T is providing.

Remainder of page intentionally blank

10.2. Additional Examples

The following diagrams serve as an example of how a Respondent shall answer the use case questions. Diagrams may be necessary with step-by-step demonstration callouts to document the overall traffic flow for the system. Respondents are encouraged to use their own diagram(s) to illustrate the traffic flow from end to end.

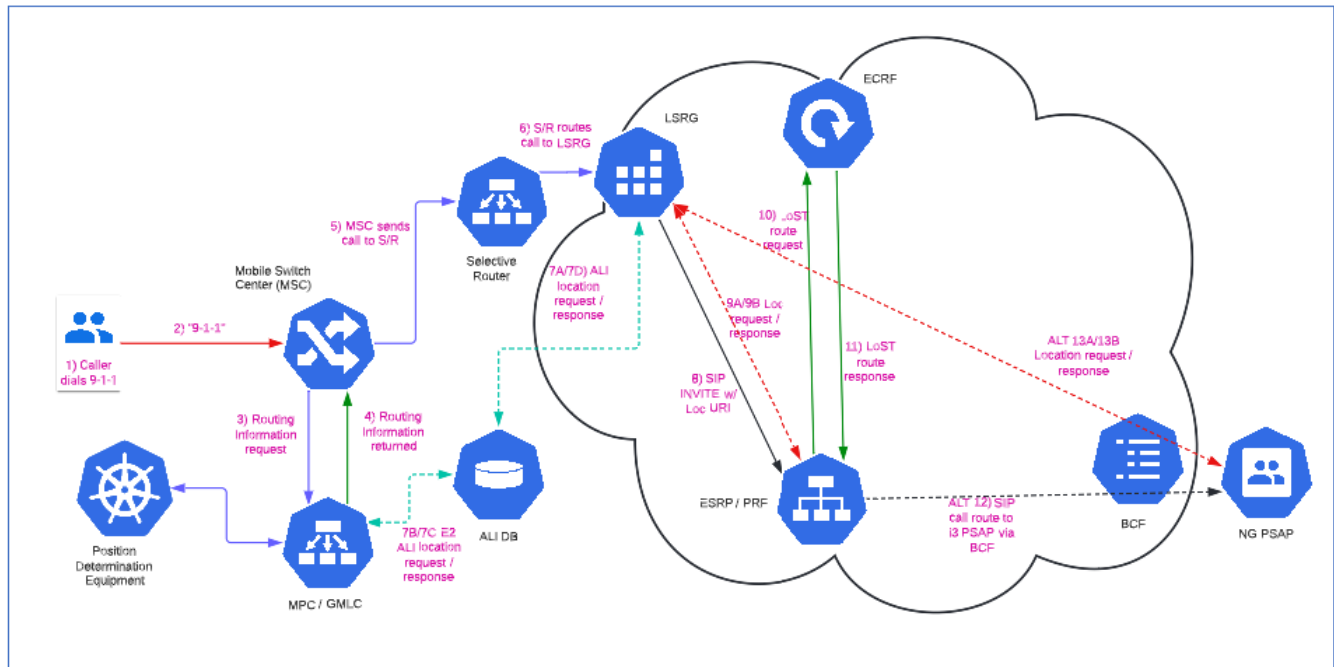


Figure 4: NENA Call Flow Scenario 1

AT&T Response:

Comply.

Remainder of page intentionally blank

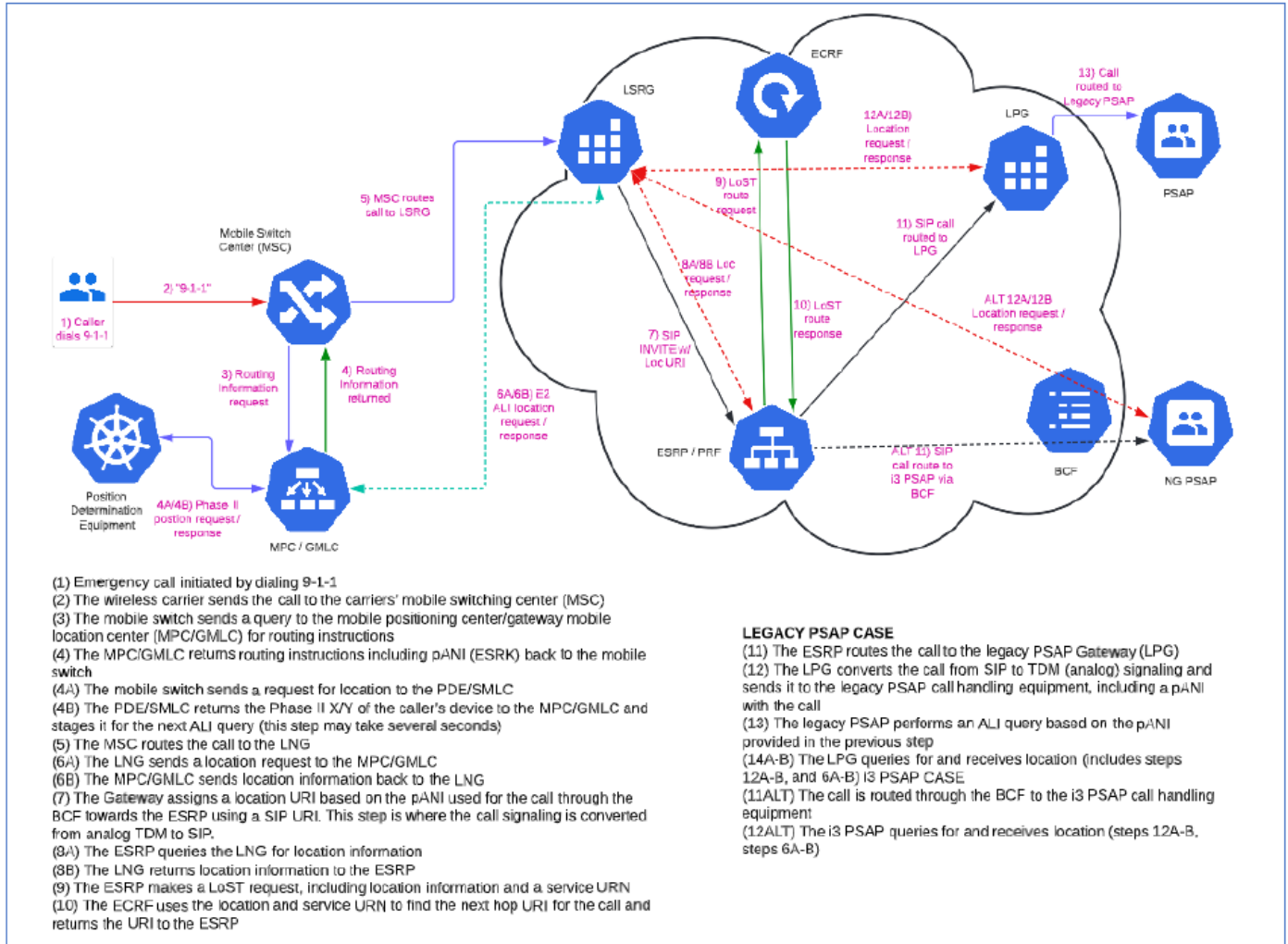


Figure 5: NENA Call Flow Scenario 2

AT&T Response:

Comply.

Remainder of page intentionally blank



5. COST SHEET

Costs must be submitted as provided in the Cost Proposal (Appendix A). The Cost Proposal must include a complete response on all requested pricing information. Bidders may not take exception to any specific terms provided in the Cost Proposal.

The points awarded to a bidder will be determined by the following formula:

Points to Award = Lowest Bidder's Total Cost Submitted ÷ Bidder's Total Cost Submitted x Maximum Possible Points.

AT&T Response:

Comply.

AT&T understands this requirement.



6. RESPONSE TO TERMS

Bidder should read the Terms provided with this RFP and must initial either “Accept All Terms and Conditions Within Section as Written” or “Exceptions Taken to Terms and Conditions Within Section as Written” in the table below (or include the same table in their solicitation response). If the bidder takes any exceptions, they must provide the following within the “Exceptions” field of the table; if an exception is not explicitly taken, it is deemed to be accepted as stated. The bidder may provide responses in separate attachment if multiple exceptions are taken. Exceptions must include:

- 1. The specific clause, including section reference, to which an exception has been taken;
- 2. An explanation of why the bidder took exception to the clause; and
- 3. Provide alternative language to the specific clause within the solicitation response.

Accept All Terms within Section as Written (initial)	Exceptions Taken to Terms Within Section as Written (Initial)	Exceptions: (Bidder must note the specific clause, including section reference, to which an exception has been taken, an explanation of why the bidder took exception to the clause, and provide alternative language to the specific clause within the solicitation response.)
DA		

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

AT&T Response:

Comply.



7. CONTRACTUAL AGREEMENT FORM

The Contractual Agreement Form must be signed manually in ink, or by DocuSign or other electronic signature system, and returned by the opening date and time along with the bidder's solicitation. By signing the Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

AT&T Response:

By executing the Contractual Agreement Form, AT&T affirms compliance with the provisions of the solicitation and agrees to the terms and conditions set forth therein, except as otherwise expressly noted in writing within AT&T's proposal.

AT&T intends to execute the Contractual Agreement Form using an approved electronic signature solution, Adobe Acrobat, which satisfies the solicitation requirement for execution via DocuSign or other electronic signature systems.



CONTRACTUAL AGREEMENT FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

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

 X NEBRASKA VENDOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Vendor. "Nebraska Vendor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this Solicitation. All vendors who are not a Nebraska Vendor are considered Foreign Vendors under Neb. Rev Stat § 73-603 (c).

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

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

FORM MUST BE SIGNED MANUALLY IN INK OR BY DOCUSIGN

BIDDER:	AT&T Enterprises, LLC
COMPLETE ADDRESS:	208 S. Akard St. Dallas, TX 75202
TELEPHONE NUMBER:	214-991-0049
FAX NUMBER:	N/A
DATE:	April 6, 2026
SIGNATURE:	 Date: 2026.04.15 13:17:20 -05'00'
TYPED NAME & TITLE OF SIGNER:	Dustin Alexander / Regional Sales Director



8. ADDITIONAL REQUESTED ITEMS



9. AT&T APPENDICES

- [Appendix A - AT&T Staff Resumes.pdf](#)
- [Appendix B - ATT ESInet Operational Readiness Test Plans i3 PSAPs.pdf](#)
- [Appendix C - ATT ESInet Operational Readiness Test Plans RFAI PSAPs.pdf](#)
- [Appendix D - ORT-Acceptance Test Plan.pdf](#)
- [Appendix E - AT&T 9-1-1 EGDMS User Guide.pdf](#)
- [Appendix F - AT&T ESInet Training Plan.pdf](#)
- [Appendix G - NGCS_ESInet_Risk_Register_Template.pdf](#)
- [Appendix H - NGCS_ESInet_Risk_Acceptance_Form.pdf](#)
- [Appendix I - AT&T Business Continuity & Emergency Management.pdf](#)
- [Appendix J - AT&T ESInet Call Flow Scenarios.pdf](#)
- [Appendix K - AT&T ESInet-to-ESInet Interface Specification SIP Basic_v3.4.1.pdf](#)
- [Appendix L - AT&T 2025 Annual Report.pdf](#)
- [Appendix M - PSAP Implementation Project Plan Nebraska AT&T.pdf](#)



Appendix A - AT&T Staff Resumes

AT&T NATIONAL DIRECTOR OF PUBLIC SAFETY NEXT GENERATION 9-1-1

MICHAEL GUERRA

SUMMARY

An accomplished, performance driven, highly experienced Director of Product Marketing, demonstrating an excellent career history of business development, designing go-to-market strategies, coordinating sales enablement and creating product promotions to increase company revenue. Demonstrates proficiency in leadership concepts for complex projects and deliverables, business process analysis, customer and client relations. Results-oriented, seasoned leader with cross-organizational team management skills offering outstanding industry knowledge and business development expertise.

CORE COMPETENCIES

- Telecommunications Markets/Industry
- Hosted Voice/UC Industry
- Vertical Market Strategies
- Go To Market Strategies
- Product Promotions
- Product Launch
- Business Development
- Global Telecom
- Foreign Market Requirements
- Vendor Negotiations
- Vendor Partnerships
- Sales Enablement

PROFESSIONAL EXPERIENCE

- Oct. 2018 – Present **Director, AT&T Next Generation 9-1-1 Product Management**
- Director for AT&T Public Safety Portfolio.
 - P&L responsibilities for AT&T's full Next Generation 9-1-1 and Legacy 9-1-1 products to Include Next Gen 9-1-1, ESInet, PSAP Solutions and School Safety.
 - Proven sales leader responsible for AT&T's national footprint managing over \$300 million in annual revenue for next generation 9-1-1 solutions.
- Aug. 2014 – Oct. 2018 **Director, AT&T Mobile and Business Marketing Solutions - Dallas/Fort Worth Area**
- Responsible for developing and delivering to market a new business hosted voice and unified communication product. Managed a large development team of 6 direct reports and team members from Labs, Technology Development, Channel Support and Sales organizations. Directed efforts for vendor selection, business development, go to market strategy, sales enablement, product promotions and digital marketing content.
- Duties and Responsibilities:
- Branding activity for customer facing clients and portals
 - Go to market strategy and product launch activity
 - Sales enablement and training content
 - Product promotions specific to segments and vertical markets
 - Sales advisory content and distribution
 - Digital marketing content
 - Demand and lead generation
 - Financial responsibility for \$150M project development budget
 - Vendor selection and contract negotiation
- 2008 - 2013 **Director, AT&T Global Enterprise SIP Trunking Services - Bedminster, New Jersey**
- Responsible for Business VoIP footprint expansion in US and global markets. Managed relationship with FCC, State PUCs, and global suppliers. Managed a team of 14 direct reports. Partnered closely with Legal and Regulatory teams along with Network to coordinate deployments.
- Duties and Responsibilities:
- Defined market entry strategy for both domestic and global footprint expansion

- Lead vendor selection and negotiations for global partnerships
- Large customer sales support related to solution design and site coverage

2000 – 2008

Director, Toll Free and Local Product Manager, AT&T Business Services

- Toll-Free Product manager responsible for \$2.3B annual revenue. Created new Mass Calling Application services targeted for voting reality shows and mass promotions.
- Key accounts included American Idol, X Factor, America's Got Talent, and Phillip Morris mass promotion campaign.
- Mass Calling service generated over \$50M in annual revenue. Identified and championed a change in AT&T's payphone compensation business rules that drove an annual expense savings of \$30M.
- Achieved \$10M cost saving by redesigning routing plans for prepaid platform calls.

1995 - 2000

Lead Network Planner, AT&T Network, Planning and Engineering

- Network and customer capacity planning and engineering. Analyzed call patterns along with sales opportunities to forecast and engineer network capacity to support business traffic.
- Developed methodology and network database to support just in time network buildout. Reduced cycle time dramatically by lowering unit cost while increasing revenue.

EDUCATION

- University of Maryland – 1995
 - Bachelor of Science (B.S.), Business Management and Marketing

AT&T ESInet™ LEAD PRODUCT & DEVELOPMENT MANAGER – PUBLIC SAFETY SOLUTIONS

MARK TITUS

SUMMARY

Visionary leader with 36+ years of experience driving innovation in public safety communications, mobility advanced solutions and internet technologies. Known for bringing new technology innovation to market like text-to-911, Wireless Emergency Alerts (WEA) and Location Based Services (LBS), he has received over 30 U.S. patents in wireless voice, short message service (SMS), and location services. He currently is responsible for managing AT&T's ESInet™ service and driving adoption of next-generation public safety solutions such as Artificial Intelligence, NG9-1-1 integration with FirstNet, Text to 9-1-1, GIS, and cybersecurity. He has also served in multiple terms on the FCC Communications Security, Reliability, and Interoperability Council's (CSRIC) and been the recipient of AT&T's Visionary Award for transformative impact on Next Gen 911.

CORE COMPETENCIES

- Next Generation 9-1-1 Emergency Services
- Product Management & Marketing
- Strategic Planning and P&L Oversight
- Marketing Communications Product Launch
- Cloud Based Services
- High Availability System Architecture & Design
- Public Safety Communications & Alerting Systems
- Software Development Life Cycle
- Agile Software Development
- Intellectual Property Creation

PROFESSIONAL EXPERIENCE

2014-Present AT&T ESInet Lead Product & Development Manager

- Lead product marketing management for AT&T's ESInet™ service, overseeing strategic positioning, product roadmap development and go-to-market adoption.
- Spearheaded growth of AT&T's Next Gen 9-1-1 ESInet business; honored with AT&T Visionary Award.
- Oversaw portfolio management of emerging solutions including IP-based call handling, CAD, GIS, Text to 911, cloud computing, and mobile apps for first responders.
- Collaborated cross-functionally to ensure high availability architectures and user-centered design in mission-critical systems.
- Provided expert commentary on wireless public safety and text messaging technology for prominent business and trade media outlets including The Washington Post, New York Daily News, Federal News Radio, and Wireless Week.

FCC Communications Security, Reliability & Interoperability Council (CSRIC)

- CSRIC VII – Working Group 4: Assessed 911 security vulnerabilities during IP transition.
- CSRIC III – Working Group 2: Contributed to Next Generation Alerting strategies.
- CSRIC II – Working Group 5A: Supported CAP (Common Alerting Protocol) implementation for emergency communications.

EDUCATION

- University of Maryland
 - Master of Science – Telecommunications Management
- Cleveland State University
 - Bachelor of Science – Computer Science

AT&T REGIONAL SALES DIRECTOR – PUBLIC SAFETY SOLUTIONS

DUSTIN ALEXANDER

SUMMARY

Dynamic and results-driven professional with over 26 years of experience in the telecommunications industry, specializing in public safety and 9-1-1 products and services. Proven ability to lead cross-functional teams, deliver on revenue objectives, and achieve profit margin targets in fast-paced, complex environments. Strong technical expertise in engineering design, configuration tools, and network platforms, complemented by advanced education in Business Administration and Management Information Systems. Recognized for leadership, initiative, and a customer-centric approach to driving business success.

CORE COMPETENCIES

- Strategic Account Management & Planning
- Next Generation 9-1-1 System Architecture
- Client/Vendor Relationship Management
- Budget Planning & Execution
- Cross-Functional Team Management
- Complex Contract Negotiations

PROFESSIONAL EXPERIENCE

- Apr. 2014 - Present **Regional Sales Director – AT&T Public Safety**
- Lead, coach and develop a cross-functional team of 9 sellers and systems engineers responsible for 9-1-1 products and services sales for the Central and Gulf States Region of the United States.
 - Deliver on current revenue objectives and profit margin targets of the business unit.
 - Provide leadership to a team responsible for over \$106 million in annual revenue for next generation 9-1-1 solutions.
 - Provide sales leadership to internal and external clients in support of 13 states in the Central and Gulf States region of the United States.
 - Negotiate complex contracts with state, county & local governments for AT&T products and services.
 - Present AT&T Public Safety Solutions portfolio, to include AT&T ESInet™, at various local and regional events.
 - Past Board Member of the Texas Chapter of the Association of Public-Safety Communications Officials (APCO).
- Jun. 2007 – Apr. 2014 **Technical Sales Consultant III – Emerging Technologies – AT&T**
- Provided consultative support and developed tailored technology solutions for state/local government, education, and healthcare clients.
 - Managed strategic accounts and large-scale deployment projects, ensuring seamless pre- and post-sales support.
 - Sold and positioned advanced solutions including IP Telephony, Data Center, and Managed Services, becoming a trusted advisor to clients.
 - Collaborated with internal teams to deliver integrated, multi-product solutions.
- Jan. 2001 – Jun. 2007 **Design Engineer II - AT&T Global Business Solutions, Inc.**
- Engineered complex voice and data solutions for businesses of all sizes using Nortel and Avaya products.
 - Provided engineering design, scope of work, and pricing support for sales on PBX, Hybrid Voice/VoIP, and IP telephony systems.
 - Key member of the AT&T/SBC merger integration team, developing consolidated CPE sales process flows.

- Chaired the Southern Region Voice Engineering task force to drive process improvements and knowledge sharing for accurate designs and superior customer service.
- Trained Design Engineers and Technical Sales staff on Nortel and Avaya products and configuration tools.
- Served as one of three AT&T delegates on Nortel's Power User Advisory Forum.

Jul. 2000 –
Jan. 2001

Work Group Administrator/Web Designer - SBC Telecom Inc.

- Developed and maintained internal content and provided user support.
- Installed, configured, and troubleshoot end-user workstations and applications.
- Delivered on-site service and upgrades for small business computer systems.
- Trained employees on Windows and various applications, boosting technical proficiency.
- Created telecommunications training aids to enhance employee engagement.

Feb. 1996 –
Aug. 2000

Emergency Medical Evacuation Supervisor (Sergeant – E5) - United States Army

- Provided emergency medical care, surgical assistance, triage, MEDEVAC, and patient education in high-pressure situations.
- Implemented and managed MEDPROS to track Anthrax immunizations for the 82nd Airborne Division.
- Developed an Excel-based system to track 600+ immunization records, increasing productivity by 80%.
- Ensured security and accountability for a barracks complex of 250+ personnel, mission critical equipment and weapons.
- Received multiple awards for leadership, initiative, and program effectiveness.

EDUCATION AND CERTIFICATIONS

- Dallas Baptist University – Dec. 2003
 - Master of Business Administration – Management Information Systems
- Dallas Baptist University – Aug. 2002
 - Bachelor of Business Studies – Business Administration

ADDITIONAL TRAINING AND CERTIFICATIONS

- AT&T ESInet™ Training Program
- AT&T Security Proficiency Program
- AT&T Network & Platform Proficiency
- AT&T Emerging Technologies University Bachelor's program for Hosting & Application Services
- Primary Leadership Development Course (PLDC) – 18th Airborne Corps NCO Academy
- United States Army Medical Specialist Course resulting in Emergency Medical Technician Certification
- U.S. Department of Defense Training for Medical Occupational Database Network system.
- Additional Technology Training Courses to include: VMware Technical Sales Professional (VTSP), Nortel Certified Design Expert/Support Expert/Design Specialist/Technology Specialist/Sales Professional, Cisco Interconnecting Cisco Network Devices 2, Cisco Data Center Discovery Workshop Enterprise (DCDW-E-C)

AT&T APPLICATION SALES EXECUTIVE – PUBLIC SAFETY SOLUTIONS

JEFF BIEVENUE

SUMMARY

Jeff Bievenue has over 25 years' experience in the telecom and technology industries with over 23 of those years directly involved in the sales and support of 9-1-1 services. In his current role, Jeff provides account management and presales support to 9-1-1 customers in Texas, Nebraska and New Mexico. Jeff is overall responsible for preparation of responses, contract negotiation and post-sales support.

CORE COMPETENCIES

- Strategic Account Management & Planning
- Next Generation 9-1-1 System Architecture
- Client/Vendor Relationship Management
- Client Needs Assessment
- Complex Contract Negotiations

PROFESSIONAL EXPERIENCE

July 2016 -
Present

Application Sales Executive – AT&T Public Safety

- Responsible for 9-1-1 customer base in North Texas, Nebraska and New Mexico.
- Supports customer sales of Next Generation 9-1-1 Call handling solutions, NGCS, ESInet and Text to 9-1-1.
- Serves as trusted advisor to customers regarding complex public safety/9-1-1 solutions.
- Resolves customer issues and offers input to mitigate future potential issues.
- Meets with 9-1-1 customers across territory to assist in developing roadmap for future CPE, NG9-1-1 and ESInet deployments.
- Negotiate complex contracts with state, county & local governments for AT&T products and services.
- Presents AT&T Public Safety Solutions portfolio, to include AT&T ESInet™, at various local and regional events.

Oct 2008 –
July 2016

Supervisor Technology – AT&T E9-1-1 Public Safety

- Collaborated with Sales Teams and Project Managers to drive increased customer satisfaction and identify synergies within 9-1-1 projects.
- Coordinated work activities to achieve the volume expected to meet operational requirements across a highly complex and sensitive customer base.
- Planned, directed, supervised, and evaluated workflow of employees.
- Effectively manage a team of 10 Communication Consultants in 5 states whose responsibilities include but are not limited to the following AT&T Public Safety Customer Service activities: complex service order activity, service deficiencies, responding to customer requests, billing adjustments, ICB pricing, system pricing and customer premise sales and service.
- Supported Technology Partner: AT&T
- Provided complex technical 911 products and services for Public Safety and 911 Customers
- Worked closely with technology partners in the areas of strategic planning, design, quotation, and sales support.
- Led joint meetings with customers and partners to educate and assist with their NG911 strategy.
- Partnered closely with key decision makers at the Local, County, State Government levels to include PSAP Directors, Commission Representatives, and Police/Fire/EMS/Chiefs/Sheriffs.
- Expert understanding of Legacy 911 & Emerging Solutions (VIPER, ECaTS, NG911,

Oct. 2003 –
Oct. 2008

Communication Consultant – AT&T E9-1-1 Public Safety

- Responsible for the day-to-day activities of over 100 E9-1-1 customers in the State of Missouri.
- Designed, implemented and managed changes of E9-1-1 networks for customers in Missouri.
- Coordinated implementation of Private Switch 9-1-1 services in Missouri.
- Met with E9-1-1 customers to discuss network implementation and equipment procurement.
- Effectively worked with ILEC's and CLEC's to implement 9-1-1 Landline/Wireless networks and equipment.
- Project managed installation of 9-1-1 services, equipment and networks across the State of Missouri.
- Proactively managed records in the E9-1-1 Contingency Database with a less than 1% error rate.
- Facilitated purchases of network, database and 9-1-1 CPE in the State of Missouri.

EDUCATION

- Associate of Business – Marketing
- AT&T ESInet™ Training Program
- AT&T Security Proficiency Program
- AT&T Network & Platform Proficiency

LEAD SALES SYSTEM ENGINEER – PUBLIC SAFETY SOLUTIONS

BILLY BLANKENSHIP

SUMMARY

Billy Blankenship has 50 years of telecommunications experience, including over 34 years focused on the design, installation, and consulting of 9-1-1 solutions. As a key member of the AT&T ESInet™ team, Billy plays a critical role in the design, testing, and deployment of AT&T's NG911 services.

Throughout his career, Billy has developed and delivered technical training for Southwestern Bell and AT&T and currently provides design expertise across multiple transport technologies, including T1, MPLS, Layer 2 Ethernet, direct fiber, satellite, and LTE. As an AT&T ESInet™ Subject Matter Expert and frequent state and national presenter, Billy is widely recognized for his ability to guide customers through the transition from legacy 9-1-1 to Next Generation 9-1-1.

CORE COMPETENCIES

- Sales Strategy & Enablement
- Public Safety Technology (NG911, ESInet, CHE)
- Technical Pre-Sales & Solution Architecture
- IP Networking, SIP, MPLS, Cisco Infrastructure
- Stakeholder Engagement & Executive Presentations
- RFP & Contract Development
- Disaster Recovery & Continuity Planning
- Team Collaboration Across Regional Territories

PROFESSIONAL EXPERIENCE

- Apr. 1976 – Present **Lead Sales System Engineer 3 - AT&T Public Safety – 10-State Territory**
- Leads sales engineering strategy for public safety clients across a ten-state region, supporting sales executives in capturing and closing complex technology deals.
 - Designs tailored 911 network solutions involving MPLS, IP routing, LTE fail over, and microwave integration, contributing to key revenue-driving wins.
 - Acts as senior technical expert in customer engagements, executive briefings, and solution presentations, enhancing client confidence and reducing sales cycle time.
 - Directs creation of project scopes, technical diagrams, statements of work, and contract-ready solution packages.
 - Supports end-to-end system implementations, including planning, cutover execution, and post-deployment optimization.
 - Delivers APCO and NENA presentations to demonstrate AT&T's innovation and commitment to public safety.

EDUCATION

- Bachelor of Science, Computer Science
 - McMurray University

ADDITIONAL TRAINING AND CERTIFICATIONS

- AT&T ESInet™ Training Program, AT&T Security Proficiency, AT&T Network & Platform Proficiency
- Vesta 911 Equipment
- Viper 911 Equipment
- Southwestern Bell Telephone Company Certified Instructor

Additional Training Courses to include:

ISDN Diagnostics & Troubleshooting, ATM/Newbridge, Cisco Router Installation and Maintenance, National ISDN Installation & Maintenance, Digital Circuit Technology, Special Service Applications, Principles of Digital Transmission, Instructional Design, Fujitsu FLM 150/600 Terminal Admin., SONET Overview, Principles of LAN

AT&T SENIOR PRODUCT MANAGER & PRINCIPAL ARCHITECT – PUBLIC SAFETY SOLUTIONS

JAMES (JIMMY) LICHTENSTEIN

SUMMARY

Innovative IT, sales and product management leader with 20+ years of experience driving public safety technology initiatives, digital transformation, and operational efficiency across government and private sectors. Proven success leading AI-driven technology deployments, cloud-based communications solutions, and enterprise-wide system modernization. Recognized for delivering multimillion-dollar, mission-critical programs on time and within budget, and for aligning technology innovation with business goals. Expertise in public safety systems, AI-enabled emergency response solutions, and SaaS product management, with a strong focus on customer-centric design and stakeholder collaboration.

CORE COMPETENCIES

- Public Safety SaaS Solutions
- AI Implementation
- Cloud Communications Platforms
- Product Management
- Customer Experience (CX)
- Contact Center Technologies
- Emergency Response Systems
- Stakeholder Engagement
- Agile Development

PROFESSIONAL EXPERIENCE

2018 – Present	<u>Senior Product Manager & Principal Architect, Public Safety Solutions Next Generation 9-1-1 – AT&T – NASHVILLE, TN</u> • Lead strategic sales of over \$250M in public safety contracts between FY18 and FY20 in Tennessee, Maryland, Washington DC, and Virginia achieving over 500% of annual sales targets. • Recognized sales leader with AT&T's Diamond Club (Top 1%) and Run Through the Warehouse (Top 3%) awards for exceeding performance benchmarks and client satisfaction. • Act as Public Safety Solutions Capture Manager, orchestrating strategic pursuit efforts, shaping RFP responses, and aligning technical solutions with customer requirements to win multimillion-dollar NG9-1-1 and public safety contracts. • Represent AT&T as a featured speaker at major public safety and 9-1-1 conferences nationwide, promoting advancements in NG9-1-1, cloud-based communications and AI-enhanced emergency response solutions. • Lead product management and solution architecture for AI-enhanced Public Safety Services, including NG9-1-1 cloud communications and real-time decision support systems for 9-1-1 and first responders. • Spearheaded the integration of AI technologies into emergency call handling, incident prioritization, and analytics platforms, increasing efficiency and improving response outcomes.
2010 – 2018	<u>Product Development and Delivery Executive Next Generation 9-1-1 – AT&T – NASHVILLE, TN</u> • Developed AT&T Emergency Services IP Network (AT&T ESINet™) product, a Top 10 initiative of the Governor of Tennessee. • Directed the \$82M Tennessee NG 9-1-1 program, setting a national benchmark for statewide ESINet systems.

- Ensured seamless coordination between product development, sales, and client teams to deliver innovative public safety solutions.

2004 – 2010 **Chief Information Officer / Assistant Commissioner Information Technology Department – State of Tennessee - Nashville, TN**

- Led staff of 100+ professionals managing multiple state Departments (Children’s Services, Finance & Administration, General Services, and Safety).
- Created and implemented the technology vision, security, application development, project management, infrastructure management, and system support for 2,000 users, and over 300 servers.
- Spearheaded statewide initiatives, such as the Statewide Automated Child Welfare Information System (SACWIS), Real ID and driver’s license production systems, under budget.
- Delivered critical technology solutions, including a mobile broadband network, body worn camera solution, and crash reporting for state troopers, increasing revenue, efficiency, and reducing costs.

2000 – 2003 **IT Development Manager & Senior Project Manager Business Systems Integration - MCI – DALLAS, TX**

- Led teams of contractors and employees across multiple states to consolidate, convert, and decommission legacy systems.
- Delivered \$300M of increased revenues through identification and correction of missed and/or erroneous billings.
- Developed and implemented a project management intranet reporting site, providing real-time project status for stakeholders and customers.

1998 – 2000 **Business Developer - American Management Systems – Dallas, TX**

- Established a market strategy focusing on CLEC’s, Carriers, Independent Telcos, ISPs, and Cable companies.

EDUCATION

- Capella University – Minneapolis, MN
 - Bachelor of Science in Information Technology

AT&T PRINCIPAL ARCHITECT – PUBLIC SAFETY SOLUTIONS

KEITH MARTIN, ENP

SUMMARY

Technical Sales Consultant Keith Martin has over 25 years' experience in the information technology and telecom industry and has been directly involved with the installation, consulting and design of 9-1-1 solutions. Keith is a key member of the AT&T Public Safety team as a Principal Architect and works with customers across the United States assisting them with premise-based solutions, hosted NG 9-1-1 solutions and our AT&T ESInet offer. Proficient as an AT&T ESInet deployment Engineer, Tier 3 support, Layer 3 deployment and Field Engineering Services

CORE COMPETENCIES

- NG9-1-1 Network Architecture & Design
- Project Design and Management
- Transport design for network interconnection
- Technical Pre-Sales & Solution Architecture
- IP Networking, SIP, MPLS, Cisco Infrastructure
- Disaster Recovery & Continuity Planning

PROFESSIONAL EXPERIENCE

- Jan. 2013 - Present **Principal Architect – AT&T Public Safety Solutions**
- Support customers across the United States to discuss NG 9-1-1 and ESInet projects during pre- and post-sale.
 - Provide technical expertise with 9-1-1 clients and 3rd party vendors in both hardware and network design.
 - Respond to RFPs for equipment, network and services related to 9-1-1 call handling equipment.
 - Work with 911 customers, vendors and peers on presenting AT&T ESINET to customers onsite and at state conferences.
 - Integrate various transport technologies such as LTE, MPLS, Layer 2 and T1 networks that best fit the customer requirements.
 - Assist customers with redundancy options that provide reliability for their 9-1-1 needs.
- Jan. 2000 - Jan. 2013 **Systems Technician - AT&T**
- Maintain, install, and troubleshoot 9-1-1 hosted systems across Oklahoma's two largest metropolitan regions, serving a combined population exceeding 1.5 million residents.
 - Collaborate directly with Public Safety Answering Point (PSAP) directors, state officials, and IT teams to design and deploy telephony solutions integrating PBX systems and external IP networks with 9-1-1 infrastructure.
 - Participate in monthly Council of Governments meetings to address customer issues and provide guidance on future system enhancements; support the sales team at the annual Oklahoma Public Safety Conference by addressing customer inquiries and concerns.
 - Partner with AT&T Public Safety engineering and implementation teams on network architecture and deployment, including server configuration and Cisco networking equipment setup.
 - Lead and manage 9-1-1 project implementations statewide, ensuring timely and successful deployment of critical emergency communication solutions.

EDUCATION, TRAINING AND CERTIFICATIONS

- Cisco CCNA, CCDA, CCNA Security
- NENA ENP (Emergency Number Professional)
- Vesta 911 Equipment training
- Intrado VIPER 911 Equipment training

AT&T SENIOR CONSULTANT PROGRAM MANAGER

REPRESENTATIVE EMPLOYEE (TBD)

SUMMARY

Dynamic and results-oriented Program Manager with over 7 years of experience driving cross-functional teams, delivering complex projects, and managing multi-million-dollar projects from conception to completion. Proven track record of implementing strategic solutions, optimizing operational efficiency, and exceeding stakeholder expectations in fast-paced environments. Adept at risk management, resource allocation, and building collaborative relationships with internal and external partners.

CORE COMPETENCIES

- Program & Project Management
- Strategic Planning & Execution
- Stakeholder Engagement
- Risk Assessment & Mitigation
- Team Leadership & Development
- Process Optimization

PROFESSIONAL EXPERIENCE

- Sep. 2023 – Present **Senior Consultant Program Manager: Capitol Area Emergency Communications District (Austin, TX)**
- Lead for NG911 Project moving to AT&T ESInet i3, New Call Handling Deployment, text to 911 (ESInet), Rapid Deploy, Eclipse, and new network coordination for 10 counties and 27 PSAPs totaling 285 seats.
 - Migration and Analyzed all END OFFICES wireline traffic to AT&T ESInet.
 - Coordinate cross-functional teams across engineering, network, ESInet, Call Handling, and client success to achieve program milestones.
 - Implement program roadmaps and reporting tools to support executive decision-making.
 - Identify risks and execute mitigation strategies, reducing project delays.
 - Foster strong relationships with stakeholders
- Jul. 2021 – Sep. 2023 **Senior Consultant Program Manager: Bexar Metro District (San Antonio, TX)**
- Lead for NG911 Project moving to AT&T ESInet for 3 counties and 19 PSAPs.
 - Analyzed, Scheduled, and Organized the move of Wireline Traffic from 46 End Offices to AT&T ESInet
 - Coordinated the move of AT&T VoIP, BVoIP, and AT&T Mobility OSP traffic to AT&T ESInet.
 - Implement program roadmaps and reporting tools to support executive decision-making.
 - Identify risks and execute mitigation strategies, reducing project delays.
 - Foster strong relationships with stakeholders
- Apr. 2019 – Jul. 2021 **Senior Consultant Program Manager: Capitol Area Emergency Communications District (Austin, TX)**
- Lead for NG911 Project moving to AT&T ESInet (RAI) for 10 counties and 27 PSAPs totaling 285 seats.
 - Coordinate cross-functional teams across engineering, network, ESInet, Call Handling, and client success to achieve program milestones.
 - Implement program roadmaps and reporting tools to support executive decision-making.
 - Identify risks and execute mitigation strategies, reducing project delays.
 - Foster strong relationships with stakeholders
- Jun. 2008 – Apr. 2019 **E911 Director, Pickens County, SC**
- Director of 3 PSAPs: Easley PD, Pickens County Sheriff's Office, and Clemson University PD.

- Maintained all 911 equipment and 911 Network across all 3 centers.
- Coordinated all funding within the county through wireline and wireless fees within the 911 fund within the county, as well as coordinating all funding from the state.
- Lead for all addressing and establishing of road names for county planning and development.

EDUCATION

- Bob Jones University – 1998
 - Bachelor of Science in Criminal Justice

ADDITIONAL TRAINING AND CERTIFICATIONS

Certifications

- Emergency Number Professional Certification (ENP)
- Registered Public Safety Leader (RPL)

Technical Skills

- Project Management Tools: MS Project, Excel
- Data Analysis: Excel, Power BI
- Collaboration: Microsoft Teams

AT&T 9-1-1 SERVICE MANAGER REPRESENTATIVE EMPLOYEE (TBD)

SUMMARY

The AT&T 911 Service Manager (SM) will act as the ongoing AT&T liaison to the State of Nebraska and its represented PSAPs in support of the AT&T ESInet™ when it is fully operational. The AT&T 911 SM will collaborate with county and PSAP representatives to act as the customer advocate with AT&T organizations, both internal teams and external vendor partners, on behalf of the State of Nebraska.

CORE COMPETENCIES

- Telecommunications Service Management
- Next Generation 911 Emergency Services
- Escalation Management
- AT&T Policies and Procedures
- 24x7 Availability

PROFESSIONAL EXPERIENCE

Service Manager – AT&T

- Minimum 15 years of AT&T employment
- Minimum 5 years of experience working with AT&T 911 Services and Systems
- The AT&T 911SM is the primary contact for escalation requests related to ESInet service and performs the following tasks as part of the ongoing relationship:
 - Partners with the AT&T ESInet™ Program Manager to ensure consistent communication with the State of Nebraska and its designated PSAP representatives
 - Advocates on behalf of the State of Nebraska with organizations supporting AT&T ESInet™ including but not limited to:
 - AT&T 911 Resolution Center
 - AT&T Technology Reliability Center
 - AT&T Ethernet Operations Center
 - Intrado Network Operations Center
- Provides critical escalation support to the PSAPs within the State of Nebraska for AT&T ESInet™ impairments and outages
- Acts as the primary point of contact for questions related to AT&T ESInet™ service
- Provides maintenance notifications (both planned and emergent)
- Delivers after-event reports
- Coordinates user access to operational support tools e.g., AT&T ESInet™ customer web portal

The AT&T 9-1-1 SM will be available 24 hours a day, 7 days a week for critical outage support as well as customer escalations related to service impairments of the AT&T ESInet™.



Appendix B - ATT ESInet Operational Readiness Test Plans i3 PSAPs



AT&T ESInet™

Operational Readiness Test Plan

i3 PSAPs

<PSAP Name>

<Test Date>

Trademark Ownership

All trademarks used herein are the property of their respective owners.

Non-Disclosure

The information contained in this document and provided to PSAP is Corporate Confidential in its entirety. This restricts the disclosure of any information herein to a third-party and other terms and conditions under the terms of a Non-Disclosure Agreement.

Open Records Act Request

PSAP will immediately advise in writing of any Open Records Act type of requests as it may relate to this proposal or any information contained herein.

Introduction

The AT&T ESInet™ Operational Readiness Test Plan described in this document provides an overview of testing and a list and description of test cases for the implementation of the AT&T ESInet™ services. The objective for this test plan is to demonstrate the network and call processing equipment readiness to receive 9-1-1 traffic using the AT&T ESInet™ service. Test participants include <PSAP NAME> and AT&T ESInet™ Service Delivery.

The AT&T ESInet™ Operational Readiness Test Cases will demonstrate feature functionality of the AT&T ESInet™. The Test calls will deliver simulated “9-1-1” calls from the AT&T end office to the PSAPs over the AT&T ESInet™ to the call handling equipment installed at the <PSAP NAME>.

AT&T manages the testing process and coordinates all test calls documented in the AT&T ESInet™ Operational Readiness Test Plan. The testing is scheduled in accordance with the PSAP’s availability. The PSAP may be asked to provide a resource to answer the test calls and to provide documentation (i.e. screen prints and recordings) for certain calls.

The list of standard tests demonstrates feature functionality of the AT&T ESInet™ to include:

- Operation of the AT&T ESInet™ PSAP Network Edge equipment
- Call handling and routing processes:
 - Call transfer and bridging functions
 - Alternate and default routing
 - Independent i3 component availability
 - PSAP abandonment routing
 - PAD abandonment routing



AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

Test #	Test Case	Type	Testing Criteria	Time	Pass/Fail and Comments
TEST LOCATION: <PSAP NAME> DATE & TIME: <DATE/TIME> CALL ORIGINATOR: AT&T			CALL TAKER: ON-DUTY CALL-TAKER ANI: <ANI>		
1	Trunk Verification (SIP)	Call Routing	Egress trunks manually busied out to force calls through each SIP Contact Test call sent to <TEST PSAP>. SBC1: <SBC Name> SBC2: <SBC Name> SBC3: <SBC Name> Note: This is an egress SIP from SBC to PSAP	<5 min	HH:MM MT – Trunk(s) busied out HH:MM MT – Test call made to <TEST PSAP>, call routed to <TEST PSAP> as expected with good ANI/ALI, location, subscriber information and Voice delivered. <PASS/FAIL>
2	Trunk Verification (SS7 Ingress from LSR)	Call Routing	Know the Ingress primary and alternate trunk groups for the project. Caller dials PSAP test number multiple times into the primary trunk group. Monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the	<30 min	HH:MM MT – Each ingress trunk channels tested. Voice quality of each channel is tested. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

			MetaSwitch, busy out the primary trunk group. Calls then should traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested. If all of the channels test okay, then have the primary trunk group restored. Note: from the LSR, the trunk groups should be set to most idle. From the MetaSwitch the trunk groups should be set to least idle.		
3	Trunk Verification (SS7 Egress from AGC to LSR)	Call Routing	Know the Egress primary and alternate trunk groups for the project. Caller dials PSAP test number. After the call is established, the PSAP call taker will need to place multiple conference calls to a friendly off net PSAP. Monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group. Calls then should	<30 min	HH:MM MT – Each egress trunk channels tested. Voice quality of each channel is tested <PASS/FAIL>

			traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested. If all of the channels test okay, then have the primary trunk group restored. Note: From the MetaSwitch the trunk groups should be set to most idle.		
4	Perform reboot and validation on each West network edge router at PSAP	Failover test	○ Place test call ○ Reboot PSAP router A ○ Observe PSAP router B become VRRP master for all applicable networks ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router B ○ Login to router A; enable monitoring, verify routing neighborships and VRRP have restored to pre-event states ○ Reboot PSAP router B ○ Observe PSAP router A become VRRP master for all applicable networks ○ Identify any audio disruptions		

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

			○ Validate failover of BGP to use routes from PSAP router A ○ Login to router B; enable monitoring, verify routing neighborships and VRRP have restored to pre-event states Note: Test cases should also include hard power down/up of the routers and the physical disconnection of the WAN. Need onsite resource with knowledge of networking equipment to support this test case.		
5	Perform WAN interface shutdown and validation on each West network edge router at PSAP	Failover	○ Place test call ○ Perform automatic reload on router A ○ Shut down WAN interface ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router B ○ Restore connectivity on PSAP router A ○ Perform automatic reload on router B ○ Shut down WAN interface ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router A		

			○ Restore connectivity on PSAP router B Note: Test cases should also include hard power down/up of the routers and the physical disconnection of the WAN. Need onsite resource with knowledge of networking equipment to support this test case.		
6	Perform reboot and validation on each ATT Interface Router (between CPE and West router)		○ Place test call ○ Unplug interface on ATT Interface router A facing WEST ESINet Edge router A. ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from WEST ESINet Edge router B ○ Restore connectivity between ATT Interface router A facing WEST ESINet Edge router A. ○ Validate traffic restores to primary path after appropriate time. ○ Unplug interface on ATT Interface router A facing CPE Network equipment (could be router or switch) ○ Identify any audio disruptions		

			○ Validate failover of BGP to use routes from WEST ESINet Edge router A to ATT interface router A, then downstream using the Side link to AT&T Interface Router B. ○ Restore connectivity between AT&T Interface Router A and the CPE Network Equipment. ○ Validate traffic restores to primary path after appropriate time. ○ Power down AT&T Interface router A by either unplugging the power or shutting off the power switch. alidate traffic restores to primary path after appropriate time. ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from WEST ESINet Edge router B to ATT interface router B to CPE Router B. ○ Restore power to AT&T Interface Router B. Once fully restore, verify all traffic resumes on via the A side link on the WEST ESINet edge router and the ATT Interface Router.		

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

			Repeat all steps for the ATT Interface Router B. Please note, no disruptions in audio are experienced during the testing of ATT Interface Router B. Note: All test cases should include powering down or unplugging of cables. Soft reloads and administrative shutdowns should not be used. Additionally, onsite expertise should be used for WAN failover testing of WEST ESINet Edge routers to remove WAN circuits on 'street side' of TELCO demarcation if possible to force routing protocols and hello intervals to work rather than forcing a router interface status change.		
7	Wireline Call Routed to PSAP through AT&T ESInet	Equipment	Wireline test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, & Voice delivered. <PASS/FAIL>
8	Wireless Call Routed to PSAP through AT&T ESInet	Equipment	Wireless test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Note: actual caller's number with no location data. Location will be tested during cutover.	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI and voice delivered. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

9	VOIP Call Routed to PSAP through AT&T ESInet	Equipment	VOIP test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Note: actual caller's number with no location data. Location will be tested during cutover.	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI and voice delivered. <PASS/FAIL>
10	CPE bids i3 Components	Call Handling	Test call sent to <PSAP NAME>. Call taker performs manual rebid on the ANI.	<5 min	HH:MM MT - HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, responder info, and voice delivered. AT&T verifies CPE can independently bid the ECRF, LIS, and ADR. <PASS/FAIL>
11	i3 Routing Fails, Routing via SRDB for Wireline call	Call Routing	Test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	<10 min	Place a call from TN with no X/Y provisioned in ALI. Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
12	i3 Routing via ECRF for Wireline call	Call Routing	Test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	<10 min	Make a call from TN with X,Y provisioned. Note: need TNs in advance. HH:MM MT – TN re-inserted to ALI/LIS. Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

13	i3 Transfer: Fixed Bridge Conferencing Confirmation (Call to IP PSAP then bridge to i3 PSAP if available – willing PSAP)	Call Handling	Test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Test call transferred to <i3 TRANSFER PSAP (URI)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects. Note: at day of cut, test conference/transfer with neighbor PSAPs	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (URI)>; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
14	S/R Transfer: Selective Bridge Conferencing Confirmation, if used by the PSAP	Call Handling	Test call transferred to <Police, Fire or EMS>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to correct agency for given TN record; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
15	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <CAMA TRANSFER PSAP (URI)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <CAMA TRANSFER PSAP (URI)>; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
16	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <SIP TRANSFER PSAP (URI)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <SIP TRANSFER PSAP (URI)>; good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
17	PSTN Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (XXX-XXX-XXXX)>. All parties on the bridge talk to confirm conferencing is	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (XXX-XXX-XXXX)>; good ANI and voice delivered. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

			established. Call taker at <TRANSFER PSAP> disconnects.		
18	Manual Transfer to valid local TN	Call Handling	Test call sent to <TEST PSAP>; Manual Transfer to local TN: <NPA-NXX-XXXX>	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI, location, subscriber information and voice delivered; manual transfer to <NPA.NXX.XXXX>; good Voice delivered; conferencing established. <PASS/FAIL>
19	Manual conference bridging to invalid unassigned number	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to an unassigned TN: 574-243-9761	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and voice delivered; manual transfer to <NPA.NXX.XXXX>; Ensure Caller and PSAP can talk over announcement or tones. <PASS/FAIL>
20	Manual conference bridging to a valid 8YY number	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to a 8YY TN TN: 800-225-5288	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual transfer to <NPA.NXX.XXXX>; good Voice delivered; conferencing established. Ensure caller can interact with the IVR by pressing DTMF digit 1. Ensure call taker can interact with the IVR by pressing DTMF digit 3. <PASS/FAIL>
21	Manual conference bridging to a valid Busy number	Call handling	Test call sent to <PSAP NAME>; Manual Transfer to a Busy TN TN: <???-???-????>	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual transfer to <NPA.NXX.XXXX>; Ensure Caller and PSAP can talk over busy tones. <PASS/FAIL>
22	Manual conference bridging Multi-Party Conference	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to <6> Additional parties. (Number of parties is determined by the customer requirements.)	<20 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual conference to add <6> additional parties to <NPA.NXX.XXXX>; Ensure all parties have voice

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

					path. Verify voice path as parties drop from conference. <PASS/FAIL>
23	Manual conference bridging to valid long distance cell	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to long distance cell: <NPA-NXX-XXXX>	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, & Voice delivered; manual transfer <NPA-NXX-XXXX>; good ANI and voice delivered; conferencing established. <PASS/FAIL> Ensure all parties have voice path. Verify voice path as parties drop from conference. <PASS/FAIL>
24	Alternate Routing	Call Routing	All trunks busied to force all calls to route to Alternate Route. Test call sent to <PSAP NAME>, call routed to <ALTERNATE ROUTE> as expected.	<10 min	HH:MM MT - Trunks busied out. HH:MM MT - Test call generated from AT&T to <PSAP NAME>; call routed to <ALTERNATE ROUTE> as expected. <PASS/FAIL>
25	Ring no Answer Timer	Call Routing	Test call sent to <TEST PSAP>, call is allowed to ring continuously until rolling over to Alternate route (3xRNA TIMER): call routes to <ALTERNATE ROUTE> as expected.	<5 min	HH:MM: MT – Test call behaves as expected and rolls over to expected destination. <PASS/FAIL>
26	No position Logged In	Call Routing	Log all positions out. Place test call to <TEST PSAP>. System should return 486. Network should attempt to route call over alternate paths. After call cannot be delivered on alternate paths call should overflow to alternate location – <ALTERNATE ROUTE>	<5 min	HH:MM MT - Test call behaves as expected and rolls over to expected destination. <PASS/FAIL>
27	Abandonment Routing	Call Routing	PSAP is manually put into an abandoned state	<20 min	HH:MM MT – PSAP Abandoned HH:MM MT - Test call generated from AT&T to <PSAP NAME>; call routed to <ABANDONMENT

AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

			Test call sent to <PSAP NAME>, call routed to <ABANDONMENT ROUTE> as expected. Note: Alternate routes used for errors, timeout or if trunks are out of service. Abandonment route – PSAP put in abandonment mode with PSAP Busy Device (PAD) or by calling Resolution Center (CMP)		<ROUTE> as expected with good ANI, location and subscriber information, and voice delivered. <PASS/FAIL>
28	Un-Abandonment Routing	Call Routing	PSAP is manually put into an un-abandoned state Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected.	<10 min	HH:MM MT - PSAP Un-Abandoned HH:MM MT - Test call generated from AT&T to <PSAP NAME>; call routed to <PSAP NAME> as expected with good ANI, location and subscriber information, and voice delivered.. <PASS/FAIL>
29	Abandonment Routing – PAD Testing (if PAD available)	Call Routing	PSAP is manually put into an abandoned state using the PSAP Abandonment Device. Test call sent to <PSAP NAME>, call routed to <ABANDONMENT ROUTE> as expected.	<20 min	HH:MM MT – PSAP Abandoned using PAD HH:MM MT - Test call generated from AT&T to <PSAP NAME>; call routed to <ABANDONMENT ROUTE> as expected with good ANI, location and subscriber information, and voice delivered.. <PASS/FAIL>
30	Un-Abandonment Routing – PAD Testing (if PAD available)	Call Routing	PSAP is manually put into an un-abandoned state Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected.	<10 min	HH:MM MT - PSAP Un-Abandoned using PAD HH:MM MT - Test call generated from AT&T to <PSAP NAME>, call routed to <PSAP NAME> as expected with good ANI, location and subscriber information, and voice delivered..



AT&T ESINET OPERATIONAL READINESS TEST PLAN: i3 PSAPS

					<PASS/FAIL>
31	Test line appearances that appear on each CPE	Call Processing	Make additional test calls to validate remaining line appearances.	<5 min	HH:MM MT – Remaining trunks each hit with a test call. <PASS/FAIL>
32	TTY call	Call handling	Ingress TTY call to a PSAP and verify two-way communication with no anomalies Note: TTY devices in ATT San Ramon and Sacramento PSAP labs	<5 min	HH:MM MT – Trunk(s) placed back into service. Ensure that no anomalies are observed during a 2 way TTY conversation. <PASS/FAIL>
33	TTY conference call	Call handling	Ingress TTY call to a PSAP and verify two-way communication with no anomalies Add conferenced party and verify no anomalies Note: TTY devices in ATT San Ramon and Sacramento PSAP labs	<5 min	HH:MM MT – Trunk(s) placed back into service. Ensure that no anomalies are observed during a 3 way TTY conversation. <PASS/FAIL>



Appendix C - ATT ESInet Operational Readiness Test Plans RFAI PSAPs



AT&T ESInet™

Operational Readiness Test Plan

RFAI PSAPs

<PSAP Name>

<Test Date>



Trademark Ownership

All trademarks used herein are the property of their respective owners.

Non-Disclosure

The information contained in this document and provided to PSAP is Corporate Confidential in its entirety. This restricts the disclosure of any information herein to a third-party and other terms and conditions under the terms of a Non-Disclosure Agreement.

Open Records Act Request

PSAP will immediately advise in writing of any Open Records Act type of requests as it may relate to this proposal or any information contained herein.

Introduction

The AT&T ESInet™ Operational Readiness Test Plan described in this document provides an overview of testing and a list and description of test cases for the implementation of the AT&T ESInet services. The objective for this test plan is to demonstrate the network and call processing equipment readiness to receive 9-1-1 traffic using the AT&T ESInet service. Test participants include <PSAP NAME> and AT&T ESInet Service Delivery.

The AT&T ESINET Operational Readiness Test Cases will demonstrate feature functionality of the AT&T ESInet. The test calls will deliver simulated "9-1-1" calls from the AT&T end office to the PSAPs over the AT&T ESInet to the call processing equipment installed at the <PSAP NAME>.

AT&T manages the testing process and coordinates all test calls documented in the AT&T ESInet Operational Readiness Test Plan. The testing is scheduled in accordance with the PSAP's availability. The PSAP is asked to provide a resource to answer the test calls and may be asked to provide documentation (i.e. screen prints and recordings) for certain calls.

The list of standard tests demonstrates feature functionality of the AT&T ESInet to include:

- Operation of the AT&T ESInet PSAP Network Edge equipment
- Call handling and routing Processes:
 - Call transfer and bridging functions
 - Alternate and default routing
 - PSAP abandonment routing
 - PAD abandonment routing

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

Test #	Test Case	Type	Testing Criteria	Time	Pass/Fail and Comments
TEST LOCATION: <TEST PSAP> DATE & TIME: <DATE/TIME> CALL ORIGINATOR: AT&T			CALL TAKER: ON-DUTY CALL-TAKER ANI: <ANI>		
1	Trunk Verification	Call Routing	Egress trunks manually busied out to force calls through each SIP Contact Test call sent to <TEST PSAP>. SBC1: <SBC Name> SBC2: <SBC Name> SBC3: <SBC Name> Note: This is an egress SIP from SBC to PSAP	<5 min	HH:MM MT – Trunk(s) busied out HH:MM MT – Test call made to <TEST PSAP>, call routed to <TEST PSAP> as expected with good ANI/ALI, location, subscriber information and Voice delivered. <PASS/FAIL>
2	Trunk Verification (SS7 Ingress from LSR)	Call Routing	Know the Ingress primary and alternate trunk groups for the project. Caller dials PSAP test number multiple times into the primary trunk group. Monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group. Calls then should traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested.	<30 min	HH:MM MT – Each ingress trunk channels tested. Voice quality of each channel is tested. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			If all of the channels test okay, then have the primary trunk group restored. Note: from the LSR, the trunk groups should be set to most idle. From the MetaSwitch the trunk groups should be set to least idle.		
3	Trunk Verification (SS7 Egress from AGC to LSR)	Call Routing	Know the Egress primary and alternate trunk groups for the project. Caller dials PSAP test number. After the call is established, the PSAP call taker will need to place multiple conference calls to a friendly off net PSAP. Monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group. Calls then should traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested. If all of the channels test okay, then have the primary trunk group restored. Note: From the MetaSwitch the trunk groups should be set to most idle.	<30 min	HH:MM MT – Each egress trunk channels tested. Voice quality of each channel is tested <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

4	Perform reboot and validation on each West network edge router at PSAP	Failover test	○ Place Test call ○ Reboot PSAP router A ○ Observe PSAP router B become VRRP master for all applicable networks ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router B ○ Login to router A; enable monitoring, verify routing neighbor-ships and VRRP have restored to pre-event states ○ Reboot PSAP router B ○ Observe PSAP router A become VRRP master for all applicable networks ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router A ○ Login to router B; enable monitoring, verify routing neighbor-ships and VRRP have restored to pre-event states ○ Note: Test cases should also include hard power down/up of the routers and the physical disconnection of the WAN.		HH:MM MT – 1.) Ensure that there is very little loss of audio < 2 seconds. 2.) Ensure that the call remains connected, and is not dropped. <PASS/FAIL> Comments include the following assumptions: Test plans would need to take into account the following: 1. Some PSAPs may not have redundant connections 2. All WEST ESINet WAN routers could be thoroughly tested without impact to customer.

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			Note: Need onsite resource with knowledge of networking equipment to support this test case.		
5	Perform WAN interface shutdown and validation on each West network edge router at PSAP	Failover	○ Place test call ○ Perform automatic reload on router A ○ Shut down WAN interface ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router B ○ Restore connectivity on PSAP router A ○ Perform automatic reload on router B ○ Shut down WAN interface ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from PSAP router A ○ Restore connectivity on PSAP router B Note: Test cases should also include hard power down/up of the routers and the physical disconnection of the WAN. Need onsite resource with knowledge of networking equipment to support this test case.		

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

6	Perform reboot and validation on each ATT Interface Router (between CPE and West router)	Equipment	○ Place test call ○ Unplug interface on ATT Interface router A facing WEST ESINet Edge router A. ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from WEST ESINet Edge router B ○ Restore connectivity between ATT Interface router A facing WEST ESINet Edge router A. ○ Validate traffic restores to primary path after appropriate time. ○ Unplug interface on ATT Interface router A facing CPE Network equipment (could be router or switch) ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from WEST ESINet Edge router A to ATT interface router A, then downstream using the Side link to AT&T Interface Router B. ○ Restore connectivity between AT&T Interface Router A and the CPE Network Equipment. ○ Validate traffic restores to primary path after appropriate time.		

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			○ Power down AT&T Interface router A by either unplugging the power or shutting off the power switch. validate traffic restores to primary path after appropriate time. ○ Identify any audio disruptions ○ Validate failover of BGP to use routes from WEST ESINet Edge router B to ATT interface router B to CPE Router B. ○ Restore power to AT&T Interface Router B. Once fully restore, verify all traffic resumes on via the A side link on the WEST ESINet edge router and the ATT Interface Router. ○ Repeat all steps for the ATT Interface Router B. Please note, no disruptions in audio are experienced during the testing of ATT Interface Router B. Note: All test cases should include powering down or unplugging of cables. Soft reloads and administrative shutdowns should not be used. Additionally, onsite expertise should be used for WAN failover testing of WEST ESINet Edge routers to remove WAN circuits on 'street side' of TELCO demarcation if possible to force routing protocols and hello intervals to work		

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			rather than forcing a router interface status change.		
7	Wireline Call Routed to PSAP through AT&T ESInet	Equipment	Wireline test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI, location, subscriber information and Voice delivered. <PASS/FAIL>
8	Wireless Call Routed to PSAP through AT&T ESInet	Equipment	Wireless test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Note: actual caller's number with no location data. Location will be tested during cutover.		HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI and Voice delivered. <PASS/FAIL>
9	VOIP Call Routed to PSAP through AT&T ESInet	Equipment	VOIP test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Note: actual caller's number with no location data. Location will be tested during cutover.		HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI and Voice delivered. <PASS/FAIL>
10	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call sent to <TEST PSAP> and transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TEST PSAP> disconnects. Caller confirms that caller and call taker at <TRANSFER PSAP> are still bridged.	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI, location, subscriber information and Voice delivered; transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and & Voice delivered; conferencing established. <PASS/FAIL>
NOTE: A separate call will not be needed for each of the remaining fixed bridge test cases. A single call can be made and transferred multiple times.					
11	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call sent to <TEST PSAP> and transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI, location, subscriber information and Voice delivered; transfer to <TRANSFER PSAP (*XX)>;

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			conferencing is established. Call taker at <TRANSFER PSAP> disconnects.		good ANI/ALI, location, subscriber information and Voice delivered; conferencing established. <PASS/FAIL>
12	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and Voice delivered; conferencing established. <PASS/FAIL>
13	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and Voice delivered; conferencing established. <PASS/FAIL>
14	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and Voice delivered; conferencing established. <PASS/FAIL>
15	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and voice delivered; conferencing established. <PASS/FAIL>
16	S/R Transfer: Fixed Bridge Conferencing Confirmation	Call Handling	Test call transferred to <TRANSFER PSAP (*XX)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	<5 min	HH:MM MT - Transfer to <TRANSFER PSAP (*XX)>; good ANI/ALI, location, subscriber information and voice delivered; conferencing established. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

17	Manual Transfer to valid local TN	Call Handling Processing	Test call sent to <TEST PSAP>; Manual Transfer to local TN: <NPA-NXX-XXXX>	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI, location, subscriber information and voice delivered; manual transfer to <NPA.NXX.XXXX>; good Voice delivered; conferencing established. <PASS/FAIL>
18	Manual conference bridging to invalid unassigned number	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to an unassigned TN: 574-243-9761	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and voice delivered; manual transfer to <NPA.NXX.XXXX>; Ensure Caller and PSAP can talk over announcement or tones. <PASS/FAIL>
19	Manual conference bridging to a valid 8YY number	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to a 8YY TN TN: 800-225-5288	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual transfer to <NPA.NXX.XXXX>; good Voice delivered; conferencing established. Ensure caller can interact with the IVR by pressing DTMF digit 1. Ensure call taker can interact with the IVR by pressing DTMF digit 3. <PASS/FAIL>
20	Manual conference bridging to a valid Busy number	Call handling	Test call sent to <PSAP NAME>; Manual Transfer to a Busy TN TN: <???-???-????>	<5 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual transfer to <NPA.NXX.XXXX>; Ensure Caller and PSAP can talk over busy tones. <PASS/FAIL>
21	Manual conference bridging Multi-Party Conference	Call Handling	Test call sent to <PSAP NAME>; Manual Transfer to <6> Additional parties. (Number of parties is determined by the customer requirements.)	<20 min	HH:MM MT - Test call generated from AT&T to <PSAP NAME>; good ANI, location and subscriber information, and Voice delivered; manual conference to add <6> additional parties to <NPA.NXX.XXXX>; Ensure all parties have voice path. Verify voice path as parties drop from conference. <PASS/FAIL>
22	Manual Transfer to valid long distance cell phone	Call Handling	Test call sent to <TEST PSAP>; Manual Transfer to long distance cell: <NPA-NXX-XXXX>	<5 min	HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI and Voice delivered; manual transfer <NPA-NXX-XXXX>; good ANI, location, subscriber

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

					information and Voice delivered; conferencing established. <PASS/FAIL>
23	DTMF Transfer	Call Handling	Test call sent to <TEST PSAP>; Manual Transfer to DTMF Test Line TN: 720-494-6650, option 1 selected. Call taker verifies “Digit Verified” message reached.		HH:MM MT - Test call generated from AT&T to <TEST PSAP>; good ANI/ALI, location, subscriber information and voice delivered; manual transfer to 720-494-6650. Call taker hears recording and presses 1, verifies that they hear “digit verified” recording. <PASS/FAIL>
24	Alternate Routing	Call Routing	All trunks busied to force all calls to route to Alternate Route. Test call sent to <TEST PSAP>, call routed to <ALTERNATE ROUTE> as expected.	<10 min	HH:MM MT - Trunks busied out. HH:MM MT - Test call generated from AT&T to <TEST PSAP>; call routed to <ALTERNATE ROUTE> as expected. <PASS/FAIL>
25	Ring no Answer Timer	Call Routing	Test call sent to <TEST PSAP>, call is allowed to ring continuously until rolling over to Alternate route (3xRNA TIMER): call routes to <ALTERNATE ROUTE> as expected.	<5 min	HH:MM: MT – Test call behaves as expected and rolls over to expected destination. <PASS/FAIL>
26	No position Logged In	Call Routing	Log all positions out. Place test call to <TEST PSAP>. System should return 486. Network should attempt to route call over alternate paths. After call cannot be delivered on alternate paths call should overflow to alternate location – <ALTERNATE ROUTE>	<5 min	HH:MM MT - Test call behaves as expected and rolls over to expected destination. <PASS/FAIL>
27	Abandonment Routing	Call Routing	PSAP is manually put into an abandoned state Test call sent to <TEST PSAP>, call routed to <ABANDONMENT ROUTE> as expected. Note:	<20 min	HH:MM MT – PSAP Abandoned HH:MM MT - Test call generated from AT&T to <TEST PSAP>; call routed to <ABANDONMENT ROUTE> as expected with good ANI/ALI & Voice. <PASS/FAIL>

AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			Alternate routes used for errors, timeout or if trunks are out of service. Abandonment route – PSAP put in abandonment mode with PSAP Busy Device (PAD) or by calling Resolution Center (update CMP).		
28	Un-Abandonment Routing	Call Routing	PSAP is manually put into an un-abandoned state Test call sent to <TEST PSAP>, call routed to <TEST PSAP> as expected.	<10 min	HH:MM MT - PSAP Un-Abandoned HH:MM MT - Test call generated from AT&T to <TEST PSAP>; call routed to <TEST PSAP> as expected with good ANI/ALI & Voice. <PASS/FAIL>
29	Abandonment Routing – PAD Testing	Call Routing	PSAP is manually put into an abandoned state using the PSAP Abandonment Device. Test call sent to <TEST PSAP>, call routed to <ABANDONMENT ROUTE> as expected.	<20 min	HH:MM MT – PSAP Abandoned using PAD HH:MM MT - Test call generated from AT&T to <TEST PSAP>; call routed to <ABANDONMENT ROUTE> as expected with good ANI/ALI, location, subscriber information and voice delivered. <PASS/FAIL>
30	Un-Abandonment Routing – PAD Testing	Call Routing	PSAP is manually put into an un-abandoned state Test call sent to <TEST PSAP>, call routed to <TEST PSAP> as expected.	<10 min	HH:MM MT - PSAP Un-Abandoned using PAD HH:MM MT - Test call generated from AT&T to <TEST PSAP>, call routed to <TEST PSAP> as expected with good ANI/ALI, location, subscriber information and Voice delivered. <PASS/FAIL>
31	Test line appearances that appear on each CPE	Call Processing	Make additional test calls to validate remaining line appearances.	<5 min	HH:MM MT – Remaining trunks each hit with a test call. <PASS/FAIL>
32	TTY call	Call handling	Ingress TTY call to a PSAP and verify two-way communication with no anomalies	<5 min	HH:MM MT – Trunk(s) placed back into service. Ensure that no anomalies are observed during a 2 way TTY conversation.



AT&T ESINET OPERATIONAL READINESS TEST PLAN: RFAI PSAPS

			Note: TTY devices in ATT San Ramon and Sacramento PSAP labs		<PASS/FAIL>
33	TTY conference call	Call handling	Ingress TTY call to a PSAP and verify two-way communication with no anomalies Add conferenced party and verify no anomalies Note: TTY devices in ATT San Ramon and Sacramento PSAP labs	<5 min	HH:MM MT – Trunk(s) placed back into service. Ensure that no anomalies are observed during a 3 way TTY conversation. <PASS/FAIL>



Appendix D - ORT-Acceptance Test Plan

AT&T ESInet™

Operational Readiness Test Plan

Version 8.4 08/06/2025

Trademark Ownership

All trademarks used herein are the property of their respective owners.

Non-Disclosure

The information contained in this document and provided to PSAP is Corporate Confidential in its entirety. This restricts the disclosure of any information herein to a third-party and other terms and conditions under the terms of a Non-Disclosure Agreement.

Open Records Act Request

PSAP will immediately advise in writing of any Open Records Act type of requests as it may relate to this proposal or any information contained herein.

© 2025 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary and Confidential. AT&T Proprietary: The information contained herein is for use i) by authorized persons only, not for general distribution, and ii) in accordance with the applicable AT&T Master Agreement or Non-Disclosure Agreement.

Introduction

The AT&T ESInet™ Operational Readiness Test Plan described in this document provides an overview of testing and a list and description of test cases for the implementation of the AT&T ESInet™ services. The objective for this test plan is to demonstrate the network and call processing equipment readiness to receive 9-1-1 traffic using the AT&T ESInet™ service. Test participants include the in test PSAP and AT&T ESInet™ Service Delivery.

The AT&T ESInet™ Operational Readiness Test Cases will demonstrate feature functionality of the AT&T ESInet™. The Test calls will deliver simulated “9-1-1” calls from the ILEC SR to the PSAPs over the AT&T ESInet™ to the call handling equipment installed at the in test PSAP.

AT&T manages the testing process and coordinates all test calls documented in the AT&T ESInet™ Operational Readiness Test Plan. The testing is scheduled in accordance with the PSAP's availability. The PSAP may be asked to provide a resource to answer the test calls and to provide documentation (i.e. screen prints and recordings) for certain calls.

The list of standard tests demonstrates feature functionality of the AT&T ESInet™ to include:

- Operation of the AT&T ESInet™ PSAP Network Edge equipment
 - AVPN failover
 - Call handling and routing processes:
 - Call transfer and bridging functions
 - Alternate and default routing
 - Independent i3 component availability
 - PSAP abandonment routing
 - PAD abandonment routing
 - FirstNet AVPN Failover and Functional tests

CONFIDENTIAL AND PROPRIETARY AT&T INFORMATION – DO NOT DISCLOSE TO THIRD PARTIES WITHOUT THE AUTHORIZATION OF AT&T

Test LocationPSAP:

Test Date:

CALL ORIGINATOR: AT&T

CALL TAKER: ON-DUTY CALL-TAKER

Calling Party POTS ANI: XXX-XXX-XXXX

Dialable Test (TN Forwards 911): XXX-XXX-XXXX

Dialable Test TN (Forwards PSAP Pilot Number): XXX-XXX-XXXX

Inbound Trunk Info:

<PSAP NAME>

<i>ILEC 2-6</i>	<i>Gateway</i>	<i>LSR Owner Or OSP</i>	<i>LSR Owner Or OSP</i>	<i>Direction</i>	<i>Pri/Alt</i>	<i>Default PSAP</i>	<i>Qty</i>	<i>CICs</i>	<i>P/F</i>	<i>911</i>

Test Case	Test Description	Status	Date / Time	Testing Criteria	Method	Expected Results	Notes / Observations
TC-01	Wireline Call Routed to PSAP through AT&T ESInet * Run in conjunction with TC-02 (Transfer Number)			Wireline test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	Call is initiated with test TNs or dialer.	Call routes to <PSAP NAME> as expected with good two way audio.	
TC-02	Verify ANI/ALI and Location Data * Run in conjunction with TC-01 (Transfer Number)			Wireline test call sent to <PSAP NAME>. Caller confirms ANI/ALI and XY is displayed.	Call is initiated with test TNs or dialer.	Call routes to <PSAP NAME> as expected with good ANI and good location data.	
TC-03	VNS - Verify Preference vs Load Share			Note: for Multi-Node PSAPs only. VNS to verify that CPE routing method matches the specifications detailed in VNS CPE Manufacturer's documentation. •Preference Node A (Active/Passive). •Load Share between Node A and Node B (Active/Active).	VNS to verify Priority-Q Values in MP.	Priority-Q Values should meet criteria detailed in the VNS CPE Manufacturer's documentation.	
TC-04	VNS - Verify ECRF Routing enabled			For ESI-Net to perform ECRF/GIS routing, the ROUTE TYPE for ITG's in ESInet must be set to "ECRF;" VNS support to confirm.	VNS to check the setting of Route Type for ITG's in ESInet to ensure it's set to "ECRF", not "Selective".	Route Type is set to "ECRF".	
TC-05	VNS - SIP contacts Verification * (Transfer Number)			VNS to manually busy out SIP contacts. Test call sent to PSAP. Repeat process for each SIP contact built. SBC1: <ECMC1a> / <ECMC1b> SBC2: <ECMC2a> / <ECMC2b> SBC3: <ECMC3a> / <ECMC3b>	VNS to manually busy out all SIP contacts except one. Test call sent to <PSAP NAME> using the TRANSFER test TN. Repeat for every SIP Contact.	Calls route to <PSAP NAME> as expected. Good ANI/ALI, Location Data, and two way audio.	
TC-06	Busy on Incoming Transfer (Transfer Number)			All SIP contacts busied to force calls to Busy on Incoming transfer. Verify destination with data collection workbook (DCW).	Test call sent to <PSAP Name> using TRANSFER test TN. Call routes to <BUSY ON INCOMING>.	Call routes to <BUSY ON INCOMING> as expected. Good two way audio.	
TC-07	Alternate Routing (Handoff Number)			Test case is n/a if destination Matches Busy on Incoming Transfer Destination. All SIP Contacts busied to force all calls to Alternate Route. Verify with data collection workbook.	Test call sent to <PSAP Name> using HANDOFF test TN. Call routes to <ALTERNATE ROUTE>.	Call routes to <ALTERNATE ROUTE> as expected. Good two way audio.	
TC-08	Back up Route (Transfer Number)			VNS enables Back Up Routing in Management Portal (MP).	Test call sent to <PSAP Name> using TRANSFER test TN. Call routes to <Back up Route>.	Call routes to <Back up Route> as expected. Good two way audio.	
TC-09	VNS - Normalize PSAP (Transfer Number)			VNS to normalize PSAP profile in MP. Wireline test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	VNS to ensure all SIP contacts are "Equipped" and "In Service". And that Backup Routing has been disabled.	Call routes to <PSAP NAME> as expected with good ANI and good two way audio.	
TC-10	Ring no Answer Timer (Transfer Number)			Call is allowed to ring continuously until rolling over to Alternate route.	Test call sent to <PSAP NAME>. Call is allowed to ring continuously for (3xRNA TIMER). Call routes to <ALTERNATE ROUTE> as expected. Ensure there is no abandoned call on the CPE abandoned call list.	Call Routed to <ALTERNATE ROUTE> as expected. Good two way audio. Ensure there is no abandoned call on the CPE abandoned call list.	
TC-11	CPE line appearances (Transfer Number)			Make test calls to validate all line appearances. Make total x+1 calls where x is line limit.	Make test calls to validate line appearances. Make total x+1 calls where x is line limit. X calls shall busy out all the lines, and the last call (x+1) shall be re-routed to an alternate destination.	Call routes to <ALTERNATE ROUTE> as expected. Good two way audio.	

TC-12	CAMA Trunk Validation			-Borrow one of the Legacy CAMA trunks for testing. -Connect trunk to Intrado PGM and the new 66 block. -Perform Call-Through test, run KP48 test, and check for battery. -Punch down through remaining ports on the 66 block, running KP48 tests and battery check. -Repeat with other PGM(s) if applicable. -Swing borrowed trunk back to Legacy configuration. Note: Generally, a WRLN trunk is borrowed to ~~reduce impact to the PSAP~~	Test call sent to <PSAP NAME>; good ANI/ALI, location, subscriber information and Voice delivered; check that KP48 and battery checks are successful and that the expected PTMs are being punched down to according to PGM diagram.	Verify implementation matches design for trunk rout	
TC-12	Trunk Verification (SS7 Ingress from LSR) (N/A if the trunk groups had been already tested before) * Also see TC-13 and TC-14 (Transfer Number)			Know the Ingress primary and alternate trunk groups for the project.	Caller dials PSAP test number multiple times into the primary trunk group.	VNS to monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group. Calls then should traverse the alternate trunk group. Caller dials PSAP test number multiple times into the alternate trunk group.	
TC-13	Trunk group Default PSAP verification (N/A if the trunk groups had been already tested before) * Should be tested during TC-12 (Handoff Number)			Each trunk group will be provisioned with a default PSAP. If the call comes to ESInet with an ANI not in the SRDB, it will default route based on the incoming trunk group.	A) Verifying the Pri trunk group Default PSAP: Do not busy out the Pri trunk group. Using a phone (cell or landline) its ANI is NOT provisioned in the SRDB, dial the Test TN that out-pulses 911 to make a call. Verify the call routes to the default PSAP on a 911 trunk. B) Verifying the Alt trunk group Default PSAP: Busy out the Pri trunk group, but leave Alt trunk group in service. Using a phone (cell or landline) its ANI is NOT provisioned in the SRDB, dial the Test TN that out-pulses 911 to make a call. Verify the call routes to the default PSAP associated with Alt Trunk group on a 911 trunk. Put both trunk groups back to service once done. C) Repeat the above steps for all new ITGs. Both SS7. It is the responsibility of ATT to identify all new ITGs. There may be different ITGs for different call types (WRLN, WRLS, VOIP), LECs, LSRs, or other ESINET.	Call is routed to the default PSAP.	
TC-14	Trunk Verification (SS7 Egress from AGC to LSR) * Update after Transfer testing is completed			Know the Egress primary and alternate trunk groups for the project. Note: From the MetaSwitch the trunk groups should be set to most idle.	Caller dials PSAP test number. After the call is established, the PSAP call taker will need to place multiple conference calls to a friendly off net PSAP. Monitor from the MetaSwitch that all channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group. Calls then should traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested. If all of the channels test okay, then have the primary trunk group restored.	All egress channels tested and have good voice quality.	

TC-15	Augmented Trunk Verification (SS7 Egress from AGC to LSR) *			Know the Egress primary and alternate trunk groups for the project. Note: From the MetaSwitch the trunk groups should be set to most idle.	Note: This test case is applicable to pre existing trunk groups that will be augmented. 1.) Ensure that the Camp-on feature is enabled from the MetaSwitch. By doing so, this will prevent the MetaSwitch from disconnecting any live egress calls. 2.) Have VNS place all of the first 23 channels of the primary trunk group OOS, and leave the last channel available for live calls. 3.) Caller dials PSAP test number. After the call is established, the PSAP call taker will need to place multiple conference calls to a friendly off net PSAP. Monitor from the MetaSwitch that all of the augmented channels get utilized for the multiple calls, and all calls have good voice quality. If all of the primary TG channels test okay, then from the MetaSwitch, busy out the primary trunk group, and have VNS busy out the first 23 channels of the alternate trunk group. Calls then should traverse the alternate trunk group. Continue to place multiple calls until all of the alternate trunk group channels have been tested. If all of the channels test okay, then have VNS restore all busied out channels for both the Primary and Alternate trunk group.		
TC-16	NNI TGRP Default PSAP verification (only applies for 911 NNI ingress Markets) *			A Handoff number must be provided by the Originating Service Provider (OSP) to complete this Test Case For NNI ingress to a primary PSAP that gets its own TGRP, which has a unique default route. Using a phone (cell or landline) its ANI is NOT provisioned in the SRDB, dial the Test TN for NNI ingress that out-pulses 911 to make a call.	Refer to TC-14 for detailed instructions Intrado VNS needs to verify the call routes to the default PSAP as expected. Note: At time of ORT, if a default PSAP is supposed to be a live ESInet PSAP but that PSAP has not yet been in live, the default route may go to an off-net dial plan legacy live PSAP.	Call is routed to the default PSAP.	
TC-17	i3 Routing via ECRF for Wireline call (Handoff Number)			Test call sent to <PSAP NAME>. Caller confirms routing and audio quality.	Call is initiated from a geocoded landline phone to the Handoff Number, which out-pulses 911. Call routing is verified by VNS. ORT Lead can verify in the CDR, by searching for MODEL_USED (ECRF Routing) and confirming the expected DESTINATION.NAME was listed. ORT Lead to record timestamp and save a copy of the CDR (right click "save as")	Call routed to the Live Instance of <PSAP NAME> as expected. Good ANI/ALI, Location Data, and two way audio.	
TC-18	i3 Routing Fails, Routing via SRDB (Handoff Number)			Test call sent to <PSAP NAME>. Caller confirms routing and audio quality. SRDB Routing is performed when i3 Routing fails. Place a call from TN with no X/Y and is NOT provisioned in ALI. Recommended to request VNS temporarily add a cell phone number to SRDB.	Call is initiated using a non-geocoded phone number, which is provisioned in SRDB, to the Handoff number which out-pulse 911. Call routing is verified by VNS. ORT Lead can verify in the CDR, by searching for MODEL_USED (Selective Routing) and confirming the expected DESTINATION.NAME was listed.	Call routed to <PSAP NAME> as expected with good two way audio.	
TC-19	i3 Component Verification via Wireline (Transfer Number) To be run in conjunction with TC-20			Test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Call taker confirms Responding Agency Data (<i>Police, Fire, EMS</i>), ANI/ALI, and location data has all populated correctly. Call taker Captures a screenshot of above information for documentation.	Call is initiated using a geocoded landline number to the Transfer Number. Call taker takes a screenshot of Responding Agency Data (<i>Police, Fire, EMS</i>) ALI, and location data.	Call routed to the <PSAP NAME> as expected. Good ANI/ALI, Location Data, two way audio. Good Responding Agency Data (<i>Police, Fire, EMS</i>). Good LIS/ADR (<i>Service, Subscriber, Provider, and Held</i>).	

TC-20	CPE Rebid for i3 Components Verification via Wireline <i>To be run in conjunction with TC-19</i>			After the Test call is sent to <PSAP NAME>. Call Taker performs a rebid. Call taker confirms Responding Agency Data (<i>Police, Fire, EMS</i>), ANI/ALI , and location data has all populated correctly. Call taker Captures a screenshot of above information for documentation.	Call taker performs a rebid. Call taker takes a screenshot of Responding Agency Data (<i>Police, Fire, EMS</i>) ALI , and other location data . 	Call taker performs a rebid. Good ANI/ALI, Location Data, two way audio. Good Responding Agency Data (<i>Police, Fire, EMS</i>). Good LIS/ADR (<i>Service, Subscriber, Provider, and Held</i>).	
TC-21	i3 Component Verification via Wireless (Transfer Number) <i>To be run in conjunction with TC-22</i>			Test call placed to 911 from a cell phone at a neighboring Live on ESinet PSAP <SELECTED PSAP>. Call taker at <SELECTED PSAP> will attempt an On-Net transfer to <PSAP NAME> utilizing <Pilot TN 1>. <PSAP NAME> Call taker confirms Responding Agency Data, ANI/ALI, and location Data has all populated correctly. Call taker Captures a screenshot for documentation.	Call is initiated using a Cell phone to the 911 . Call is delivered to a Live ESinet PSAP . Call is transferred to <PSAP NAME> via an On-Net transfer utilizing the Pilot TN listed in MP. Call taker takes a screenshot of Responding Agency Data (<i>Police, Fire, EMS</i>) ALI , and other location data . 	Wireless calls may return "not Found" in the Aways due to being out of region. Call routed to the <PSAP NAME> as expected. Good ANI/ALI, Location Data, two way audio. Good Responding Agency Data (<i>Police, Fire, EMS</i>). Good LIS/ADR (<i>Service, Subscriber, Provider, and Held</i>).	
TC-22	CPE Rebid for i3 Components Verification via Wireless <i>To be run in conjunction with TC-21</i>			After the Test call is sent to <PSAP NAME>, Call taker performs a rebid. Call taker confirms Responding Agency Data (<i>Police, Fire, EMS</i>), ANI/ALI, and location data has all populated correctly. Call taker Captures a screenshot of above information for documentation.	Call taker performs a rebid. Call taker takes a screenshot of Responding Agency Data (<i>Police, Fire, EMS</i>) ALI , and other location data . 	Wireless calls may return "not Found" in the Aways due to being out of region. Call taker performs a rebid. Good ANI/ALI, Location Data, two way audio. Good Responding Agency Data (<i>Police, Fire, EMS</i>). Good LIS/ADR (<i>Service, Subscriber, Provider, and Held</i>).	
TC-23	Manual On-net Transfer (Transfer Number)			Test call sent to <PSAP NAME>. Caller confirms routing and audio quality. Call taker performs a manual on-Net transfer to a Live on ESinet PSAP utilizing their Pilot TN. <PSAPNAME> <XXX-119-XXXX> Note: wording on which transfer button to be used varies between vendors.	Test call sent to <PSAP NAME>; Manual on-Net Transfer to Live ESinet PSAP utilizing Pilot TN 1. 	Call Routed to <PSAP NAME>; good two way audio, ANI/ALI, and location Data. Manual transfer to <NPA-119-XXXX>; good two way audio, ANI/ALI, and location Data; with conferencing established.	
TC-24	S/R and PSTN Transfers: Fixed Bridge Conferencing Confirmation (Transfer Number)			Test call transferred to <SIP TRANSFER PSAP (URI)>. All parties on the bridge talk to confirm conferencing is established. Call taker at <TRANSFER PSAP> disconnects.	Call taker performs transfer after receiving initial test call.	Transfer to <SIP TRANSFER PSAP (URI)>; good ANI, location and subscriber information, and good two way audio.	
TC-25	Manual Transfer to valid local TN (Transfer Number)			Test call transferred to valid local TN.	Test call sent to <PSAP NAME>; manual transfer to local TN: <NPA-NXX-XXXX>.	Call routed to <PSAP NAME>; good two way audio, ANI/ALI, and location Data. Manual transfer to <NPA.NXX.XXXX>; good two way audio; conferencing established.	
TC-26	Manual conference to invalid unassigned number (Transfer Number)			Test call transferred to invalid unassigned TN.	Test call sent to <PSAP NAME>; manual transfer to an unassigned TN: 574-231-0945.	Call routed to <PSAP NAME>; good two way audio, ANI/ALI, and location Data. Manual transfer to <574-231-0945>; ensure caller and call taker can talk over announcement or tones.	
TC-27	Manual conference to a valid Busy number (Transfer Number)			Test call transferred to busy TN.	Test call sent to <PSAP NAME>; manual transfer to a busy TN: <316-262-0277>.	Call routed to <PSAP NAME>; good two way audio, ANI/ALI, and location Data. Manual transfer to <316-262-0277>; ensure caller and call taker can talk over busy tones.	

TC-28	Manual conference to a valid 8YY number (Transfer Number)			Test call transferred to 8YY number.	Test call sent to <PSAP NAME>; manual transfer to an 8YY TN: TN: 800-225-5288 (ATT).	Call routed to <PSAP NAME>; good two way audio, ANI/ALI, and location Data. Manual transfer to <800-225-5288>; good two way audio; conferencing established.	
TC-29	DTMF pass through verification * (Transfer Number)			Test call sent to <PSAP NAME>. Verify tones for caller and call-taker.	Call Taker conferences on the test IVR by dialing 631-791-8378. Caller waits for the IVR response. <i>"One moment please, this is uLaw please record your test message and press pound".</i> Select #. <i>Wait for the IVR response.</i> select 2 for DTMF testing. <i>Wait for the IVR response.</i> <i>"enter as many as 75 DTMF keys and then press # for a readout."</i> Selects 0-9 * then #. Verify that the IVR reads back the digits entered. Repeat DTMF testing from the PSAP's call taker. Note: The outbound call must have access to the PSTN network to execute this test.	Ensure that DTMF is recognized by the IVR from the caller and call takers input.	
TC-30	Manual conference bridging Multi-Party Conference (Transfer Number)			Test call sent to <PSAP NAME>; Manual Transfer to <6> Additional parties.	Test call sent to <PSAP NAME>; Manual Transfer to <6> Additional parties.	Call Routed to <PSAP NAME>; good two way audio. Manual conference to add <6> additional parties to <NPA.NXX.XXXX>; Ensure all parties have good two way audio. Verify voice path as parties drop from conference.	
TC-31	TTY * (Transfer Number)			TTY Test call sent to <PSAP NAME>.	TTY Test call sent to <PSAP NAME>; and verify two-way communication with no anomalies. Call Taker sends typed message. <i>Caller replies confirming message.</i> Call Taker sends a Canned Response. <i>Caller replies confirming message.</i>	Call Routed to <PSAP NAME>; good two way TTY communication	
TC-32	TTY Conference *			Test call transferred to an additional TTY Device.	Repeat testing from TC-32, including the additional Party. Call taker sends typed message. <i>Caller replies confirming message.</i> <i>Third party replies confirming message.</i> Call taker sends a Canned Response. <i>Caller replies confirming message.</i> <i>Third party replies confirming message.</i>	Call routed to <PSAP NAME>; good three way TTY communication. Ensure the three parties can view all messages.	
TC-33	Wireline caller Abandoned call (Transfer Number)			Verify the CPE handles abandoned call as expected.	Test call sent to <PSAP NAME>. Caller abandons call before to call taker answering. Verify the CPE handles abandoned call as expected.	Call Displays in abandon queue. Call Taker can redial . Call clears from abandon queue after Call Taker redials.	
TC-34	Abandonment Routing (Transfer Number)			Call routes to Abandonment PSAP when test PSAP is abandoned.	PSAP is manually put in abandonment mode using MP. Test call sent to <PSAP NAME>, call routed to <ABANDONMENT ROUTE> as expected.	Call routes to <PSAP NAME>; call delivered to <ABANDONMENT ROUTE> as expected with good two way audio.	
TC-35	Un-Abandonment Routing (Transfer Number)			Call routes to test PSAP when PSAP is un-abandoned.	PSAP is manually put into "Normalized" state in MP. Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected.	Call routes to <PSAP NAME> as expected. Good ANI/ALI, location data, and good two way audio.	
TC-36	Abandonment Routing PAD (Transfer Number)			PSAP is manually put into an abandoned state using the PSAP Abandonment Device (PAD), call routes to alternate PSAP.	PSAP is manually put into an abandoned state using the PSAP Abandonment Device (PAD). Test call sent to <PSAP NAME>, call routed to <ABANDONMENT ROUTE> as expected.	Call routes to <PSAP NAME>; call delivered to <ABANDONMENT ROUTE> as expected with good two way audio.	

TC-37	Un-Abandonment Routing PAD (Transfer Number)			PSAP is manually put into an un-abandoned state using the PSAP Abandonment Device (PAD), call routes to test PSAP.	PSAP is manually put into "Normalized" state using the PSAP Abandonment Device (PAD). Test call sent to <PSAP NAME>, call routes to <PSAP NAME> as expected.	Call routes to <PSAP NAME> as expected. Good ANI/ALI, location data, and good two way audio.	
TC-38	No position logged in (Transfer Number)			Call routes to alternate PSAP when no call takers are logged in. Note: If the live PSAPs positions share a queue with the test PSAP, we cannot logout the live positions. In this situation, the test case may be performed during cut.	Call taker logs out of all positions. Test call sent to <PSAP NAME>. System should return 486 or 600. Network should immediately attempt to route call to <BUSY ON INCOMING> destination.	Call routed to <BUSY ON INCOMING> as expected. Good two way audio.	
TC-39	Local Hold / Park (Transfer Number)			Call on hold is maintained.	Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected. Call Taker places the call on Local Hold / Park for 20 seconds. Call Taker is able to retrieve call after 20 seconds with <u>no anomalies</u> .	Call routed to <PSAP NAME> as expected with good two way audio. Call taker is able to retrieve call after it has been on Hold for 20 seconds.	
TC-40	System Hold / Park (Transfer Number)			Call on hold is maintained and can be retrieved by another call-taker.	Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected. Call Taker places the call on System Hold / Park for 20 seconds. Call Taker is able to retrieve call after 20 seconds with <u>no anomalies at a second position</u> .	Call routed to <PSAP NAME> as expected with good two way audio. Call taker is able to retrieve call after it has been on Hold for 20 seconds from a second position.	
TC-41	Subnet Verification			If call taker positions are located on multiple subnets, ingress a test call to each subnet. In order to run this test the PM/CPE Vendor/System Integrator must provide the subnet list to the ORT tester. One test position located on each subnet will be required to receive a test call.	Caller dials PSAP test number. Call answered on subnet1. Repeat until all subnets take a call and verify audio path.	Each subnet receives a test call with good 2-way audio.	
TC-42	Verification of call through Backup Unit (BU)			This test case is for a BU which has the same PSAP ID (same Instance). Note: if a BU has its own (different) PSAP ID, a separate full ORT on the BU is required.	Caller dials PSAP test number. Call is delivered to backup location.	On site tech needs to go to the location where the BU resides and login to the position to take a test call in order to verify good two-way audio and ANI/ALI.	
TC-43	CPE Failover			Verify CPE failover is working as expected (within-node or node-node). Note: This testcase is intended to be run only if the CPE is NEW and has NO existing live traffic on it.	See Sacramento Lab (Jay/Akhil) for details related to the Viper PSAP or see San Ramon (Audrey/Steve) for details related to the Solacom or Vesta PSAPs.	CPE failure and test call behaves as expected and rolls over to expected destination.	
TC-44	LAN/WAN Speed Verification (Pre-Router Failover) *			This test case is to verify the ESInet Router LAN interface matches the CPE router/Firewall WAN interface. Both should be set to auto negotiate, and the interfaces should report full duplex at 1000Mbps.	VNS and CPE vendor need to confirm that the speed is 1000 Mbps and Full Duplex.		

TC-45	Network Failover - Intrado Network Edge Router (Power Cycle - WAN - LAN) *			Perform power-down and validation on each Intrado network edge router at host/node site, Perform WAN and LAN interfaces shutdown and validation on each host/node site, and power-down ATT interface router testing. Please be sure there is no live traffic or live remote PSAPs. Otherwise this test cannot be performed. This test case is for new Host site. TC is n/a for i3 conversions. Note: Needs a person physically on site to hard power down/up the routers and for the physical disconnection of the WAN and LAN. Will need an onsite resource with knowledge of networking equipment to support this test case. Two persons are needed on site to run this test case if the equipment room (Routers) is separated from the room of CPEs, in order to verify two-way audio.	Intrado network engineer leads this effort. For power-down of Intrado Edge routers: •Place test call, with a call in progress, power down router A. •Observe router B become VRRP master for all applicable networks, identify any audio disruptions. •Validate failover of BGP to use routes from PSAP router B. •Login to router A; enable monitoring, verify routing neighborships and VRRP have restored to pre-event states. •Power down PSAP router B. •Observe PSAP router A become VRRP master for all applicable networks, identify any audio disruptions. •Validate failover of BGP to use routes from PSAP router A. •Login to router B; enable monitoring, verify routing neighborships and VRRP have restored to pre-event states. WAN Failover: •Place test call. •Perform automatic reload on router A. •Shut down (or unplug the cable) WAN interface, identify any audio disruptions. •Validate failover of BGP to use routes from router B.	1.)Ensure that there is very little loss of audio < 2 seconds. 2.)Ensure that the call remains connected, and is not dropped.	
TC-46	Network Failover - ATT Interface Router (WAN - LAN- Power Cycle) *			Perform power-down validation on each Intrado network edge router at host/node site, Perform WAN and LAN interfaces shutdown validation on each host/node site, and power-down ATT interface router testing. Note: A person will physically need to be on site to hard power down/up the routers and the physical disconnection of the WAN and LAN. An on-site person is needed with knowledge of networking equipment to support this test case. Two persons are needed on site to run this test case if the equipment room (Routers) is separated from the room of CPEs, in order to verify two-way audio. Equipment to support this test case.	An AT&T network engineer, e.g. MIKE MANION or BARNEY MANION will lead this effort. •Place test call. •Perform automatic reload on router A. •Shut down (unplug cable) WAN interface. •Identify any audio disruptions. •Validate failover of BGP to use routes from PSAP router B. •Restore connectivity on PSAP router A. •Perform automatic reload on router B. •Shut down (unplug cable) WAN interface. •Identify any audio disruptions. •Validate failover of BGP to use routes from PSAP router A. •Restore connectivity on PSAP router B.	1.)Ensure that there is very little loss of audio < 2 seconds. 2.)Ensure that the call remains connected, and is not dropped. If customer has agreed to go live with a single AVPN circuit at PSAP Primary location, we will perform this test once the 2nd AVPN circuit is installed in the field. Below are the procedures for live AVPN failover. For Viper PSAP: TO ESTABLISH A TEST CALL TO THE PSAP WE TEST, THE LIVE TRAFFIC TO THE PSAP sent to XXXX as backup unit (BU). The PSAP remains live; The PSAP Call takers will move to their backup location and log into their PSAP profiles with agent roaming to take live calls. The technician places a test call from the primary PSAP site, a normal call-taker can answer the call from the BU. At BU site (XXXX), place it on-hold, and then ATT tech at the primary site takes the call off-hold thus the test call now will be on the primary PSAP so we can do failover testing:	

TC-47	Network Failover - ATT Interface PSAP Router (LAN - Power Cycle) * Remote or Hosted Only			Perform power-down and LAN validation on each ATT interface router and LAN Interface. This is for remote site AVPN failover test (AKA PSAP router failover). Note: A person will physically need to be on site to hard power down/up the routers and for the physical disconnection of the WAN and LAN. Will need an onsite resource with knowledge of networking equipment to support this test case. Two persons are needed on site to run this test case if the equipment room (Routers) is separated from the room of CPEs, in order to verify two-way audio.	An AT&T network engineer, e.g. MIKE MANION or BARNEY MANION will lead this effort. •Place test call. •With a call in progress, unplug the interface on ATT Interface router A facing Intrado ESInet Edge router A. •Identify any audio disruptions. •Validate failover of BGP to use routes from Intrado ESInet Edge router B. •Restore connectivity between ATT Interface router A facing Intrado ESInet Edge router A. •Validate traffic restores to primary path after appropriate time. •Unplug interface on ATT Interface router A facing CPE Network equipment (could be router or switch). •Identify any audio disruptions. •Validate failover of BGP to use routes from Intrado ESInet Edge router A to ATT interface router A, then downstream using the Side link to AT&T Interface Router B. •Restore connectivity between AT&T Interface Router A and the CPE Network Equipment. •Validate traffic restores to primary path after appropriate time. •Power down AT&T Interface router A by either unplugging the power or shutting off the power	If customer has agreed to go live with a single AVPN circuit at PSAP Primary location, we will perform this test once the 2nd AVPN circuit is installed in the field. Below are the procedures for live AVPN failover. For Viper PSAP: TO ESTABLISH A TEST CALL TO THE PSAP WE TEST, THE LIVE TRAFFIC TO THE PSAP sent to XXXX as backup unit (BU). The PSAP remains live; The PSAP Call takers will move to their backup location and log into their PSAP profiles with agent roaming to take live calls. AT&T tech places a test call from the primary PSAP site, a normal call-taker can answer the call from the BU. At BU site (XXXX), place it on hold, and then ATT tech at the primary site takes the call off-hold thus the test call now will be on the primary PSAP so we can do failover testing: Proceed with the ATT router 1 and router 2 failure testing (not Intrado Edge routers): •Unplug the LAN cable of router 1 and router 2, respectively, to verify call is failover to	
TC-48	Network Failover Interface Router / Firewall (For a 3rd Party Managed PSAP) *			This test case is to be executed when the PSAP network equipment is 3rd party / customer owned or managed. It is best practice to perform failover testing of the network firewall / routers prior to placing live 911 traffic on the system. It is wholly the responsibility of the customer, and the vendor to validate that no live traffic is on the equipment to be failed over and to ensure that no live traffic would be impacted while executing this test. Perform power-down and LAN validation on each interface router / firewall and its LAN Interface. Note: A person will physically need to be on site to hard power down/up the routers and for the physical disconnection of the WAN and LAN. Will need an onsite resource with knowledge of networking equipment to support this test case. Two persons are needed on site to run this test case if the equipment room (Routers) is separated from the room of CPEs, in order to verify two-way	The 3rd party or PSAP network engineer will lead this effort. •Place test call. •With a call in progress, unplug LAN interface on the Interface router / Firewall A, facing Intrado ESInet Edge router A. •Identify any audio disruptions. •Validate failover of BGP to use routes from Intrado ESInet Edge router B. •Restore connectivity between the Interface router / firewall A facing Intrado ESInet Edge router A. •Validate traffic restores to primary path after appropriate time. •Unplug (LAN) interface on the interface router A facing CPE network equipment (could be router or switch). •Note any audio disruptions. •Validate failover of BGP to use routes from Intrado ESInet Edge router A to the interface router / firewall A, then downstream using the Side link to the Interface Router / firewall B. •Restore the (LAN) connectivity between the interface router / firewall A and the CPE network equipment. •Validate traffic restores to primary path after appropriate time.	If customer has agreed to go live with a single AVPN circuit at PSAP Primary location, we will perform this test once the 2nd AVPN circuit is installed in the field. Below are the procedures for live AVPN failover. Proceed with the router 1 and router 2 failure testing (not Intrado Edge routers): •Unplug the LAN cable of router 1 and router 2, respectively, to verify call is failover to router 2 and router 1 accordingly. •Power down router 1 and router 2, respectively, to verify call is failover to router 2 and router 1 accordingly. •Unplug both LAN cables of router 1 and router 2 to verify call is failover to BU. While doing so, make sure there is no active live call. •Power down both router 1 and router 2 to verify call is failover to BU. While doing so, make sure there is no active live call. Two technicians will need to be on site.	
NOTE	If text is included as part of this project, contact text team to run their test cases	Note	n/a	N/A	N/A	N/A	

FirstNet Wireless Backup test cases with a New PSAP

Prior to running tests on the FirstNet Wireless AVPN, the PSAP site must meet the minimum criteria listed below.

- 1.) A Site survey has been completed, and a permanently mounted external antenna or Cradle Point modem with internal self contained antenna's (preferred), phased to the applicable cell tower.
- 2.) The Cradle Point modem must be fully wired, configured, and the applicable 4FF SIM card is installed.
- 3.) A minimum signals strength must be 60% and above for the site to qualify for FirstNet Wireless Backup connectivity.

Note: The AT&T Onsite Tech has access and will perform the Speed Testing/Bandwidth Testing for FirstNet

Signal Strength(%)	db	RSSI	Bandwidth (Mbps)		Max Simul calls	Number of dropped calls	Duration Test (minutes)	Average MOS	Average Latency	Average Jitter
			Download	Upload						
100%	0	-53	87.7	26.9	14	0	10	4.33	60.9	19.94
60%	20	-74	74.3	6.3	14	0	10	4.34	66.79	21.25
50%	25	-79	61.2	1.9	14	0	10	3.97	357.99	482.85
46%	30	-83	42.4	0.6	4	calls dropped, re-presented				
40%	40	-85	20.2	0.3	0					

AVPN-01	AVPN to FirstNet Failover			Place a test call to that applicable PSAP under test. Verify that the audio is good and ANI/ALI has been received. Keep the call connected. If all is good, then disconnect the wired AVPN WAN port. At that point the call should move over to the Wireless FirstNet Circuit. verify if there is any interrupt of two-way audio, as the active call failover to the FirstNet wireless network. Intrado Network. If all is good then the call can be hung up. Intrado Networking is needed	Call may lose less than 5 Seconds audio. Ensure the call is not dropped.
AVPN-02	Verify Call over FirstNet			Place a New landline phone that has x/y coordinate provisioned. Verify the two-way audio is good. The rebid ALI. Intrado Networking needed	Verify the two-way audio is good. Verify ANI/ALI and x/y coordinate display on the CPE GUI screen is correctly. Intrado will verify all the LIS/ADR/ECRF-LoST messages from Axway logs, Verify CDR and the call is being delivered as a handoff
AVPN-03	Fail Back To AVPN from FirstNet			Plug the WAN cable back to the router. Intrado Networking needed	Network engineer to verify that the active call is back to primary AVPN network (not at wireless network.
WNF-01	Wireless Net Failover to backup PSAP			Fail the WAN and LAN respectively, and verify that there is less than 5 second of audio loss when failing over to the backup PSAP.	Verify the active call failover to the Backup site is successful, and ensure that the is very little loss of audio.
WNF-02	Additional calls can be established to the backup PSAP			Place 3 additional calls, which should be delivered to the backup PSAP	Ensure that the backup PSAP is reached, and 2 way audio is observed.

FirstNet Functional test cases

FN-01	Wireline Call Routed to PSAP through ESInet via FirstNet			Test call sent to each listed PSAP. Caller confirms routing and audio quality.	Verify that the call is delivered to the correct PSAP. Verify CMP CDR to ensure the call is ingressed via FirstNet Wireless backup
FN-02	Subscriber/ALI Verification			Place a call to the ESInet applicable PSAP manually make a call with a landline phone with x/y geo-coded to a test i3 PSAP. Once the call is up, then do a manual bid/update. Verify in the CDR that PIDF-LO has been passed for i3 calls.	Test call generated from AT&T to <PSAP NAME>; good ANI, location (civic address, and geo-location coordinate's longitude and latitude if provisioned in GIS), dispatch dynamic agent (fire dept., police dept., and med emergence if applicable), and subscriber information, & Voice delivered.
FN-03	Maximum Simultaneous Calls			Place multiple calls over the Firstnet AVPN. The maximum simultaneous calls allowed are less than or equal to 14.	Verify that all calls remain connected and voice quality is good.
FN-04	Normalized Call			Call routes to primary PSAP when PSAP is un-abandoned.	PSAP is manually put into an un-abandoned state. Test call sent to <PSAP NAME>, call routed to <PSAP NAME> as expected.



Appendix E - AT&T 9-1-1 EGDMS User Guide



9-1-1 EGDMS
User Guide
Software Release 2020.3

Contents

About This Guide	3
New in This Release	3
Document Conventions	4
Problem Reporting	4
Introduction	5
Quick Tips for 9-1-1 EGDMS	5
Connecting to 9-1-1 EGDMS	6
Data Upload	10
Overview	10
Optional EGDMS Uploads	10
Prepare GIS Data for Upload	10
9-1-1 EGDMS Zip File Structure	11
Data Upload	13
Optional ALI to GIS Comparisons	18
ALI/GIS Comparison Report with ESN	18
ALI/GIS Comparison Report without ESN	19
Data Management	20
Overview	20
Upload History	20
Configuration	33
Agency Details	33
Reports	35
Overview	35
Accessing and Viewing Reports	35
QA/QC Validations	37
Schema Tables	40
Overview	40
Authoritative/Provisioning Boundary	41
Street Centerlines	41
Address Points	43
PSAP Layers/Fire/Law/EMS	45
Municipal Boundary	46
Glossary	47

1.0 About This Guide

This user guide describes 9-1-1 Enterprise Geospatial Database Management System (9-1-1 EGDMS) version 2020.3.

1.1 New in This Release

- 9-1-1 EGDMS processing speeds have been increased for the delta detection processing steps.
- A new upload state has been added for failed processing of an upload. 9-1-1 EGDMS now sends an email if an upload's processing fails for any reason, and the *9-1-1 EGDMS Upload History* indicates that the QAQC processing failed.
- The *9-1-1 EGDMS Agency Details* screen now supports multiple email addresses (comma separated) in the 9-1-1 EGDMS Data Management Application.
- Error exception handling has been updated. Features that are marked as error exceptions are no longer exported to the error shapefile or included in the validation report error summary tables.
- For the transitional data management service (TDMS) workflow paths, the 9-1-1 EGDMS Validation Summary Report now includes the geoMSAG record change count.
- The `LOC_NOTES` field has been added to the list of fields used in the stacked and attribute duplicate detection validations for Address Points.
- A new spatial validation was added that identifies road segments that cross PSAP boundaries (Note: this is a non-critical error).

1.1.1 Continued Efforts Correcting Known Issues

In addition to the feature enhancements or feature-related CRs, the following enhancements or defects were addressed with version 2020.3:

- EGDMS schema change detection will no longer find an attribute mapping error in an unloaded layer.
- Corrected an EGDMS Upload Summary feature count reporting issue. When a feature has both shape and attribute deltas, it will no longer be counted as 2 separate changed features.

1.2 Document Conventions

Convention	Description
System-generated messages	System-generated messages, terms, and field names display in the Courier Std font.
User Entry	Information that must be typed exactly as it appears displays in the Courier Std bold font.
Buttons, screen tabs, and screen panels	Buttons, tabs across the top of the screen that are used to access additional screens, and names of screen panels are identified by bold text.
<i>Windows and Screen Names</i>	Windows and screen names are identified by italics.
<u>Web Links</u>	All web-based hyperlinks are identified by bold blue underlined text.
<u>Internal cross references</u>	Cross references made to other sections in the same guide are identified by blue font. Note that these cross references link to the section.

1.3 Problem Reporting

Report problems to AT&T at 1.844.378.0911 Option 1. Recurring issues should be reported immediately.

Before reporting a problem, gather as much of the following information as possible:

- 1 What data was entered into the system immediately before the problem occurred?
- 2 What did the system do?
- 3 What was the system expected to do?
- 4 What messages did the system display?
- 5 Are there written or printed examples of what occurred?
- 6 Can the problem be verified by duplicating it on demand?
- 7 What type of system/modem do you use?
- 8 Did you consult your user guide on proper operations?

2.0 Introduction

The 9-1-1 Enterprise Geospatial Database Management System (9-1-1 EGDMS) is a web application that serves as the front-end user interface for the NENA Spatial Interface (SI) requirement. GIS data submitted through 9-1-1 EGDMS is validated, coalesced, and used for provisioning to i3 systems (ECRF and LVF).

9-1-1 EGDMS includes the following features:

- Secure 2-factor authentication.
- A file-upload user interface that enables customers to identify the contents of the upload.
- Acceptance of file geodatabase files and shapefiles.
- Attribute field mapping configuration that is customer-driven.
- Automated schema change detection and error notification.
- Automated email notification for upload and processing status.
- GIS data validation report retrieval.

2.1 Quick Tips for 9-1-1 EGDMS

2.1.1 Attribute Field Mapping Guidelines

During the transitional period from legacy ALI/MSAG to NG9-1-1, it is recommended that the legacy street name fields (Legacy Prefix Directional, Legacy Street Name, Legacy Street Suffix, and Legacy Post Directional) be field mapped to four of the eight corresponding i3 street name fields within 9-1-1 EGDMS for provisioning the ECRF/LVF. This will also correlate to the MSAG/ALI fields used for subscriber location validation. The recommended field mapping is seen in [figure 1](#).

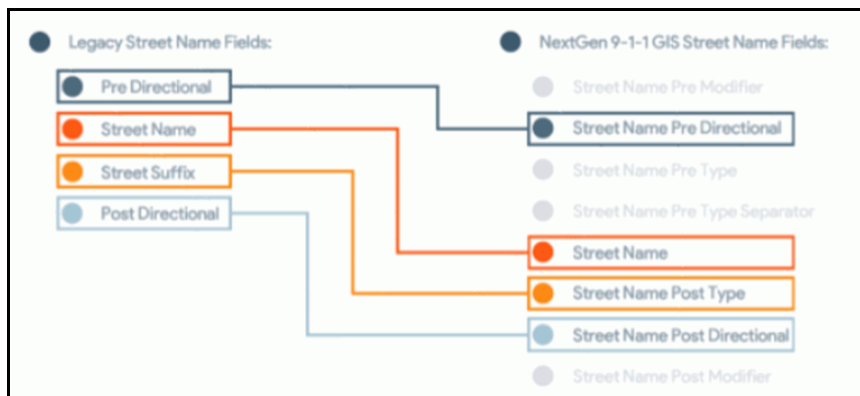


Figure 1: Recommended Field Mapping

NOTE	In the future, new specifications and standards will likely provide for consistent mechanisms to overcome these transitional issues and the fields will be used as intended.

Additionally, in this transitional period to support ALI matching to civic addresses in the GIS data, the MSAG Community from the source data set should be field mapped to the Incorporated Municipality (A3) field in the ESInet GIS data model.

2.1.2 Geometry Best Practices

- Run topology before uploading polygon boundary layers to ensure there are no gaps and overlaps in your boundaries and all features fall within your provisioning boundary.
- Ensure that there are no gaps and overlaps with neighboring agencies.
- Intrado's geometry validator uses OGC standards (not ESRI) to check for errors.
- Check for too many vertices (stroked curves, traced features, etc.).
- Check for self-intersecting geometry.
- Ensure boundary features are polygons and not polylines.

2.1.3 Field Type and Length Guidelines

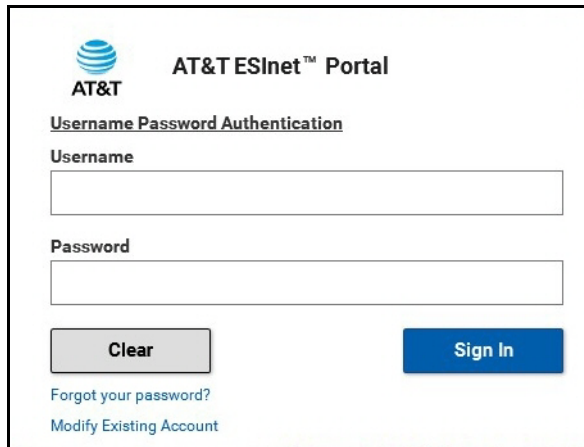
- Field type and length matters only if the data is in error. For example, an address number field can be a string but can only contain whole numbers. If an alpha character is placed in that field it will be an error.

2.1.4 Recommended Reference Documents

- NENA Standard for NG9-1-1 GIS Data Model
- NENA Standards for the Provisioning and Maintenance of GIS data to ECRF/LVF

2.2 Connecting to 9-1-1 EGDMS

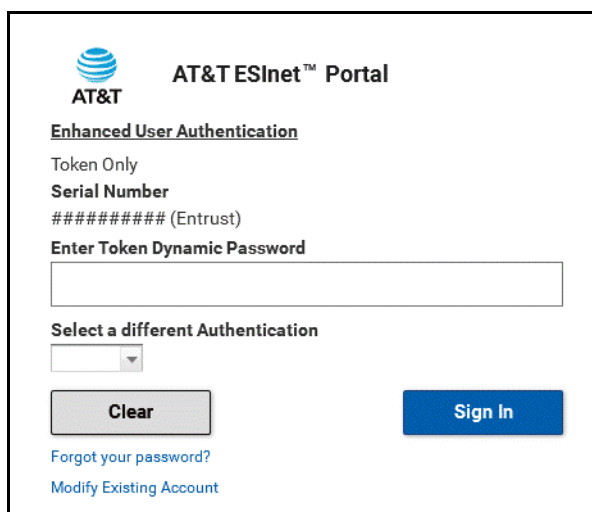
- 1 Open your browser and enter the AT&T ESInet™ Portal URL in the browser's address field: <https://portal.esinet-911.att.com>. The *AT&T ESInet Portal Login* screen displays.



The screenshot shows the AT&T ESInet Portal login interface. At the top left is the AT&T logo. To its right is the text "AT&T ESInet™ Portal". Below this is the heading "Username Password Authentication". There are two input fields: "Username" and "Password". Below the "Password" field are two buttons: a grey "Clear" button and a blue "Sign In" button. At the bottom left, there are two links: "Forgot your password?" and "Modify Existing Account".

Figure 2: ESInet Portal Login Screen

- 2 Enter your username in the `Username` field and your password in the `Password` field.
- 3 Click the **Sign In** button. The *Enhanced User Authentication* screen displays. This screen is used for dual-factor authentication and requires a token-generated, one-time use password.



The screenshot shows the AT&T ESInet Portal Enhanced User Authentication screen. At the top left is the AT&T logo. To its right is the text "AT&T ESInet™ Portal". Below this is the heading "Enhanced User Authentication". There is a "Token Only" section with a "Serial Number" field containing "##### (Entrust)". Below this is a section titled "Enter Token Dynamic Password" with an input field. Below that is a section titled "Select a different Authentication" with a dropdown menu. At the bottom left are two buttons: a grey "Clear" button and a blue "Sign In" button. At the bottom left, there are two links: "Forgot your password?" and "Modify Existing Account".

Figure 3: Enhanced User Authentication Screen

- 4 Press and hold the button on your Entrust token ([figure 4](#)) until the eight number sequence displays. Only press the button once. If you press the button without logging into the application, the token may become out of sync with the server.



Figure 4: Entrust Token

- 5 Enter the number sequence in the Enter Token Dynamic Password field.

NOTE Although the screen displays a Select a different Authentication option, the use of the dynamic token password is the only option currently supported.

- 6 Click the **Sign In** button. The *AT&T ESInet Home* screen displays.

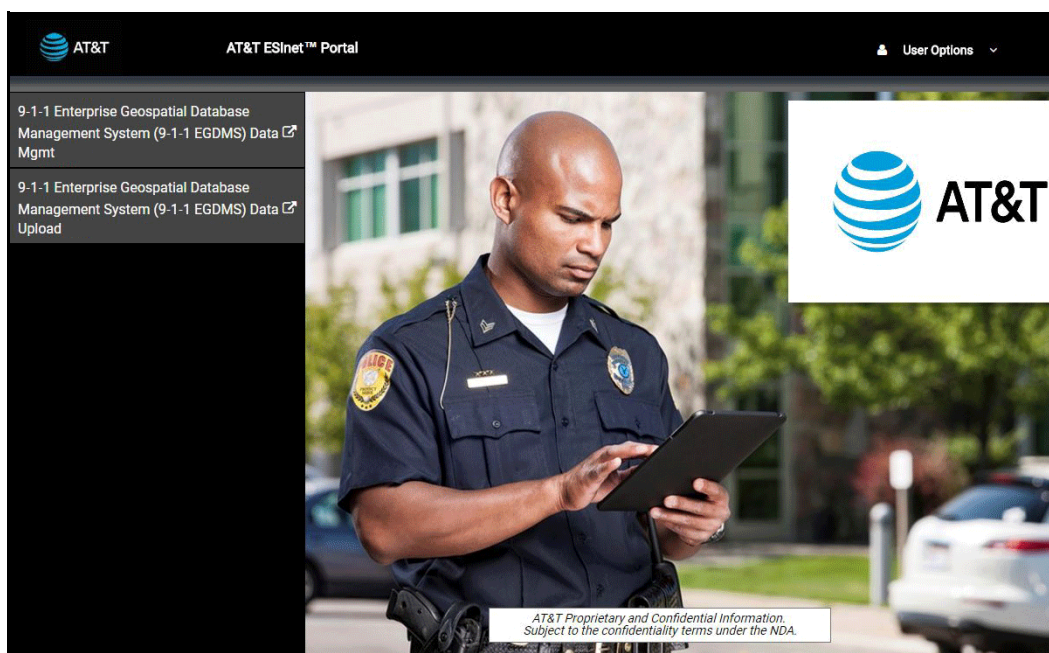


Figure 5: ESInet Portal Home Page

- 7 Click on the [9-1-1 Enterprise Geospatial Database Management System \(9-1-1 EGDMS\) Data Mgmt](#) link to launch the Data Management application or the [9-1-1 Enterprise Geospatial Database Management System \(9-1-1 EGDMS\) Data Upload](#) link to launch the Data Upload application.

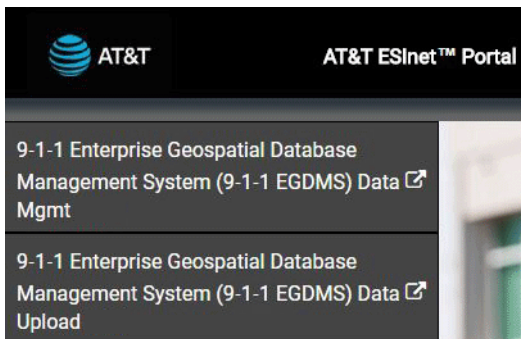


Figure 6: 9-1-1 EGDMS Data Management and Data Upload links

The 9-1-1 EGDMS Data Upload application is used to upload files containing GIS data. The 9-1-1 EGDMS Data Management application is used to configure the field mapping attributes in your database to match those in the 9-1-1 EGDMS database, as well as to review your agency's existing configuration and agency contact details.

3.0 Data Upload

3.1 Overview

The 9-1-1 EGDMS Data Upload application is used to upload files containing GIS data. This chapter describes how to prepare your file for upload and how to use the Data Upload application.

3.2 Optional EGDMS Uploads

As an option, 9-1-1 EGDMS provides the ability to submit GIS data via MapSAG Data Exchange or python script to Intrado's sSFTP application (MoveIt) for automated processing after the initial field mapping configurations have been performed in the 9-1-1 EGDMS portal. This functionality requires customer specific configuration. Contact AT&T/Intrado for more details. Charges may apply.

3.3 Prepare GIS Data for Upload

Before uploading your GIS data to the AT&T 9-1-1 EGDMS, it must be in the correct format. Accepted formats include:

- File geodatabase
- Shape file

The feature classes supported include:

- Provisioning Boundary - Provisioning Boundary polygon that covers the geographic region for which your agency has jurisdiction.
- Street Centerlines - Street centerline data for your agency's jurisdiction.
- Address/Structure Location - Address/structure points for your agency's jurisdiction.
- PSAP Area Boundary - Public Safety Answering Point boundary polygons for your agency's jurisdiction.
- PSAP1 - Pre-provisioned alternate routing PSAP polygon boundaries (1 of 3). (Not required.)
- PSAP2 - Pre-provisioned alternate routing PSAP polygon boundaries (2 of 3). (Not required.)
- PSAP3 - Pre-provisioned alternate routing PSAP polygon boundaries (3 of 3). (Not required.)
- Fire Response Boundary - Fire response boundary polygons for your agency's jurisdiction.
- Law Response Boundary - Law response boundary polygons for your agency's jurisdiction.
- EMS Response Boundary - EMS/medical response boundary polygons for your agency's jurisdiction.

- Municipal Boundary - Municipal boundary polygon(s) for your agency's jurisdiction. (Not required.)
- Emergency Service Zone - Service response boundary (ESN boundary) polygons that include Fire, Law, and EMS response agencies in your jurisdiction. (Not required.)

Files must be zipped and the recommended file name format is:

[Your agency name]GIS[today's date]

For example:

SmithCountyGIS_6212018.zip

3.4 9-1-1 EGDMS Zip File Structure

3.4.1 Zip a File Geodatabase

- 1 Right click the .gdb file.
- 2 From the menu, select **Send to**. An additional menu displays.
- 3 Select **Compressed (zipped) folder**. The zipped file displays with the same name under the zipped icon.



Figure 7: Zipped Icon

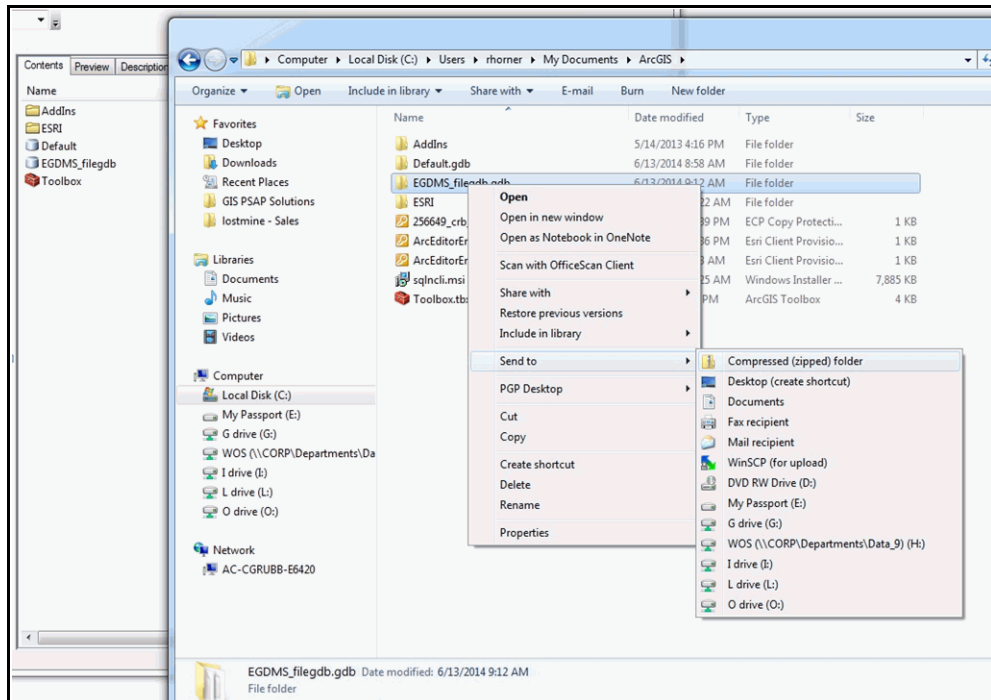


Figure 8: Zip File Geodatabase

3.4.2 Zip a Shape File

Shape files must be placed in a folder and then be zipped. The correct file structure is:

shapeGIS.zip

ShapeFileFolder

shapeFiles.shp

shapeFiles.shx

shapeFiles.sbx

shapeFiles.prj

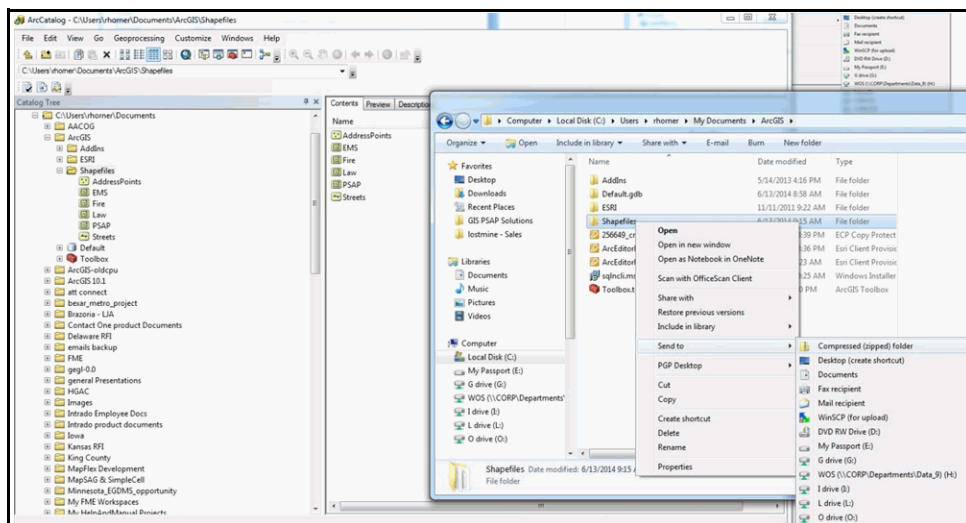


Figure 9: Zip Shape File

3.5 Data Upload

To upload a GIS database file, complete the following steps:

- 1 Log into ESInet and access the *9-1-1 EGDMS Data Upload Application* screen as described in [“Connecting to 9-1-1 EGDMS” on page 6](#). The *Select Agency* screen displays if you are assigned to multiple agencies.
- 2 If you are assigned to multiple agencies, select an agency from the drop-down menu. The *9-1-1 EGDMS Data Upload* screen displays ([figure 10 on page 14](#)).

9-1-1 EGDMS Data Upload Application

Agency:

Update GIS Data
Please submit your Agency's GIS data update using the form below. Complete the Manifest and select your Payload file to transmit your Update.

Configuration Changes
Check the box below if you have made changes to your GIS data feature classes or attributes that are not captured in your current field mapping configuration.
☐ Configuration Changes

Updated Feature Classes and Supporting Data
Please check each feature set included in this update.
☐ Check all

☐ Street Centerlines	☐ Fire Response Boundary
☐ Address/Structure Location	☐ Law Response Boundary
☐ PSAP Area Boundary	☐ EMS Response Boundary
☐ Emergency Service Zone	☐ Municipal Boundary
☐ PSAP1 Area Boundary	☐ PSAP2 Area Boundary
☐ PSAP3 Area Boundary	☐ Authoritative Boundary

GIS Data Format: File Geodatabase
Please select a GIS file to upload. Note: All GIS data must be submitted in a single, compressed (.zip, .Gzip, or .tz) format. Max size: 2GB.

* GIS Data No file chosen

Figure 10: 9-1-1 EGDMS Data Upload

- If you have made changes to your GIS data feature classes or attributes that are not captured in the current field mapping configuration, check the Configuration Changes box.

NOTE This field only appears on subsequent uploads. Initial uploads do not have this option.

- Indicate the contents of your GIS upload by selecting the feature classes that you would like to have processed by the system.

NOTE Hovering over a field displays the field description. See [figure 11](#).

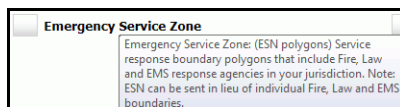


Figure 11: Field Description Pop-up

Once you have finished selecting the appropriate checkboxes, click the **Browse** button to locate the file to upload on your local computer (figure 12). The *Choose File to Upload* dialog box displays (figure 13).

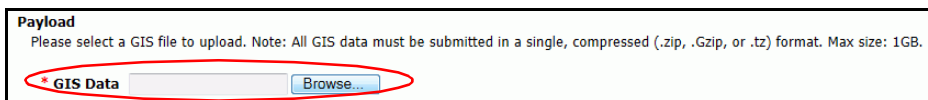


Figure 12: Upload File

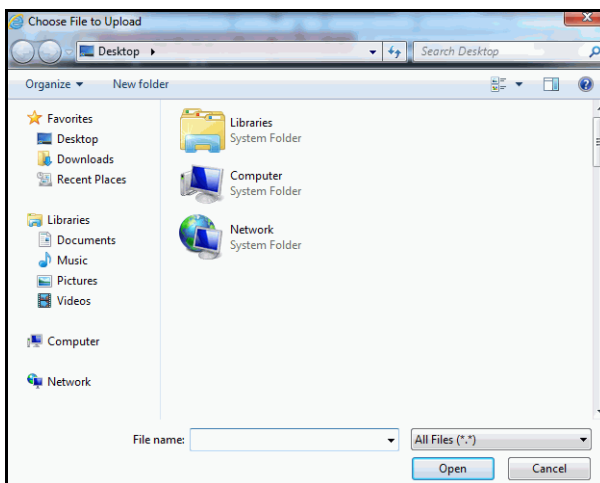


Figure 13: Choose File to Upload Dialog Box

- 5 Select the file from your computer and click the **Open** button on the dialog box. The dialog box closes and the file name appears in the **GIS Data** text box on the *EGDMS Data Upload* screen (figure 14).

IMPORTANT | Uploaded files must be zipped.

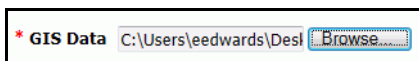


Figure 14: GIS Data Text Box

- 6 Click the **Transmit** button. A message displays indicating that the file is uploading (figure 15).

Agency TX - Wilson County Sheriffs Office

Update GIS Data
Please submit your Agency's GIS data update using the form below. Complete the Manifest and select your Payload file to transmit your Update.

Configuration Changes
Check the box below if you have made any configuration changes.
☐ Configuration Changes

Supplemental Reports
Check the appropriate boxes below to generate supplemental reports.
☐ MSAG/GIS Comparison Report

Updated Feature Classes and Supporting Data
Please check each feature set included in this update.

☐ Check all	☐ Fire Response Boundary
☐ Street Centerlines	☐ Law Response Boundary
☒ Address/Structure Location	☐ EMS Response Boundary
☒ PSAP Area Boundary	☐ Municipal Boundary
☐ Emergency Service Zone	☐ Authoritative Boundary

Payload
Click "Choose File/Browse" again if you want to **replace** the selected file with a different file.

* GIS Data C:\Users\eedwards\Desktop\Browse...

File Transmission in Progress.

Closing this window will cancel your upload.

Once processed, your data submission will be available in the Data History table in the Data Management Application. You will be notified via email if configuration and field mapping changes are required.

Figure 15: Upload in Progress Message

AT&T 9-1-1 EGDMS Data Upload Application

Agency Training_County

Update GIS Data
Please submit your Agency's GIS data update using the form below. Complete the Manifest and select your Payload file to transmit your Update.

Configuration Changes
Check the box below if you have made changes to your GIS data feature classes or attributes that are not captured in your current field mapping configuration.
☐ Configuration Changes

Updated Feature Classes and Supporting Data
Please check each feature set included in this update.
☐ Check all
☐ Street Centerlines
☐ Address/Structure Location
☐ PSAP Area Boundary
☐ Emergency Service Zone
☐ Fire Response Boundary
☐ Law Response Boundary

Click Process to complete the data transmission
Process File

GIS Data Format: File Geodatabase
Please select a GIS file to upload. Note: All GIS data must be submitted in a single, compressed (.zip, .Gzip, or .tz) format. Max size: 2GB.

* GIS Data Browse...

Cancel Transmit

AT&T Proprietary and Confidential Information
Subject to the confidentiality terms under the NDA.

Figure 16: File Upload Complete

- 7 Once the file has completed uploading, click the **Process File** button to continue.
- 8 When the upload has completed, a confirmation message displays.

GIS Data Format: File Geodatabase
Please select a GIS file to upload. Note: All GIS data must be submitted in a single, compressed (.zip, .Gzip, or .tz) format. Max size: 2GB.

* GIS Data Browse...

Cancel Transmit

The data transmission was successful. You'll be notified by email when your upload is available in the Data Management Application.

AT&T Proprietary and Confidential Information
Subject to the confidentiality terms under the NDA.

Figure 17: Upload Success Confirmation

- 9 Exit the Data Upload application by clicking the red "X" in the upper right corner of the browser window.



Figure 18: Close Browser Window

- 10 When the upload has finished processing, you will receive an email with further instructions.

Optional ALI to GIS Comparisons

NOTE Setup and configuration of these tools is required. Requests to use these optional services should be directed to AT&T/Intrado.

The ALI to GIS Comparison Report section of the Data Upload application is displayed only when the ALI Compare has been enabled for your Agency, otherwise you will not see the options. Once Street Centerlines or Address/Structure Location feature classes are selected, the ALI Compare options are enabled, if the agency has been configured for this service.

ALI/GIS Comparison Report with ESN

 A screenshot of a web application form titled 'Update GIS Data'. The form is for the 'Angelina' agency. It includes sections for 'Configuration Changes', 'Updated Feature Classes and Supporting Data', and 'ALI/GIS Comparison Report'. In the 'Updated Feature Classes' section, 'Street Centerlines' and 'Address/Structure Location' are checked. In the 'ALI/GIS Comparison Report' section, 'ALI/GIS Comparison Report with ESN' is selected and highlighted with a red box. The form also has a 'GIS Data' upload field and 'Cancel' and 'Transmit' buttons at the bottom.

Agency: Angelina

Update GIS Data
Please submit your Agency's GIS data update using the form below. Complete the Manifest and select your Payload file to transmit your Update.

Configuration Changes
Check the box below if you have made changes to your GIS data feature classes or attributes that are not captured in your current field mapping configuration.
☐ Configuration Changes

Updated Feature Classes and Supporting Data
Please check each feature set included in this update.
☐ Check all

☒ Street Centerlines	☐ Fire Response Boundary
☒ Address/Structure Location	☐ Law Response Boundary
☐ PSAP Area Boundary	☐ EMS Response Boundary
☐ Emergency Service Zone	☐ Municipal Boundary
☐ PSAP1 Area Boundary	☐ PSAP2 Area Boundary
☐ PSAP3 Area Boundary	☐ Authoritative Boundary

ALI/GIS Comparison Report
Check one of the following options to create an ALI Comparison report. The upload must include Street Centerlines or Address Points.

☐ ALI/GIS Comparison Report without ESN

☒ ALI/GIS Comparison Report with ESN

GIS Data Format: File Geodatabase
Please select a GIS file to upload. Note: All GIS data must be submitted in a single, compressed (.zip, .Gzip, or .tz) format. Max size: 2GB.

* GIS Data Browse...

Cancel Transmit

Figure 19: Run an ALI/GIS Comparison Report

If this option is selected, 9-1-1 EGDMS pulls the associated ALI records for comparison to the GIS road centerline and address points, and ESN is considered in the comparison criteria. The ALI error/fallout report is performed and packaged with the 9-1-1 EGDMS reports.

NOTE	If the ALI/GIS comparison option is checked, the comparison is performed on the address points and/or the road centerlines if they are checked and included in the GIS data upload only.

ALI/GIS Comparison Report without ESN

If this option is selected, 9-1-1 EGDMS pulls the associated ALI records for comparison to the GIS road centerline and address points, and ESN is not considered in the comparison criteria. The ALI error/fallout report is performed and packaged with the 9-1-1 EGDMS reports.

4.0 Data Management

4.1 Overview

The 9-1-1 EGDMS Data Management application is used to configure the field mapping attributes in your database to match those in the AT&T ESInet database, as well as to review your agency's current configuration details and to review and update your agency contact information. Using the primary navigation tabs at the top of the *9-1-1 EGDMS Data Management* screen, you can access the different areas of the application.



Figure 20: 9-1-1 EGDMS Data Management Navigation Tabs

The **Upload History** tab displays the *Upload History* screen (figure 22 on page 21). From this screen, you can access your data upload details via the *Upload Details* screen (figure 23 on page 22). From the *Upload Details* screen, you can launch the *Field Mapping Tool* screen to configure your field mapping attributes.

The **Configuration** tab displays the *Configuration* screens (figure 42 on page 33). These screens display your agency's current attribute field mapping configuration.

The **Agency Details** tab displays the *Agency Details* screen (figure 43 on page 34). From this screen you can review your agency's contact information and update the name, email, telephone number, and telephone number extension of your agency contact person.

4.2 Upload History

After uploading your GIS data file (as described in "Data Upload" on page 10), the file is processed and you are notified via email that further action is required.

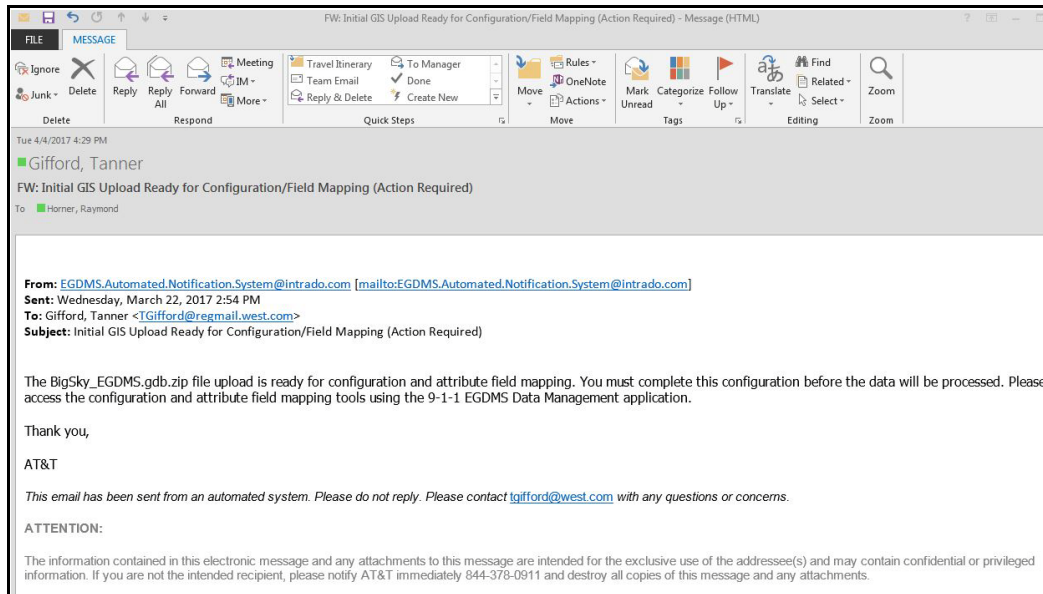


Figure 21: Sample Email Notification

- 1 After receiving the notification, log into the 9-1-1 EGDMS application by following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6](#).
- 2 Select the [9-1-1 EGDMS](#) link. The *Select Agency* screen displays if you are assigned to multiple agencies.
- 3 Choose an agency from the drop-down menu. The *Upload History* screen for the selected agency displays. This screen displays both current and historical uploads. The *Current State* field identifies which file requires action and specifies the type of action required.

Last Refresh: 15:22:52 MST Refresh						
	Start Date	Current State	GIS File Name	Upload ID	Last State Update	Reports
View	02/21/2017 15:41 MST	QA/QC Completed	RCL_AP_StreetErr.....zip	20170221T224118.bx-egdms20	02/21/2017 15:41 MST	Download
View	02/21/2017 13:52 MST	QA/QC Completed	RCL_AP_StreetErr.....zip	20170221T205232.bx-egdms20	02/21/2017 13:55 MST	Download
View	02/17/2017 14:25 MST	QA/QC Completed	RCL_AP_Clean.gdb.zip	20170217T212524.bx-egdms20	02/17/2017 14:25 MST	Download

Figure 22: Upload History

4.2.1 Configure Field Mapping Attributes

To configure field mapping attributes using the *Field Mapping Tool* screen, complete the following steps:

- 1 From the *Upload History* screen (figure 22), select the **View/Edit** button. The *Upload Details* screen for that file displays (figure 23 on page 22). Hovering over the "i" information icon displays a description of the action required (figure 24 on page 23). The *Upload Details* screen is comprised of four areas. The top section displays details of the upload, including its current state (action required, completed, etc.), the system-generated upload ID, the date of the most recent state change, and the date the file was originally uploaded. The second section identifies the configuration data included in the upload. The third section identifies the name of the GIS file and the fourth section is the activity log. The activity log captures the date, time, and a description of all state changes associated with the file.

9-1-1 EGDMS - Data Management | **Upload History** | Configuration | Agency Details

Agency: Training_County

Upload Details
Review the Update and make changes to address any corrections or errors as necessary.

State: QA/QC Completed

Upload ID: 20170404T212231.EGDMS_Trai...

Last State Update: 04/04/2017 14:23 MST

Start Date: 04/04/2017 14:22 MST

Configuration Changes
Click Launch to open the Field Mapping Tool to review this upload's attribute field map and propose changes to the configuration.

Field Mapping Tool

Updated Feature Classes
The Feature Classes included in this upload are indicated below.

☒ Street Centerlines	☐ Fire Response Boundary
☒ Address/Structure Location	☐ Law Response Boundary
☐ PSAP Area Boundary	☐ EMS Response Boundary
☐ Emergency Service Zone	☐ Municipal Boundary
	☒ Authoritative Boundary

Payload
The file(s) included in this upload are shown below.

GIS Data: BigSky_EGDMS.gdb.zip

Activity Log
Review the activity for this Upload.

User Name	Date	State
EGDMS_Training	04/04/2017 14:23:53 MST	9-1-1 EGDMS - QA/QC Processing
EGDMS_Training	04/04/2017 14:22:35 MST	9-1-1 EGDMS - Payload Review
EGDMS_Training	04/04/2017 14:22:31 MST	Upload Transmitting

Figure 23: Upload Details

Upload Details
Review the Update and make changes to address any corrections or errors as necessary.

State: Action Required - Update Attribute Field Mapping 

Last State Update: 05/29/2013 11:25 MST

Upload ID: 20130529T18

Configuration Changes

This upload is ready for configuration and attribute field mapping. Complete this using the configuration and field mapping tools below, and click Submit once all updates have been completed.

Figure 24: Action Required Description

IMPORTANT Checking or unchecking any of the feature classes listed in the **Uploaded Feature Classes** list and then selecting the **Save** button makes the feature class available or unavailable on the *Field Mapping Tool* screen, depending on your selection.

Table 1: Upload Details Button Descriptions

Button	Description
Cancel/Delete Upload	Cancels or deletes the upload.
Save/Close	Saves changes to the feature class configurations but does not submit the changes.
Submit	Submits the changes.

NOTE Uploads can only be canceled prior to QA/QC processing beginning.

- Open the *Field Mapping Tool* screen by clicking the **Launch** button. The *Field Mapping Tool* screen displays (figure 25 on page 24). This screen shows the first feature class selected. In the sample screen, *Street Centerlines* is the first feature class to display. The feature class list that displays on the upper left corner of the screen (figure 26 on page 25) identifies which one you are currently working in.

Field Mapping Tool

EGDMS Feature Class List

Select a feature class to view.
Street Centerlines
Address/Structure Location
Emergency Service Zone
Fire Response Boundary
Law Response Boundary
EMS Response Boundary
PSAP Area Boundary
Municipal Boundary
Authoritative Boundary

Feature Class Legend

Black = Available
Red *Italics* = Errors Present
Grey = Excluded from Upload
Underline = Warnings Present
Bold = Current Selection

EGDMS Feature Class

Street Centerlines
Feature Count: 0

Agency Feature Class

Select Agency Equivalent
Projection: NAD_1983_StatePlane_Texas_Cent...

State

Available for Mapping
Create Note

Select an Agency Attribute to map to the listed EGDMS Attributes.

EGDMS Attribute	Agency Attribute	Type	Length	State/Status
*Left from Address				
*Left to Address				
*Right from Address				
*Right to Address				
Parity Left				
Parity Right				
Street Pre-Modifier				
*Street Prefix Directional				
*Street Name Pre-Type				
*Street Name				
*Street Suffix Type				
*Street Post Directional				
Street Post-Modifier				
*Street Full Name				
Street Name Alias				
One Way				
Speed Limit				
Road Class				
ESN Left				
ESN Right				
Municipality Left				
Municipality Right				
County Name Left				
County Name Right				
State Left				
State Right				
*MSAG Comm. Name Left				
*MSAG Comm. Name Right				
Postal Community Name Left				
Postal Community Name Right				
ZIP Code Left				
ZIP Code Right				
*Source				
Effectivity Date				
Date Last Modified				
Data Provider				
*OBJECTID				
*SHAPE				
SHAPE_LENGTH				

ResetUndoSaveClose

Figure 25: Street Centerlines Field Mapping

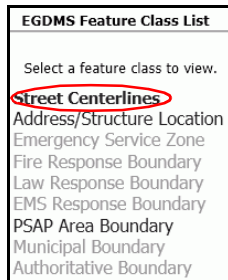


Figure 26: Feature Class List

Table 2: Field Mapping Tool Button Descriptions

Button	Description
Reset	Discards all changes made during the session and returns settings to the last known configuration.
Undo	Discards all changes made since the last save, including changes made to other feature classes.
Save	Saves changes, including those made to other feature classes.
Close	Closes the <i>Field Mapping Tool</i> screen.

- 3 Select a layer name from the *Agency Feature Class* drop-down menu (figure 27). The *Agency Attribute* column populates with drop-down menus for each field mapping attribute (figure 28 on page 26).

NOTE The *Agency Feature Class* drop-down menu filters your GIS data by feature type (point, line, or polygon).

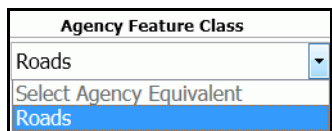


Figure 27: Agency Feature Class

Field Mapping Tool

EGDMS Feature Class List

Select a feature class to view.

- Street Centerlines
- Address/Structure Location
- Emergency Service Zone
- Fire Response Boundary
- Law Response Boundary
- EMS Response Boundary
- PSAP Area Boundary
- Municipal Boundary
- Authoritative Boundary

Feature Class Legend

Black = Available
Red Italics = Errors Present
Grey = Excluded from Upload
Underline = Warnings Present
Bold = Current Selection

EGDMS Feature Class

Street Centerlines

Feature Count: 3397

Select an Agency Attribute to map to the listed EGDMS Attributes.

EGDMS Attribute	Agency Attribute	Type	Length	State/Status
*Left from Address				
*Left to Address				
*Right from Address				
*Right to Address				
Parity Left				
Parity Right				
Street Pre-Modifier				
*Street Prefix Directional				
*Street Name Pre-Type				
*Street Name				
*Street Suffix Type				
*Street Post Directional				
Street Post-Modifier				
*Street Full Name				
Street Name Alias				
One Way				
Speed Limit				
Road Class				
ESN Left				
ESN Right				
Municipality Left				
Municipality Right				
County Name Left				
County Name Right				
State Left				
State Right				
*MSAG Comm. Name Left				
*MSAG Comm. Name Right				
Postal Community Name Left				
Postal Community Name Right				
ZIP Code Left				
ZIP Code Right				
*Source				
Effectivity Date				
Date Last Modified				
Data Provider				
*OBJECTID				
*SHAPE				
SHAPE_LENGTH				

Agency Feature Class

Roads

Projection: NAD_1983_StatePlane_Texas_Cent...

State

Available for Mapping

Create Note

Reset Undo Save Close

Figure 28: Street Centerlines Field Mapping - Agency Feature Class Selected

- 4 Select values from the drop-down menu to match your GIS data attributes to the 9-1-1 EGDMS attribute fields. Fields marked with a red asterisk are required.

NOTE If the field type does not match, a warning message displays. You can still submit with a warning, but it must be reviewed before it is accepted.

EGDMS Attribute	Agency Attribute	Type	Length	State/Status
*Left from Address	L_ADD_FROM	Integer		Pending Review
*Left to Address	L_ADD_TO	Integer		Pending Review
*Right from Address	R_ADD_FROM	Integer		Pending Review
*Right to Address	SHIELD_ID	String	10	Pending Review Field Type Discrepancy

Figure 29: Field Type Discrepancy Warning

IMPORTANT Select **N/A** (not available) for a field if you do not plan to add the attribute in the near future and do not wish to be reminded/receive errors on subsequent uploads. The field mapping is stored as **N/A** and is accepted by 9-1-1 EGDMS.

Select **NONE** if you do not wish to map the field attribute at the moment, but want to be reminded on your next upload that the field mapping is missing. Selecting **NONE** allows the current upload to proceed, but provides a reminder upon the next upload that the required field mapping is missing.

It is acceptable to map a required field to **N/A** or **NONE** - the asterisks indicate NENA-required fields, but not all NENA-required fields must be populated for geospatial call routing to function properly.

*Source	SOURCE	String	50	Accepted
*Regional Source	N/A - Not Available			Accepted Required Mapping Missing
*Date Last Modified	N/A - Not Available			Accepted
Effectivity Date	NONE - skip for this upload			
Expiration Date	ADDR_LF			
	ADDR_LT			
	ADDR_RF			
*Road Centerline UID	ADDR_RT	all Int.		Accepted Field Type Discrepancy
	C1_EXCEPTION			
	CLASS			
*Country Name Left	CREATION_DATE			Accepted
	CREATION_USER			Required Mapping Missing
	FULLNAME			

Figure 30: N/A and None Options

- 5 Click the **Save** button when you are finished. A message displays at the bottom of the screen indicating that your changes were successfully saved.

Your changes have been successfully saved.

Figure 31: Changes Saved Confirmation Message

- 6 Click on the next highlighted feature class item that displays in the upper left corner of your screen ([figure 26 on page 25](#)).
- 7 Complete steps 3-5 for each additional feature class that requires configuration.
- 8 When you are finished and have saved your data, click the **Close** button at the bottom of the screen. The *Field Mapping Tool* screen closes and the *Upload Details* screen displays.

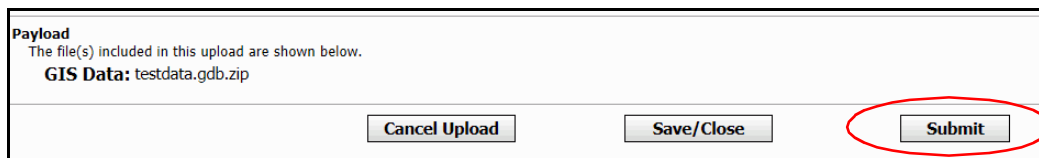


Figure 32: Upload Details - Submit Button

IMPORTANT | If any warnings persist in your field mapping, they must be corrected before submitting.

- 9 Click the **Submit** button to send the configuration changes to the AT&T ESInet. A confirmation message displays indicating that the data was successfully submitted.
- 10 When your submission has finished processing, you will receive an email either indicating that the field mapping attributes have been accepted and no further action is required or that errors were found that must be corrected.

4.2.2 Correct Field Mapping Attribute Errors

If errors are found in your field mapping configuration, you will receive an email notification telling you to log into the Data Management application to correct the errors. To correct the errors, complete the following steps:

- 1 Log into the Data Management application following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6](#).
- 2 If you are assigned to more than one agency, choose your agency from the from the *9-1-1 EGDMS Data Management Select Agency* screen. The *Upload History* screen for your agency displays. The *Current State* column identifies the action required.

	Start Date	Current State	GIS File Name	Upload ID	Last State Update	Reports
View	04/04/2017 14:35 MST	Action Required - Correct Upload Details	BigSky_EGDMS.gdb.zip	20170404T213513.EGDMS_Trai...	04/04/2017 14:42 MST	
View/Edit	04/04/2017 14:22 MST	QA/QC Completed	BigSky_EGDMS.gdb.zip	20170404T212231.EGDMS_Trai...	04/04/2017 14:23 MST	Download

Figure 33: Upload History - Correct Upload Details

- Click the **View/Edit** button to display the *Upload Details* screen. Hovering over the “i” information icon identifies the work required (figure 34 on page 29).

Upload Details
Review the Update and make changes to address any corrections or errors as necessary.

State: Action Required - Correct Upload Details ⓘ **Upload ID:** 2013052

Last State Update: 05/29/2013 16:59 MST

Configuration Changes

Our analysts have identified errors during review of the configuration and attribute field mapping updates for this upload. Please make the necessary corrections and click Submit once complete.

Figure 34: Upload Details - Information Icon

- Click the **Launch** button to open the *Field Mapping Tool* screen.
- Sections requiring corrections are highlighted in red in the EGDMS Feature Class List. Click the feature class to correct errors.

EGDMS Feature Class List

Select a feature class to view.

- Street Centerlines**
- Address/Structure Location
- Emergency Service Zone
- Fire Response Boundary
- Law Response Boundary
- EMS Response Boundary
- PSAP Area Boundary
- Municipal Boundary
- Authoritative Boundary

Figure 35: Feature Class List - Error Correction

- When the feature class requiring error correction is displayed, locate the field with the error. Fields containing errors are highlighted in red.

Field Mapping Tool

EGDMS Feature Class List: Select a feature class to view.
Street Centerlines
 Address/Structure Location
 Emergency Service Zone
 Fire Response Boundary
 Law Response Boundary
 EMS Response Boundary
 PSAP Area Boundary
 Municipal Boundary
 Authoritative Boundary

EGDMS Feature Class: **Street Centerlines**
 Feature Count: 3397

Agency Feature Class: **Roads**
 Projection: NAD_1983_StatePlane_Texas_Cent...

State: **Error(s) Present** [Create Note](#)

Select an Agency Attribute to map to the listed EGDMS Attributes.

EGDMS Attribute	Agency Attribute	Type	Length	State/Status
*Left from Address	L_ADD_FROM	Integer		Accepted
*Left to Address	L_ADD_TO	Integer		Accepted
*Right from Address	R_ADD_FROM	Integer		Accepted
*Right to Address	SHIELD_ID	String	10	Rejected Field Type Discrepancy
Parity Left				
Parity Right				
Street Pre-Modifier				
*Street Prefix Directional	PRE_DIR	String	2	Accepted
*Street Name Pre-Type	PRE_TYPE	String	30	Accepted
*Street Name	STREET	String	30	Accepted
*Street Suffix Type	SUFFIX	String	5	Accepted
*Street Post Directional	POST_DIR	String	2	Accepted
Street Post-Modifier				
*Street Full Name	RD_NAME	String	30	Accepted
Street Name Alias				
One Way				
Speed Limit				

Feature Class Legend:
 Black = Available
 Red Italic = Errors Present
 Grey = Excluded from Upload
 Underline = Warnings Present
 Bold = Current Selection

[Reset](#) [Undo](#) [Save](#) [Close](#)

Figure 36: Street Centerlines Field Mapping Tool - Error Correction

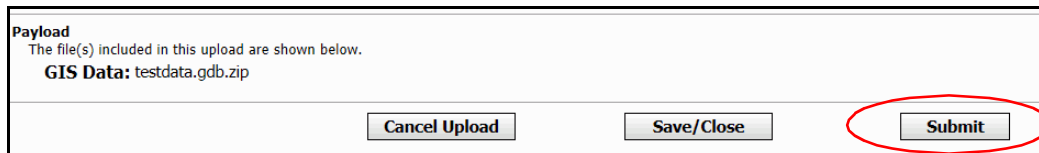
7 Select the correct value from the drop-down menu.

Select an Agency Attribute to map to the listed EGDMS Attributes.

EGDMS Attribute	Agency Attribute	Type	Length	State/Status
*Left from Address	L_ADD_FROM	Integer		Accepted
*Left to Address	L_ADD_TO	Integer		Accepted
*Right from Address	R_ADD_FROM	Integer		Accepted
*Right to Address	R_ADD_TO	Integer		Pending Review

Figure 37: Corrected Field

- 8 Repeat steps 5-7 for each feature class that contains errors.
- 9 Click the **Save** button. A confirmation message displays at the bottom of the screen indicating that your changes were successfully saved ([figure 31 on page 28](#)).
- 10 Click the **Close** button to return to the *Upload Details* screen.



Payload
The file(s) included in this upload are shown below.
GIS Data: testdata.gdb.zip

Cancel Upload Save/Close **Submit**

Figure 38: Upload Details - Submit Button

- 11 Click the **Submit** button. A confirmation message displays at the bottom of the screen indicating that your changes were successfully submitted to the AT&T ESInet.
- 12 When your submission has finished processing, you will receive an email either indicating that the field mapping attributes have been accepted and that sign-off is required or that additional errors may have been identified. If additional errors are found, repeat steps 1-9 in this section until no further errors are found.

4.2.3 Attribute Field Mapping Sign-off

Signing off on the attribute field mapping and/or configuration changes allows your upload to proceed to QA/QC processing. To sign off:

- 1 Log into the Data Management application following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6](#).
- 2 If you are assigned to more than one agency, choose your agency from the from the *9-1-1 EGDMS Data Management Select Agency* screen. The *Upload History* screen for your agency displays and the *Current State* field identifies that the data is ready for sign-off.

	Start Date	Current State	GIS File Name	Upload ID	Last State Update	Reports
View/Edit	04/04/2017 14:35 MST	Action Required - Attribute Field Mapping Signoff	BigSky_EGDMS.gdb.zip	20170404T213513.EGDMS_Trai...	04/04/2017 14:45 MST	
View	04/04/2017 14:22 MST	QA/QC Completed	BigSky_EGDMS.gdb.zip	20170404T212231.EGDMS_Trai...	04/04/2017 14:23 MST	Download

Figure 39: Upload History - Attribute Field Mapping Sign-off

- 3 Click the **View/Edit** button to displays the *Upload Details - Sign-off* screen ([figure 40 on page 32](#)).

The screenshot shows the '9-1-1 EGDMS - Data Management' interface with the 'Upload History' tab selected. The 'Agency' dropdown is set to 'Training_County'. The 'Upload Details' section shows the state as 'Action Required - Attribute Field Mapping Signoff', the upload ID as '20170404T213513.EGDMS_Trai...', and the start date as '04/04/2017 14:35 MST'. The 'Configuration Changes' section includes a 'Launch' button for the 'Field Mapping Tool'. The 'Updated Feature Classes' section lists several feature classes with checkboxes, including 'Street Centerlines' (checked), 'Address/Structure Location', 'PSAP Area Boundary', 'Emergency Service Zone', 'Fire Response Boundary', 'Law Response Boundary', 'EMS Response Boundary', 'Municipal Boundary', and 'Authoritative Boundary'. The 'Payload' section shows the file 'BigSky_EGDMS.gdb.zip'. A box prompts the user to 'Review your Upload details and click submit to signoff.' with two arrows pointing down. At the bottom, there are buttons for 'Cancel Upload', 'Save/Close', and 'Submit'. An 'Activity Log' section is also visible at the bottom left.

Figure 40: Upload Details - Sign-off

- 4 If necessary, you can review the data by launching the *Field Mapping Tool* screen. When you have finished reviewing the data, click the **Submit** button. A confirmation message displays indicating that the submission was successful.

This Upload has been successfully submitted - QA/QC Processing state.

Figure 41: Submission Confirmation

- 5 You will receive an email once QA/QC processing has begun.

4.3 Configuration

The *Configuration* screens display the current attribute field mapping configuration. These are view-only screens.

EGDMS Feature Class	Agency Feature Class	State
Street Centerlines Feature Count: 1004	roads	Validated
Projection: NAD_1983_StatePlane_Kansas_South_FIPS_1502_Feet		
EGDMS Attribute	Agency Attribute	Type Length State/Status
*Source	SOURCE	String 50 Accepted
*Regional Source	N/A	Accepted Required Mapping Missing
*Date Last Modified	MODIFY_DATE	Date Accepted
Effectivity Date		
Expiration Date		
*Road Centerline UID	Unique_ID	Small Int. Accepted Field Type Discrepancy
*Country Name Left	N/A	Accepted Required Mapping Missing
*Country Name Right	N/A	Accepted Required Mapping Missing
*State Left	N/A	Accepted Required Mapping Missing
*State Right	N/A	Accepted Required Mapping Missing
*County Name Left	N/A	Accepted Required Mapping Missing
*County Name Right	N/A	Accepted Required Mapping Missing

Figure 42: Configuration Screen

To access the *Configuration* screens:

- 1 Log into the Data Management application following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6.](#)
- 2 If you are assigned to more than one agency, choose your agency from the from the *9-1-1 EGDMS Data Management Select Agency* screen. The *Upload History* screen for your agency displays.
- 3 Select the **Configuration** tab at the top of the screen. The first feature class field mapping is displayed. Use the links in the EGDMS Feature Class List to view other feature class configurations.

4.4 Agency Details

The *Agency Details* screen displays information about your agency. From this screen, you can view the existing contact data.

AT&T

9-1-1 EGDMS - Data Management

Upload History Configuration Agency Details

Agency Training_County

* Agency Contact John Smith

* Email jsmith@trainingcounty.org

TN 800-555-1212 Ext.

* GIS Technical Contact Jane Doe

* Email jdoe@trainingcounty.com

TN 800-555-1212 Ext.

Assigned 9-1-1 EGDMS Analyst Training County Support Team

* 9-1-1 EGDMS Analyst Distro. TrainingCountysupport@west.com

* GIS Data Format FGDB

* Workflow Path REPORTS/ECRF/LVF I3 GEOSPATIAL ROUTING

GIS Authority Your Agency is not part of a larger GIS Authority.

Cancel

AT&T Proprietary and Confidential Information
Subject to the confidentiality terms under the NDA.

Figure 43: Agency Details

To access the *Agency Details* screen:

- 1 Log into the Data Management application following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6.](#)
- 2 If you are assigned to more than one agency, choose your agency from the from the *9-1-1 EGDMS Data Management Select Agency* screen. The *Upload History* screen for your agency displays.
- 3 Select the **Agency Details** tab at the top of the screen. The *Agency Details* screen displays.

5.0 Reports

5.1 Overview

9-1-1 EGDMS users can access data validation reports that identify errors and discrepancies generated during data processing. Validations include road centerline, address point, and polygon validations for each data upload. Identified errors must be corrected by resubmitting the data in 9-1-1 EGDMS.

Data validation reports are PDFs; the report package contains two types of reports:

- Data upload and GIS validation summary - this PDF report includes the date and time of the upload, the feature count, and changed feature counts from the delta detection, as well as a summary of the GIS validations showing upload counts and validation results.
- Detailed Error Shape files - shape files (per layer) that include features that contain an error, with the error type and description added to the attribute table.

5.2 Accessing and Viewing Reports

- 1 Log into 9-1-1 EGDMS following the steps described in ["Connecting to 9-1-1 EGDMS" on page 6](#).
- 2 Once available, reports are accessed from the Data Upload history table by clicking the **Download** button ([figure 22 on page 21](#)). The report package is downloaded as a .zip folder.

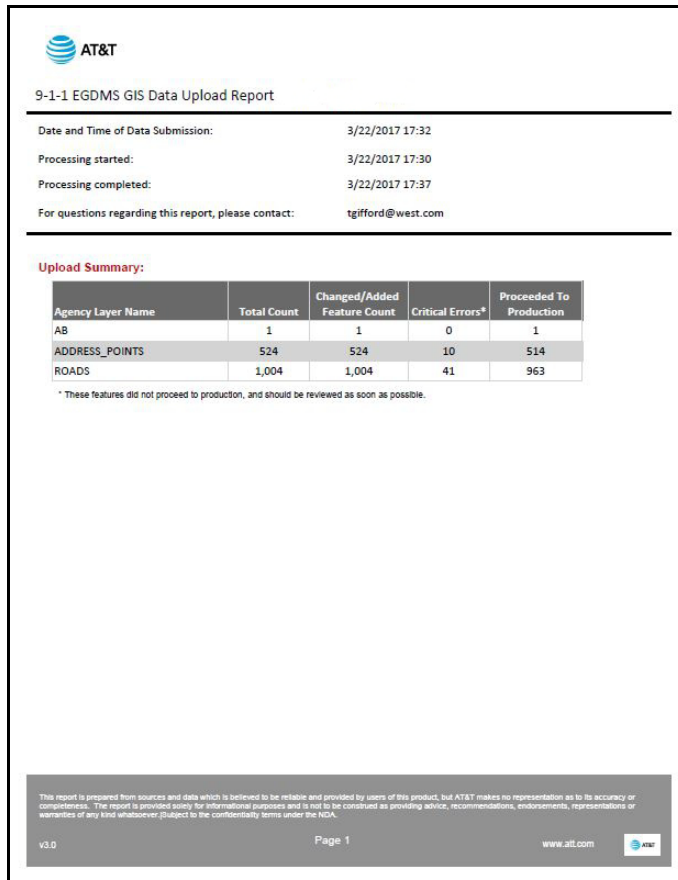


Figure 44: Sample Data Upload Report

ERRORTYPE	ERRORNAME	REASON
9	Attribute Duplicate	Attribute Duplicate, Unique Geometry
9	Attribute Duplicate	Attribute Duplicate, Unique Geometry
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	
4	Outside Authoritative Boundary	

Figure 45: Sample Shapefile Error Report

NOTE To see a detailed error view, view the shapefiles in arccatalog.

5.3 QA/QC Validations

View 9-1-1 EGDMS Report for a detailed description of the QA/QC Validations and error types. Any errors identified are included in PDF upload summary reports and shape file error layers. Reports are available in the upload history table within 9-1-1 EGDMS.

5.3.1 Validations for all Layers

- Compare the schema and data structure and properties of the source dataset with the schema and properties of the master database and report discrepancies in the 9-1-1 EGDMS Field Mapping Tool.
- Incompatible schema field value.
- Exact/stacked feature duplicate.
- Attribute Duplicate.
- Unique ID Duplicate.
- Null Value for required fields.
- Geometry error.

NOTE Any arc or ellipse feature types will be transformed into line and polygon features during processing.

5.3.2 Boundary Layer (Authoritative Boundary, PSAP, Fire, Law, EMS)

- Polygon gap/overlap validation. (For errors involving multiple agencies, participants must work with neighbor agencies to resolve issues. All polygon gap/overlap issues must be correct prior to provisioning data to the ECRF/LVF.)
- Routing URI populated and valid.

5.3.3 Street Centerlines

- Address range overlap issues

5.3.4 Error Code Descriptions

The table below includes descriptions of the validation errors used in the report:

Table 3: Critical Errors

Error Name	Error Description
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 your database.

Table 3: Critical Errors

Error Name	Error Description
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 your database Routing URI.
Routing URI	The Routing URI is either missing or invalid within the service response boundary polygon.
Field Constraint	An attribute value is incompatible with the EGDMS database schema and cannot be loaded.
True Duplicate	The exact feature is duplicated multiple times in the layer - EGDMS deletes the duplicate features, leaving a single record.
Attribute Duplicate	The feature's attributes are duplicated in multiple features, but each feature has a unique location - All records are returned as errors and must be corrected to proceed to production.
Address Range Overlap	An overlap exists in one or both sides of the address ranges between two connected and identically named street centerline segments.
Unique ID Duplicate	The feature's Unique ID is duplicated within the agency's layer - these are critical errors and must be corrected to proceed to production.
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.
NULL Value Critical	NULL value for a critical field.

5.3.5 Error Exception Codes

Certain error types can be marked as exceptions so that they do not continue to fail validation, and are able to load to production. Exceptions must be maintained in an exception field and field mapped to the exception field in the 9-1-1 EGDMS field mapping tool. The following table describes the exceptions.

Table 4: Error Exception Codes

Address Range Overlap (ARO) in Road Centerlines	Address range overlap errors can be flagged as exceptions using the "ARO" value in a mapped exception field. The ARO exception should only be used after the agency has confirmed the road segment is not a true address range overlap error or is due to inconsistent addressing.
Outside Authoritative Boundary (OAB) for Road Centerlines	Features that fall on the provisioning boundary border can be marked as exceptions by using the "OAB" value in a mapped exception field. OAB exceptions should only be used on segments that are not duplicated between the neighboring agency.

6.0 Schema Tables

6.1 Overview

The following conventions are used in the schema tables of this section:

- The **M/O** table column specifies if the attribute information for individual data fields is mandatory or optional.
 - **M** - Mandatory indicates that an attribute value must exist for the data field.
 - **O** - Optional indicates an attribute value may or may not be included in the data field.
- The **Type** table column identifies the type of data used within the data field and attributes.
 - **A** - Alphanumeric (any combination of upper and lower case letters A to Z and/or any numeral from 0 to 9).
 - **D** - Date and time fields follow the International Organization for Standardization (ISO) 8601 standard and are a NENA requirement. The ISO 8601 compliant format is YYYY-MM-DDThh:mm:ss±TZD, where Y is the year, M is the month, D is the day, T designates the switch to time, h is the hour, m is the minute, s is the second, and ±TZD is plus or minus the time zone designation based on the offset from the coordinated universal time (UTC).
For example: 2014-02-20T23:16:30-05:00
2014 = The year
02 = The month
20 = The day
23 = The hour
16 = The minute
30 = The second
-05:00 = The offset from UTC

NOTE	The offset from UTC is the optional separator to indicate the time zone designation, which in this example is -5:00 to indicate the local Eastern Standard Time (EST) time difference from UTC.

- **N** - numeric/number consisting of whole numbers only.

6.2 Authoritative/Provisioning Boundary

Table 5: Provisioning Boundary

Descriptive Name	M/O	Type	Field Width
Discrepancy Agency ID	M	A	75
Regional Source	O	A	50
Date Updated	M	D	Date
Effective Date	M	D	Date
Expiration Date	O	D	Date
Authoritative Boundary Unique ID	M	A	254

6.3 Street Centerlines

Table 6: Street Centerlines

Descriptive Name	M/O	Type	Field Width
Discrepancy Agency ID	M	A	75
Regional Source	O	A	50
Date Updated	M	D	Date
Effective Date	O	D	Date
Expiration Date	O	D	Date
Road Centerline NGUID	M	A	254
Exception	O	A	30
Country Left	M	A	2
Country Right	M	A	2
State Left	M	A	2
State Right	M	A	2
County Left	M	A	40
County Right	M	A	40
Additional Code Left	O	A	6
Additional Code Right	O	A	6
Incorporated Municipality Left	M	A	100

Table 6: Street Centerlines (Continued)

Descriptive Name	M/O	Type	Field Width
Incorporated Municipality Right	M	A	100
Unincorporated Community Left	O	A	100
Unincorporated Community Right	O	A	100
Neighborhood Community Left	O	A	100
Neighborhood Community Right	O	A	100
Left Address Number Prefix	O	A	15
Right Address Number Prefix	O	A	15
Left FROM Address	M	N	Long Int
Left TO Address	M	N	Long Int
Right FROM Address	M	N	Long Int
Right TO Address	M	N	Long Int
Parity Left	M	A	1
Parity Right	M	A	1
Postal Community Name Left	O	A	40
Postal Community Name Right	O	A	40
Postal Code Left	O	A	7
Postal Code Right	O	A	7
ESN Left	O*	A	5
ESN Right	O*	A	5
MSAG Community Name Left	O*	A	30
MSAG Community Name Right	O*	A	30
Street Name Pre Modifier	O	A	15
Street Name Pre Directional	O	A	9
Street Name Pre Type	O	A	50
Street Name Pre Type Separator	O	A	20
Street Name	M	A	60
Street Name Post Type	O	A	50
Street Name Post Directional	O	A	9
Street Name Post Modifier	O	A	25
Speed Limit	O	N	Long Int

Table 6: Street Centerlines (Continued)

Descriptive Name	M/O	Type	Field Width
One-Way	O	A	2
Road Class	O	A	15
FROM Road Level	O	A	1
TO Road Level	O	A	1
Validation Left	O	A	1
Validation Right	O	A	1
Entity Left	O**	A	3
Entity Right	O**	A	3
Exchange Left	O**	A	4
Exchange Right	O**	A	4
Legacy Street Name Pre Directional	O*	A	2
Legacy Street Name	O*	A	75
Legacy Street Name Post Type	O*	A	4
Legacy Street Post Directional	O*	A	2

* Required for Transitional Data Management Service/GeoMSAG Services and for compatibility for ALI matching in an i3 transitional period.

** Transitional Data Management Service, Entity, and Exchange Left and Right fields and values may be required to be populated within the road centerline schema where more than one selective router serves the geographic area.

6.4 Address Points

Table 7: Address Points

Descriptive Name	M/O	Type	Field Width
Discrepancy Agency ID	M	a	75
Regional Source	O	A	50
Date Updated	M	D	Date
Effective Date	O	D	Date
Expiration Date	O	D	Date
Site Unique ID	M	A	254
Country	M	A	2

Table 7: Address Points (Continued)

Descriptive Name	M/O	Type	Field Width
State	M	A	2
County	M	A	40
Additional Code	O	A	6
Additional Data URI	O	A	254
Incorporated Municipality	M	A	100
Unincorporated Community	O	A	100
Neighborhood Community	O	A	100
Address Number Prefix	O	A	15
Address Number	M	N	Long Int
Address Number Suffix	O	A	15
Street Name Pre Modifier	O	A	15
Street Name Pre Directional	O	A	9
Street Name Pre Type	O	A	50
Street Name Pre Type Separator	O	A	20
Street Name	M	A	60
Street Name Post Type	O	A	50
Street Name Post Directional	O	A	9
Street Name Post Modifier	O	A	25
ESN	O*	A	5
MSAG Community Name	O*	A	30
Postal Community Name	O	A	40
Postal Code	O	A	7
ZIP Plus 4	O	A	4
Building	O	A	75
Floor	O	A	75
Unit	O	A	75
Room	O	A	75
Seat	O	A	75
Additional Location Information	O	A	225
Complete Landmark Name	O	A	150

Table 7: Address Points (Continued)

Descriptive Name	M/O	Type	Field Width
Mile Post	O	A	150
Place Type	O	A	50
Placement Method	O	A	25
Longitude	O	DOUBLE	-
Latitude	O	DOUBLE	-
Elevation	O	DOUBLE	-
Legacy Street Name Pre Directional	O*	A	2
Legacy Street Name	O*	A	75
Legacy Street Name Post Type	O*	A	4
Legacy Street Post Directional	O*	A	2

*Required for compatibility and ALI matching in an i3 transitional period.

6.5 PSAP Layers/Fire/Law/EMS

Table 8: PSAP Layers/Fire/Law/EMS

Descriptive Name	M/O	Type	Field Width
Discrepancy Agency ID	M	A	75
Regional Source	O	A	50
Date Updated	M	D	Date
Effective Date	O	D	Date
Expiration Date	O	D	Date
(PSAP/Fire/Law/EMS)_Unique_ID	M	A	254
Agency ID	M	A	100
Service URI	M	A	254
Service URN*	M	A	50
Service Number	O	A	15
Agency vCard URI	M	A	254
Display Name	M	A	60

*Note that the service URN is not required as this value is assigned by a layer within 9-1-1 EGDMS.

6.6 Municipal Boundary

Table 9: Municipal Boundary

Descriptive Name	M/O	Type	Field Width
Discrepancy Agency ID	M	A	75
Regional Source	O	A	50
Date Updated	M	D	Date
Effective Date	O	D	Date
Expiration Date	O	D	Date
Incorporated Municipality Unique_ID	M	A	254
Country	M	A	2
State	M	A	2
County	M	A	75
Additional Code	O	A	6
Incorporated Municipality	M	A	100

7.0 Glossary

Table 10: Glossary

Attribute	Definition
Additional Code	A code that specifies a geographic area. Used in Canada to hold a standard geographical classification code; it differentiates two municipalities with the same name in a province that does not have counties.
Additional Code Left	The additional code on the left side of the road segment relative to the FROM node.
Additional Code Right	The additional code on the right side of the road segment relative to the FROM node.
Additional Data URI	URI(s) for additional data associated with the site/structure address point. This attribute is contained in the site/structure address points layer and will define the service URI of additional information about a location, including building information (blueprints, contact info, floor plans, etc.).
Additional Location Information	A part of a sub-address that is not a building, floor, unit, room, or seat.
Address Number	The numeric identifier of a location along a thoroughfare or within a defined community.
Address Number Prefix	An extension of the address number that precedes it and further identifies a location along a thoroughfare or within a defined area.
Address Number Suffix	An extension of the address number that follows it and further identifies a location along a thoroughfare or within a defined area.
Agency ID	A domain name system (DNS) domain name which is used to uniquely identify an agency. An agency is represented by a domain name. Each agency must use one domain name consistently in order to correlate actions across a wide range of calls and incidents. Any domain name in the public DNS is acceptable so long as each distinct agency uses a different domain name. This ensures that each agency ID is globally unique.
Agency vCard URI	A vCard is a file format standard for electronic business cards. The agency vCard URI is the Internet address of an eXtensible markup language (XML) data structure which contains contact information (name of agency, contact phone numbers, etc.) in the form of a vCard (RFC 6350). vCard files may be exported from most email programs or created with a text editor. The vCard URI is used in the service boundary layers to provide contact information for that agency. The agency locator will provide these URIs for agencies listed in it.

Table 10: Glossary

Attribute	Definition
Building	One among a group of buildings that have the same address number and complete street name.
Complete Landmark Name	The name by which a prominent site/structure is publicly known.
Country	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters.
Country Left	The name of the country on the left side of the road segment relative to the FROM node, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters.
Country Right	The name of the country on the right side of the road segment relative to the FROM node, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters.
County	The name of a county or county-equivalent where the address is located. A county (or its equivalent) is the primary legal division of a state or territory.
County Left	The name of a county or county-equivalent on the left side of the road segment relative to the FROM node. A county (or its equivalent) is the primary legal division of a state or territory.
County NENA Globally Unique ID	The NENA globally unique ID for each county (or its equivalent) boundary. Each record in the counties or equivalents layer must have a globally unique ID. When coalescing data from other local 9-1-1 authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID."
County Right	The name of a county or county-equivalent on the right side of the road segment relative to the FROM node. A county (or its equivalent) is the primary legal division of a state or territory.
Date Updated	The date and time that the record was created or last modified. This value must be populated upon modifications to attributes, geometry, or both.
Discrepancy Agency ID	Agency that receives a discrepancy report (DR), should a discrepancy be discovered, and will take responsibility for ensuring discrepancy resolution. This may or may not be the same as the 9-1-1 authority. This must be represented by a domain name that is an agency identifier as defined in the NENA master glossary.
Display Name	A description or name of the service provider that offers services within the area of a PSAP or an emergency service boundary. This value must be suitable for display.
ECRC	Emergency call relay center.
Effective Date	The date and time that the record is scheduled to take effect.

Table 10: Glossary

Attribute	Definition
Elevation	The elevation, given in meters above a reference surface defined by the coordinate system, associated with the site/structure address.
Emergency Service Boundary NENA Globally Unique ID	The NENA globally unique ID for each emergency service boundary and PSAP boundary. Each record in the emergency service boundary layer and the PSAP boundary layer must have a globally unique ID. When coalescing data from other local 9-1-1 authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID." Emergency service boundary data is unique in that the data fields and their attributes are only a template to be reused for each emergency service boundary. For the emergency service boundary, there may be a separate dataset for law, fire, and EMS, and other emergency services such as poison control, forest service, coast guard, etc.
Entity Left	The entity on the left side of the road segment. Entity is a legacy MSAG system data element used to simplify data management by grouping MSAG records. The entity represents a geographical area that generally corresponds to E9-1-1 selective routing boundaries.
Entity Right	The entity on the right side of the road segment. Entity is a legacy MSAG system data element used to simplify data management by grouping MSAG records. The entity represents a geographical area that generally corresponds to E9-1-1 selective routing boundaries.
ESN	A 3-5 character alphanumeric string that represents an emergency service zone (ESZ).
ESN Left	The emergency service number (ESN) on the left side of the road segment relative to the FROM node.
ESN Right	The emergency service number (ESN) on the right side of the road segment relative to the FROM node.
ESRI	Environmental systems research institute.
Exception	A field used to mark features as error exceptions.
Exchange Left	The exchange on the left side of the road segment. Exchange is a defined area, served by one or more telephone central offices, within which a local exchange carrier furnishes service.
Exchange Right	The exchange on the right side of the road segment. Exchange is a defined area, served by one or more telephone central offices, within which a local exchange carrier furnishes service.
Expiration Date	The date and time when the information in the record is no longer considered valid.
Floor	A floor, story, or level within a building.

Table 10: Glossary

Attribute	Definition
From Road Level	Specifies the elevation of a segment FROM node (start point). This field does not require actual elevation in terms of real-world measurements. The value is only used to determine whether a turn is allowed from one street to a street that intersects it in a 2-dimensional space, similar to floors in a building. Nodes at the lowest level are assigned 0, with overlapping nodes representing additional level(s)/overpass(es) are assigned the next sequential integer value accordingly.
Incorporated Municipality	The name of the incorporated municipality or other general-purpose local governmental unit (if any) where the address is located.
Incorporated Municipality Left	The name of the incorporated municipality or other general-purpose local governmental unit (if any), on the left side of the road segment relative to the FROM node.
Incorporated Municipality NENA Globally Unique ID	The NENA globally unique ID for each incorporated municipality boundary. Each record in the incorporated municipality boundary layer must have a globally unique ID. When coalescing data from other local 9-1-1 authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID."
Incorporated Municipality Right	The name of the incorporated municipality or other general-purpose local governmental unit (if any), on the right side of the road segment relative to the FROM node.
Latitude	The angular distance of a location north or south of the equator as defined by the coordinate system, expressed in decimal degrees.
Left Address Number Prefix	An extension of the address number that precedes it and further identifies a location along a thoroughfare or within a defined area, on the left side of the road segment relative to the FROM node. It contains any alphanumeric characters, punctuation, and spaces preceding the left FROM address and left TO address.
Left FROM Address	In a GIS road centerlines layer, each feature has a begin point and an endpoint. The FROM node is the begin point while the TO node is the endpoint. Each has a left side and a right side relative to a begin node and an end node. The left FROM address is the address number on the left side of the road segment relative to the left FROM node.
Left TO Address	In a GIS, each feature has a begin point and an endpoint. The FROM node is the begin point while the TO node is the endpoint. Each has a left side and a right side relative to a begin node and an end node. The left TO address is the address number on the left side of the road segment relative to the left TO node.
Legacy Street Name	The street name field as it would appear in the MSAG, as assigned by the local addressing authority.

Table 10: Glossary

Attribute	Definition
Legacy Street Name Post Directional	The trailing street direction suffix as it previously existed prior to the adoption of the NG9-1-1 data model as assigned by the local addressing authority.
Legacy Street Name Pre Directional	The leading street direction prefix as it previously existed prior to the adoption of the NG9-1-1 data model as assigned by the local addressing authority.
Legacy Street Name Type	The valid street abbreviation as it previously existed prior to the adoption of the NG9-1-1 data model as assigned by the local addressing authority.
LVF	Location validation function.
Longitude	The angular distance of a location east or west of the prime meridian of the coordinate system, expressed in decimal degrees.
Mile Post	A distance traveled along a route such as a road or highway, typically indicated by a milepost sign. There is typically a post or other marker indicating the distance in miles/kilometers from or to a given point.
MSAG Community Name	The community name associated with an address as given in the MSAG and may or may not be the same as the community name assigned by the United States Postal Service (USPS).
MSAG Community Name Left	The existing MSAG community name on the left side of the road segment relative to the FROM node.
MSAG Community Name Right	The existing MSAG community name on the right side of the road segment relative to the FROM node.
Neighborhood Community	The name of an unincorporated neighborhood, subdivision, or area, either within an incorporated municipality or in an unincorporated portion of a county or both, where the address is located.
Neighborhood Community Left	The name of an unincorporated neighborhood, subdivision or area, either within an incorporated municipality or in an unincorporated portion of a county or both, on the left side of the road segment relative to the FROM node.
Neighborhood Community Right	The name of an unincorporated neighborhood, subdivision or area, either within an incorporated municipality or in an unincorporated portion of a county or both, on the right side of the road segment relative to the FROM node.
OGC	Open geospatial consortium.

Table 10: Glossary

Attribute	Definition
One-Way	The direction of traffic movement along a road in relation to the FROM node and TO node of the line segment representing the road in the GIS data. The one-way field has three possible designations: B (Both), FT (From-To) and TF (To-From). ■ B - Travel in both directions allowed ■ FT - One-way traveling from FROM node to TO node ■ TF - One way traveling from TO node to FROM node
Parity Left	The even or odd property of the address number range on the left side of the road segment relative to the FROM node.
Parity Right	The even or odd property of the address number range on the right side of the road segment relative to the FROM node.
Placement Method	The methodology used for placement of the address point.
Place Type	The type of feature identified by the address.
Postal Code	A system of 5-digit (US) or 7-character codes (Canada) that identify the individual USPS or Canadian Post Office or metropolitan area delivery station associated with an address.
Postal Code Left	The postal code on the left side of the road segment relative to the FROM node.
Postal Code Right	The postal code on the right side of the road segment relative to the FROM node.
Postal Community Name	A city name for the ZIP code of an address, as given in the USPS city state file.
Postal Community Name Left	A city name for the ZIP code of an address, as given in the USPS city state file on the left side of the road segment relative to the FROM node.
Postal Community Name Right	A city name for the ZIP code of an address, as given in the USPS city state file on the right side of the road segment relative to the FROM node.
Provisioning Boundary NENA Globally Unique ID	The NENA globally unique ID for each provisioning boundary. Each record in the provisioning boundary layer must have a globally unique ID. When coalescing data from other local 9-1-1 authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID."
Regional Source	The regional source of data. This field is used if a regional data source is responsible for data coalescing and provisioning.

Table 10: Glossary

Attribute	Definition
Right FROM Address	In a GIS road centerlines layer, each feature has a begin point and an endpoint. The FROM node is the begin point while the TO node is the endpoint. Each has a left side and a right side relative to a begin node and an end node. The right FROM address number is the address number on the right side of the road segment relative to the right FROM node.
Right TO Address	In a GIS road centerlines layer, each feature has a begin point and an endpoint. The FROM node is the begin point while the TO node is the endpoint. Each has a left side and a right side relative to a begin node and an end node. The right TO address number is the address number on the right side of the road segment relative to the right TO node.
Road Centerline NENA Globally Unique ID	The NENA globally unique ID for each road centerline. Each record in the road centerlines layer must have a globally unique ID. When coalescing data from other local 9-1-1 authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID."
Road Class	The general description of the type of road. The road classifications used in this document are derived from the US census MAF/TIGER feature classification codes (MTFCC), which is an update to the now deprecated census feature class codes (CFCC).
Room	A single room within a building.
Seat	A place where a person might sit within a building.
Service Number	The numbers that would be dialed on a 12-digit keypad to reach the emergency service appropriate for the location. This is not the same as an emergency service number (ESN) in legacy E9-1-1 systems. This field is used for all emergency boundaries including PSAP; law; fire; EMS; and others such as poison control. Within the United States the service number for most emergency services is 9-1-1, however, there may be emergency service boundaries that have a different number that may be associated with them such as poison control. Additionally, in areas outside of the United States, different numbers may be used for law, fire, and EMS - this field would be used to denote those numbers.
Service URI	URI for call routing. This attribute is contained in the emergency service boundary layer and will define the service URI of the service. The URI is usually a session initiation protocol (e.g., SIP or SIPs) URI but may be a telephone number (e.g., tel) URI that defines the route to reach the service.
Service URN	The URN used to select the service for which a route is desired. The ECRF is queried with a location and a service URN that returns the service URI.

Table 10: Glossary

Attribute	Definition
Site NENA Globally Unique ID	The NENA globally unique ID for each site/structure address point. Each record in the site/structure address points layer must have a globally unique ID. When coalescing data from other local 9-1-1 Authorities into the ECRF and LVF, this unique ID must continue to have only one occurrence. One way to accomplish this is to append the 9-1-1 authority's domain to the end of the "locally unique ID."
Speed Limit	Posted speed limit in MPH in US or Km/h in Canada
State	The name of a state or state equivalent, represented by the two-letter abbreviation. A state is a primary governmental division of the United States.
State Left	The name of a state or state equivalent on the left side of the road segment relative to the FROM node, represented by the two-letter abbreviation.
State Right	The name of a state or state equivalent on the right side of the road segment relative to the FROM node, represented by the two-letter abbreviation.
Street Name	The official name of the road, usually defined by the lowest jurisdictional authority (e.g., city). The street name does not include any street types, directionals, or modifiers.
Street Name Post Directional	A word following the street name element that indicates the direction taken by the road from an arbitrary starting point or line, or the sector where it is located.
Street Name Post Modifier	A word or phrase that follows and modifies the street name element, but is separated from it by a street name post type or a street name post directional or both.
Street Name Post Type	A word or phrase that follows the street name element and identifies a type of thoroughfare in a complete street name.
Street Name Pre Directional	A word preceding the street name element that indicates the direction taken by the road from an arbitrary starting point or line, or the sector where it is located.
Street Name Pre Modifier	A word or phrase that precedes and modifies the street name element but is separated from it by a street name pre type or a street name pre directional or both.
Street Name Pre Type	A word or phrase that precedes the street name element and identifies a type of thoroughfare in a complete street name.
Street Name Pre Type Separator	A preposition or prepositional phrase between the street name pre type and the street name.

Table 10: Glossary

Attribute	Definition
To Road Level	Specifies the elevation of a segment TO node (end point). This field does not require actual elevation in terms of real-world measurements. The value is only used to determine whether a turn is allowed from one street to a street that intersects it in a 2-dimensional space, similar to floors in a building. Nodes at the lowest level would be assigned 0, with overlapping nodes representing additional level(s)/overpass(es) will be assigned the next sequential integer value accordingly.
Unincorporated Community	The name of an unincorporated community, either within an incorporated municipality or in an unincorporated portion of a county, or both, where the address is located.
Unincorporated Community Left	The unincorporated community, either within an incorporated municipality or in an unincorporated portion of a county, or both, on the left side of the road segment relative to the FROM node.
Unincorporated Community Right	The unincorporated community, either within an incorporated municipality or in an unincorporated portion of a county, or both, on the right side of the road segment relative to the FROM node.
Unit	A group or suite of rooms within a building that are under common ownership or tenancy, typically having a common primary entrance.
Validation Left	Indicates if the address range on the left side of the road segment should be used for civic location validation. A value of "Y" may be entered if any address number within the address range on the left side of the road segment should be considered by the LVF to be valid. A value of "N" may be entered if the address number should only be validated using the site/structure address points layer. If not present, a value of "Y" is assumed.
Validation Right	Indicates if the address range on the right side of the road segment should be used for civic location validation. A value of "Y" may be entered if any address number within the address range on the right side of the road segment should be considered by the LVF to be valid. A value of "N" may be entered if the address number should only be validated using the site/structure address points layer. If not present, a value of "Y" is assumed.
ZIP Plus-4	The addition of the ZIP plus-4 refines the mail delivery point down to a specific block or building, and may prove useful to validate locations. ZIP plus-4 codes change more often than US postal codes.



Appendix F - AT&T ESInet Training Plan



AT&T ESI^{net}TM Training Plan

CONTENTS

1.	INTENTION	3
2.	OVERVIEW.....	3
3.	LOCATION DATABASE TRAINING	3
3.1.	DESCRIPTION/OBJECTIVE.....	3
3.2.	AUDIENCE.....	3
3.3.	DELIVERY METHOD/DURATION/EQUIPMENT NEEDED	3
3.4.	TRAINING MATERIAL	3
3.5.	SCHEDULE.....	3
3.6.	CLASS SIZE	3
3.7.	PREREQUISITES	4
4.	SPATIAL INTERFACE TRAINING.....	4
4.1.	DESCRIPTION	4
4.2.	AUDIENCE.....	4
4.3.	DELIVERY METHOD/DURATION/EQUIPMENT NEEDED	4
4.4.	TRAINING MATERIAL	4
4.5.	SCHEDULE.....	4
4.6.	CLASS SIZE	4
4.7.	PREREQUISITES	4
5.	ECATS TRAINING.....	4
5.1.	DESCRIPTION	4
5.2.	AUDIENCE.....	4
5.3.	DELIVERY METHOD/DURATION/EQUIPMENT NEEDED	5
5.4.	TRAINING MATERIAL	5
5.5.	SCHEDULE.....	5
5.6.	CLASS SIZE	5
5.7.	PREREQUISITES	5
6.	CUSTOMER MANAGEMENT PORTAL TRAINING	5
6.1.	DESCRIPTION	5
6.2.	AUDIENCE.....	5
6.3.	DELIVERY METHOD/DURATION/EQUIPMENT NEEDED	5
6.4.	TRAINING MATERIAL	5
6.5.	SCHEDULE.....	5
6.6.	CLASS SIZE	5
6.7.	PREREQUISITES	5
7.	LOCATION VALIDATION FUNCTION TRAINING	6
7.1.	DESCRIPTION	6
7.2.	AUDIENCE.....	6
7.3.	DELIVERY METHOD/DURATION/EQUIPMENT NEEDED	6
7.4.	TRAINING MATERIAL	6
7.5.	SCHEDULE.....	6
7.6.	CLASS SIZE	6
7.7.	PREREQUISITES	6

8.	TRouble TICKET SYSTEM TRAINING.....	7
8.1.	USER GUIDES	8

1. Intention

This Training Plan is intended to provide an overview of all the applicable training for users of the AT&T ESInet. This includes PSAP staff, State/Regional Authorities, GIS Authorities, as well as OSPs. Training is application specific, and this plan provides guidance on the recommended audience for the training and when the initial training will be scheduled. AT&T ESInet is provided as a service and the training plan does not cover maintenance, configuration, or replacement of any functional elements or hardware as those are fully serviced by AT&T and are covered by separate training plans.

2. Overview

This document will serve as the overarching guide regarding the training provided by AT&T to access the various applications that make up the service provided for subscribers to the AT&T ESInet. Each section will provide details of the training that include (but are not limited to) description of application, intended audience, class size, delivery method, and training materials.

3. Location Database Training

3.1. Description/Objective

LDB (Location Database) is a server that retains all of the current information, functionality, and interfaces of today's ALI and can utilize the new protocols required in an NG9-1-1 deployment. LDB training provides users instructions on accessing and using 911NET (the online application used to manage ALI and MSAG information).

3.2. Audience

LDB training applies both PSAP users that maintain the MSAG records along with OSP resources which maintain their records in the LDB (formerly ALI).

3.3. Delivery Method/Duration/Equipment Needed

LDB training is an instructor led web-based training that typically lasts 2 hours. Attendees will need a computer that can access the internet.

3.4. Training Material

LDB training material includes the 911Net User Guide as well as demonstration of the application for users.

3.5. Schedule

LDB training is scheduled prior to a PSAP's deployment onto ESInet and are intended for a specific PSAP or multiple PSAPs deploying in the same time frame. The AT&T Project Manager assigned to the PSAP deployment will coordinate the training when applicable in a PSAPs deployment schedule.

3.6. Class Size

Class sizes are unlimited.

3.7. Prerequisites

Attendees should have a basic knowledge of 9-1-1 and be an authorized user of the system.

4. Spatial Interface Training

4.1. Description

Spatial Interface (SI) is a standardized interface between the GIS data and the functional elements that consume GIS data, such as the ECRF, LVF, Map Database Services, etc. Training covers a SI overview, field mapping, validation report interpretation and error correction consulting. At the conclusion of training, users will be able to submit data via the SI to be uploaded to AT&T ESInet's ECRF/LVF.

4.2. Audience

SI training applies only to those users who submit their GIS data via the Spatial Interface to be uploaded to the ECRF/LVF. Typical users are GIS administrators at a PSAP, County, or State level.

4.3. Delivery Method/Duration/Equipment Needed

SI training is an instructor led web-based training that consists of 3 training sessions typically last 2 hours. Attendees will need a computer that can access the internet.

4.4. Training Material

SI training material includes the Enterprise Geospatial Database Management System (EGDMS) User Guide, a GIS Roles and Expectations Document as well as demonstration of the application for users.

4.5. Schedule

SI training is scheduled at least 90 days prior to a PSAP's deployment onto ESInet.

4.6. Class Size

Class sizes are unlimited.

4.7. Prerequisites

Attendees should have a basic knowledge of GIS Data including how to edit data. Attendees, while not required, are encouraged to complete the ESInet Portal Enrollment Form to get access built prior to the training.

5. ECaTS Training

5.1. Description

ECaTS (Emergency Call Tracking System) will collect, analyze, and report on the raw Call Detail Record (CDR) and/or i3 data for your PSAP, and where applicable, for all PSAPs in your jurisdiction. Depending on the PSAP/State's subscription, ECaTS will provide CPE MIS Reporting and/or i3 reporting.

5.2. Audience

ECaTS training only applies to users of the system and is not mandatory to manage the system but provides valuable reporting. Typical users are PSAP/Regional administrators, managers, supervisors at a PSAP, County, or State level.

5.3. Delivery Method/Duration/Equipment Needed

ECaTS training is an instructor led web-based training that typically last 2 hours. Attendees will need a computer that can access the internet.

5.4. Training Material

ECaTS training material includes the ECaTS Training Manual as well as demonstration of the application for users.

5.5. Schedule

ECaTS training is scheduled after a PSAP's deployment onto ESInet. ECaTS uses actual live call data for that PSAP specifically to make the training customized for the individual group.

5.6. Class Size

Class sizes are unlimited.

5.7. Prerequisites

Attendees should have a basic knowledge of 9-1-1 and be an authorized user of the system.

6. Customer Management Portal Training**6.1. Description**

The Customer Management Portal (CMP) provides participating PSAPs and approved personnel 24x7x365 access to a reporting suite including call detail records through a secure, web-based portal. Call detail records provide the user with all the pertinent information for each call. CMP also provides a dashboard of PSAP operation state. Access is roles based and therefore PSAPs only get access to their data while Regional/State authorities can see data for their area of responsibility. CMP also provides the users with the optional ability to change update the Policy Routing Function (PRF). This access is only given to authorized users and not all who have access to the system will be given this ability.

6.2. Audience

CMP training only applies to users of the system and is not mandatory to manage the system but provides valuable reporting. Typical users are PSAP/Regional administrators, managers, supervisors at a PSAP, County, or State level.

6.3. Delivery Method/Duration/Equipment Needed

CMP training is an instructor led web-based training that typically last 2 hours. Attendees will need a computer that can access the internet.

6.4. Training Material

CMP training material includes the CMP User Guide as well as demonstration of the application for users.

6.5. Schedule

CMP training is scheduled after a PSAP's deployment onto ESInet. CMP training uses actual route lists, CDRs, and other information specific to the PSAP to make the training customized for the individual group.

6.6. Class Size

Class sizes are unlimited.

6.7. Prerequisites

Attendees should have a basic knowledge of 9-1-1 and be an authorized user of the system. Authorization is determined by PSAP/State/Regional leadership.

7. Location Validation Function Training

7.1. Description

Location Validation Function (LVF) is a functional element in an NGCS that is a LoST protocol server where civic location information is validated against the authoritative GIS database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call and adequate and specific enough to direct responders to the right location. LVF training does not adhere to classroom style training as the LoST query used to access the LVF is a machine to machine query/response. LVF “training” will consist of AT&T working with i3 Originating Service Providers (OSPs) to enable the connection between OSP and LVF along with the exchange of digital certificates.

7.2. Audience

LVF training applies only to i3 OSPs that will be querying the LVF to validate their address information.

7.3. Delivery Method/Duration/Equipment Needed

LVF connections will be set up for each i3 OSP and coordinated between the technical teams at both AT&T and the i3 OSP. i3 OSPs should have already completed their development of a application which can perform a LoST query.

7.4. Training Material

AT&T provides a LVF-LoST Interface Specification to the OSPs prior to testing of the LVF query to provide education and documentation above and beyond the NENA i3 specification.

7.5. Schedule

LVF implementation is scheduled at least 90 days prior to a PSAP’s deployment onto ESInet.

7.6. Class Size

Class sizes are not applicable as training will be conversations and testing between the i3 OSP and AT&T.

7.7. Prerequisites

Attendees should have a basic knowledge of NENA i3 as well as LoST servers. Attendees should have already developed their application and read the LVF-LoST Interface Specification.

8. Change-management Requests, Processes, and Tools

8.1. Description

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. AT&T utilizes both the Incident / Problem Management module and the Change Management module of Remedy 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. 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.

8.2. Audience

Change Management training only applies to super users that have an interest in how AT&T conducts maintenance activities, upgrades and enhancements for platform wide changes in the AT&T ESInet™ Core Routing platform. Most maintenance activities on the AT&T ESInet™ solution are completed with no scheduled downtime for the customer. Typical users are PSAP/Regional administrators, managers, supervisors at a PSAP, County, or State level.

8.3. Delivery Method/Duration/Equipment Needed

The Change Management overview will be conducted via online web conferencing.

8.4. Training Material

There are no materials available for this course as it is a function of the AT&T internal NOC and Operations organizations that requires no intervention from the end user.

8.5. Schedule

Change Management is an ongoing operation, monitored by AT&T. AT&T's Service Management Organization will provide advanced notice of maintenance events, when there is possible customer impact identified.

8.6. Class Size

There is no limit on class size as the overview would be conducted via web conference.

8.7. Prerequisites

None.

9. Trouble Ticket System Training

There is no formal training offered for using the AT&T trouble ticket system. Informal training is completed during participant onboarding by the AT&T PgM. The process to report a trouble ticket is addressed below.

AT&T 9-1-1 Resolution Center Contact

During the course of providing services to the PSAP there will be times where it is necessary for the PSAP, AT&T Network or Vendor partners to contact the 9-1-1 Resolution Center to resolve technical and/or procedural issues, provide updates or to notify the 9-1-1 Resolution Center of current activities or report cases of trouble. Below are the activities that would require the PSAP, AT&T Network or Vendor partners to contact the 9-1-1 Resolution Center and the processes that should be followed.

Contacting the 9-1-1 Resolution Center to Report Trouble

- In the case where the PSAP, AT&T Network and or Vendor partners are made aware of a trouble condition that has impacted the CPE, network elements, 9-1-1 call completion or the delivery of location information, it is requested that the 9-1-1 Resolution Center must be notified (if possible)

prior to taking any action. Once notified the 9-1-1 Resolution Center will open a trouble ticket and provide the reporting agency/organization with the ticket number.

- The reporting agency/organization must provide the 9-1-1 Resolution Center with the following information when reporting trouble.
 - Description of trouble – The description must include
 - The impact to services, e.g., cannot receive 9-1-1 calls, not receiving location information, cannot transfer, etc.
 - The impact to equipment , e.g., the phone at position 5 (number 312-740-xxxx) cannot receive calls
 - Location of trouble, e.g., the PSAP, back up Center
 - Name of the person and agency/organization reporting the trouble, e.g., John Smith at the NMC
 - Call back number of the person and agency/organization reporting the trouble
 - The ticket number (if any) that was generated by the reporting agency/organization
 - Actions that were taken (if any) to resolve the trouble prior to contacting the 9-1-1 Resolution Center

9.1. User Guides

9.1.1. CMP User Guide

The Customer Management Portal (CMP) is a web-based application that provides access to one or more PSAP-level accounts deployed on AT&T's Emergency Services IP network (ESInet).

9.1.2. EGDMS User Guide

The 9-1-1 Enterprise Geospatial Database Management System (9-1-1 EGDMS) is a web application that serves as the front-end user interface for the NENA Spatial Interface (SI) requirement.

9.1.3. AT&T ESInet Reports User Guide

The AT&T ESInet reports are accessed through a web-based application for viewing, printing, and exporting reports. The User Guide provides users with information on how to access the reports as well as general description of each report.

9.1.4. ECaTS PSAP Training Manual

The ECaTS training manual will serve as a living document that will describe how to use ECaTS from the PSAP perspective. As the system continues to grow and expand in functionality and available reports, this document will encompass all aspects of creating, executing, analyzing, and saving reports. PSAP users can access the latest version of the manual online after logging onto the ECaTS application. The matrix below shows a description of the available ECaTS reports and the applicable users.



Appendix G - NGCS_ESInet_Risk_Register_Template

NGCS_ESInet_Risk_Register_Template

[illegible]



Appendix H - NGCS_ESInet_Risk_Acceptance_Form

Risk ID: RA-NG911-003

Date Submitted: March 15, 2026

Affected Asset(s):

- ☒ ESInet Network Element
- ☐ NGCS Application
- ☐ Cloud / Third-Party Service

Asset Description:

ESInet last-mile connectivity provided by third-party carrier to rural PSAP locations.

Risk Description:

Certain rural PSAP locations rely on third-party last-mile carrier facilities where true physical path diversity cannot be fully guaranteed despite contractual requirements.

Threat and Vulnerability

- Threat: Fiber cut or carrier facility outage
- Vulnerability: Limited ability to enforce physical conduit diversity controlled by third-party carrier

Impact Assessment (select all that apply):

- ☒ Call Delivery
- ☐ Routing / Location Accuracy
- ☐ Latency / Performance
- ☒ Availability / Resilience
- ☐ Security / Data Protection

Likelihood Rating:

☐ Very Low ☐ Low ☒ Medium ☐ High ☐ Very High

Impact Rating:

☐ Very Low ☐ Low ☐ Medium ☒ High ☐ Critical

Overall Risk Rating:

☐ Low ☐ Medium ☒ High ☐ Critical

Associated Non-Compliance (if applicable):

- Requirement: Physical path diversity for ingress connectivity
- Reason: Last-mile facilities owned and controlled by third-party carrier
- Duration: Ongoing (structural limitation)

Risk Treatment Decision

- ☐ Reduce
- ☐ Avoid
- ☐ Transfer
- ☒ Accept

Justification for Risk Acceptance

The risk cannot be fully eliminated due to infrastructure constraints outside the Contractor's control. The residual risk is reduced to an acceptable level through layered compensating controls and does not prevent the Contractor from meeting NG911 service availability targets.



Appendix I - AT&T Business Continuity & Emergency Management



AT&T Business Continuity & Emergency Management

Introduction and Overview

This document outlines the strategies and procedures AT&T uses to plan, respond, and recover from events that may have potential impact to the AT&T Network. It provides an overview of AT&T's business continuity and emergency management programs, and:

- Cybersecurity
 - Disaster prevention/fire prevention and code compliance
 - Restoration priorities
 - U.S. Government interface and partnership
-

Business Continuity

Planning for and responding to crises is something that AT&T performs on a routine basis. The company has extensive experience responding to a wide variety of situations, from hurricanes to floods, to power outages, work stoppage contingency planning, and man-made disasters. AT&T has a global team of experts who practice responses to these types of scenarios several times each year.

AT&T has a team of industry-leading, certified, and experienced business continuity experts engaged in AT&T's internal business continuity management program. This team requires that key business processes have documented business continuity plans that are updated and exercised on a predetermined schedule.

Exercises are designed around specific scenarios to test the plans' viability and capability. Plan development and exercise execution are based on the concept of continuous improvement with the focus on maintaining business operations. As part of that planning, AT&T has performed an extensive corporate-wide risk assessment and has implemented incident response and contingency planning on several broad fronts.

In 2015, AT&T became the first telecom service provider to be certified under the new international Business Continuity Management standard (ISO 22301:2012) for the Department of Homeland Security Voluntary Private Sector Preparedness Program (PS-Prep™). The company completed its latest recertification in 2020. The PS-Prep™ recertification demonstrates AT&T's continued commitment to be equipped to resume business operations and product/service delivery to our customers in the vital hours and days after a disaster strikes. In the event of a disaster or emergency, we are prepared to quickly resume network traffic and field customer calls in the communities that we serve.



In addition to ISO 22301, AT&T's business continuity management program is also:

- Certified by the Cellular Telecommunications & Internet Association (CTIA) as part of its Business Continuity/Disaster Recovery Program since 2004
- Aligned with the Disaster Recovery Institute International (DRII) Professional Practices since 2004
- Aligned with the National Incident Management System (NIMS) as suggested by the U.S. Department of Homeland Security since 2004
- ISO 27001 certified for information security since 2010
- Aligned with the Business Continuity Institute (BCI) Good Practice Guidelines since 2011

Event Management Framework (EMF) & Emergency Management Operations (EMO)

The purpose of AT&T's Event Management Framework (EMF) is to provide an incident command structure that is 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. The EMF and the resulting EMO are an integral part of our business continuity program.

EMO Response Teams

The EMO structure establishes multiple response teams which are focused on the restoration of key business processes. These processes cover technology operations and infrastructure, customer sales and service capabilities, provisioning, maintenance, and other key areas.

The AT&T Global Emergency Management Center (GEMC) performs corporate activities during a significant event, including:

- Accounting for employees, personnel impact assessment, and work-ready status.
- Crisis communication and message management.
- Consolidated event status reports by business unit including the identification of assistance requirements, impacts on employees, customer service, and business operations.
- Corporate resources need assessment including the engagement of senior management, if required.
- Business unit emergency management activities during a significant event, including:
 - Accounting for employees
 - Recovery of business processes and operations
 - Interfacing with customers
 - Prioritization and movement of resources



- Network emergency management activities during a significant event, including:
 - Assessment of network damage
 - Prioritization of network response
 - Provide resources and internal status

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.

	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 Units, 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



Network Emergency Management Centers

AT&T Network Emergency Management Centers are designated either as an Emergency Operations Center (EOC) or as a Local Response Center (LRC). These centers are elements of AT&T's Network Emergency Management Plan and are activated during events when local damage assessment or network recovery exceeds business-as-usual (BAU) capabilities. Depending upon the severity of the event or the potential impact on the business, these centers may be required to operate 24-hours a day for the duration of an event.

Emergency Operations Centers

AT&T has Emergency Operations Centers (EOCs) with defined geographic responsibilities in the United States. The EOCs are strategically placed in AT&T's Central, East and West regions. There are numerous Local Response Centers supporting the United States.

The EOC members are key corporate organizational representatives who, during a widespread and/or multi-state disaster, work together to:

- establish restoration priorities
- make provisioning decisions
- provide overall event command and control

The response team members are empowered to develop strategies and to make decisions for the organizations they represent.

Local Response Centers

Local Response Centers (LRCs) are usually focused on a specific territory and will handle local emergency events that exceed BAU capabilities. They provide command and control for damage assessment and field restoration efforts. If the disaster or emergency is regional, or if multiple LRCs are activated, an EOC will be activated and will take overall control providing prioritization of AT&T resources across the impacted area.

Activation and Notification

The decision to activate an LRC or EOC is made by the AT&T Emergency Management Center (EMC) leadership team.

Alternate EOC and LRC Succession Planning

Each LRC and EOC has an emergency management center plan that allows an LRC or an EOC to transfer its work and responsibilities to a neighboring center. This provides for continuity of the command and control functions if a primary center's capabilities are compromised.

**EOC/LRC Communications**

Each EOC and LRC is equipped with redundant communications channels to guarantee continuity of communications to and from the EOC/LRC. These tools include wired communications from redundant central offices, wireless communications, satellite communications, and high frequency radios. AT&T is a NCS SHARES member.

EOC/LRC Emergency Power

Each EOC and LRC has emergency power sources that will automatically carry the center's critical load to ensure continuity of operations throughout the emergency event and to maintain EOC/LRC integrity.

EOC/LRC Security

Access to an EOC or LRC is allowed only to EOC/LRC team members and other EMO authorized personnel. Identification badges are issued upon entrance, worn by all personnel while in an EOC/LRC, and are surrendered to an EOC/LRC manager when personnel leave.

Global Technology Operations Center

The AT&T Global Technology Operations Center (GTOC) (formerly known as the Global Network Operations Center [GNOC]) monitors and proactively manages the entirety of the AT&T Network (domestic and global) twenty-four hours a day, seven days a week on a business-as-usual (BAU) basis. It is the overall command and control center for the AT&T Network. Any information about the AT&T Network that is communicated, internally or externally, is validated by the GTOC acting as the single "voice" of the network. The EOCs and LRCs provide event status information to the GTOC as part of the overall network assessment.

Exercises

Exercises are designed to validate various aspects of AT&T's disaster response capability and to identify any processes requiring further development or training. Each EOC/LRC is required to exercise annually. Critiques are conducted immediately following each exercise. Findings and recommendations are shared with the appropriate management teams and improvements are integrated into updated plans.

Types of EOC and LRC Exercises

Tabletop exercises are usually the smallest in scope and are the easiest to conduct. Participants are presented with a scenario and specific simulated emergency situations without time constraints. The exercises are designed to elicit constructive discussion among participants as they examine and resolve problems based on existing disaster response plans.

Functional exercises involve external "simulators" who transmit messages concerning simulated emergency events to the participants. Participants determine what action should be taken and convey decisions and directions back to the simulators.



Cybersecurity

The AT&T Chief Security Office (CSO) establishes policies and requirements, as well as comprehensive programs, to incorporate security into all facets of AT&T's computing and networking environments. The AT&T program implements security policies through a rich set of initiatives, processes, and procedures administered by the AT&T security organization worldwide. The program is certified to meet the ISO/IEC 27001:2005 Information Security Management Standard.

These program initiatives are executed on an ongoing basis by each region and are supported by global network security teams. The goals of the program are to protect AT&T's Global Network, service offerings, and all internal/customer information and resources as outlined below.

- Support technology services for global incident response, network-based security services, and managed security services, assist account teams with customer engagements, and perform applied security research for emerging services.
- Collaborate with Business Units to ensure that AT&T employs the highest standards in protecting both AT&T and customer's assets, evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices.
- Maintain a comprehensive global Information Security organization dedicated to the security of the AT&T global network and its service offerings. AT&T is committed to protecting its customers' and its own information and resources from unauthorized access, disclosure, corruption or disruption of service.

Disaster Prevention

AT&T uses many techniques to prevent disastrous events from impacting customer service. Many of these techniques are proprietary and are not described in this document. However, some portions of our disaster prevention program are either required by state/local codes or are federal/state mandates, including:

- Fire Prevention Program/Code Compliance
- Federal Interface Requirement
- Business Continuity Planning
- Pandemic Planning/Management
- Cybersecurity Programs

Fire Prevention Program/Code Compliance

The AT&T Fire Protection Program protects our employees from fire hazards and safeguards AT&T central office facilities from major service interruptions due to fire. The program establishes preventative measures, proper emergency response processes, and recovery mechanisms.



The AT&T Fire Safety Program and Emergency Plan (OP130) requires that each AT&T Network organization follow the rules, standards, codes of the National Electric Safety Code (NESC), National Fire Protection Association (NFPA), American National Safety Institute (ANSI), American Society for Testing and Materials (ASTM) and government safety laws, codes and mandates as they relate to fire protection and life safety.

Restoration Priorities

AT&T follows special procedures to restore service after an event causes widespread and/or severe damage or when other emergency conditions exist. Our ability to effectively restore service may require the prioritization of restoration efforts to support the emergency response.

When a city, county, or state has an order declaring a major disaster, an extraordinary situation or other emergency, the restoration and provisioning of telecommunication services will be done in accordance with the National Response Plan and the FCC's Telecommunications Service Priority (TSP) procedures.

AT&T begins coordinated restoration prioritization as soon as safety and working conditions permit. The period required for restoring service throughout an impacted area, state, or region will vary widely due to differences in the location and severity of an event, the complexity of our network infrastructure, central office equipment impacted, and the type of services provided in an area (e.g., broadband, wireless). In general, in the absence of any additional priority service requirements, service restoration will be met in the following sequence:

1. Telecommunications Service Priority (TSP): priority repair and installation of critical infrastructure services as required by the FCC's TSP program.
2. Public Safety: communications to essential community agencies (e.g., E-911, fire, police, hospitals) not already addressed by the TSP program.
3. Restoration of the full community and outside service using permanent and/or temporary facilities (whichever is the most expedient and practicable).

Telecommunications Service Priority

AT&T fully supports the FCC's Telecommunications Service Priority (TSP) program. It establishes the legal basis for service providers to act, when authorized by the FCC, on a priority basis in the provisioning and restoration of services supporting NSEP mission requirements. TSP is applicable to services such as dedicated private lines, access lines, dial-tone lines, high-capacity digital systems, and trunks between another carrier's switching or wireless nodes. Many activities to restore critical services will occur concurrently and may be influenced by the direction of government agencies.



Government Sponsored Priority Service

Government Emergency Telecommunications Service

Government Emergency Telecommunications Service (GETS) is a calling card program supporting wireline services that is available to federal, state, local, and other government-authorized National Security Emergency Preparedness (NSEP) critical users in the public or private sector. GETS calls receive priority treatment in the network and have a higher probability of completion when a disaster occurs or in situations that result in wireline network congestion.

Wireless Priority Service

Wireless Priority Service (WPS) is a dial program supporting wireless services that is available to federal, state, local, and other government-authorized NSEP critical users in the public or private sector. AT&T Mobility supports NSEP critical users' needs for priority wireless call processing. AT&T Mobility manages all WPS related operations and administration in accordance with National Communication System guidelines. WPS capability can be enhanced when used with GETS priority treatment.

U.S. Government Interface and Partnership

AT&T has full-time U.S. National Coordinating Center (NCC) representation for the National Security Emergency Preparedness (NSEP) programs. As the primary interface for the enterprise, the representative is involved in matters associated with national security and emergency preparedness response. AT&T NSEP/NCC representatives work regularly with the:

- National Communications System (NCS)
- Federal Emergency Management Agency (FEMA)
- Federal Department of Homeland Security (DHS)
- DHS National Cybersecurity and Communications Integration Center (NCCIC) Unified Coordination Group (UCG)

AT&T maintains partnerships with federal agencies as well as with many state, county and local governments, which serve to reinforce and strengthen AT&T's emergency preparedness programs. This strategy includes information sharing, mutual exercises, and often leads to joint methods of understanding (MOUs) and Disaster Recovery Plan (DRP) interdependencies with government and other critical infrastructure segments.



Appendix J - AT&T ESInet Call Flow Scenarios



AT&T ESInet Call Flow Scenarios

Contents

1.0	Overview.....	1
1.1	Version History	1
1.2	Definitions, Acronyms, and Abbreviations	1
2.0	Basic Structure for Call Flows.....	4
2.1	Back-to-Back User Agent Control Summary	4
2.2	CAMA PSAP and Nominal Call Flow	6
3.0	IP PSAP Call Flows.....	38
3.1	Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer)	38
3.2	Call Flow A2—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Blind Call Transfer).....	48
3.3	Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference).....	52
4.0	Loss of RTP Call Flow	79
4.1	Call Flow B: Generic ‘Loss of RTP’ Call Flow	79
4.2	Section 1.2.3—Loss of RTP—Single LOR Re-Presentation—Sunny Day	80
5.0	Telephone Service Provider Interactions Call Flows	91
5.1	ISDN/PRI Signaling to AT&T Routing Network.....	92
5.2	CAMA Signaling to AT&T Routing Network	93

List of Figures

Figure 1:	Back-to-Back User Agent Call Control—Ringing State	4
Figure 2:	Back-to-Back User Agent Call Control—Answered State.....	5
Figure 3:	“Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic 1 of 3).....	6
Figure 4:	“Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic 2 of 3).....	8
Figure 5:	“Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic-3 of 3).....	10
Figure 6:	Call Flow 1 – SS7 End Office ‘Trunk Only Routing’ (TOR) Call to Fast Busy Tone (Graphic 1 of 2).....	12
Figure 7:	Call Flow 1 – SS7 End Office ‘Trunk Only Routing’ (TOR) Call to Fast Busy Tone (Graphic 2 of 2).....	14
Figure 8:	Call Flow 2—DS1 CAMA End Office Trunk Only Routing (TOR) SS7 Handoff to Foreign Selective Router (Graphic 1 of 2)	16
Figure 9:	Call Flow 2—DS1 CAMA End Office Trunk Only Routing (TOR) SS7 Handoff to Foreign Selective Router (Graphic 2 of 2)	18
Figure 10:	Call Flow 4—VSP Call from AT&T V9-1-1 Network - Selective Routing – Attempted Termination to ECMC PSAP #1, then ECMC PSAP #2 (both in abandon) Termination to ECMC PSAP #3 (10 digit EMF).....	20
Figure 11:	Call Flow 5—SS7 NCAS A3 Origination-Selective Routing—Termination to ECMC PSAP 8 Digit—Selective Bridge to another ECMC PSAP (EMF) (Graphic 1 of 2).....	23

Figure 12: Call Flow 5—SS7 NCAS A3 Origination-Selective Routing—Termination to ECMC PSAP 8 Digit—Selective Bridge to another ECMC PSAP (EMF) (Graphic 2 of 2).....	25
Figure 13: Call Flow 13—MSC (SS7– NCAS A1) Caller Abandons, Deliver ANI to ECMC PSAP (EMF).....	30
Figure 14: Call Flow 17—Test Call—PSAP Trunk Test to ECMC PSAP Trunk Member ...	32
Figure 15: Call Flow 18—Test Call—PSAP Call-Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 1 of 3)	34
Figure 16: Call Flow 18—Test Call—PSAP Call Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 2 of 3)	36
Figure 17: Call Flow 18—Test Call—PSAP Call-Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 3 of 3)	37
Figure 18: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 1 of 5).....	39
Figure 19: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 2 of 5).....	41
Figure 20: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 3 of 5).....	42
Figure 21: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 4 of 5).....	44
Figure 22: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 5 of 5).....	46
Figure 23: Call Flow A2—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Blind Call Transfer) (Graphic 1 of 2).....	48
Figure 24: Call Flow A2—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Blind Call Transfer) (Graphic 2 of 2).....	50
Figure 25: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 1 of 4).....	52
Figure 26: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 2 of 4).....	53
Figure 27: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 3 of 4).....	54
Figure 28: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 4 of 4).....	55
Figure 29: Call Flow B1—SS7 Ingress to ECR and Core (Graphic1 of 4)	56
Figure 30: Call Flow B2—SS7 Ingress to ECR and Core (Continued Graphic 2 of 4).....	57
Figure 31: Call Flow B3—SS7 Ingress to ECR and Core (Continued Graphic 3 of 4).....	58
Figure 32: Call Flow B4—SS7 Ingress to ECR and Core (Continued Graphic 4 of 4).....	59
Figure 33: Call Flow B5—Series 2—Compact Format—SS7 to TDM PSAP (Graphic 1 of 2).....	60
Figure 34: Call Flow B6—Series 2—Compact Format—SS7 to TDM PSAP (Graphic 2 of 2).....	61
Figure 35: Call Flow B7 to B19—Bring Ingress Caller onto MS.....	62
Figure 36: Call Flow B7 to B19—Interaction with i3 Components to Build PIDF/LO Plus Additional Data and Routing—SS7 to i3 PSAP.....	62
Figure 37: Call Flow B7 to B19—Send to T-ESRP	63
Figure 38: Call Flow B7 to B19—Call Teardown	63
Figure 39: Call Flow B7 to B19—Alternate Routing to an i3 PSAP	64
Figure 40: Call Flow B7 to B19—Alternate Routing to a TDM PSAP	65
Figure 41: Call Flow B7 to B19—Route to Fast Busy—Destination Unavailable.....	65
Figure 42: Call Flow B7 to B19—Abandonment Routing to an i3 PSAP	66
Figure 43: Call Flow B7 to B19—Abandonment Routing to a TDM PSAP	67
Figure 44: Call Flow B7 to B19—LIS Failure—Default Routing to an i3 PSAP	68

Figure 45: Call Flow B7 to B19—ECRF Failure—Routing to an i3 PSAP	69
Figure 46: Call Flow B7 to B19—CIDB Failure—Routing to an i3 PSAP.....	70
Figure 47: Call Flow B7 to B19—TDM PSAP Alternate Routes to an i3 PSAP.....	71
Figure 48: Generic “Loss of RTP” Call Flow Summary.....	79
Figure 49: Detection of the LOR Event Prompts the BYE (Graphic 1 of 3).....	80
Figure 50: Detection of the LOR Event Prompts the BYE (Graphic 2 of 3).....	81
Figure 51: Detection of the LOR Event Prompts the BYE (Graphic 3 of 3).....	81
Figure 52: SS7 Signaling to Access AT&T Routing Network.....	91
Figure 53: ISDN/PRI Signaling to Access AT&T Routing Network	93
Figure 54: CAMA Signaling to Access AT&T Routing Network.....	94

List of Tables

Table 1: Version History.....	1
Table 2: Definitions, Acronyms, and Abbreviations.....	1

1.0 Overview

This document describes a subset of the Emergency Call Routing Service (ECRS) call flows. The call flows in the first section of this document show the messages and parameters which flow between the major Emergency Call Management Complex (ECMC) components for 9-1-1 calls to an analog PSAP (that is, a PSAP using 2 wire analog loops conforming to Telcordia GR-350-CORE “E911 Public Safety Answering Point: Interface Between a 1/1AESS Switch and Customer Premises Equipment” and GR-2953-CORE “Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface”). These call flows are illustrative, not comprehensive.

1.1 Version History

A version history of document changes is provided in Table 1.

Table 1: Version History

Date	Changes
08/21/2015	Initial Release
10/16/2015	- Added Section 1.1 Table 1 Version History - Updated Table 2 Definitions, Acronyms, and Abbreviations - Updated Section 2.2.7 - Updated Call Flow A - Added Call Flow A2 - Added Call Flow A3
05/2020	Added IP ingress call flows

1.2 Definitions, Acronyms, and Abbreviations

Table 2: Definitions, Acronyms, and Abbreviations

Term	Definition
ACM	Address Complete Message—An SS7 message indicating that the IAM is acceptable, and that routing is proceeding
ANI	Automatic Number Identification—Typically the Calling Party Number, or alternatively the Charge Number
ANI Failure	An ANI without the expected number of digits
AUS	Application Unique String
CAMA	Centralized Automatic Message Accounting—Historical MF-based

Term	Definition
	signaling method
CIDB	Call Information Database
CPE	Customer Premise Equipment—Equipment not owned by a service provider, but owned by our customer (the PSAP), and located at the PSAP location
CPG	Call ProGress Message—An SS7 message indicating some event during the setup of a call
DNS	Domain Name Server/Service/System
DS1	Digital Signal Level 1—A Digital facility at 1.544 Mb/s (could be carried on a higher order digital facility, such as DS3)
ECR	Emergency Call Routing Application
ECRF	Emergency Call Routing Function
ECRS	Emergency Call Routing Service
ECMC	Emergency Call Management Complex—A site, or collection of elements that contain the core network elements and functionality to replace a given legacy selective router.
ESCO	Emergency Services Central Office
ESN	Emergency Services Number—Used to derive a Route List
ESRD	Emergency Service Routing Digits—pANI indicating location used for CAS/HCAS wireless calls
ESRK	Emergency Service Routing Digits—pANI indicating location used for NCAS wireless calls
ESRP	Emergency Service Routing Protocol
ESSID	Emergency Services Switching ID—Equivalent to a Selective Router
IAM	Initial Address Message—An SS7 call setup message
IP	Internet Protocol
IPM	Interruptions Per Minute—Examples are Busy tone = 60 IPM, and Re-Order/Fast Busy = 120 IPM
ITG	Incoming Trunk Group

Term	Definition
LNG	Legacy Network Gateway
LOST	Location to Service Translation
LPG	Legacy PSAP Gateway
MF	Multi-Frequency—Trunk-side version of a dual tone signaling method
MGC	Media Gateway Controller
MS	Media Server
OBCI	Optional Backward Call Indicator—An SS7 parameter that can be in many SS7 messages, including ACMs and CPGs. The OBCI includes a ‘Inband Information Indicator’ parameter in these call flows, which sets up a one-way talk path in the backward direction to allow the calling party to hear tones, announcements, etc.
POI	Point of Interface
POST	An HTTP request method which asks a server to accept and store data enclosed in the message body.
PSAP	Public Safety Answering Position—Location of the call takers who answer the 9-1-1 call
RL	Route List—List of up to 10 destinations
RTP	Real-time Transport Protocol
SBC	Session Border Controller—IP component that protects the trusted AT&T IP infrastructure from non-trusted IP networks
SIP	Session Initiation Protocol
SR	Selective Router
SRDB	Selective Router DataBase
SS7	Signaling System 7 (ANSI)
URI	Uniform Resource Identifier

2.0 Basic Structure for Call Flows

2.1 Back-to-Back User Agent Control Summary

The ECR operates as a SIP Back-to-Back User Agent (B2BUA) for most of the call flows. **Error! Reference source not found.** shows the ECR in three logical parts, as the ECR is typically connected to the Media Server via three legs.

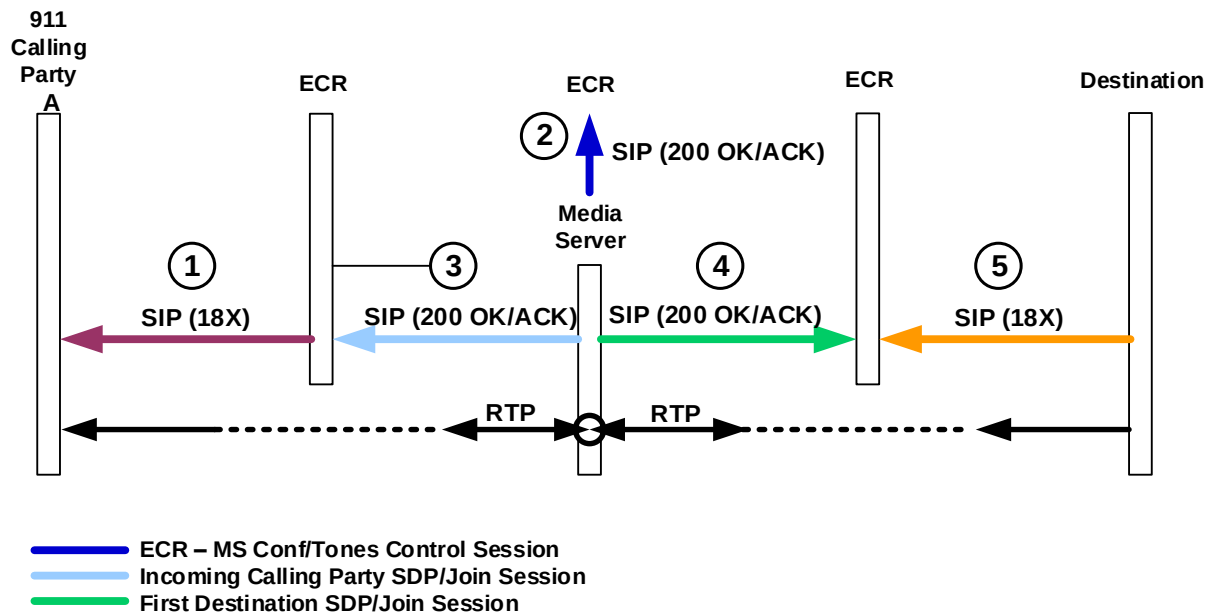


Figure 1: Back-to-Back User Agent Call Control—Ringing State

- Leg #1 is the SIP signaling for the ingress leg between the 9-1-1 caller and the ECR.
- Leg #2 is the SIP signaling for the control channel between the ECR and the Media Server.
- Leg #3 is the SIP signaling for the ingress leg between the ECR and the Media Server.
- Leg #4 is the SIP signaling for the egress leg between ECR and the Media Server.
- Leg #5 is the SIP signaling for the egress leg between the ECR and the destination (e.g., PSAP).

The picture is showing a “snap-shot” of a typical scenario of a call flow during the ringing state, where the calling party is hearing audible ringing from the called party destination via “early media”. Two items are worth noting:

- The end points (i.e., 9-1-1 Calling Party and Destination) are in an 18X state, awaiting a final response. The early media requested in the call setup ensures a one-way talk path from the destination PSAP to the Calling Party.
- At the same time, the Media Server in the middle of the diagram is in a “connected” state, as the signaling has progressed through a 200 OK and the ACK for the initial INVITE. The Media Server is operating now with two-way talk path setup.

This configuration allows the answer signal from the destination to bypass the MS altogether, and to be relayed by the ECR directly to the Calling Party, as shown in

Figure 2 on Page 5.

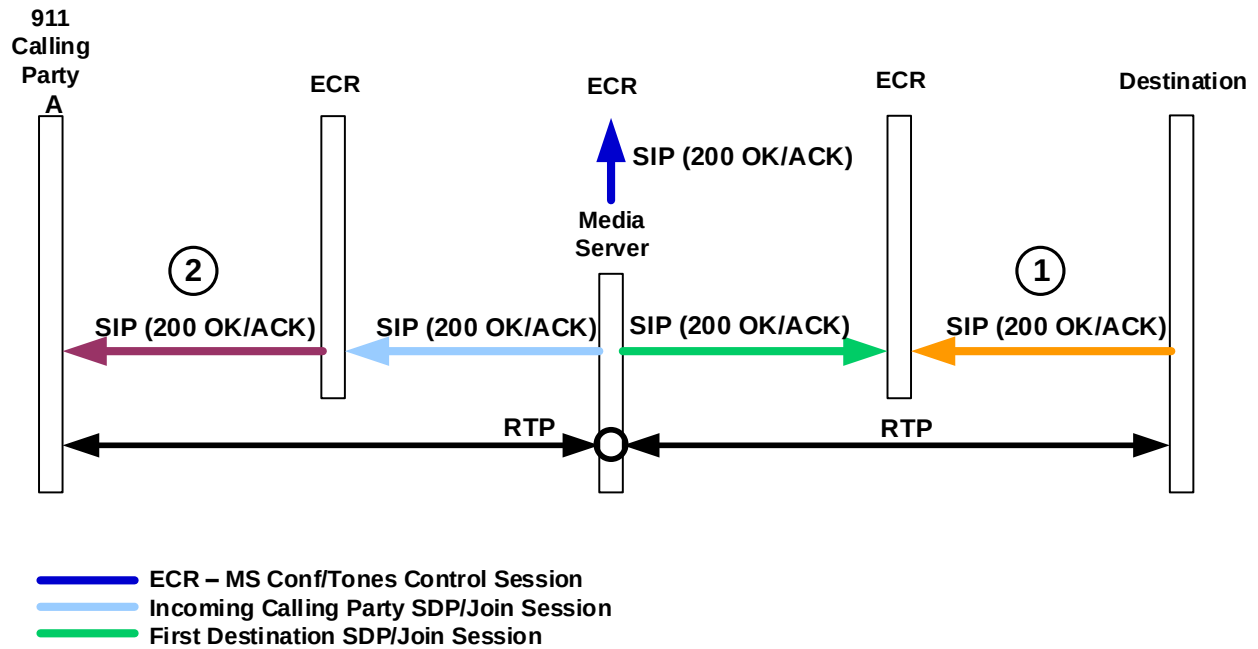
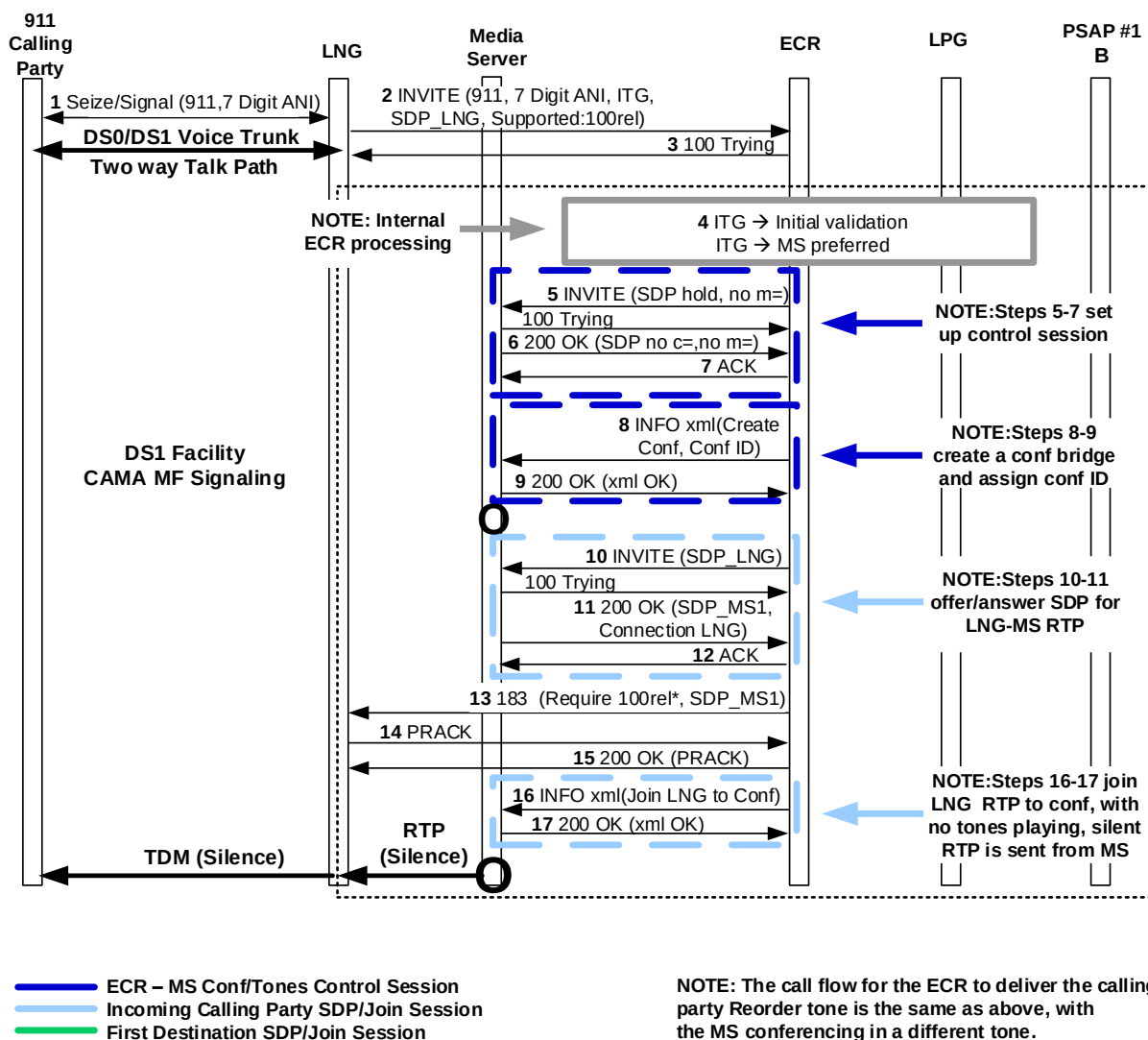


Figure 2: Back-to-Back User Agent Call Control—Answered State

2.2 CAMA PSAP and Nominal Call Flow

2.2.1 Happy Day Call Flow—Digital CAMA EO Trunk Only Routing (TOR) to 10-Digit EMF ECMC PSAP

Figure 3, below, depicts the call flow for a common 9-1-1 emergency call originating from an End Office and using CAMA signaling over a DS1 to ingress into ESRP. As part of the call processing, this call shows Trunk Only Routing being used (instead of Selective Routing), and termination of the call is to a PSAP using 10-digit EMF signaling.



Call Flow Continued In Next Figure

Figure 3: “Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic 1 of 3)

1. Caller dials 9-1-1 off an End Office. The EO signals the call to the ECMC LNG via CAMA MF signaling on a DS1 facility, with 9-1-1 as Called Party Number, and the originators 7 digit ANI as the Calling Party Number. The NPA of the ANI is provisioned on both ends of the trunk, but not transmitted via MF signaling. CAMA signaling for interoffice trunks does not have answer supervision tied to the far end answer state, but uses the supervision normally associated with answer to instead signal the originating end of the trunk to send the ANI MF digits. This causes the trunk to be open with two way talk path immediately after the ANI has been sent.
2. LNG sends SIP INVITE to the near ECR site (i.e., Load Balancers and ECRs). This INVITE includes 9-1-1 as the Called Number, the ANI as the Calling Number, the original Charge Number, Incoming Trunk Group (ITG) identifier for this particular SS7 trunk group, and the SDP offer for the LNG (labeled SDP_LNG in the ladder diagram).
3. ECR responds to the LNG INVITE with a 100 Trying.
4. ECR performs the following processing based on the parameters of this SIP INVITE:
 - A. The ECR performs initial validation on the ITG, to ensure a database match, etc.
 - B. The ITG also indicates the preferred MS.
5. The ECR sends an INVITE to the MS to initiate a control channel. This INVITE has an SDP IP address of 0.0.0.0 (i.e., hold), an a=send only line, and no media line passing the port number. The MS responds to INVITE with a 100 Trying.
6. The MS then sends the ECR a 200 OK, with SDP, but without a control or media line.
7. ECR finishes the control session setup by sending an ACK back to the MS.
8. On the above control session, the ECR sends XML based control instructions (MOML/MSML) in an INFO message requesting the MS to set up a bridge. The ECR assigns the conference ID.
9. MS responds to the INFO with a 200 OK.
10. On a new SIP session, (as a third party controller, acting on behalf of the LNG), the ECR sends an INVITE to the MS, with an SDP offer indicating RTP setup to the LNG SDP address and port.
11. The MS responds with a 100 Trying and a 200 OK. The 200 OK includes the SDP answer indicating the MS SDP RTP port (labeled SDP_MS1 in the ladder diagram).
12. ECR finishes this step by sending an ACK back to the MS.
13. ECR responds to step 2) INVITE by sending a 183 Session Progress to the LNG. This 183 Session Progress contains the SDP answer to the SDP offer in the 2) INVITE, indicating the MS port providing RTP. To ensure PRACK confirmation of the 183, a Require 100rel is included in the 183, to ensure the provisional SIP signaling from end-to-end to support early media. (Early media is 'pre-answer' talk path, and we are concerned that the calling party can hear the audible ringing from the PSAP at the very beginning of the call.)
14. LNG acknowledges the 183 by sending a provisional ACK, or PRACK, to the ECR.
15. ECR responds to PRACK with a 200 OK.
16. On the incoming calling party session, the ECR sends an INFO to the MS, to join the MS RTP connection ID signaled in step 11 to the MS conference ID assigned back in step 8.
17. The MS responds with a 200 OK 'XML OK'.

At this point in the call, the calling party will be temporarily connected to a quiet conference. Audible ringing will occur shortly, either generated by the MS, from a PSTN switch (EO or 9-1-1 tandem), or from PSAP CPE.

continued

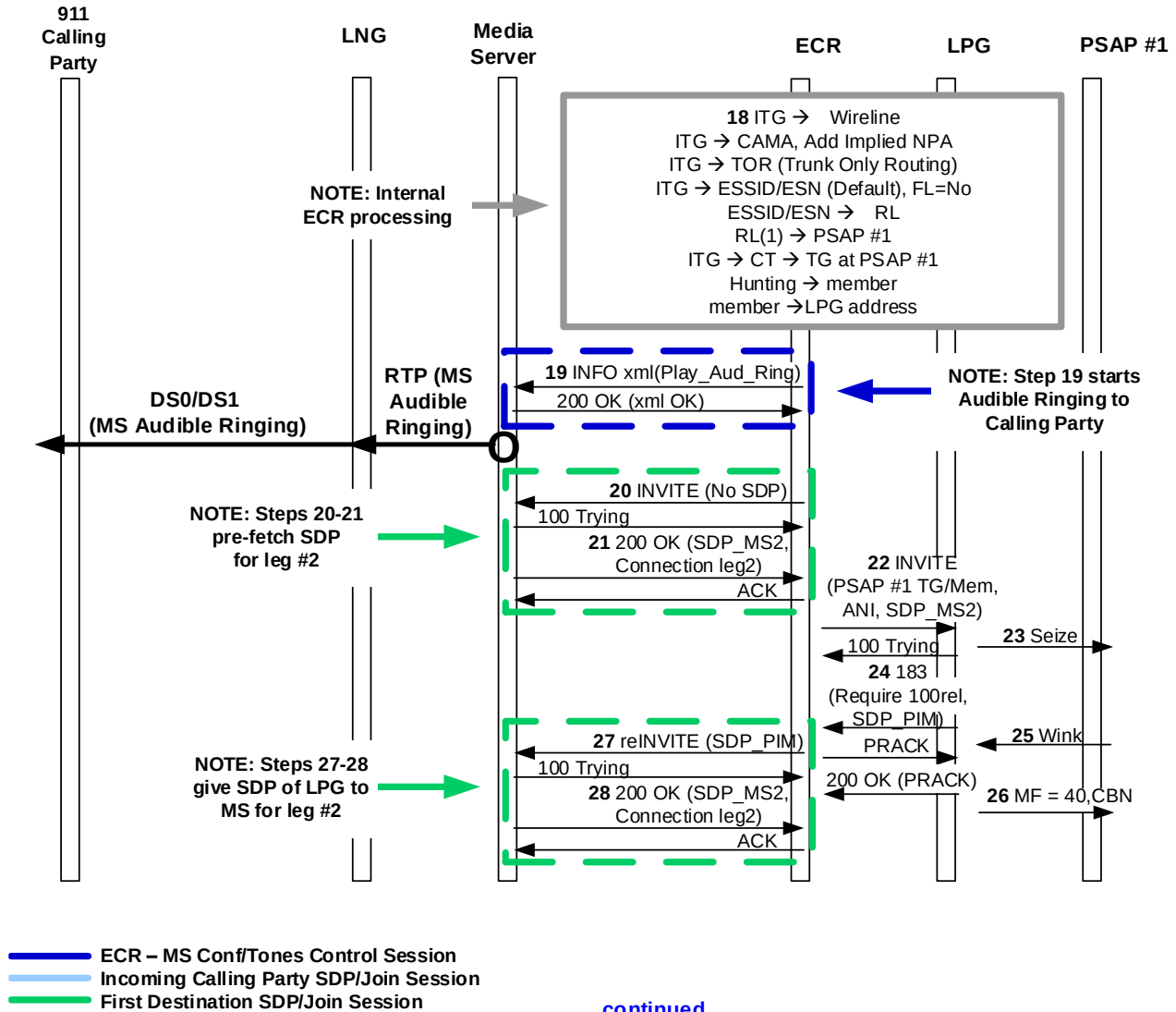


Figure 4: “Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic 2 of 3)

18. ECR finishes the processing of the parameters of the SIP INVITE from Step 2:
 - A. The ITG will have a signaling attribute provisioned, indicating that this is a wireline call.
 - B. The ITG will also indicate CAMA signaling, including the implied NPA for this trunk.
 - C. The ITG will have a call handling method provisioned, in this case, Trunk Only Routing.
 - D. The ITG will also have a provisioned ESSID and ESN, and whether Flashing is Yes or No for this ESSID/ESN.

- E. The ESSID and ESN are used to lookup the Route List (RL), which has as its first entry, the destination of PSAP #1.
 - F. The ITG will have a Call Type provisioned, which will be used to derive the Trunk Group at PSAP #1.
 - G. The ECR hunts through the trunk group, finds an idle member, and derives the LPG address.
19. The ECR (knowing that the call is to be routed to an ESRP PSAP) sends an INFO to the MS within the control session requesting that audible ringing tones be mixed into the conference so that they are heard by the calling party. The MS responds with a 200 OK. At this point the calling party is hearing audible ringing tones over the early media path established earlier.
 20. Anticipating an INVITE to the PTM (step 22 below), the ECR goes to the MS to 'pre-fetch' the SDP information. The ECR does this by sending an INVITE with no SDP to the MS on a new session, called the 'First Destination SDP/Join Session' in the diagrams. The MS responds with a 100 Trying.
 21. The MS then responds with a 200 OK, which includes the SDP information (labeled SDP_MS2) as well as the connection ID for this RTP stream (labeled Connection leg2).
 22. The ECR sends the INVITE to the LPG hosting the selected PTM. This INVITE uses the Request URI/TO: and FROM: formats. For this call, the Request URI and TO: have the format of <sip:BLDRCOPDPM101@10.108.30.10:5060>, where BLDRCOPDPM1 is the LPG name, followed by 01 which is the PTM number, @LPG IP or DNS name. The FROM: has the format From: <sip:**II+10 Digit ANI**@10.108.30.10:5060>;tag. . ., where the II digits are 40 for our call (40 for a normal call, no flashing – 44 for flashing) and the 10 digit ANI to be signaled to the PSAP. The LPG responds with 100 Trying.
 23. As the ECR sets up the connection to the LPG in step #22 above, the LPG will signal the PSAP via loop-start supervisory signaling. The first signal the ECR provides is the loop start seizure, to indicate off-hook to the PSAP.
 24. The LPG returns a 183 Session Progress to the ECR. The 183 includes a REQUIRE: 100rel (to ensure PRACKs and early media) and also includes the SDP of the LPG (SDP_LPG). [The ECR PRACKs this 183, and the LPG 200 OKs the PRACK.]
 25. The PSAP CPE winks back to the LPG to indicate that the CPE is ready to receive the MF digits.
 26. The LPG signals out the II digits '40' (i.e., normal, or not flashing) and the 10 digit CBN via MF to the PSAP CPE.
 27. The ECR, on the first destination session, sends a reINVITE to the MS which includes the SDP_LPG received in the 183 of step 24.
 28. The MS responds with a 200 OK which repeats the SDP_MS2 and Connection leg2 ID of step 8.

continued

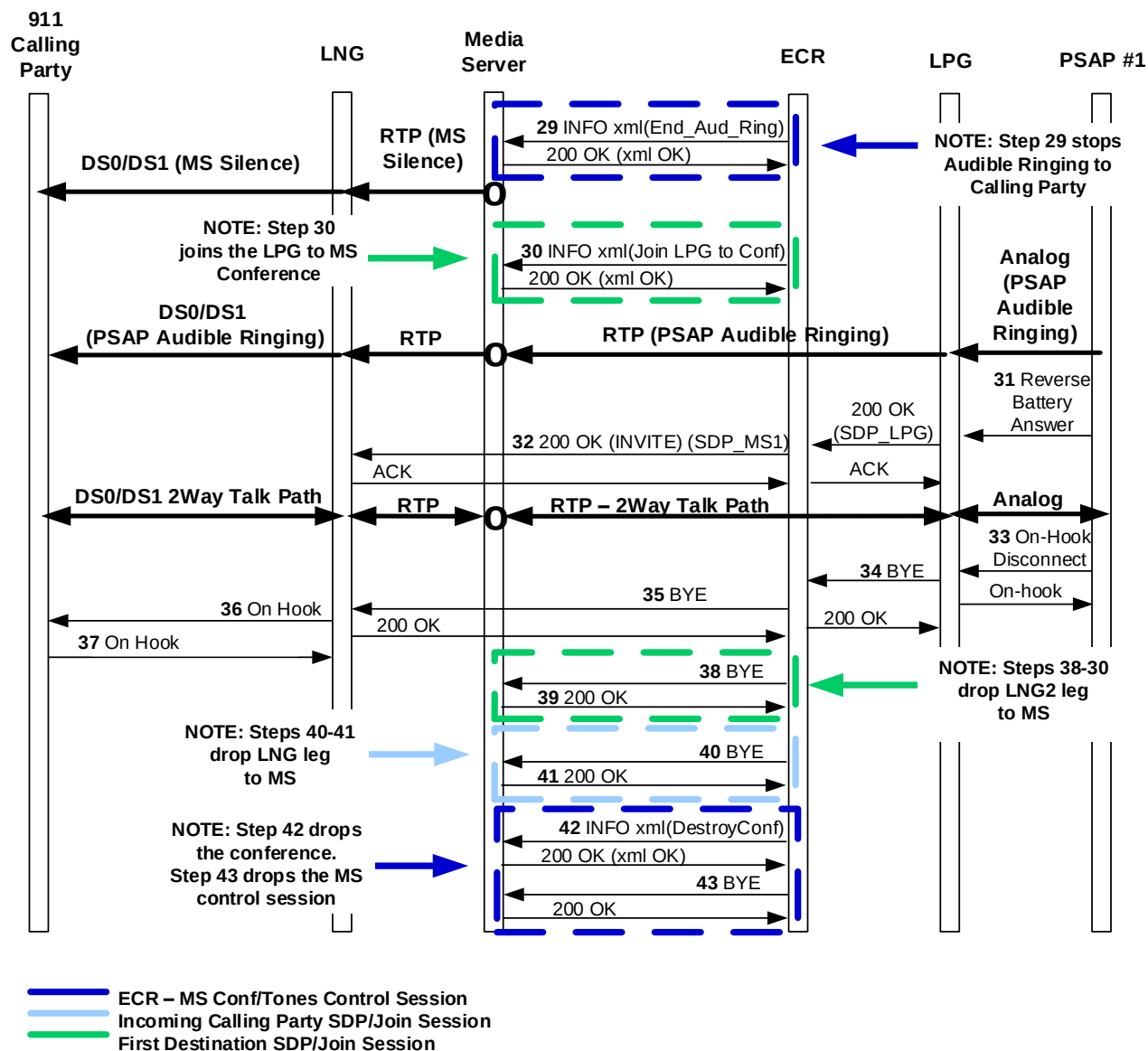


Figure 5: “Happy Day” Call Flow—Digital CAMA EO Trunk-Only Routing (TOR) Call to 10-Digit EMF ECMC PSAP (Graphic-3 of 3)

29. Within the control session, the ECR sends an INFO requesting that Audible Ringing be turned off. The MS responds with a 200 OK confirming.
30. Within the first destination SDP/Join session, the ECR requests the MS to join the LPG leg to the conference. The MS responds with a 200 OK.

At this point, a talk path is established from the PSAP to the calling party. When the PSAP CPE starts generating audible ringing, the 9-1-1 calling party will hear it.
31. The PSAP call taker answers the call by reversing battery on tip and ring. The LPG signals this with a 200 OK (to the step 22 INVITE) to the ECR, repeating the SDP_LPG. And the ECR ACKs the LPG INVITE session.
32. The ECR passes this answer signal to the calling party in the form of a 200 OK to the LNG, repeating the SDP_MS1 in step 13 when the ECR sent a 183 to the LNG. The LNG ACKs the INVITE session.
33. The PSAP #1 call taker disconnects, or goes On-Hook, which is signaled (by the inverting of reverse battery back to normal battery) to the LPG. The LPG also goes On-Hook, which returns this PTM to idle.
34. The LPG tears down the SIP signaling to the ECR with a BYE. The ECR responds with a 200 OK.
35. The ECR tears down the SIP signaling to the LNG with a BYE. The LNG responds with a 200 OK.
36. The LNG tears down the call to the EO by going 'on-hook' via A/B signaling on the DS1.
37. The originating EO returns the on-hook. After guard timing, this trunk is idle.
38. The ECR starts to clean up the MS conference by sending a BYE on the first destination session.
39. The MS responds with a 200 OK, and this first destination session is dropped.
40. The ECR then sends a BYE to the MS on the incoming calling party session.
41. The MS responds with a 200 OK, and this session is dropped.
42. The ECR then instructs the MS to destroy the call conference, on the control session. The ECR waits for the MS to respond with a 200 OK indicating the conference was destroyed.
43. The ECR then sends a BYE to the MS on the control session, which the MS responds to with a 200 OK and this session is dropped.

2.2.2 Call Flow 1 – SS7 End Office ‘Trunk Only Routing’ (TOR) Call to Fast Busy Tone

The following call flow is a 9-1-1 emergency call originating from an End Office via SS7. This call shows Trunk Only Routing, and termination of the call to Reorder/Fast Busy (120 IPM) after it is found that all the primary PSAP trunks are busy with emergency calls (and no alternate routing in effect).

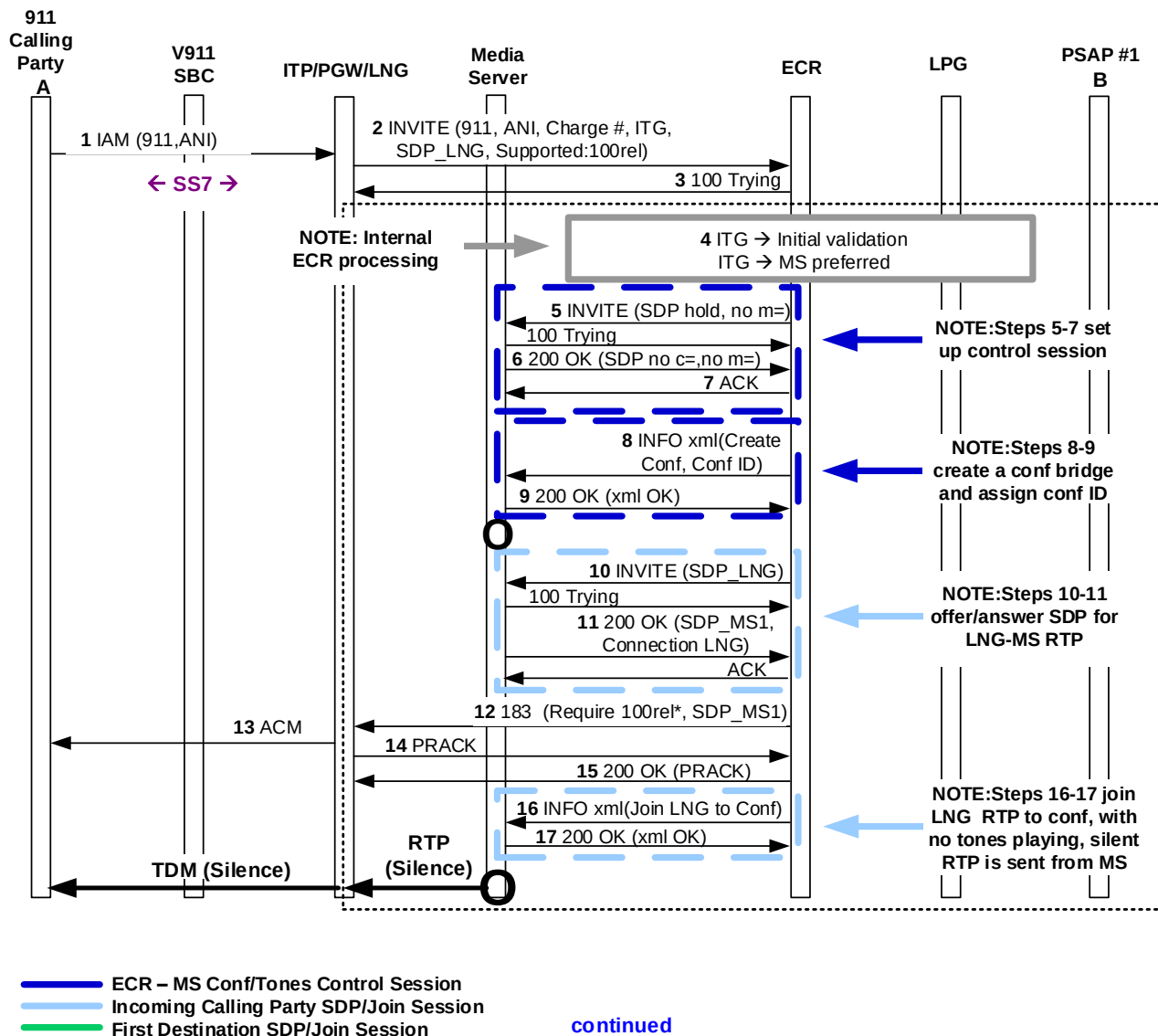


Figure 6: Call Flow 1 – SS7 End Office ‘Trunk Only Routing’ (TOR) Call to Fast Busy Tone (Graphic 1 of 2)

1. Caller dials 9-1-1 off an End Office. The EO signals the call to the ECMC SGW via SS7 Initial Address Message (IAM), with 9-1-1 as Called Party Number, the originators TN as the Calling Party Number, and for this example, a different 10 digit number (i.e., not the Calling Party Number) as the Charge Number.
2. LNG sends a SIP-GTD INVITE to the ECR site (i.e., Load Balancers and ECRs) which includes the existing SS7 ISUP parameters. This INVITE includes 9-1-1 as the Called Number, the ANI as the Calling Number, the original Charge Number, the Incoming Trunk Group (ITG) identifier for the particular SS7 trunk group, and the SDP offer for the LNG (labeled SDP_LNG in the ladder diagram).
3. ECR responds to the PGW INVITE with a 100 Trying.
4. ECR performs the following processing based on the parameters of this SIP-GTD INVITE:
 - A. The ECR performs initial validation on the ITG, to ensure a database match, etc.
 - B. The ITG also indicates the preferred MS.
5. The ECR sends an INVITE to the MS to initiate a control channel. This INVITE has an SDP IP address of 0.0.0.0 (i.e., hold), a=sendonly line, and no media line passing the port number. The MS responds to INVITE with a 100 Trying.
6. The MS then sends the ECR a 200 OK, with SDP but without a control or media line.
7. ECR finishes the control session setup by sending an ACK back to the MS.
8. On the above control session, the ECR sends XML based control instructions (MOML/MSML) in an INFO message requesting the MS to set up a bridge. The ECR assigns the conference ID.
9. MS responds to the INFO with a 200 OK.
10. On a new SIP session, (as a third party controller, acting on behalf of the PGW), the ECR sends an INVITE to the MS, with an SDP offer indicating RTP setup to the LNG SDP address and port.
11. The MS responds with a 100 Trying and a 200 OK. The 200 OK includes the SDP answer indicating the MS SDP RTP port (labeled SDP_MS1 in the ladder diagram). ECR finishes this step by sending an ACK back to the MS.
12. ECR responds to step 2) INVITE by sending a 183 Session Progress to the PGW. This 183 Session Progress contains the SDP answer to the SDP offer in the 2) INVITE, indicating the MS port providing RTP. Typically, to ensure PRACK confirmation of the 183, a Require 100rel would be included in the 183, to ensure the provisional SIP signaling from end-to-end to support early media. (Early media is 'pre-answer' talk path, and we are concerned that the calling party can hear the audible ringing from the PSAP later in the call.)
13. PGW sends Address Complete Message (ACM) to EO, indicating yes in the 'In-band Information Indicator' in the Optional Backward Call Indicator (OBCI) and opening up the talk path back to the 9-1-1 caller to hear the audible ringing soon to be set up.
14. As configured, the PGW acknowledges the 183 with a PRACK.
15. ECR responds to PRACK with a 200 OK.
16. On the incoming calling party session, the ECR sends an INFO to the MS, to join the MS RTP connection ID signaled in step 11 to the MS conference ID assigned back in step 8.
17. The MS responds with a 200 OK 'XML OK'.

continued

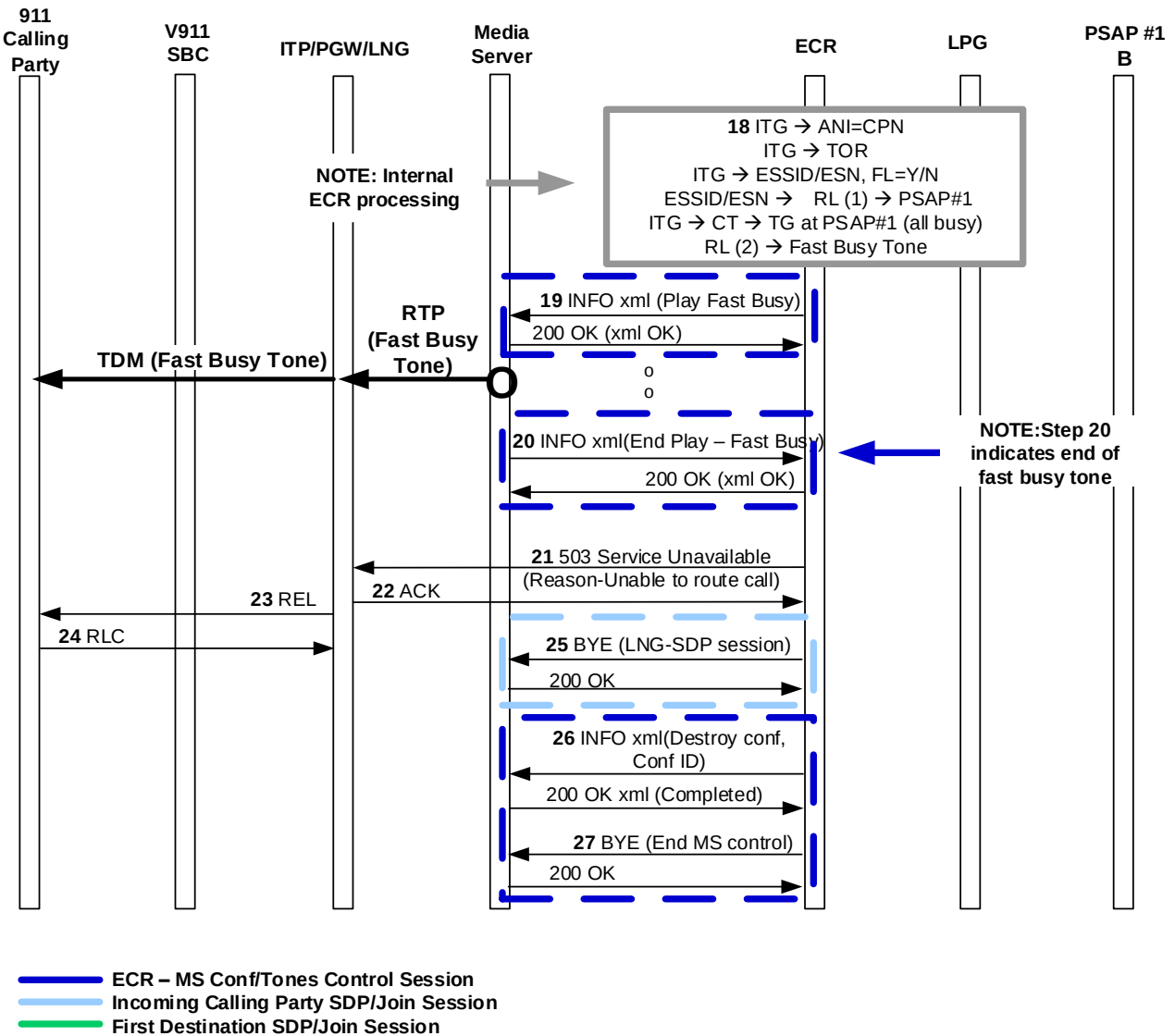


Figure 7: Call Flow 1 – SS7 End Office ‘Trunk Only Routing’ (TOR) Call to Fast Busy Tone (Graphic 2 of 2)

18. ECR finishes the processing of the parameters of the SIP INVITE from Step 2:

- The ITG will have a signaling attribute provisioned, indicating that the number to use as ANI is in the Calling Party Parameter, (and not in the Charge Parameter).
- The ITG will have a call handling method provisioned, in this case, Trunk Only Routing.
- The ITG will also have a provisioned ESSID and ESN, and whether Flashing is Yes or No for this ESSID/ESN.
- The ESSID and ESN are used to lookup the Route List (RL), which has as its first entry, the destination of PSAP #1.

- E. The ITG will have a Call Type provisioned, which will be used to derive the Trunk Group at PSAP #1. For this call, all members of this trunk group are busy.
 - F. The ECR alternate routes to the second entry of the Route List, which is Reorder Tone.
19. The ECR sends an INFO to the MS within the control session requesting that 120 IPM fast busy tones be mixed into the conference so that they are heard by the calling party. The MS responds with a 200 OK. At this point the calling party is hearing fast busy tones over the early media path established earlier.
 20. When the MS is done playing the requested tones for the duration specified in step 19, it sends an INFO to the ECR.
 21. The ECR sends a 503 Service Unavailable (Q.850 cause=16, TRDO cause=20 “Unable to Route call”) to the PGW to begin tearing down the original INVITE session.
 22. The PGW responds with an ACK to close the original INVITE transaction of step 2.
 23. The PGW sends a RELEASE (REL) SS7 message to the EO to ask to drop the SS7 trunk.
 24. The EO responds with a RELEASE COMPLETE (RLC) to the PGW to drop the SS7 trunk.
 25. The ECR sends a BYE to the MS to drop the LNG RTP leg into the MS. This BYE is within the incoming Calling Party SDP/Join session between the ECR and the MS. The MS responds with a 200 OK to the BYE.
 26. On the ECR-MS control session, the ECR sends an INFO message with XML data telling the MS to Destroy the conference, giving the Conference ID of this call. The MS responds to the INFO with a 200 OK indicating that the XML script was completed.
 27. The ECR sends a BYE to close the MS control session. The MS responds to the BYE with a 200 OK. The call is entirely cleaned up at this point.

Note that there is no 200 OK from the ECR in response to the original PGW INVITE in step 2. There is no need to answer the call if we are only providing call treatment tones to the calling party.

2.2.3 Call Flow 2—DS1 CAMA End Office Trunk Only Routing (TOR) SS7 Handoff to Foreign Selective Router

The following call flow is a 9-1-1 emergency call originating from an End Office via CAMA MF signaling on a DS1 facility. This call is Trunk Only Routed (TOR), with the first destination being a Foreign PSAP TN, requiring routing off the ECMC to a legacy Selective Router.

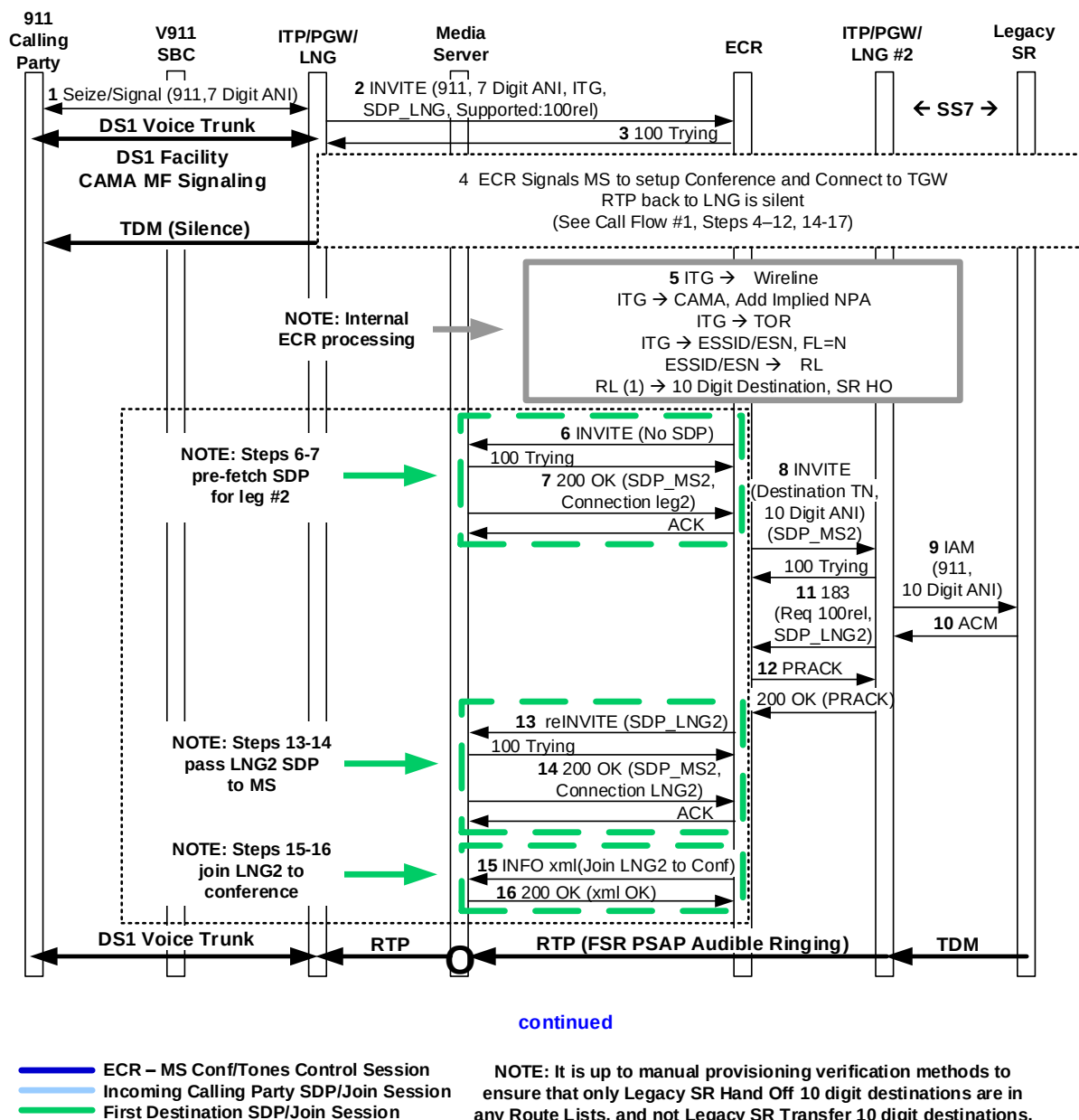


Figure 8: Call Flow 2—DS1 CAMA End Office Trunk Only Routing (TOR) SS7 Handoff to Foreign Selective Router (Graphic 1 of 2)

1. Caller dials 9-1-1 off an End Office which is using dedicated DS1 trunking facilities and CAMA MF signaling to the ECMC LNG. The EO CAMA trunk only signals a 7 digit ANI to the LNG. (Dedicated 9-1-1 CAMA trunk signaling always sends 9-1-1, or 11, or 1, or nothing, for the Called Party Number.) Because of the nature of inter-office CAMA signaling, there is a two way talk path set up from the EO to the LNG at the end of the MF 911/ANI signaling sequence.
2. LNG sends SIP (not SIP-GTD) INVITE to the near ECR which includes 9-1-1 as the Called Number (in the SIP To: header), the 7 digit ANI as the Calling Number (in the SIP From: header), Incoming Trunk Group (ITG) identifier for this particular CAMA trunk group, and the SDP offer from the LNG (labeled SDP_LNG in the ladder diagram).
3. ECR responds to the LNG INVITE with a 100 Trying.
4. Step 4 for this call flow is identical to Steps 4-16 of Call Flow 1. At the end of this step the calling party has an early media path to the MS, which is currently silent.
5. ECR performs the following processing on the ITG received in the INVITE of step 2:
 - A. The ITG delivered by the LNG INVITE will have a call type provisioned, in this case, Wireline.
 - B. The ITG will also have a signaling attribute provisioned indicating that for this particular CAMA trunk group, there is a particular NPA that should be pre-pended to the 7 digit ANI. This 10 digit ANI is used for the remaining signaling.
 - C. The ITG delivered by the LNG INVITE will have a call handling method provisioned, in this case, Trunk Only Routing (TOR).
 - D. The ITG will also have a provisioned ESSID and ESN. The ESSID and ESN are used to lookup the Route List (RL). The ESSID/ESN will also have a Flashing indicator, which in this case = No.
 - E. The first (of up to 10) Route List entries indicate routing to a 10 digit destination with an attribute indicating SR Handoff. The ECR then looks up the associated media gateway group supporting the trunk group for this 10 digit TN. The ECR then selects a media gateway out of this group.
6. Anticipating an INVITE to the destination of step 5.e, the ECR goes to the MS to 'pre-fetch' the SDP information. The ECR does this by sending an INVITE with no SDP to the MS on a new session, called the 'First Destination SDP/Join Session' in the diagram above. The MS responds with a 100 Trying.
7. The MS then responds with a 200 OK, which includes the SDP information (labeled SDP_MS2) as well as the connection ID for this RTP stream (labeled Connection leg 2).
8. The ECR sends a SIP-GTD INVITE to the PGW #2, which is associated with the media gateway selected in step 5.e, using the 10 digit destination obtained from the Route List in the SIP TO: header and Request URI. This 10 digit TN is used by PGW #2 to select the egress trunk group. The 9-1-1 caller's calling party number is in the FROM: header. The MS SDP, SDP_MS2 is also included in this INVITE. Since the ECR knows that the egress signaling is SS7, the ECR setup the INVITE GTD mime parameters with all the required SS7 parameters. These GTD parameters are setup for Wireline/NCAS A2 SS7 format, and include: Called Party= 911, Calling Party= Calling Party Number (ANI) of the original 9-1-1 caller, OLI= Wireline, CpCAT= Emergency. PGW #2 responds with a 100 Trying.
9. PGW #2 sends the SS7 IAM to the foreign SR, using the SS7 parameters of the SIP-GTD mime in the INVITE of step 8.
10. The legacy SR responds to the IAM from PGW #2 with an Address Complete Message (ACM).
11. PGW #2 sends a 183 Session Progress to the ECR Requiring PRACK with 100rel, and with the LNG #2 SDP_LNG2 SDP answer to the SDP offer in the INVITE of step 8.
12. The ECR PRACKs the 183, and PGW #2 responds by 200 OK-ing the PRACK.

13. On the first destination MS session, the ECR re-INVITES the MS to pass the SDP obtained in the step 11 183 (SDP_LNG2). The MS responds with a 100 Trying.
14. The MS then responds with a 200 OK, passing again the SDP and connection information previously sent in step 7.
15. The ECR then sends the MS (on the first destination session) an INFO, instructing the MS to join the connection of step 14 to the conference of step 4. This will connect the second leg of the call into the call conference.
16. The MS responds with a 200 OK. At this point there is talk path from the PSAP off the foreign SR, through the ECMC MS, back to the original 9-1-1 calling party, so that the calling party can hear audible ringing provided by the foreign SR PSAP CPE.

continued

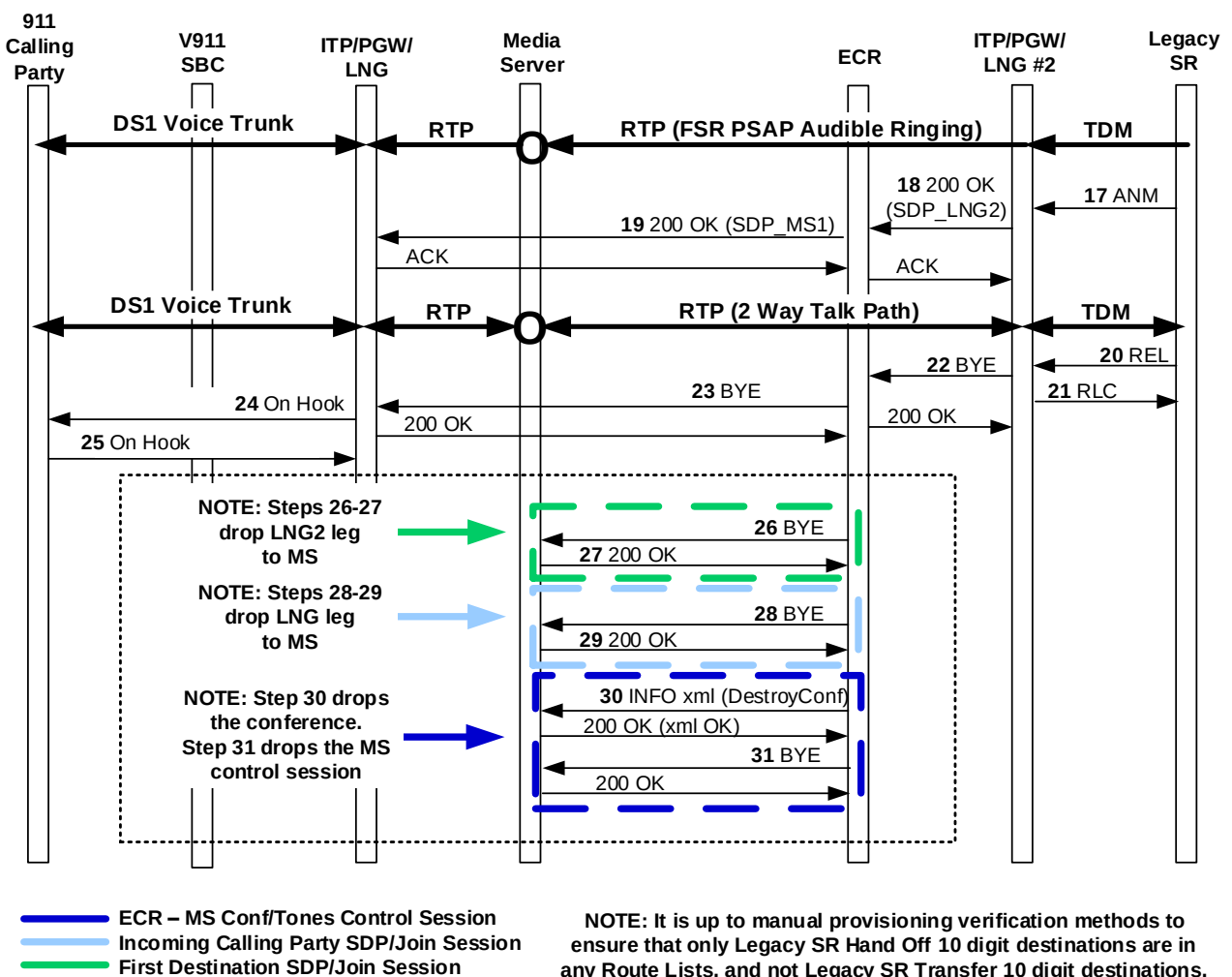


Figure 9: Call Flow 2—DS1 CAMA End Office Trunk Only Routing (TOR) SS7 Handoff to Foreign Selective Router (Graphic 2 of 2)

17. The legacy SR signals that the PSAP it hosts has answered the call, by sending the SS7 ANM (Answer Message) to PGW #2.
18. PGW #2 then sends a 200 OK to the ECR, in which PGW #2 repeats the SDP_LNG2 answer.
19. The ECR sends the original LNG a 200 OK which repeats the SDP_MS1 answer within step 4. ACKs follow and a two way RTP talk path now exists from the PSAP hosted by the foreign SR back to the original 9-1-1 caller.
20. The call taker at the PSAP hangs up, which causes the legacy SR to send an SS7 RELEASE to PGW #2.
21. PGW #2 responds to the RELEASE with a RELEASE COMPLETE.
22. PGW #2 also starts to tear down the call via the ECR, by sending the ECR a BYE. The ECR returns a 200 OK.
23. As a back-to-back user agent, the ECR is now prompted to send a BYE to the original LNG, and the LNG responds with a 200 OK.
24. The original LNG then tears down the CAMA trunk to the End Office by sending On-hook (i.e., supervisory disconnect signaling).
25. The EO replies by also going On-hook.
26. The ECR starts to clean up the MS conference by sending a BYE on the first destination session.
27. The MS responds with a 200 OK, and the session is dropped.
28. The ECR then sends a BYE to the MS on the incoming calling party session.
29. The MS responds with a 200 OK, and this session is dropped.
30. The ECR then instructs the MS to destroy the call conference, on the control session. The ECR waits for the MS to respond with a 200 OK indicating the conference was destroyed.
31. The ECR then sends a BYE to the MS on the control session, which the MS responds to with a 200 OK and this session is dropped.

2.2.4 Call Flow 4—VSP Call from AT&T V9-1-1 Network - Selective Routing – Attempted Termination to ECMC PSAP #1, then ECMC PSAP #2 (both in abandon) Termination to ECMC PSAP #3 (10 digit EMF)

The following call flow is a 9-1-1 emergency call originating from the AT&T V9-1-1 Network for VoIP and Wireless Service Providers. The Service Types must be segregated on different trunks from the V9-1-1 Network, so that either 'VoIP' or 'Wireless' will be assigned to each ITG. If the ITG is provisioned for Selective Routing, the ESQK will be used (via SRDB lookup) to derive the ESSID/ESN. If the ITG is provisioned for Trunk Only Routing, or if Selective Routing has a problem and the call is default routed, the ESRN will be used to derive the ESSID/ESN. Only if there is a problem with the ESRN-derived ESSID/ESN, will the ITG-derived ESSID/ESN be used. This call flow will attempt to route to a couple of ECMC PSAPs which are in Abandon, before it terminates on a 10-digit EMF PSAP interface.

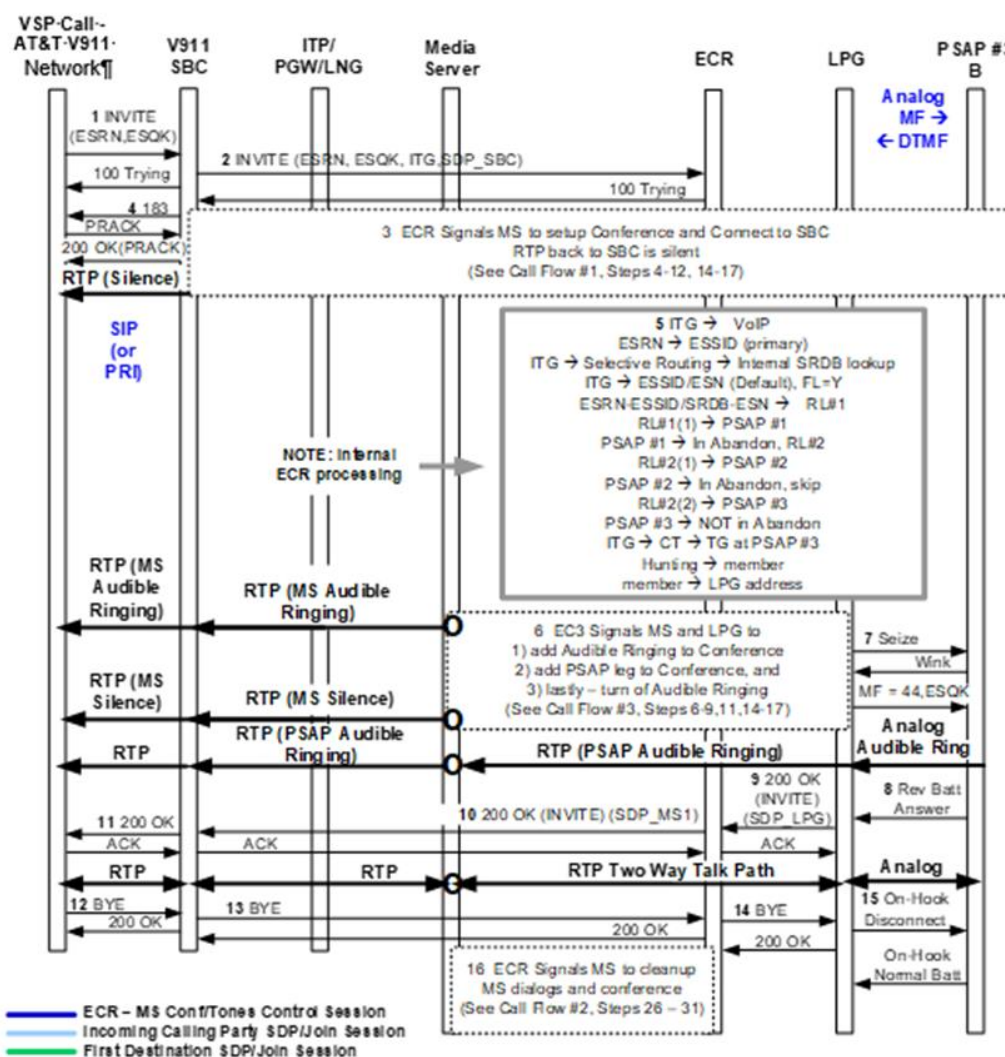


Figure 10: Call Flow 4—VSP Call from AT&T V9-1-1 Network - Selective Routing – Attempted Termination to ECMC PSAP #1, then ECMC PSAP #2 (both in abandon) Termination to ECMC PSAP #3 (10 digit EMF)

1. VoIP caller dials 9-1-1 via a VSP using the AT&T V9-1-1 Network. The VSP may have PRI, or SIP connections to the V9-1-1 Network. Either way, the V9-1-1 Network routes the call through the V9-1-1 SBC, on its way to the ESRP network. The call will enter the V9-1-1 network with 9-1-1 as the called number, and with the originators ANI, but after an IPS query the called number will be changed to an ESRN, and the ANI will be changed to the ESQK pANI. This is the format of the INVITE to the V9-1-1 SBC for the ESRP call. A 100 Trying is the response to the INVITE.
2. The V9-1-1 network will route the call based on ESRN. The V9-1-1 network will know which ESRNs are to be routed to the ECR sites. Each V9-1-1 SBC will route the appropriate calls to the near ECR site as the preference. (Only V9-1-1 calls with ESRNs handled by the ECMC will be routed to the ECR.) The V9-1-1 INVITE to the ECR will have the ESRN, ESQK, an ITG (unique for each VSP customer) and V9-1-1 SDP_SBC. The ECR responds with a 100 Trying.
3. The ECR now sets up a conference in the MS, to which it connects the incoming V9-1-1 call leg. No tones or announcements are played, so the calling party hears silence.
4. As part of the signaling of step 3, the V9-1-1 SBC returns a 183 Session Progress to the V9-1-1 network, requesting PRACKs and early media. This provides a one way talk path on this initial call leg, to prepare for audible ring-back from the PSAP CPE when the second leg of the call is added to the conference later in the call (the end of step 6). This generates a PRACK, and its associated 200 OK.
5. ECR performs the following processing:
 - A. The V9-1-1 INVITE will have an ITG parameter identifying the VSP customer. The ITG will have a call type provisioned, in this case, VoIP.
 - B. The ESRN from the INVITE is used to derive the ESSID for this call. This ESRN derived ESSID will have precedence over the SRDB returned ESSID.
 - C. The ITG delivered by the INVITE will have a call handling method provisioned, in this case, Selective Routing – indicating a lookup to the internal SRDB.
 - D. The ITG will also have a provisioned ESSID and ESN to use ONLY in the case of Default Routing (e.g., if the Selective Routing SRDB query fails). The ESSID/ESN will also have a Flashing indicator to be used ONLY in the case of Default Routing, which in this case = Yes, because we would want flashing at the PSAP to clue them in that this Selective Routing call was Default routed, if that was the case.
 - E. Using the ESQK, an internal SRDB query retrieves an ESSID/ESN pair. The SRDB derived ESN, together with the ESRN derived ESSID, indicate a Route List to use, Route List #1.
 - F. The Route List #1's first destination is PSAP #1.
 - G. The ECR checks PSAP #1, and sees that it is in abandon, and uses its abandon RL, RL#2.
 - H. Route List #2's first destination is PSAP #2.
 - I. The ECR checks PSAP #2, and sees that it is also in abandon, and so this destination is skipped, as the rule is to not to go more than one abandon route list deep.
 - J. Route List #2's second destination is PSAP #3.
 - K. The ECR checks PSAP #3, and sees that it is NOT in abandon.
 - L. The ITG Call Type (i.e., VoIP), is used by the ECR to find the correct trunk group (TG) at PSAP #3.
 - M. The ECR performs Hunting on this trunk group, to find the appropriate idle member.
 - N. This TG Member will belong to a particular LPG, so the ECR looks up this LPGs IP address.
6. The ECR now signals the MS and LPG to:
 - A. Play audible ringing to the calling party,

- B. Add the PSAP leg to the conference in the MS, and
 - C. Lastly, turn off the audible ringing tones in the conference. This leaves the conference connecting the calling party through the MS to PSAP #3, so the calling party can hear the audible ringing produced by the PSAP. This boxed portion of the call flow is the same as many other call flows, which add a PSAP leg to the conference. The details are discussed in Call Flow3, steps 6-9, 11, 14-17.
7. As the ECR sets up the connection to the LPG in step 6 above, the LPG will signal the PSAP via loop-start. The first signal is the loop start seizure, to indicate off-hook to the PSAP. The PSAP CPE winks back (with a temporary battery reversal) to the LPG to indicate that the CPE is ready to receive the MF digits. The LPG signals out the II digits '44' (i.e., flashing, call was redirected because of abandon PSAP condition) and the 10 digit ESQK via MF to the PSAP CPE.
 8. The PSAP call taker answers the call, which is signaled with a reverse battery to the LPG.
 9. The LPG relays the answer with a 200 OK to the ECR (using the SDP, SDP_LPG). The response is an ACK.
 10. The ECR relays the answer to the V9-1-1 SBC with a 200 OK, forwarding the SDP for the incoming call leg, SDP_MS1. The response is an ACK.
 11. The V9-1-1 SBC then sends the 200 OK towards the V9-1-1 originator, and the response is an ACK. There is a two way talk path from 9-1-1 calling party to PSAP #3.
 12. The V9-1-1 calling party terminates the call, which is signaled with a BYE to the V9-1-1 SBC. The SBC returns a 200 OK.
 13. The SBC relays this BYE to the ECR, which responds with a 200 OK.
 14. The ECR tears down the call with a BYE to the LPG, which responds with a 200 OK.
 15. The LPG tears down the call to the PSAP by going on-hook (i.e., opening up tip and ring). The PSAP CPE responds by going on-hook, which means returning to normal battery on tip and ring.
 16. The ECR now cleans up the MS dialogs and conference, using the signaling of call flow 2, steps 26-31.

2.2.5 Call Flow 5—SS7 NCAS A3 Origination-Selective Routing—Termination to ECMC PSAP 8 Digit—Selective Bridge to another ECMC PSAP (EMF)

The following call flow is a 9-1-1 emergency call originating from a wireless MSC using SS7 to signal to the ECMC LNG. The configuration is NCAS A3, which indicates the ESRK is in the Charge Number. The call terminates to PSAP #1, who then Selectively Bridges to PSAP #2. PSAP #1 then goes on-hook to leave the 9-1-1 caller connected to PSAP #2. PSAP #2 then goes on-hook to drop the call.

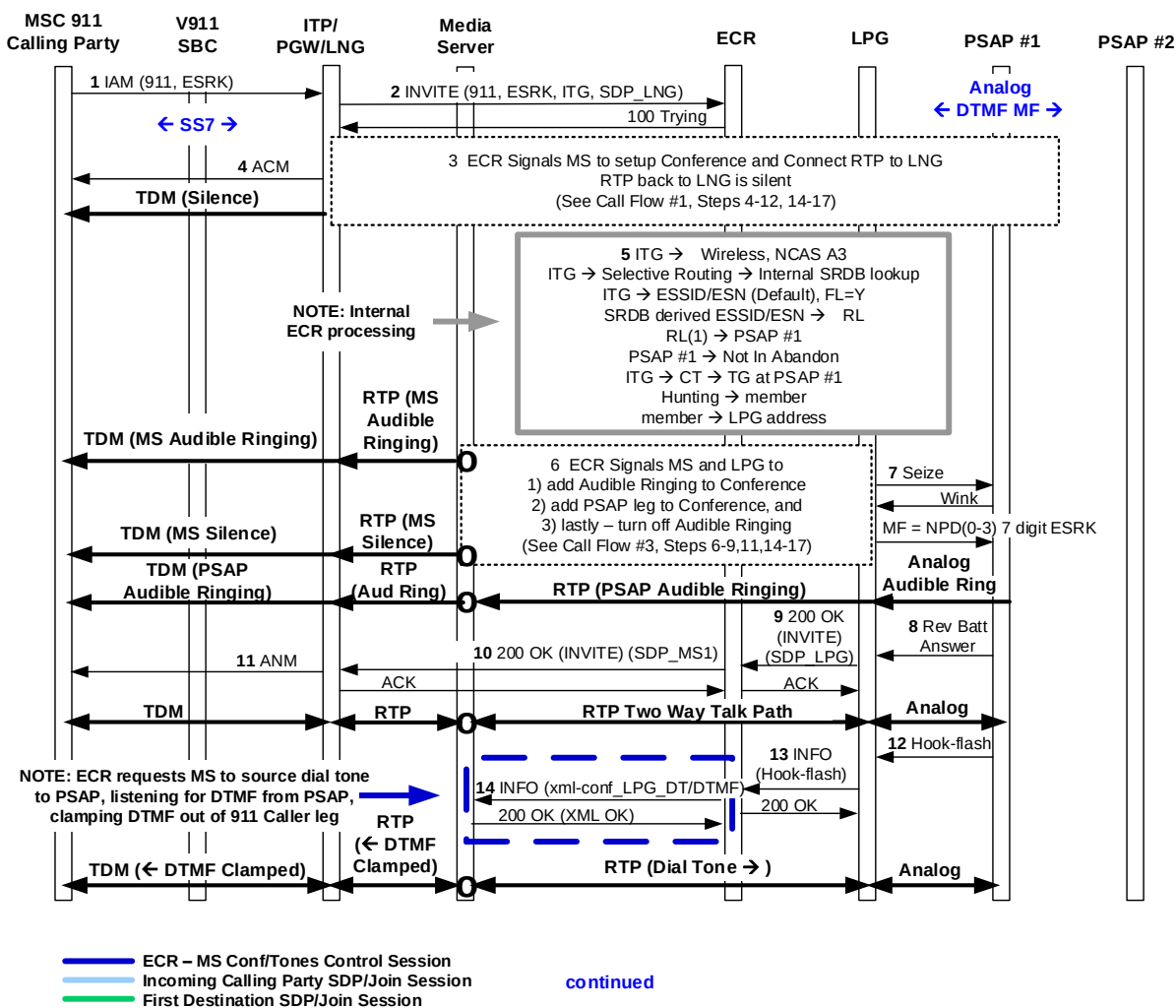


Figure 11: Call Flow 5—SS7 NCAS A3 Origination-Selective Routing—Termination to ECMC PSAP 8 Digit—Selective Bridge to another ECMC PSAP (EMF) (Graphic 1 of 2)

1. Caller dials 9-1-1 off an MSC. The MSC signals the call to the ECMC SGW via SS7 Initial Address Message (IAM), with 9-1-1 as Called Party Number, and the ESRK as the Charge Number. (NCAS A3 format.)

2. PGW sends SIP-GTD INVITE to the near ECR which includes the required SS7 ISUP parameters. This INVITE includes 9-1-1 as the Called Number, ESRK in the Charge Number, Incoming Trunk Group (ITG) identifier for this particular SS7 trunk group, and the SDP offer from the LNG (labeled SDP_LNG in the ladder diagram). (ECR responds to the INVITE with 100 Trying.)
3. Step 3 for this call flow is identical to Steps 4-16 of Call Flow 1. The ECR now sets up a conference in the MS, to which it connects the incoming call leg. No tones or announcements are played, so the calling party hears silence.
4. The PGW has returned an ACM to the originating MSC as a part of executing step 3. See Call Flow 1, steps 12 and 13.
5. ECR performs the following processing on the ITG received in the INVITE of step 2:
 - A. The ITG delivered by the PGW INVITE will have a call type provisioned, in this case, Wireless. The ITG will also have a signaling attribute provisioned indicating that for this particular SS7 trunk group, NCAS A3 format is used, implying the ESRK pANI is the Charge Number, and 9-1-1 is in the Called Party Number.
 - B. The ITG will have a call handling method provisioned, in this case, Selective Routing, which uses an internal SRDB to retrieve an ESSID/ESN based on the ANI of the call.
 - C. The ITG will also have a provisioned ESSID and ESN to use ONLY in the case of Default Routing (e.g., if the Selective Routing SRDB query fails). The ESSID/ESN will also have a Flashing indicator to be used ONLY in the case of Default Routing, which in this case = Yes, because we would want flashing at the PSAP to clue them in that this Selective Routing call was Default routed, if that was the case.
 - D. The ESSID/ESN retrieved from the SRDB lookup points to a Route List.
 - E. For this call, the first entry of the Route List is PSAP #1.
 - F. The ECR sees that PSAP #1 is not in abandon.
 - G. Using the call type derived in 5.a above (i.e., wireless), the ECR alternates through all the appropriate wireless trunks terminating to this PSAP, and then selects the one longest idle.
 - H. The LPG Trunk Member (PTM) has an associated LPG address to which to send the INVITE.
6. This part of the call is identical to Call Flow 3, Steps 6-9, 11, 14-17. Within the ECR-MS control session, the ECR sends an INFO to the MS requesting that audible ringing tones be mixed in the conference so they can be heard by the calling party. Also, the ECR INVITEs to the LPG hosting the selected PTM in step 5, and adds the LPG leg to the conference. Finally, when the LPG is done spilling out the ANI digits, the ECR tells the MS to turn off audible ringing tones, so that the calling party can hear the audible ringing tones from the PSAP CPE.
7. As a part of the ECR setting up the connection to the LPG in step #6 above, the LPG will signal the PSAP via loop-start supervisory signaling. The first signal the ECR provides is the loop start seizure, to indicate off-hook to the PSAP. The PSAP winks back to indicate 'ready to receive digits'. Since this is an 8 digit CAMA PTM, the LPG signals out the NPD digit associated with the NPA of the ESRK (i.e., digit in the range of 0-3, which also indicates normal, or not flashing) and the remaining 7 digits of the ESRK via MF to the PSAP CPE.
8. The PSAP call taker answers the call, which is signaled with reverse battery.
9. The LPG relays the answer with a 200 OK to the ECR (with SDP of SDP_LPG). The ECR ACKs the 200 OK.
10. The ECR relays the answer to the PGW with a 200 OK, signaling the MS SDP of this leg, SDP_MS1. The PGW ACKs this 200 OK.
11. The PGW then sends the SS7 Answer Message (ANM) to the MSC, and there is a two way talk path from 9-1-1 calling party to PSAP #1.

12. While the 9-1-1 caller and the PSAP #1 call taker are talking, the PSAP call taker decides that another PSAP is needed to handle this call, so the call taker signals a hook-flash on the analog PSAP trunk (by reversing battery for approximately 0.5 seconds).
13. The LPG detects the hook-flash, and sends a SIP INFO message to the ECR.
14. The ECR signals the MS with an XML based INFO message to have the MS set up the PSAP #1 leg so that the PSAP call taker hears both the 9-1-1 caller and dial tone. In addition, the MS will detect any DTMF tones sourced by the PSAP CPE. The MS will also clamp any DTMF tones so that the 9-1-1 caller will not hear them.
15. The PSAP call taker hears dial tone, and then dials a selective transfer code, *0/1X (*11, for example).

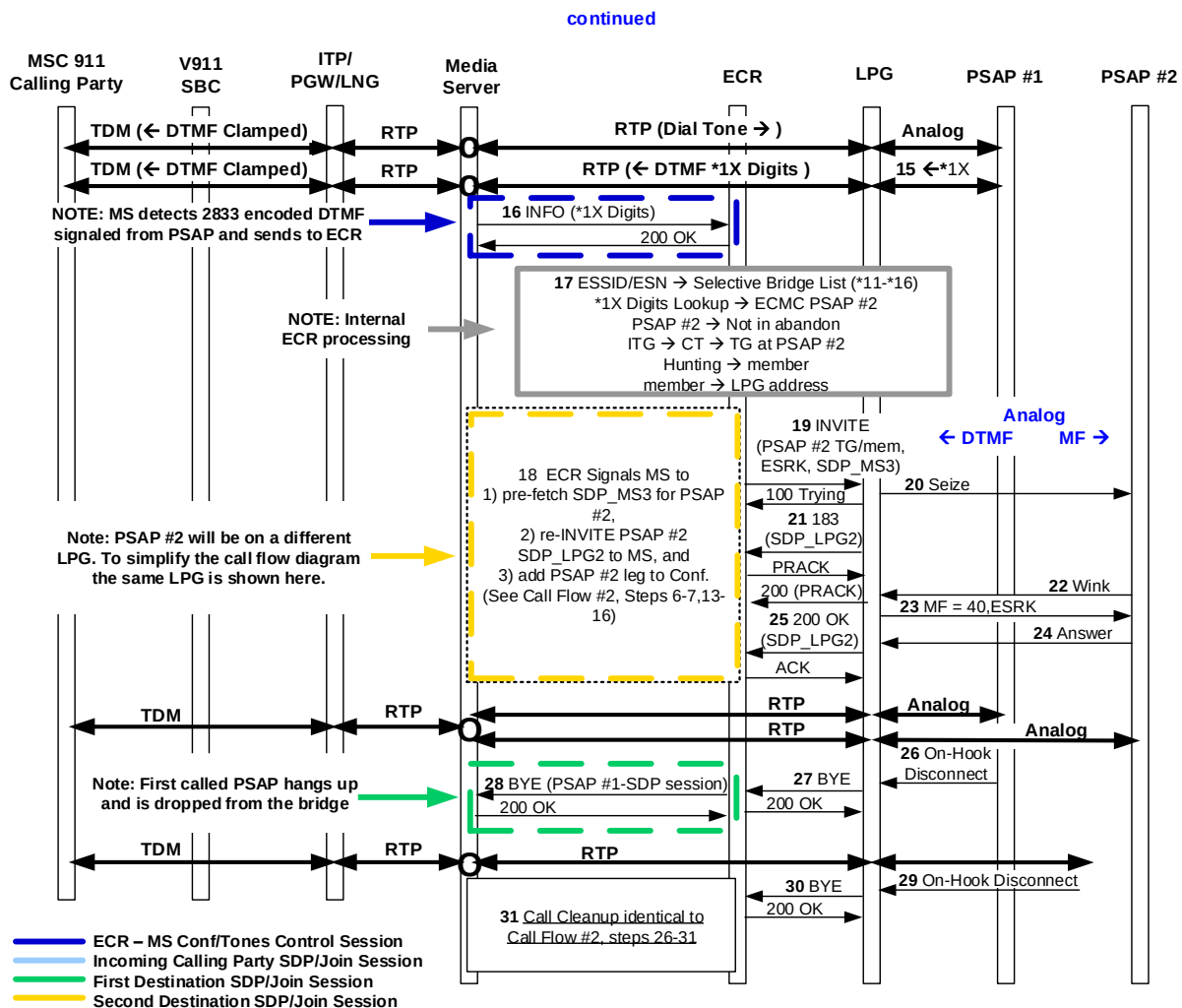


Figure 12: Call Flow 5—SS7 NCAS A3 Origination-Selective Routing—Termination to ECMC PSAP 8 Digit—Selective Bridge to another ECMC PSAP (EMF) (Graphic 2 of 2)

16. The MS detects the *11 DTMF digits, and sends them in an INFO message to the ECR. Since 'barge-in' is enabled for this Play and Collect at the MS, the dial tone is removed as soon as the first DTMF digit is detected. The ECR responds with a 200 OK.
17. ECR performs the following processing:
 - A. Based on the ESSID/ESN obtained from the SRDB query, the ECR looks up the selective bridge route list for *11-*16.
 - B. The single bridge destination for *11 is PSAP #2.
 - C. The ECR sees that PSAP #2 is NOT in abandon.
 - D. The original ITG is used to look up the call type, which is wireless. So a wireless trunk group is found at PSAP #2.
 - E. The ECR performs Hunting on this trunk group, to find the appropriate idle member.
 - F. This TG Member will belong to a particular LPG, so the ECR looks up this LPGs IP address. The ECR also looks up the signaling format for this TK member, and finds that it is a 10 digit EMF trunk. Note that the diagram shows the same LPG used to get to PSAP #2 that was used to get to PSAP #1. This will not be the case in deployed networks. A LPG will typically server only one PSAP. (Using a single LPG was done for the diagram to enhance the readability of the call flow.)
18. This part of the call is the same as Call Flow 2, Steps 6-7, 13-16, where the ECR pre-fetches an SDP from the MS (SDP_MS3), re-INVITES the MS with the SDP received in the 183 from the LPG, and adds the PSAP #2 leg to the conference. During this step, the PSAP #2 is signaled as covered in steps 19-25.
19. The ECR INVITES to the LPG using the address obtained in 17.f. The ESRK is coded into the From header in '10 digit' format (i.e., '40' '10 digit ESRK'). The pre-fetched SDP of the MS (SDP_MS3) from step 18 is offered to the LPG. (LPG returns a 100 trying.)
20. The CAMA interface for the PSAP #2 PTM seizes the CAMA trunk by providing a loop closure.
21. The LPG returns a 183 Session Progress with the SDP answer of 'SDP_LPG2' to the ECR. [The 183s would also require a 100_rel, which requires a provisional ACK (PRACK), because the LPG is configured for PRACK for all calls.]
22. The PSAP CPE indicates that it has seen the seizure, and is ready to accept MF digits by returning a reverse battery wink of approximately 250 ms.
23. The LPG then sends the MF digits, in the form of KP 40 NPA-NXX-XXXX STP, where the NPA-NXX-XXX is the 10 digit ESRK. Note – Even if the original PSAP did not receive the ESRK NPA because of 8 digit signaling (e.g., if there was no NPD assigned to that NPA, so that NPD=0 was used as a default), the original NPA will remain with the call and be correctly delivered to the second PSAP using 10 digit signaling.
24. The PSAP CPE answers the call by reversing battery.
25. The LPG again returns the same SDP_LPG2 answer in a 200 OK to the ECR. At this point there is a 3 party conference between the original calling party, PSAP #1, and PSAP #2.
26. The original PSAP, PSAP #1 decides to leave the conference, and goes on-hook.
27. The LPG sends the BYE to the ECR to clear this leg of the call. 200 OK is sent in response.
28. The ECR forwards the BYE to the MS to clear this second leg. The MS replies with 200 OK. Now only the original 9-1-1 caller and PSAP #2 are in the bridge.
29. The call ends when PSAP #2 goes on-hook.
30. The LPG again sends the BYE to the ECR to clear the remaining legs of the call. 200 OKs are sent in response.
31. See Call Flow 2, steps 26-31 for the details of call clean up for the MS resources and the call legs.

2.2.6 Call Flow 6—End Office (PRI) origination—Selective Routing to ECMC PSAP 10-Digit (EMF)—Fixed Bridge to a Foreign SR PSAP via SS7 Direct Trunk Group

The following call flow is a 9-1-1 emergency call all flow originating from a Wireline End Office using PRI to signal to the ECMC LNG. The call terminates to PSAP #1, who then performs a Fixed Bridge to a Foreign Selective Router's PSAP. After talking, this Foreign SR's PSAP then goes on-hook to leave the 9-1-1 caller connected to PSAP #1. PSAP #1 then goes on-hook to drop the call.

This call flow is very similar to Call Flow 5 with a couple of differences.

1. The origination is PRI instead of SS7.
 - A. Caller dials 9-1-1 off an End Office (or possibly a PBX). The EO signals the call to the ECMC LNG via a Q.931 PRI SETUP message (instead of an SS7 IAM message), with 9-1-1 as Called Party Number, and the originators Calling Party Number used as the ANI for the call. *(It may be required to use a Billing Number associated with the PRI facility as the ANI instead of the CPN. This would be determined on a PRI basis.)*
 - B. Different from SS7, the LNG now returns a Call Proceeding Q.931 message to the End Office to indicate call is progressing so that the EO can turn off its SETUP response timer.
 - C. The remaining PRI signaling follows the SS7 call flow, with PRI using Call Progress instead of SS7 ACM, PRI using CONNECT/CONN ACKs instead of SS7 ANM, and PRI using DISCONNECT/RELEASE/REL COMPLETE instead of SS7 REL and RLC.
2. The ECR processing is different from step 17 in Call Flow 5:
 - A. For Fixed Bridges, the ECR will receive DTMF digits in the range of *20-*49.
 - B. The ECR will look up routing for the received *20-*49 in a table associated with the PSAP.
3. Different from Call Flow 5 steps 18-25, this call flow bridges on an SS7 egress leg to a foreign SR.
 - A. The SS7 signaling will be NCAS A2, with the original ANI in the Calling Party Number.
4. Different from Call Flow 5 steps 26 – end, this call flow has the added bridge disconnect after the 3 party bridge has been established, leaving the original 2 party call in place. *Not shown in this call flow, the PSAP call taker could then invoke another bridge request if desired.*
5. When the PSAP call taker goes on-hook, call cleanup is similar to Call Flow 2.

2.2.7 Call Flow 11—SS7 Non-Emergency Call Sent to Fast Busy

Note: You will notice in this document that Call Flow 11 follows Call Flow 6. Some pre-defined AT&T call flows are not detailed in this document as they are not technically relevant.

This call flow is an ‘error’, or mis-provisioned call scenario. Normally, all SS7 emergency calls from End Offices, MSCs, or SR handoff trunk groups coming to the ECMC will have 911, 11, 1, or nothing as the Called Party Number, and will also have the Calling Party Category (CpCAT) parameter = ‘Emergency’. If a call comes from an EO/MSR/SR-HO and has 1) something other than 911/11/1/null in the Called Party Number AND 2) the CpCAT=Non-emergency, the ECMC will return Fast Busy to the calling party.

Note: The above calls are in contrast to transfers from FSR, where we expect a 10 digit TN in the Called Party Number.

As background, some Selective Routers will accept non-emergency calls with a 10 digit TN in the Called Party Number and route them as ‘Anonymous’ calls to the PSAP associated with the Called Number, after replacing the real ANI with 000-911-0000. These are sometimes used for anonymous Tip lines. ECMC will not support this behavior Note that this discussion implies that CAMA trunks from EO/MSR/SR-HO with non-9-1-1 called numbers will be changed to 9-1-1 and routed to the PSAP.

This call flow is similar to Call Flow 1 with a couple of differences.

1. The origination IAM is from an MSC, and there is a 10 digit TN in the Called Party Number.
2. The IAM has a Calling Party Category (CpCAT) that is NOT “emergency”.
3. The ECR processing of step 18 is simply detecting the above two conditions. No other processing is required. The calling party gets reorder treatment.

2.2.8 Call Flow 12—DS1 CAMA EO Origination—Selective Routing/Default Routing (Bad ANI)—Termination to ECMC PSAP 10 Digit with Flashing

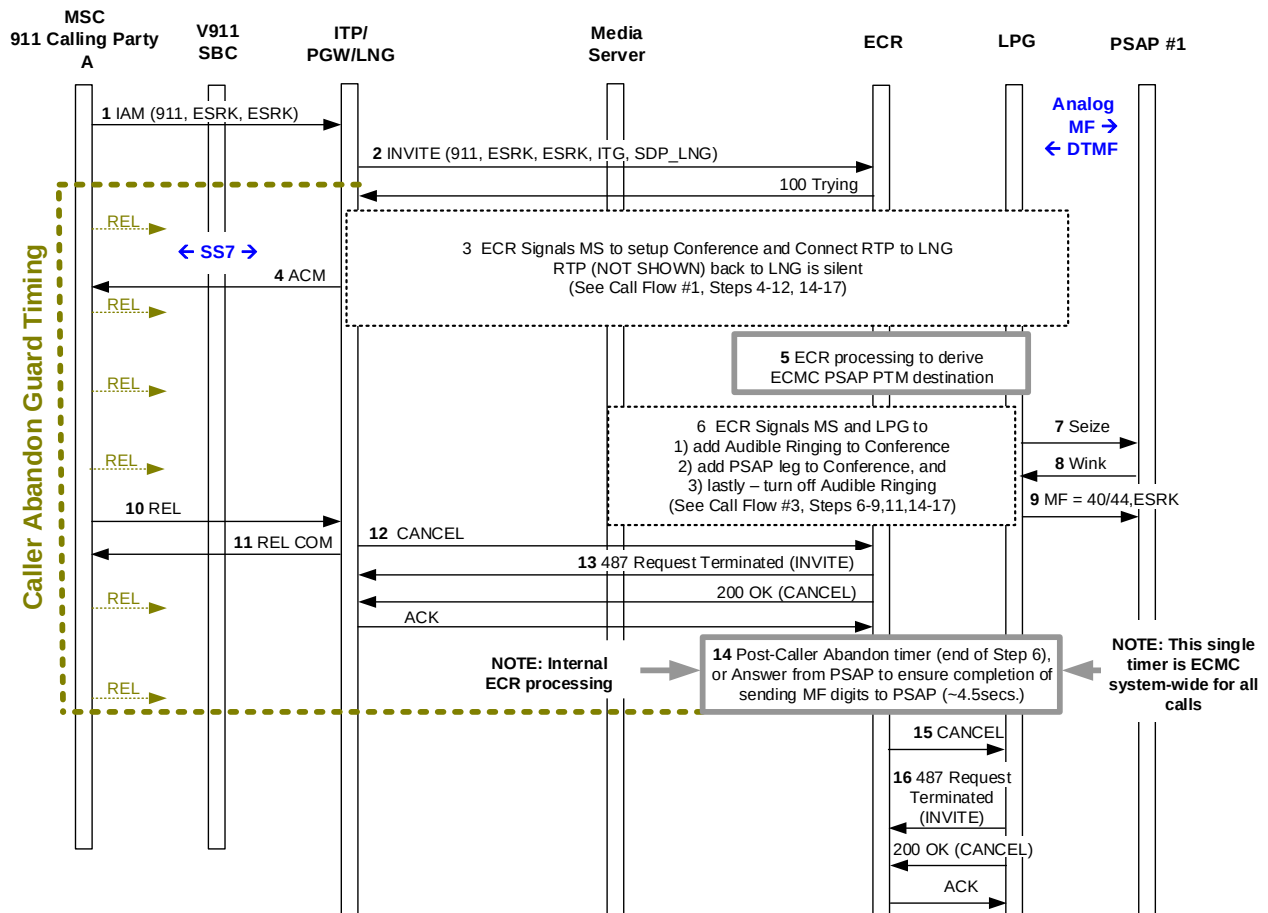
This call flow shows the call handling when a CAMA trunk garbles the ANI for a 9-1-1 call. This is shown below as a call with a 4 digit ANI. Even though Selective Routing is provisioned for this CAMA trunk, since the ANI is not valid, an ESCO based ANI will be substituted and Default Routing will occur instead of Selective Routing. As the call terminates to the PSAP, flashing is signaled to indicate that this call encountered problems.

This call flow is similar to Call Flow 5 with a couple of differences.

1. The origination is DS1 CAMA instead of SS7 NCAS A3.
 - A. See Call Flow 2 for DS1 CAMA signaling.
2. The ECR processing in step 5 of Call Flow 5 changes because of invalid ANI received in this call.
 - A. The ITG will also have a signaling attribute provisioned indicating that for this particular CAMA trunk group, there is a particular NPA that should be pre-pended to the ANI.
 - B. The ITG will also have a provisioned ESSID and ESN to use in the case of Default Routing. The ESSID and ESN are used to lookup the Route List (RL). The ESSID/ESN will also have a Flashing indicator, which in this case = Yes.
 - C. For this call, the ANI validation fails, in that for a CAMA trunk a 7 digit ANI was expected, but only 4 digits were received. Because of this, the ECR will use Default routing and the ESSID/ESN assigned to this ITG (see 2.b. above).
 - D. Because of the ANI failure, the NPA and ESCO values provisioned for this ITG will be used as the ANI for this call (i.e., NPA911TTTT).
 - E. The ESSID/ESN provisioned as the Default for this ITG are used to obtain the Default Routing RL.
 - F. The flashing indicator provisioned as the Default for this ITG is used, and in this case is YES.
 - G. The LPG signals out the II digits '44' (flashing), and the 10 digit NPA911TTTT via MF to the PSAP CPE.
3. The remaining steps of this call are the same as previous calls.

2.2.9 Call Flow 13—MSC (SS7 – NCAS A1) Caller Abandons, Deliver ANI to ECMC PSAP (EMF)

The following call flow is a 9-1-1 emergency call originating from a wireless MSC via SS7. This call shows the original calling party hanging up, or abandoning, just after the ECR receives the INVITE. It is up to the ECR to ensure that the PSAP CPE receives the ANI before the call to the LPG is torn down. (The assumption is that once the PSAP CPE is given the ANI for the call, the PSAP has the responsibility of verifying that the original caller really meant to abandon, usually by calling the original caller back on an administration line—not through the ECMC.)



NOTE: Future functionality might leave MS in call to provide announcement to PSAP.

Figure 13: Call Flow 13—MSC (SS7– NCAS A1) Caller Abandons, Deliver ANI to ECMC PSAP (EMF)

1. Caller dials 9-1-1 from a wireless MSC. The MSC signals the call to the ECMC SGW via SS7 Initial Address Message (IAM), with 9-1-1 as Called Party Number, a 10 digit ESRK pANI as the Calling Party Number, (and the same ESRK pANI in the Charge Number). (NCAS A1 format.)
2. LNG sends SIP-GTD INVITE to the near ECR which includes the required SS7 ISUP parameters. This INVITE includes 9-1-1 as the Called Number, the ESRK in the Calling Party parameter, this same ESRK in the Charge Number parameter, Incoming Trunk Group (ITG) identifier for this particular SS7 trunk group, and the SDP offer from the LNG (labeled SDP_LNG in the ladder diagram). (ECR responds to the LNG INVITE with a 100 Trying.)
3. Similar to Call Flow 1, steps 4-12, 14-17, the ECR sets up the incoming call leg to connect to the MS. RTP is not shown in this diagram, but would act just like Call Flow 1, with the caller hearing silence.
4. As a part of step 3 above, the PGW will return an SS7 ACM to the originating MSC.
5. ECR processing, as appropriate for this ITG, derives the ECMC PSAP PTM for terminating the call.
6. Knowing the destination is an ECMC PSAP, the ECR uses normal processing to add the PSAP destination to the bridge. This is the same as Call Flow 3, steps 6-9, 11, 14-17.
7. As the ECR sets up the connection to the LPG in step #6 above, the LPG will signal the PSAP via loop-start. The first signal is the loop start seizure, to indicate off-hook to the PSAP.
8. The PSAP CPE winks back to the LPG to indicate that the CPE is ready to receive the MF digits.
9. The LPG signals out the II digits '40' (i.e., normal, or not flashing) *[or 44 Flashing, if the abandon occurs before the ECR formulates the MF digit string in the INVITE to the LPG]* and the 10 digit ESRK (in the form KP NPA-NXX-XXXX STP) via MF to the PSAP CPE.
10. The original calling party hangs up/abandons, before the ECR processing is done. This results in a RELEASE SS7 message being sent from the MSC to the SGW/LNG.
11. The PGW responds with a RELEASE COMPLETE SS7 message to tear down the MSC SS7 trunk.
12. Because the original call has been dropped, the PGW CANCELS the original INVITE to the ECR.
13. The ECR responds to the CANCEL with a 487 'Request Terminated' for the original INVITE. The ECR also responds to the CANCEL with a 200 OK. This will tear down the call from the original caller to the ECR.
14. The ECR continues processing the Caller Abandon Guard Timing, which extends to either 1) a configurable timeout period after the final 183 of step 6 (approximately 4.5 seconds), or 2) the PSAP answers. The intent in either case is to ensure the PSAP CPE has received all the MF digits. *For Foreign PSAP and PSTN destinations, the ECR may add an additional timer period after the 183 Session Progress (for example, ~4.5 seconds) to ensure that the ANI has been completely delivered downstream.*
15. Because the ECR now knows that the LPG has signaled out the ANI to the PSAP CPE, the ECR can drop the call to the LPG with a CANCEL [or BYE if the PSAP has answered already].
16. The LPG responds to the CANCEL with a 487 Request Terminated, corresponding to the INVITE transaction. The LPG also sends the ECR a 200 OK response to the CANCEL method. And the call from the ECR to LPG is dropped.

Call Flow 17—Test Call—PSAP Trunk Test to ECMC PSAP Trunk Member

The following call flow consists of a Test Call Generator sending a test call to a particular PTM. This PSAP trunk test call will not ring the PSAP call taker, but only signal on the trunk to test the PSAP CPE equipment.

Note: The processing of the results of this test call needs to balance the LPG response for a successful test, vs. the LPG response when this test is attempted and the trunk is already busy with a 9-1-1 call. When already busy with a 9-1-1 call, the LPG takes approximately 30 ms to send the 486 Busy response after receiving the INVITE. Add a conservative 300 ms for WAN delays between the MOP and the LPG, and the total response time is under 350 ms. On the other hand, for the successful PSAP trunk test, lab results have shown delays ranging from 3.49 s to almost 5 s, but typically close to 4 seconds. It is engineering's judgment to use 2.0 seconds as the threshold between a failed and a successful test for 486 Busy responses. For example, when running this test, if a 486 is received in under 2 secs, the test is inconclusive, and likely due to a busy PTM. If a 486 is received in over 2 secs, and a 183 was previously received, the test is considered 'passed'.

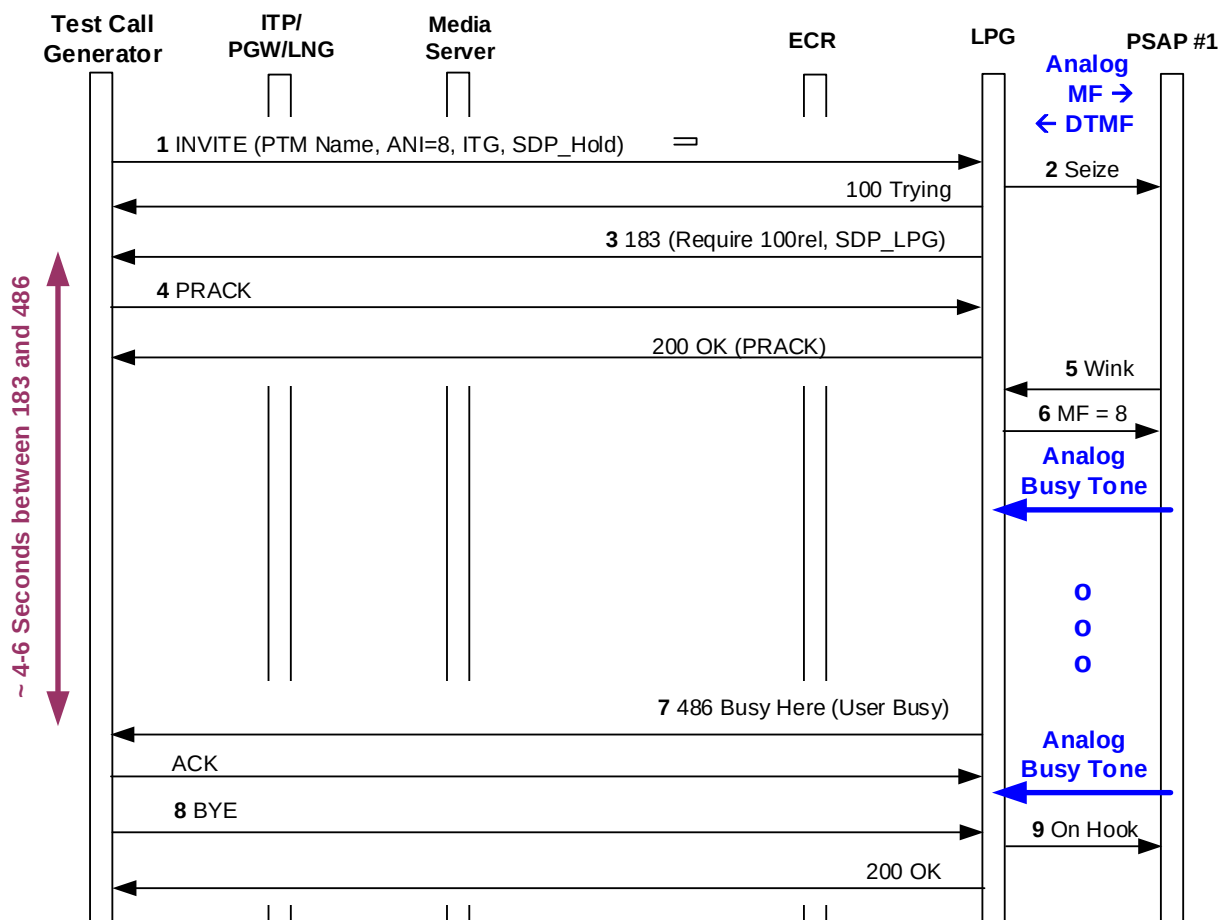


Figure 14: Call Flow 17—Test Call—PSAP Trunk Test to ECMC PSAP Trunk Member

1. Test Call Generator sends SIP INVITE to the appropriate LPG hosting the PTM to be tested. This INVITE includes a PTM name as the Called Number in the To: header, the single digit 8 as the ANI in the From: header, and the SDP offer from the TCG (labeled SDP_Hold in the ladder diagram) that should prevent the LPG from sending any RTP. (*If the PSAP trunk signaling would have been 10/20 digit EMF, the number 48 would have been placed in the From: header as the ANI.*). (LPG responds to the INVITE with 100 Trying.)
2. The LPG seizes the PTM trunk to go off-hook.
3. The LPG responds with a 183 Session Progress, with the SDP_LPG that will not be used by the TCG, as no RTP will flow for this test call.
4. The TCG PRACKs the LPG's 183 to satisfy the 183's Require:100rel. The LPG 200 OKs the PRACK.
5. If the PSAP CPE is working, a wink should be returned in under 4 seconds after the seizure.
6. Since this is an 8 digit PTM, the LPG sends KP 8 ST in MF digits to the PSAP. This causes the PSAP CPE (if functioning correctly) to send Busy tone to the LPG. If the PTM would have been a 10 or 20 digit PTM, the LPG would have signaled out a KP 48 STP in MF digits to the PSAP.
7. The LPG detects the Busy tone within 4-6 seconds, and sends a 486 Busy Here response to the TCG, which ACKs it.
8. It is up to the TCG to tear down the call with a BYE. The LPG would likely also tear down the call after a duration of no RTP. The LPG 200 OKs the BYE.
9. The LPG disconnects the PSAP trunk by going off-hook.

2.2.10 Call Flow 18—Test Call—PSAP Call Through Test to ECMC PSAP PTM

The following call flow consists of a Test Call Generator (TCG) within the Management Operation Platform (MOP) setting up a test call that will establish a talk path with an idle member of the appropriate trunk group at the PSAP. The TCG in the MOP will speak to the PSAP call taker. Because the MS is attached to the call, the PSAP call taker will be able to invoke typical transfers.

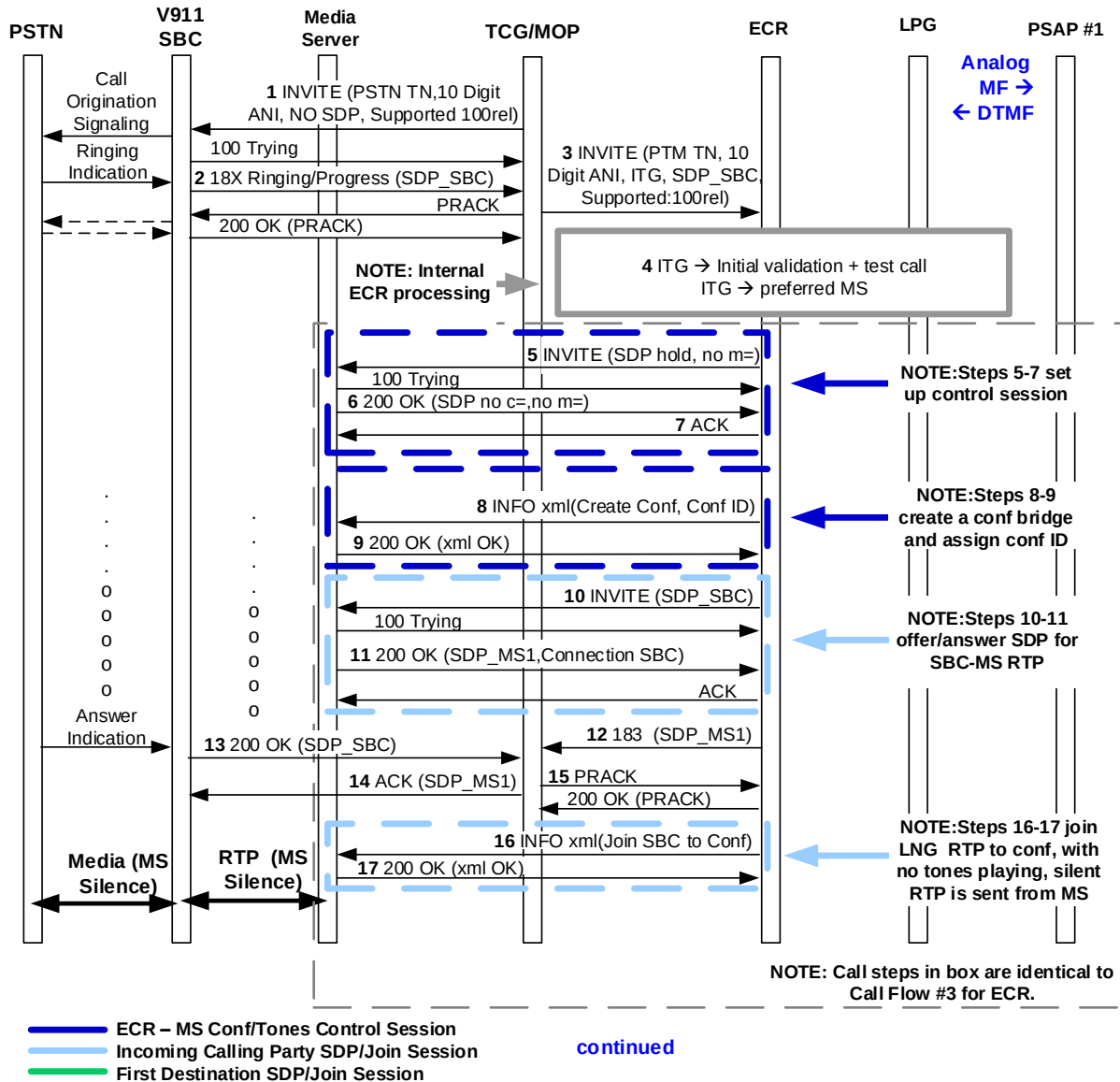


Figure 15: Call Flow 18—Test Call—PSAP Call-Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 1 of 3)

1. Test Call Generator in the MOP sends an INVITE to the V9-1-1 SBC with the TO: header containing the PSTN number of the originator of this test call. There will be no SDP offered at this point. Some test call ANI will be in the FROM: header.
2. The V9-1-1 SBC should return either a 180, or a 183, which will contain an SDP offer.
3. The TCG/MOP will use the SDP offer from step 2, to generate an INVITE to the ECR that looks nearly identical to a non-test call. The TN of the PTM to be tested will be in the TO: header, and the test call ANI will be in the FROM: header.
4. The ECR performs the following processing:
 - A. The ITG will go through basic validation. The ITG is used to derive the trunk type (test call trunk--which turns on full logging), and also the preferred MS.
5. The ECR now controls the MS, TCG, and LPG to connect the test call through the MS to PSAP #1. This boxed portion of the call flow is the same as many other call flows, and the details are discussed in Call Flow 3. Slightly different in this test call is that steps 13 and 14 show the way that the SDP offer/answer is done, with the final answer passed by the ACK in step 14. The end result is that the ingress call leg is now bridged to the MS.

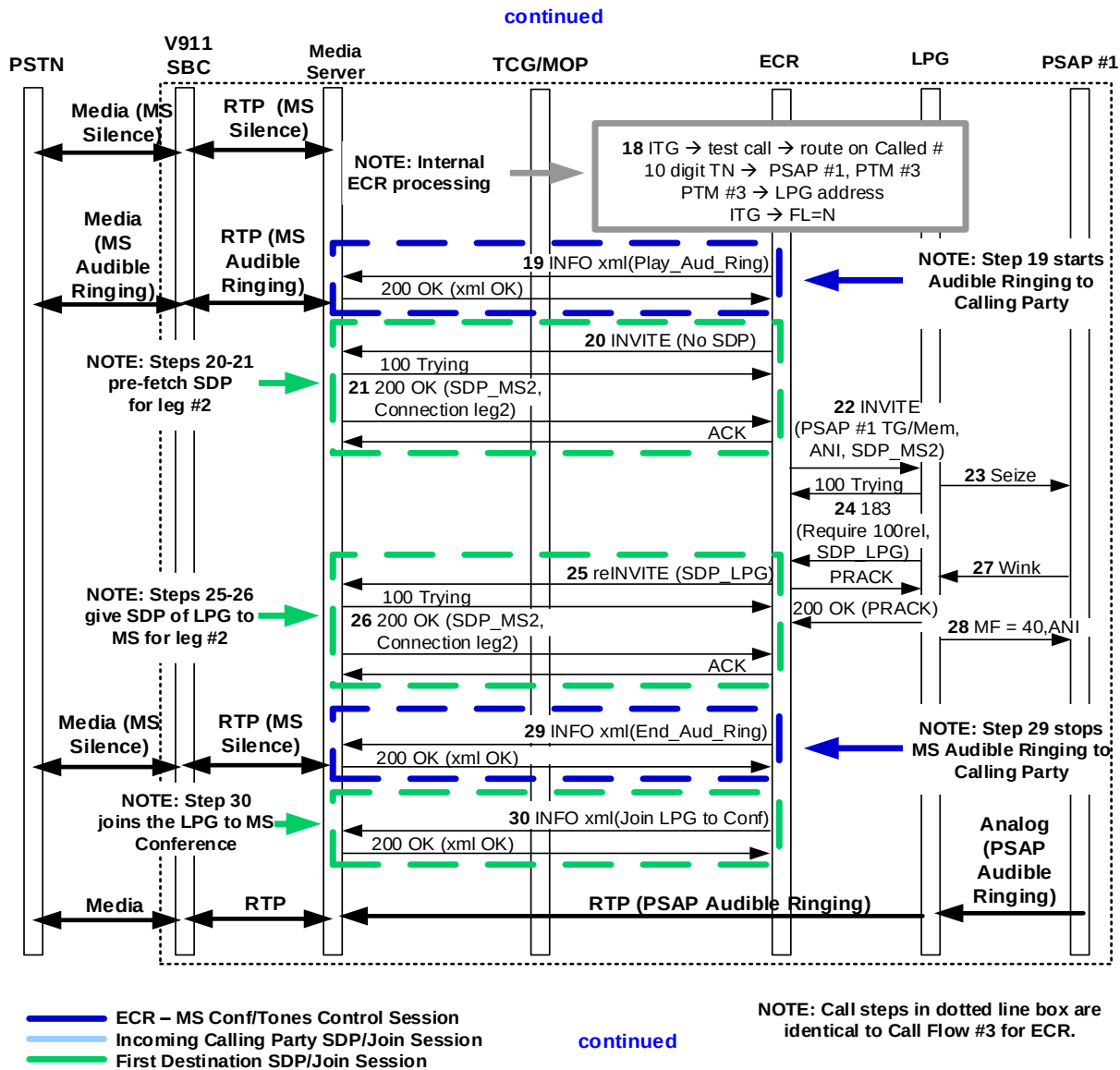


Figure 16: Call Flow 18—Test Call—PSAP Call Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 2 of 3)

6. The ECR performs the following processing:
 - A. The ITG indicates a test call, so the ECR will route on the Called Number (similar to transfer calls).
 - B. The 10 digit Called Number resolves to PTM #3 on LPG #1.
 - C. The LPG IP address is obtained.
 - D. Flashing indicator on this ITG is off.
7. Now steps 19-30 are identical to Call Flow 3 from the ECR perspective as the PTM destination is joined into the MS bridge.

continued

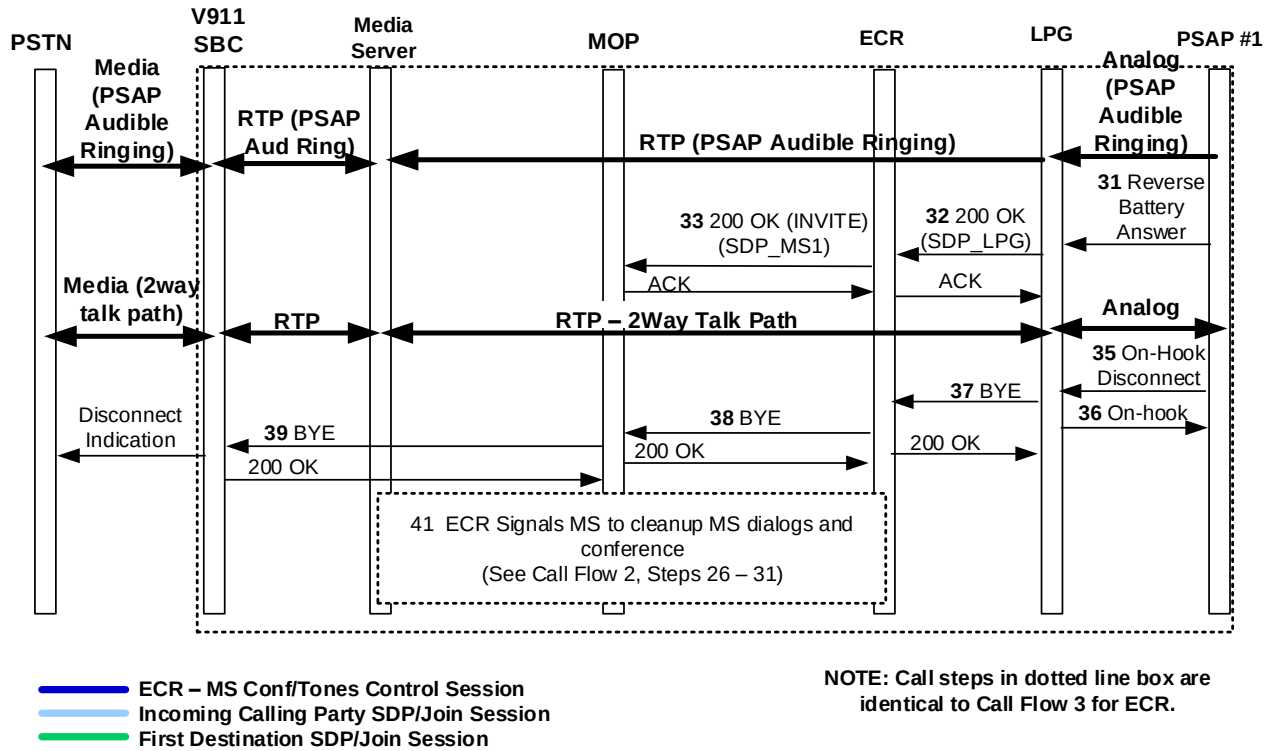


Figure 17: Call Flow 18—Test Call—PSAP Call-Through Test to ECMC PSAP (EMF) Trunk Member (PTM) (Graphic 3 of 3)

- Steps 31-41 are identical to Call Flow 3. Also, since the ECR has set up the MS bridge for this call just as if it were a 9-1-1 call, the PSAP call taker can invoke bridging in the standard ways.

3.0 IP PSAP Call Flows

This section includes call flows involving i3 IP-based PSAP terminations. The first call flow uses ECRF routing logic, followed by a series of compact format call flows covering various sunny day call flows as well as failing call flows. The compact format has the routing logic embedded within the call flow ladder diagram.

3.1 Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer)

The following call flow consists of an SS7 origination using ECRF routing logic to terminate on an i3 PSAP. Then, the i3 PSAP invokes a 3-way call to an analog PSAP to provide for attended call transfer.

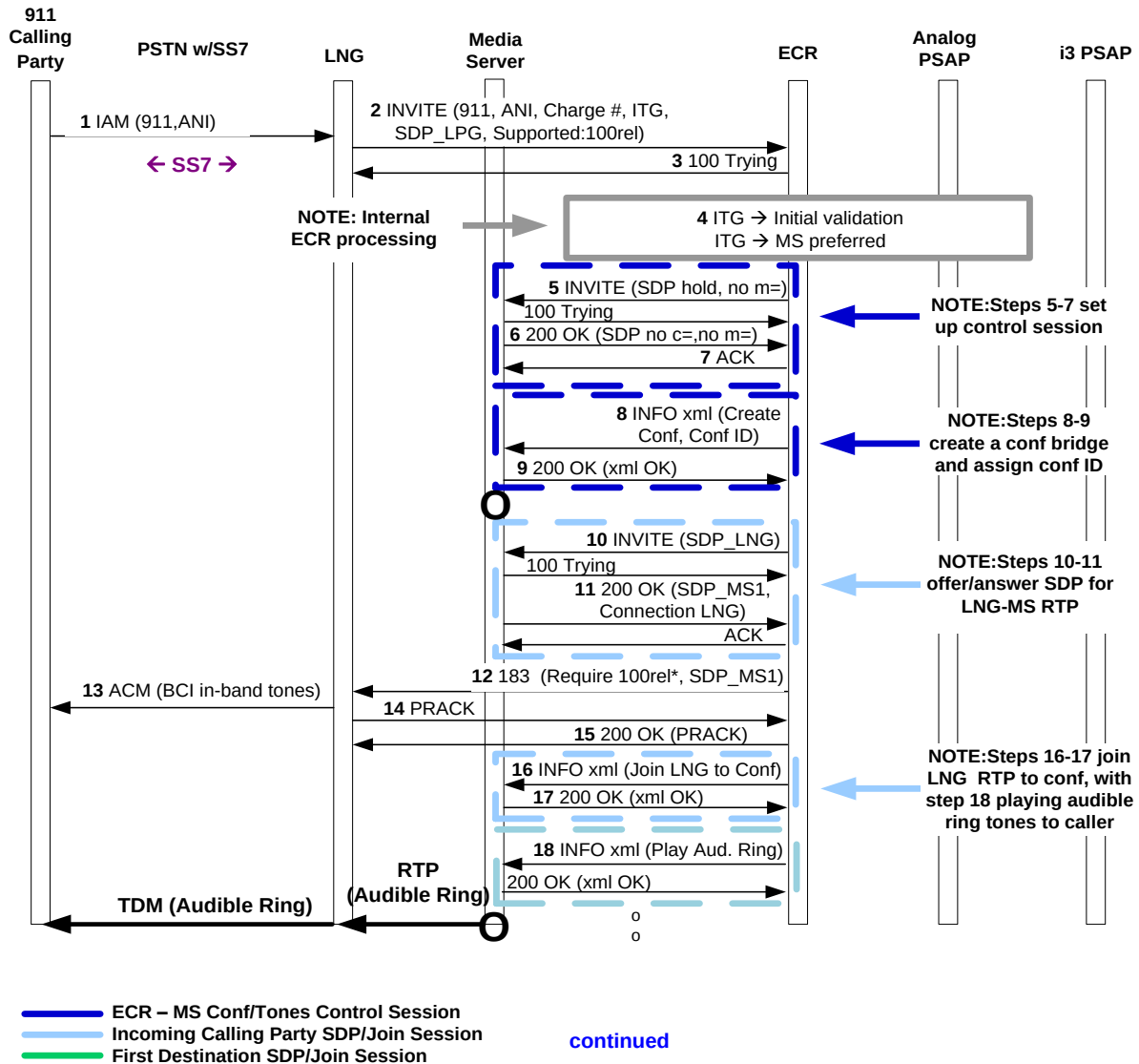


Figure 18: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 1 of 5)

1. Caller dials 9-1-1 off an end office. The EO signals the call to the LNG via SS7 Initial Address Message (IAM), with CIC, 9-1-1 as Called Party Number, the originator's TN as the Calling Party Number, and, for this example, a different 10-digit number (i.e., not the Calling Party Number) as the Charge Number. COT testing (not shown in these call flows) includes additional LNG signaling to set up the loop back and indicate test status.
2. LNG sends SIP INVITE to the directed ECR site (determined by DNS query – not shown). The SIP INVITE is sent to a load balancer (not shown), which selects the appropriate ECR node. The INVITE includes all the existing SS7 ISUP parameters: 9-1-1 as the called number, the ANI as the calling number, the original charge number, Incoming Trunk Group (ITG) identifier for this particular SS7 trunk group, and the SDP offer for the LNG (labeled SDP_LNG in the ladder diagram).
3. ECR responds to the LNG INVITE with a 100 Trying.

4. ECR performs the following processing based on the parameters of this SIP INVITE:
 - A. The ECR performs initial validation on the ITG, to ensure a database match, etc.
 - B. The ITG also indicates the preferred MS.
5. The ECR sends an INVITE to the MS to initiate a control channel. This INVITE has an SDP IP address of 0.0.0.0 (i.e., hold), a=send only line, and no media line passing the port number. The MS responds to the INVITE with a 100 Trying.
6. The MS then sends the ECR a 200 OK, with SDP but without a control or media line.
7. ECR finishes the control session setup by sending an ACK back to the MS.
8. On the above control session, the ECR sends XML-based control instructions (MOML/MSML) in an INFO message requesting the MS to set up a bridge. The ECR assigns the conference ID.
9. MS responds to the INFO with a 200 OK, indicating a bridge has been setup.
10. On a new SIP session, (as a third party controller, acting on behalf of the LNG), the ECR sends an INVITE to the MS, with an SDP offer indicating RTP setup to the LNG SDP address and port.
11. The MS responds with a 100 Trying and a 200 OK. The 200 OK includes the SDP answer indicating the MS SDP RTP port (labeled SDP_MS1 in the ladder diagram). ECR finishes this step by sending an ACK back to the MS.
12. ECR responds to step 2) INVITE by sending a 183 Session Progress to the LNG. This 183 Session Progress contains the SDP answer to the SDP offer in the 2) INVITE, indicating the MS port providing RTP. Typically, to ensure PRACK confirmation of the 183, a "Require" 100rel would be included in the 183, to ensure provisional SIP signaling for end-to-end support of early media. (Early media is 'pre-answer' talk path, and we are concerned that the calling party can hear the audible ringing from an analog PSAP later in the call, since at this point we don't know if the termination is an analog PSAP or an IP PSAP.)
13. LNG sends Address Complete Message (ACM) to the EO, including CIC, indicating yes in the 'In-band Information Indicator' in the Optional Backward Call Indicator (OBCI) and opening up the talk path back to the 9-1-1 caller to hear the audible ringing soon to be set up.
14. As configured, the LNG acknowledges the 183 with a PRACK.
15. ECR responds to the PRACK with a 200 OK.
16. On the incoming calling party session, the ECR sends an INFO to the MS to join the MS RTP connection ID signaled in step 11 to the MS conference ID assigned back in step 8.
17. The MS responds with a 200 OK 'XML OK'.
18. ECR sends an INFO to the MS to play audible ringing to the 9-1-1 caller. This is done on the incoming calling party session with the MS.

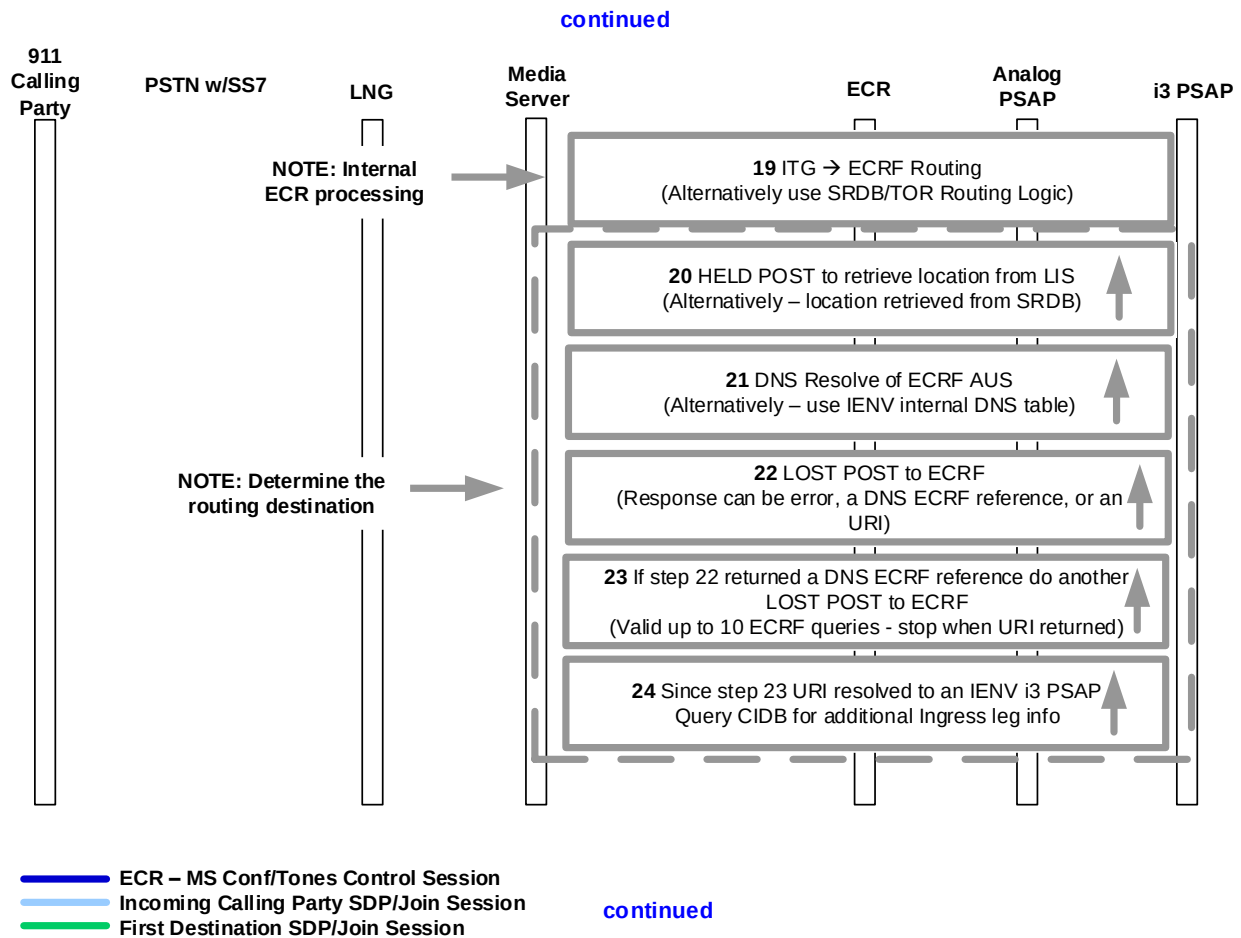


Figure 19: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 2 of 5)

19. ECR reads the ITG provisioning and sees that this ITG gets ECRF routing. (Legacy selective routing off an SRDB, or trunk only routing, are additional options at this point.)
20. ECR sends a HELD protocol POST query to the LIS. The response contains a reference to the appropriate ECRF for this call, via the ECRF AUS.
21. ECR sends a query to an external DNS server in an attempt to resolve the ECRF AUS IP address. (An alternative option would be to use the internal ECR DNS table.)
22. ECR sends a LOST protocol POST query to the ECRF indicated by the DNS response. The result could be:
 - A. A URI (indicating a serving i3 PSAP), or
 - B. Another DNS ECRF reference, or
 - C. Error
23. If step 22 returned another DNS ECRF reference, the ECR will repeat the LOST POST to the ECRF up to 10 times, stopping when a URI is returned.
24. When an URI is obtained, the ECR queries the CIDB for any additional information provisioned against this ITG. The internal Policy Routing Function then processes the call.

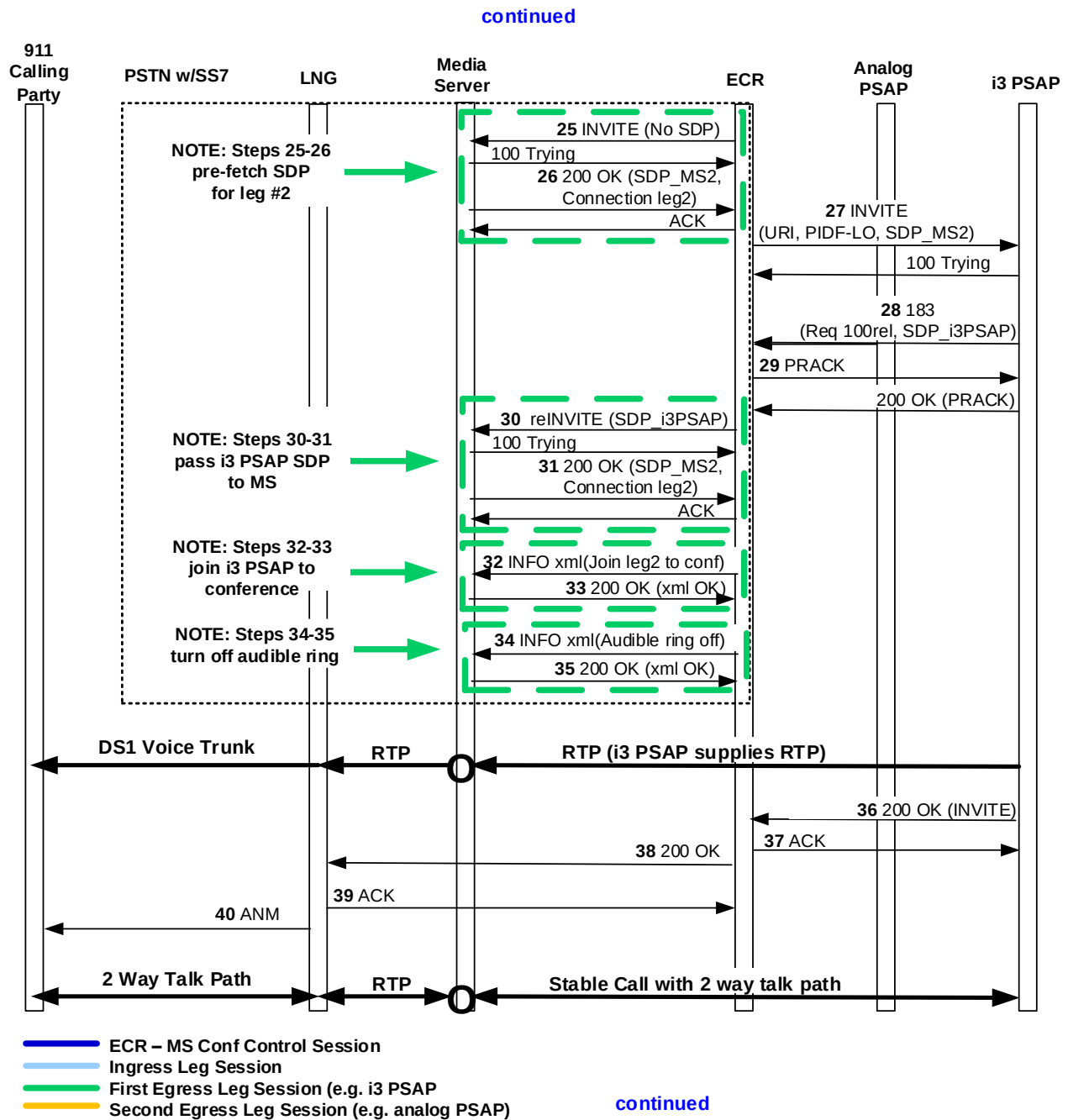


Figure 20: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 3 of 5)

25. Anticipating an INVITE to the destination of step 23, the ECR goes to the MS to 'pre-fetch' the SDP information. The ECR does this by sending an INVITE with no SDP to the MS on a new session, called the 'First Egress Leg Session' in the diagram above. The MS responds with a 100 Trying.
26. The MS then responds with a 200 OK, which includes the SDP information (labeled SDP_MS2) as well as the connection ID for this RTP stream (labeled Connection leg2).
27. The ECR sends a SIP INVITE to the i3 PSAP identified in step 23. The 9-1-1 caller's calling party number is in the FROM: header. The MS SDP, SDP_MS2 is also included in this INVITE. Most importantly, the INVITE contains the PIDF-LO information of the calling party. The i3 PSAP responds with a 100 Trying.
28. This i3 PSAP sends a 183 to emulate an analog PSAP and provide a PSAP based announcement to the 9-1-1 caller while alerting a call taker to answer this call. When the PSAP answers the call by sending a 200 OK to the ECR, the 2-way talk path is already cut through. (Alternatively, a 180 could have been returned which would tell the ECR that MS provided audible ringing remains on the conference until a 200 OK answer is received from the PSAP.)
29. The ECR PRACKs the 183, and the i3 PSAP responds by 200 OKing the PRACK.
30. On the first destination MS session, the ECR re-INVITES the MS to pass the SDP obtained in the 183 of step 28 (SDP_i3PSAP). The MS responds with a 100 Trying.
31. The MS then responds with a 200 OK, passing again the SDP (SDP_MS2) and connection information (Connection leg2) previously sent in step 26.
32. The ECR then sends the MS (on the first egress leg session) an INFO, instructing the MS to join the connection of step 31 to the conference of step 8. This will connect the second leg of the call (with the i3 PSAP) into the call conference.
33. The MS responds with a 200 OK. At this point there is a talk path from the i3 PSAP to the calling party, so that the calling party can hear audible ringing (or announcement) being played by the i3 PSAP.
34. ECR (on the first ingress leg session) sends an INFO instructing the MS to remove its audible ringing, leaving only the i3 PSAP audible ringing.
35. The MS 200 OKs back that the audible ring removal was successful.
36. When the PSAP call taker answers the call, a 200 OK is sent in response to the INVITE sent between the ECR and i3 PSAP.
37. The ECR ACKs the i3 PSAP answer.
38. The ECR answers the INVITE from step 2 with a 200 OK.
39. The LNG ACKs the answer of step 38.
40. The LNG sends the Answer (ANM) message via SS7 to the originating end office. The call is now in the stable, answered, two-way talk path state.

continued

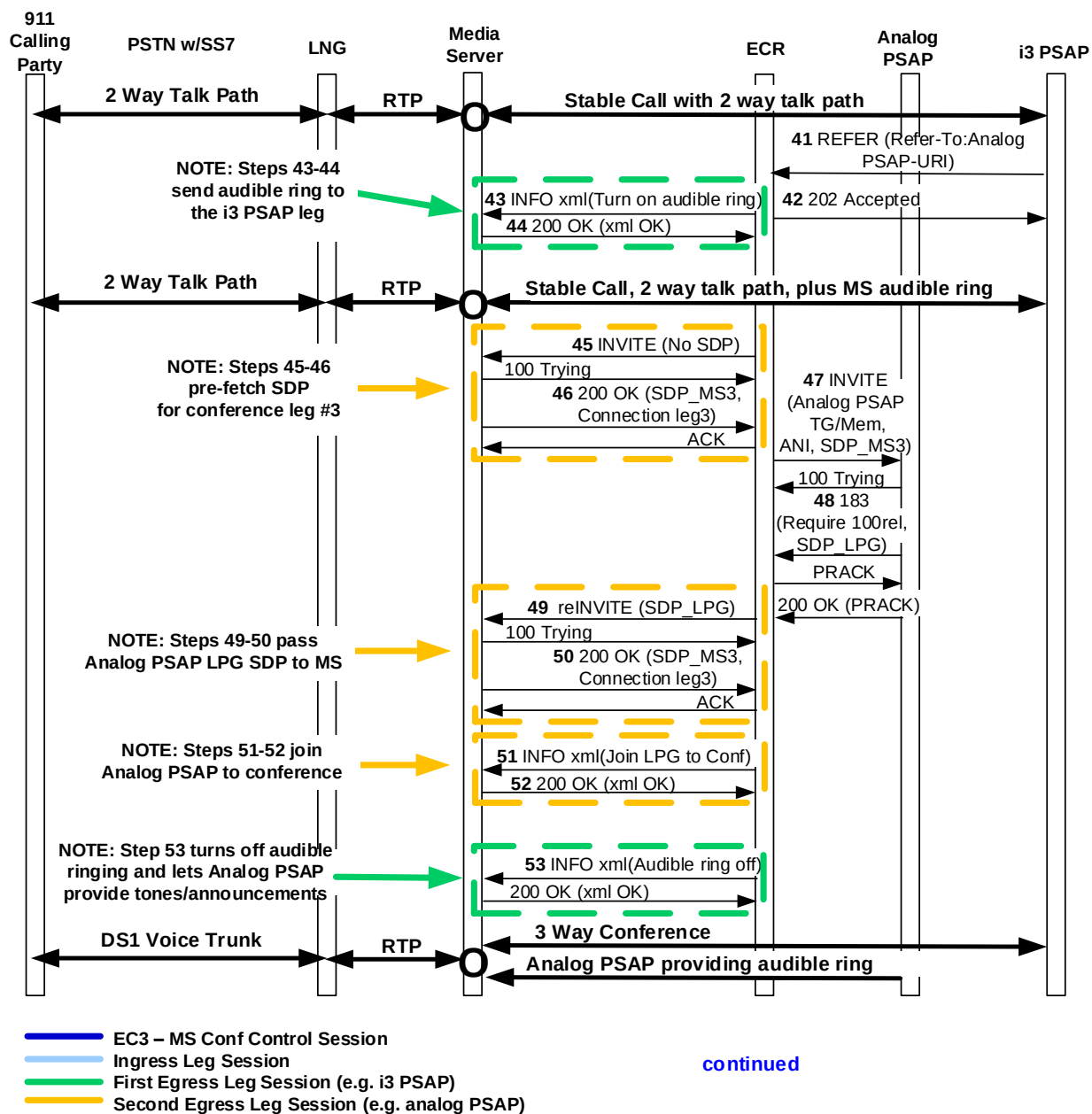


Figure 21: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 4 of 5)

41. The i3 PSAP call taker wants a 3-way bridge, so a REFER is sent to the ECR with the Refer-To set to the URI which corresponds to the analog PSAP desired to add to the conference.
42. The ECR returns a 202 Accepted agreeing to attempt the 3-way conference.
43. The ECR instructs the MS to play audible ringing to the i3 PSAP.

44. The MS 200 OKs, indicating the audible ringing is playing.
45. Similar to steps 25-35 (which added the first egress leg), steps 45– 53 add the second egress leg, starting with a pre-fetch of SDP from the MS by sending an INVITE with no SDP.
46. The MS then responds with a 200 OK, which includes the SDP information (labeled SDP_MS3) as well as the connection ID for this RTP stream (labeled Connection leg3).
47. The ECR sends a SIP INVITE to the MG of the analog PSAP identified in step 41. The MS SDP, SDP_MS3 is included in this INVITE. The MG of the analog PSAP responds with a 100 Trying.
48. The analog PSAP MG sends a 183 to the ECR with the SDP of the MG (labeled SDP_LPG). The ECR PRACKs the 183, and the analog PSAP MG responds by 200 OKing the PRACK.
49. On the second egress leg MS session, the ECR re-INVITES the MS to pass the SDP obtained in the 183 of step 48 (SDP_LPG). The MS responds with a 100 Trying.
50. The MS then responds with a 200 OK, passing again the SDP (SDP_MS3) and connection information (Connection leg3) previously sent in step 46.
51. The ECR then sends the MS (on the second egress leg session) an INFO, instructing the MS to join the connection of step 50 to the conference of step 8. This will connect the third leg of the call (with the analog PSAP) into the call conference.
52. The MS responds with a 200 OK. At this point there is a 3-way conference between the i3 PSAP, the analog PSAP (which has been alerted and is about to answer), and the calling party.
53. The ECR then sends the MS (on the first egress leg session, to the i3 PSAP) an INFO, telling the MS to remove audible ringing. At this point the 3-way conference has the analog PSAP supplying audible ringing to the conference.

continued

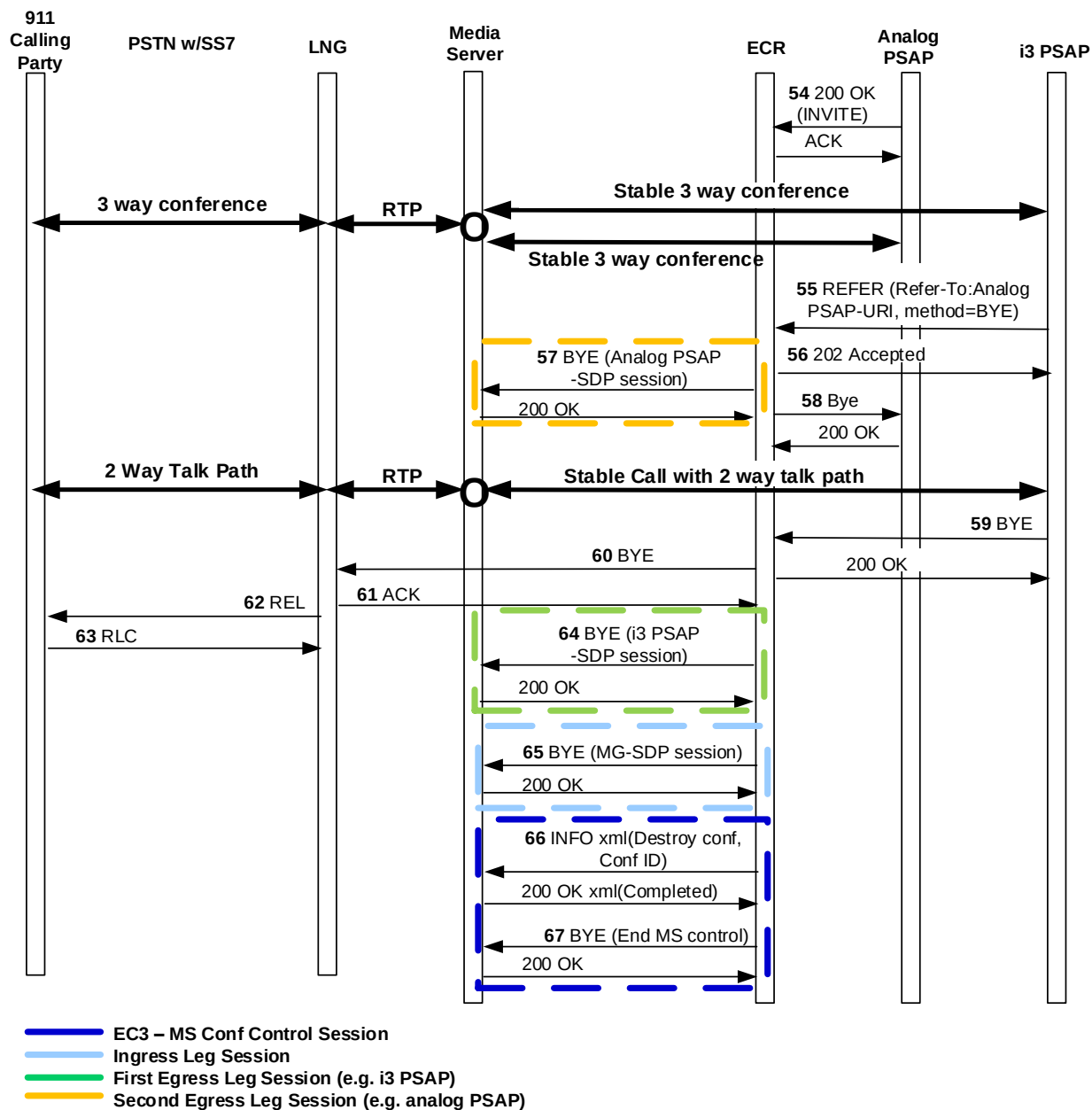


Figure 22: Call Flow A—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Attended Call Transfer) (Graphic 5 of 5)

54. The analog PSAP answers the call, so the PSAP MG sends a 200 OK to the ECR, which ACKs in response. The analog PSAP would have also removed the audible ringing, and at this point we are at the stable 3-way portion of the call.
55. The i3 PSAP decides to drop the analog PSAP from the 3-way conference, so another REFER with a BYE method, and the URI of the analog PSAP as the Refer-to is sent to the ECR.
56. The ECR 202 Accepts, indicating it understands and will process the REFER request.
57. The ECR (on the second egress leg session to the MS) sends a BYE to tear down the third leg of the conference. The MS 200 OKs, indicating the leg has been removed from the conference.
58. The ECR also BYEs the MG of the analog PSAP, which responds with a 200 OK. Now we are back to a 2-way conference call between the 9-1-1 caller and the i3 PSAP.
59. The i3 PSAP decides to disconnect, so a BYE is sent to the ECR.
60. - 67. The ECR, since there is only one (1) party left in the conference, tears down all remaining resources (MS connections and conference) as well as disconnecting the 9-1-1 calling party.

3.2 Call Flow A2—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Blind Call Transfer)

The following call flow consists of an SS7 origination using ECRF routing logic to terminate on an i3 PSAP. Then, the i3 PSAP invokes a “blind” transfer to an analog PSAP which connects the calling party to the analog PSAP while disconnecting the i3 PSAP.

The initial call setup (steps 1 – 40) is identical to the previous ‘attended call transfer’ described in Call Flow A, so this call flow starts at step #40, with the calling party in a stable call talking to the i3 PSAP call taker.

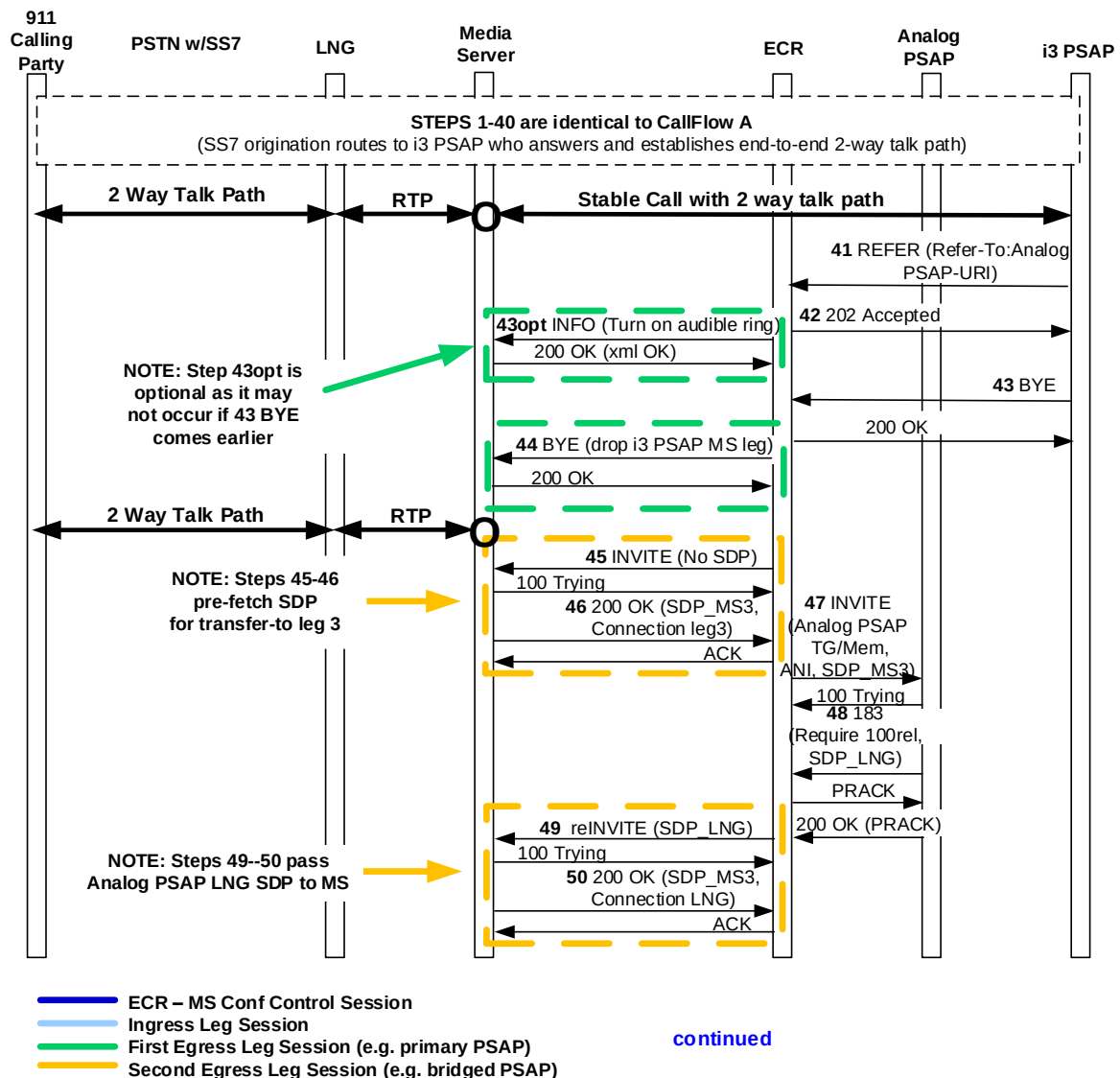


Figure 23: Call Flow A2—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Blind Call Transfer) (Graphic 1 of 2)

41. The i3 PSAP call taker wants to blind transfer to an analog PSAP, so a REFER is sent to the ECR with the Refer-To set to the URI which corresponds to the analog PSAP.
42. The ECR returns a 202 Accepted agreeing to attempt to signal the analog PSAP.
43. (This step 43 is optional and in addition to step 43 below.) Since the ECR doesn't know if this is a blind transfer or an attended transfer, if the i3 PSAP takes too long to send the BYE for the blind transfer, the ECR will assume an attended transfer and send instructions to the MS to play audible ringing to the i3 PSAP.
43. Since this is a blind transfer, shortly after sending the REFER in Step 41, the i3 PSAP sends a BYE to drop off the call.
44. The ECR sends a BYE to the MS to drop the i3 PSAP leg.
45. Similar to steps 25-35 of Call A, (which added the first egress leg), steps 45 – 52 add the analog PSAP egress leg, starting with a pre-fetch of SDP from the MS by sending an INVITE with no SDP.
46. The MS then responds with a 200 OK, which includes the SDP information (labeled SDP_MS3) as well as the connection ID for this RTP stream (labeled Connection leg3).
47. The ECR sends a SIP INVITE to the MG of the analog PSAP identified in step 41. The MS SDP, SDP_MS3 is included in this INVITE. The MG of the analog PSAP responds with a 100 Trying.
48. The analog PSAP MG sends a 183 to the ECR with the SDP of the MG (labeled SDP_LNG). The ECR PRACKs the 183, and the analog PSAP MG responds by 200 OKing the PRACK.
49. On the second egress leg MS session, the ECR re-INVITES the MS to pass the SDP obtained in the 183 of step 48 (SDP_LNG). The MS responds with a 100 Trying.
50. The MS then responds with a 200 OK, passing again the SDP (SDP_MS3) and connection information (Connection leg 3) previously sent in step 46.

57. The call is torn down on the SS7 link with the Release Complete response.
58. The ECR (on the second egress leg session to the MS) sends a BYE to tear down the analog PSAP leg of the call. The MS 200 OKs, indicating the leg has been removed from the conference.
59. The ECR also BYEs the MG of the ingress MG, which responds with a 200 OK.
60. The ECR cleans up the MS conference resource by sending a Destroy conference message.
61. The ECR tears down the last item, the control session to the MS.

3.3 Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference)

This call flow follows the same origination, routing, and i3 PSAP initial termination as the previous A and A2 Call Flows; however, in this scenario, the i3 PSAP starts a multi-way bridge. The first bridge is an analog PSAP, then this same i3 PSAP requests two additional i3 PSAPs to be added for a 5-way conference. At the end of the conference, all legs disconnect.

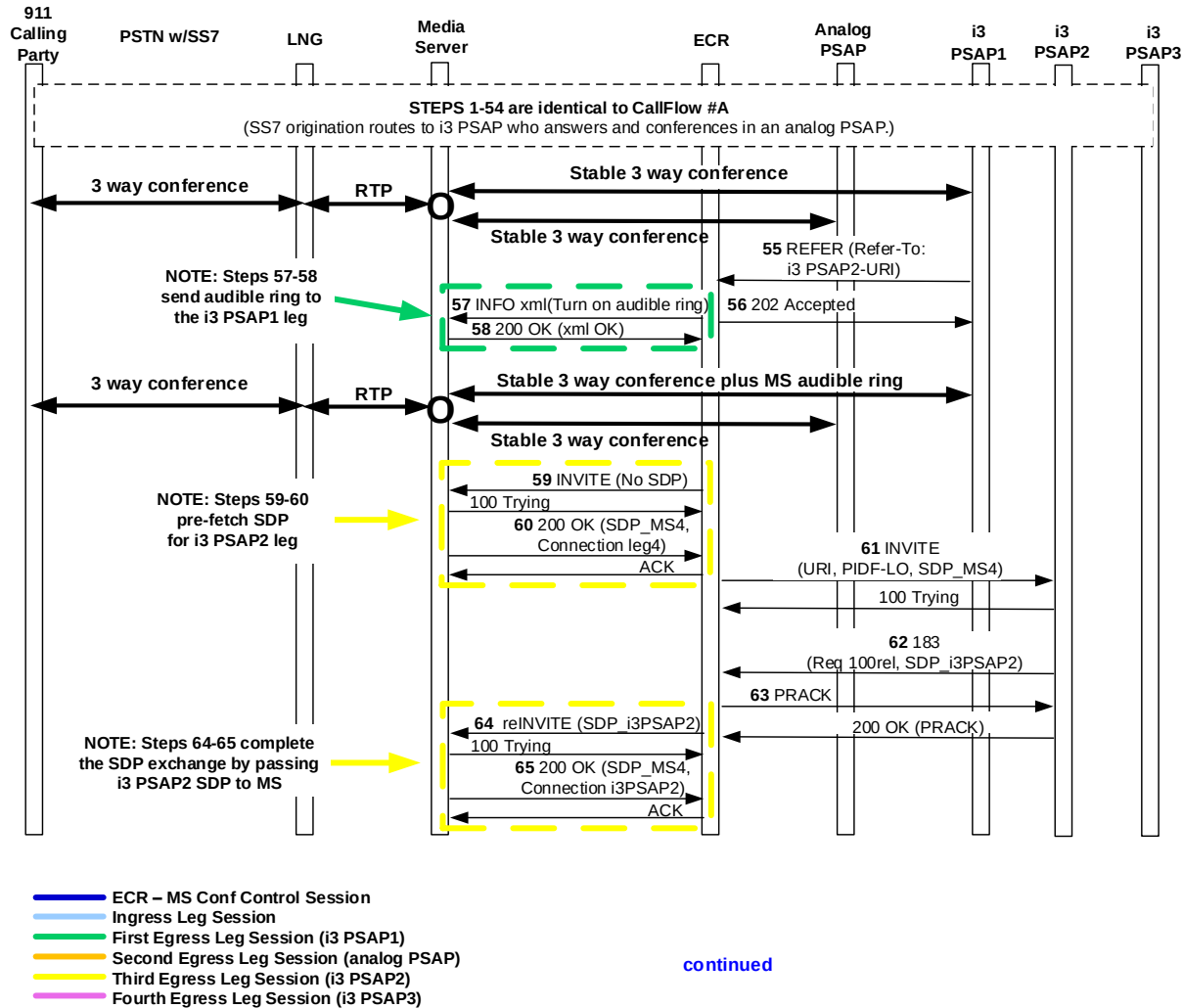


Figure 25: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 1 of 4)

1. – 54. These steps are identical to Call Flow A, and result in a stable 3-way conference between the 9-1-1 caller, the original i3 PSAP, and the last added leg (to an analog PSAP).
55. – 58. The original i3 PSAP signals a request to add i3 PSAP2 as the fourth leg of the conference, which the ECR accepts with a 202 Accepted. The ECR then turns on audible ringing towards the original i3 PSAP.
59. – 65. The ECR pre-fetches MS SDP for this fourth leg, then uses the SDP to setup the INVITE to i3 PSAP2. The i3 PSAP2 signals back the up through OKing the PRACK. The ECR then reINVITEs the MS with the SDP for i3 PSAP2.

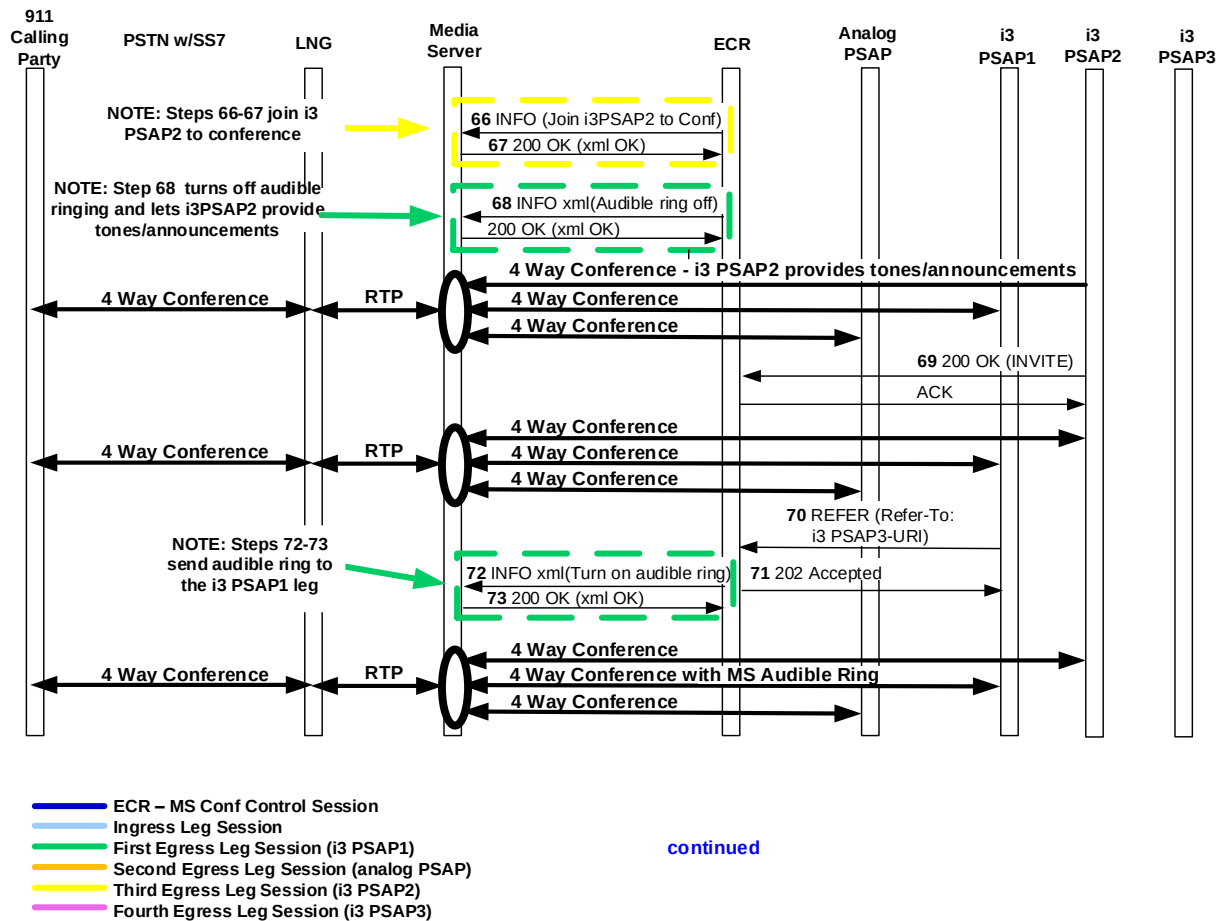


Figure 26: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 2 of 4)

66. – 68. The ECR signals the MS to join the new i3 PSAP₂ leg to the conference, and then turn off MS audible ring to i3 PSAP₁.
69. The new leg (i3 PSAP₂) answers the INVITE and creates a four-way conference call.
70. – 83. The original i3 PSAP adds a 5th leg to the conference by adding i3 PSAP₃.

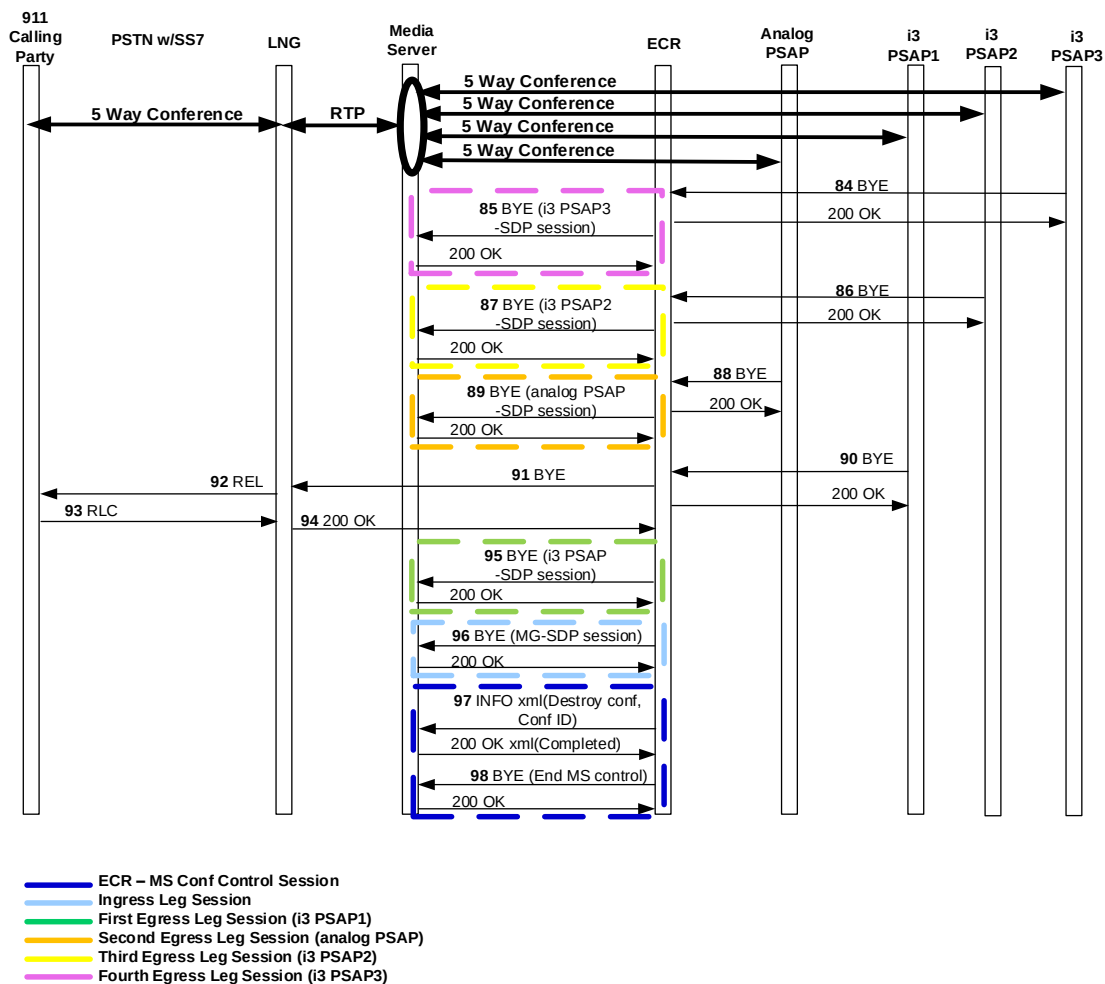


Figure 28: Call Flow A3—SS7 End Office via ECRF Routing Logic to an i3 PSAP (with Multi-Way Conference) (Graphic 4 of 4)

84. – 98. All conference participants disconnect from the call.

3.3.1 Call Flow B1—SS7 Ingress to ECR and Core

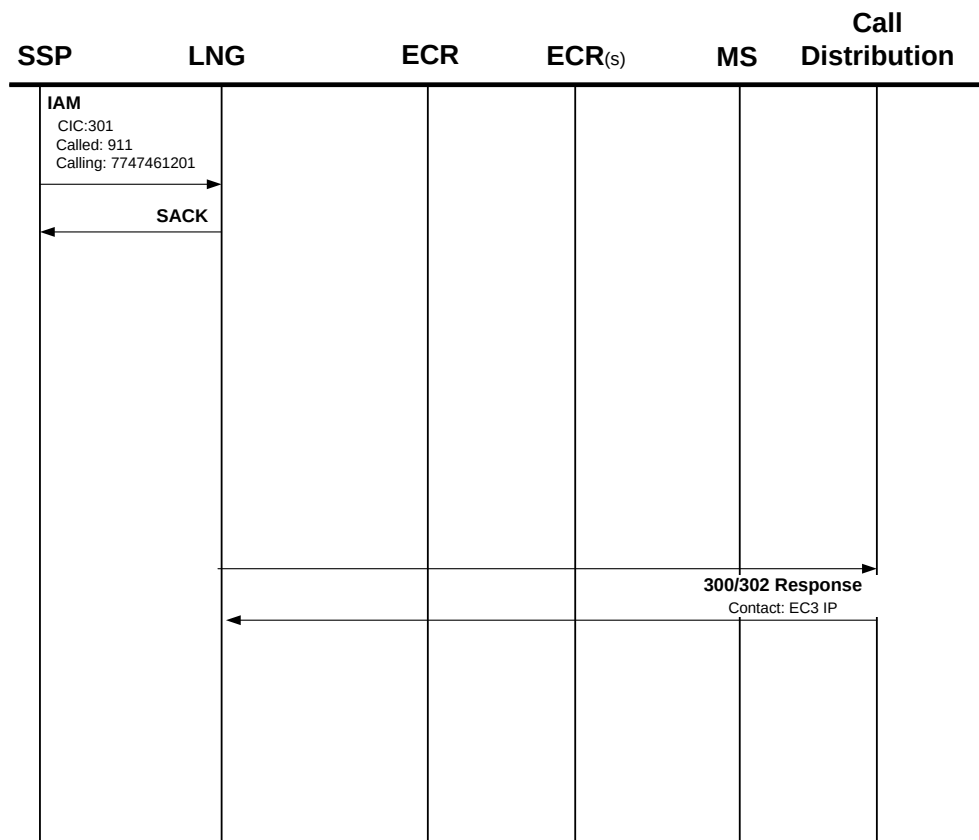


Figure 29: Call Flow B1—SS7 Ingress to ECR and Core (Graphic1 of 4)

3.3.2 Call Flow B2—SS7 Ingress to ECR and Core

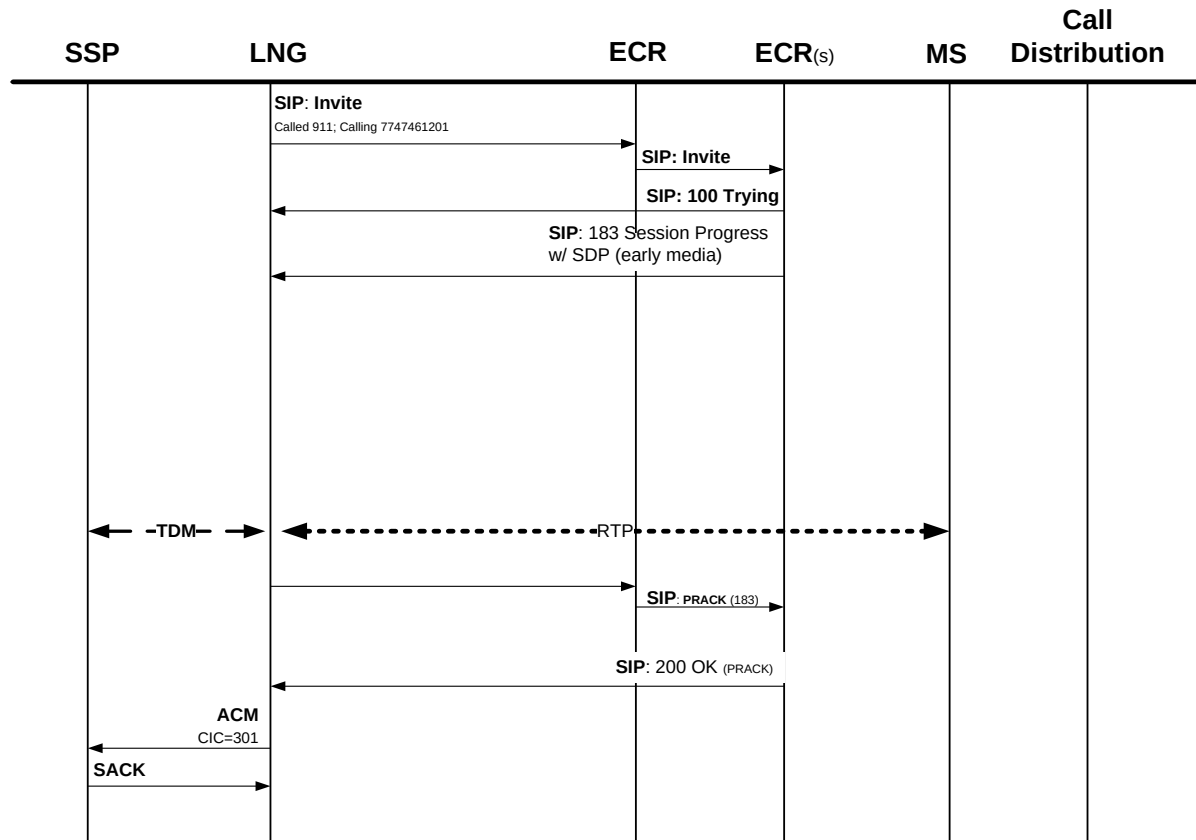


Figure 30: Call Flow B2—SS7 Ingress to ECR and Core (Continued Graphic 2 of 4)

3.3.3 Call Flow B3—SS7 Ingress to ECR and Core

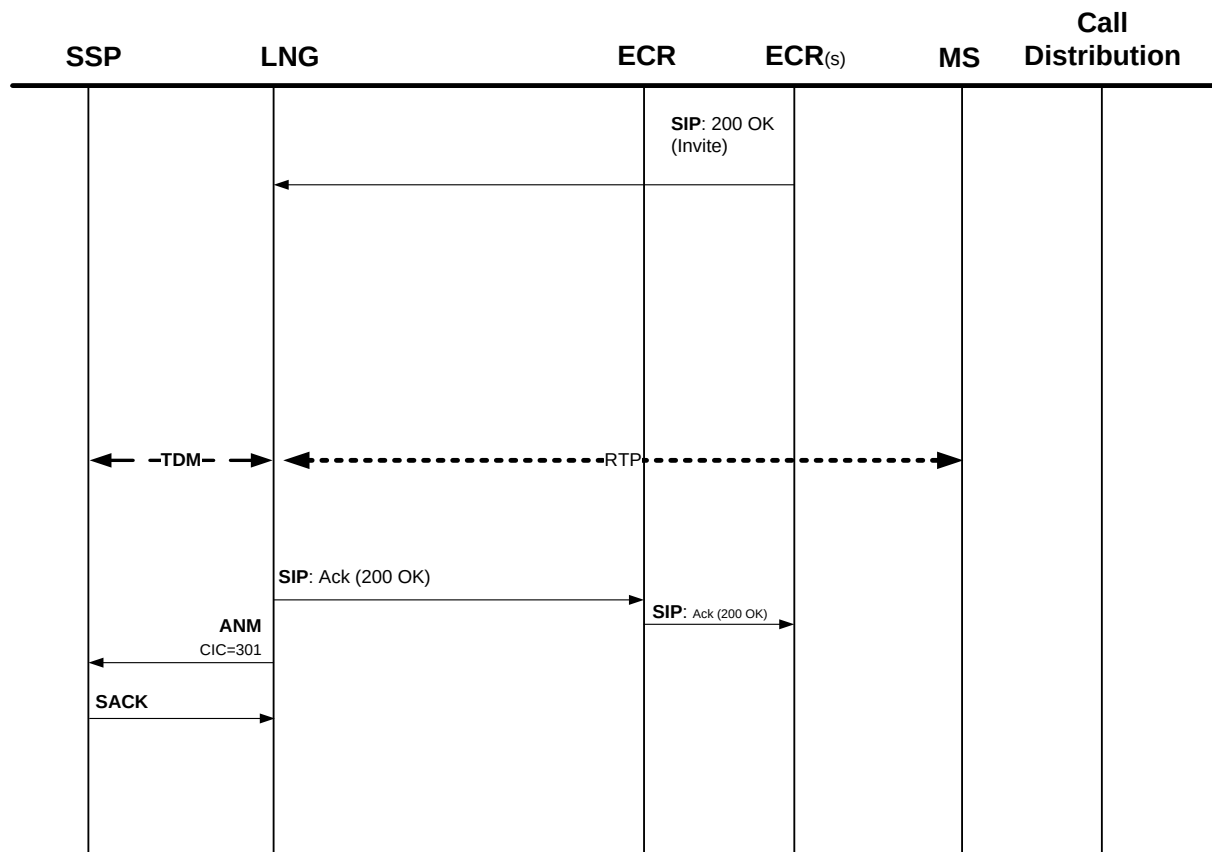


Figure 31: Call Flow B3—SS7 Ingress to ECR and Core (Continued Graphic 3 of 4)

3.3.4 Call Flow B4—SS7 Ingress to ECR and Core

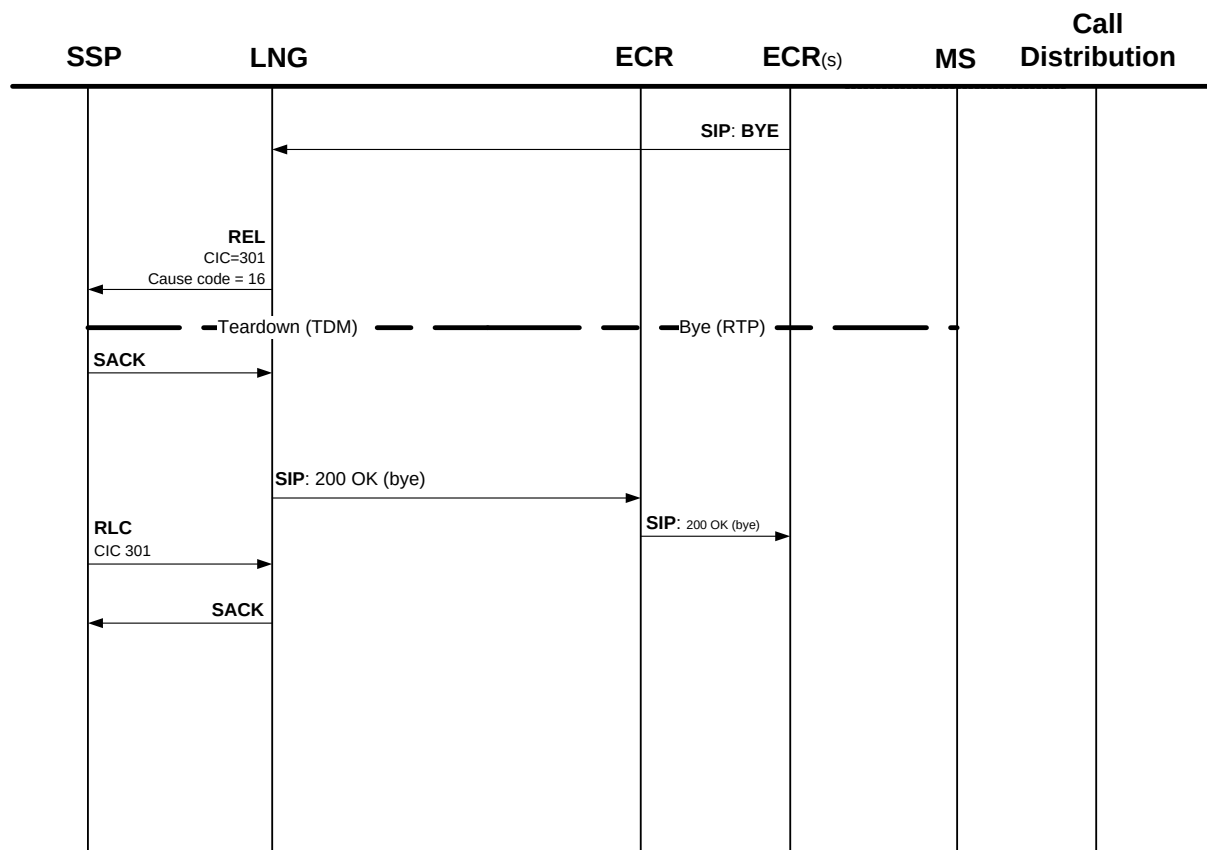


Figure 32: Call Flow B4—SS7 Ingress to ECR and Core (Continued Graphic 4 of 4)

3.3.5 Call Flow B5—Series 2—Compact Format

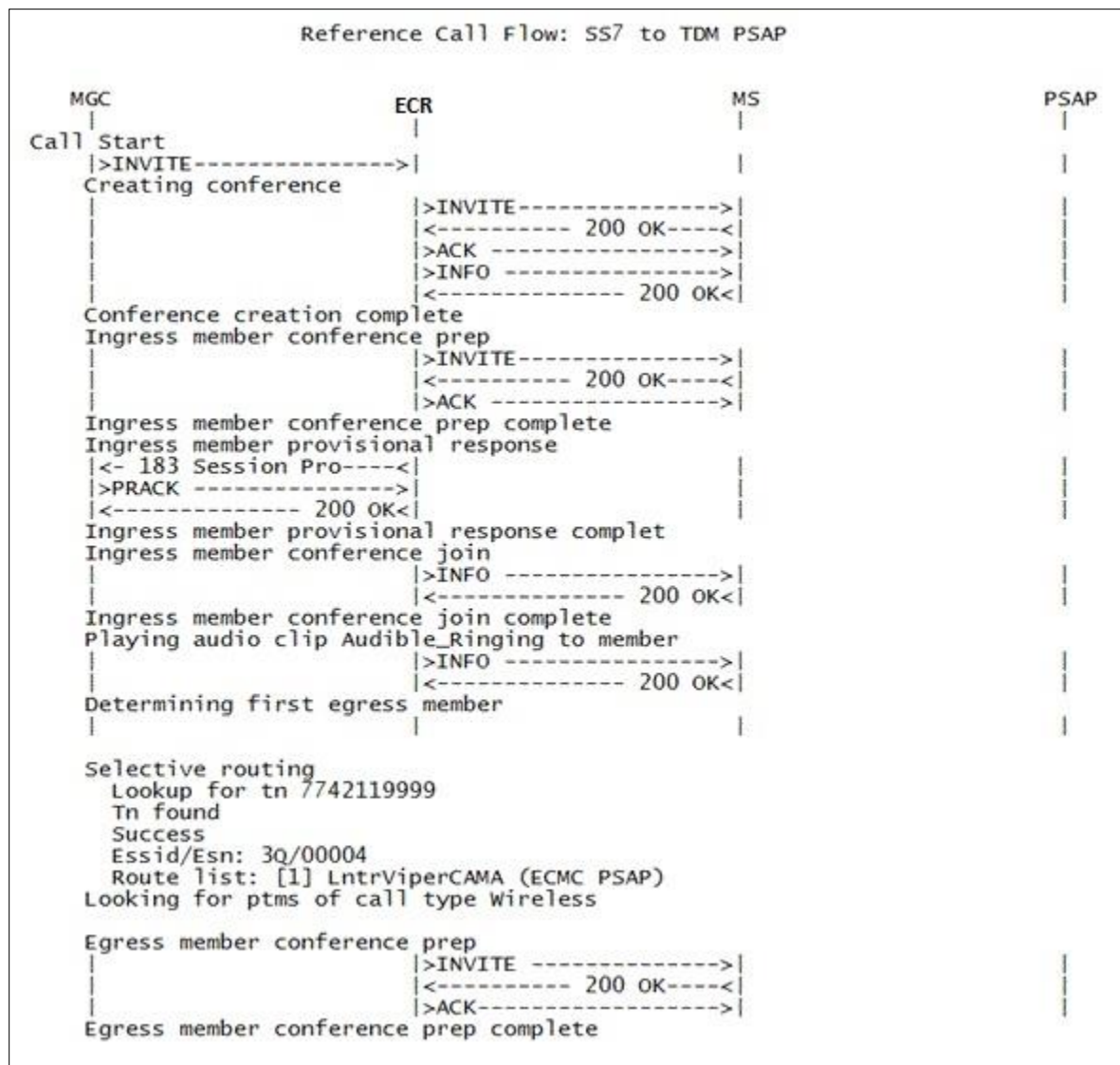


Figure 33: Call Flow B5—Series 2—Compact Format—SS7 to TDM PSAP (Graphic 1 of 2)

3.3.6 Call Flow B6—Series 2—Compact Format

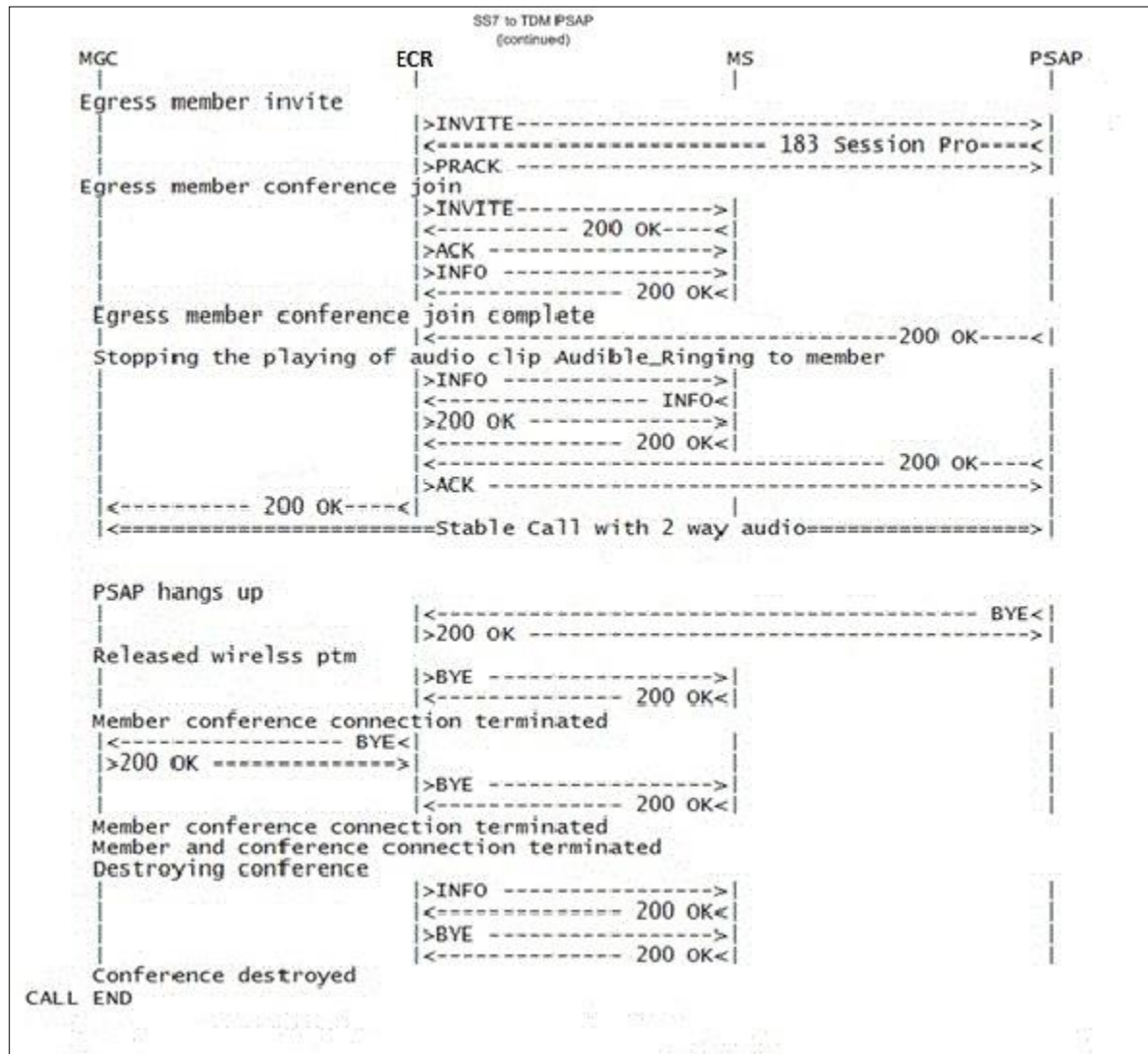


Figure 34: Call Flow B6—Series 2—Compact Format—SS7 to TDM PSAP (Graphic 2 of 2)

3.3.7 Call Flow B7 to B19—Series 2—Compact Format

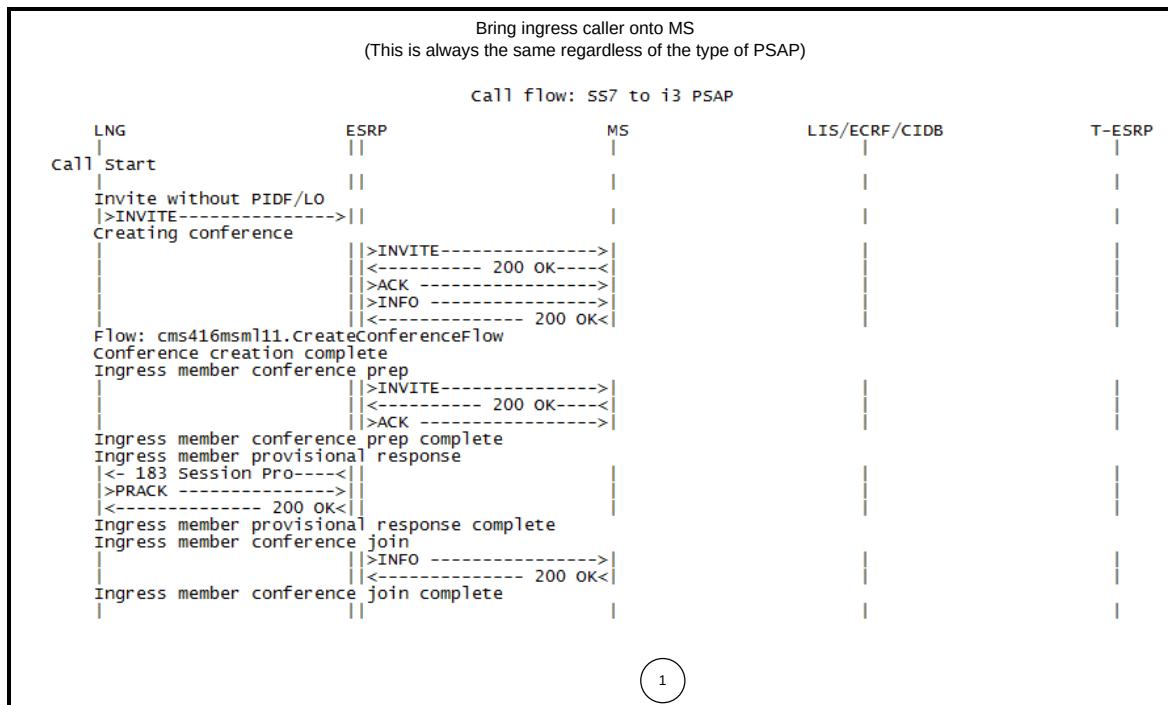


Figure 35: Call Flow B7 to B19—Bring Ingress Caller onto MS

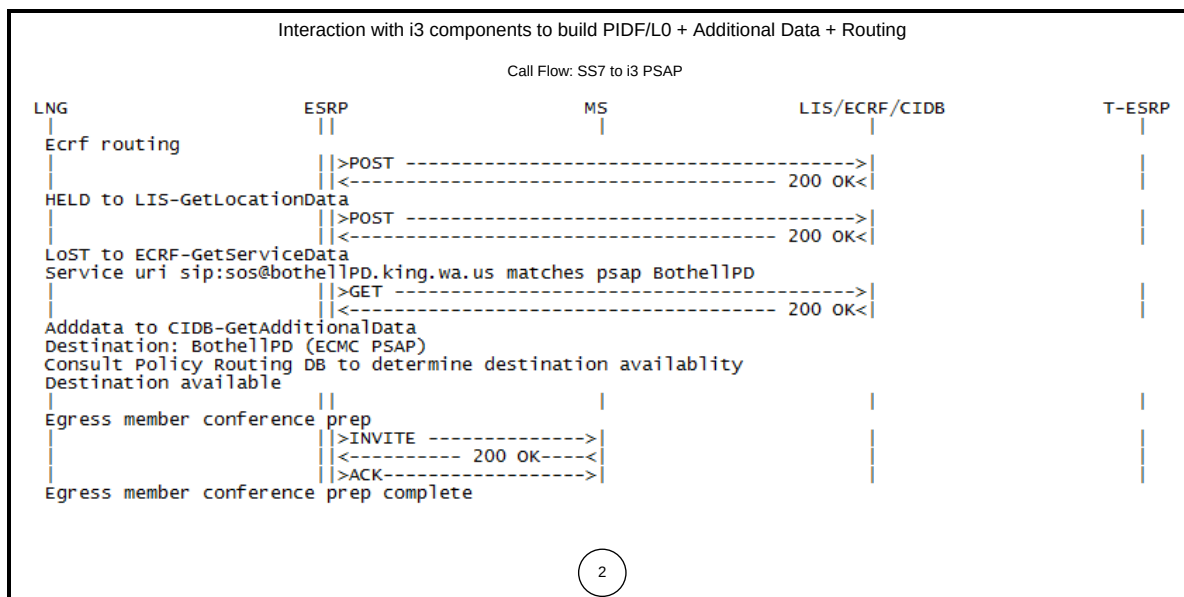


Figure 36: Call Flow B7 to B19—Interaction with i3 Components to Build PIDF/LO Plus Additional Data and Routing—SS7 to i3 PSAP

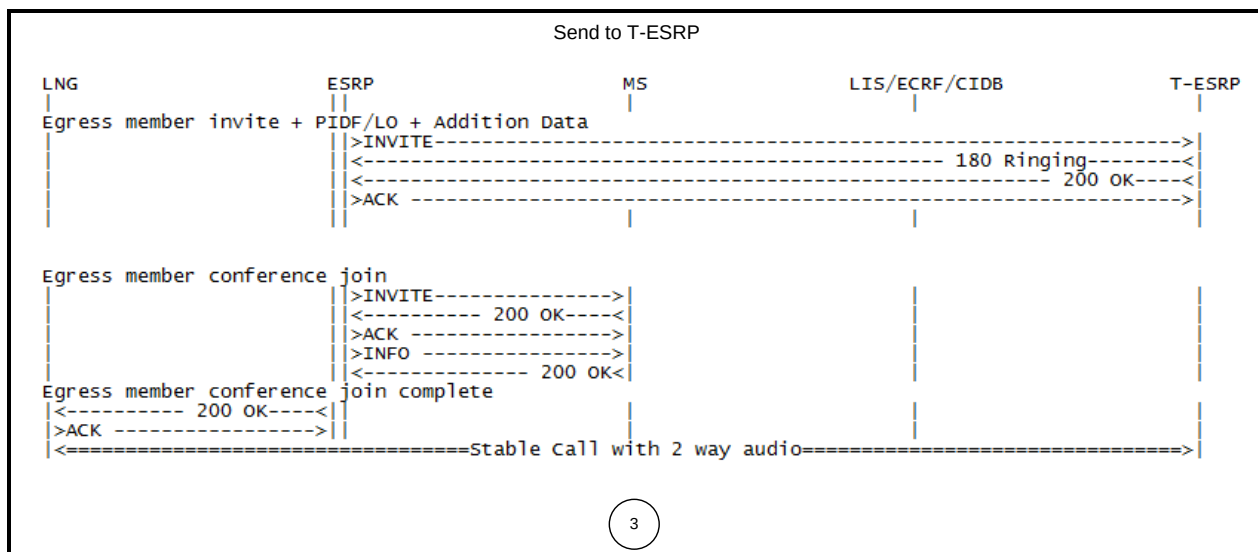


Figure 37: Call Flow B7 to B19—Send to T-ESRP

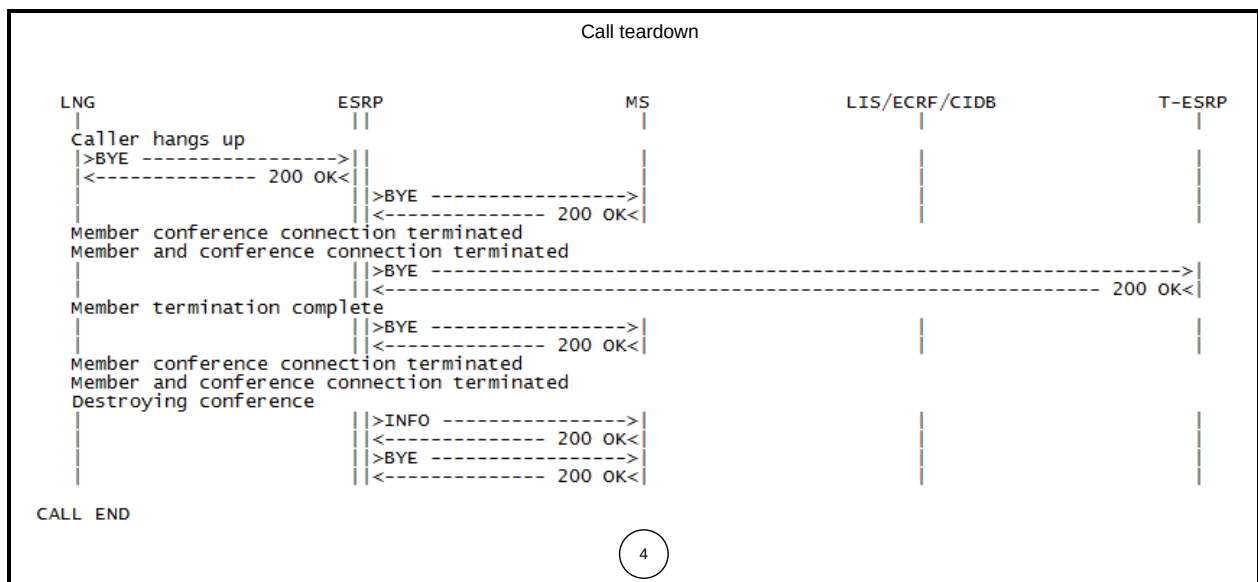


Figure 38: Call Flow B7 to B19—Call Teardown

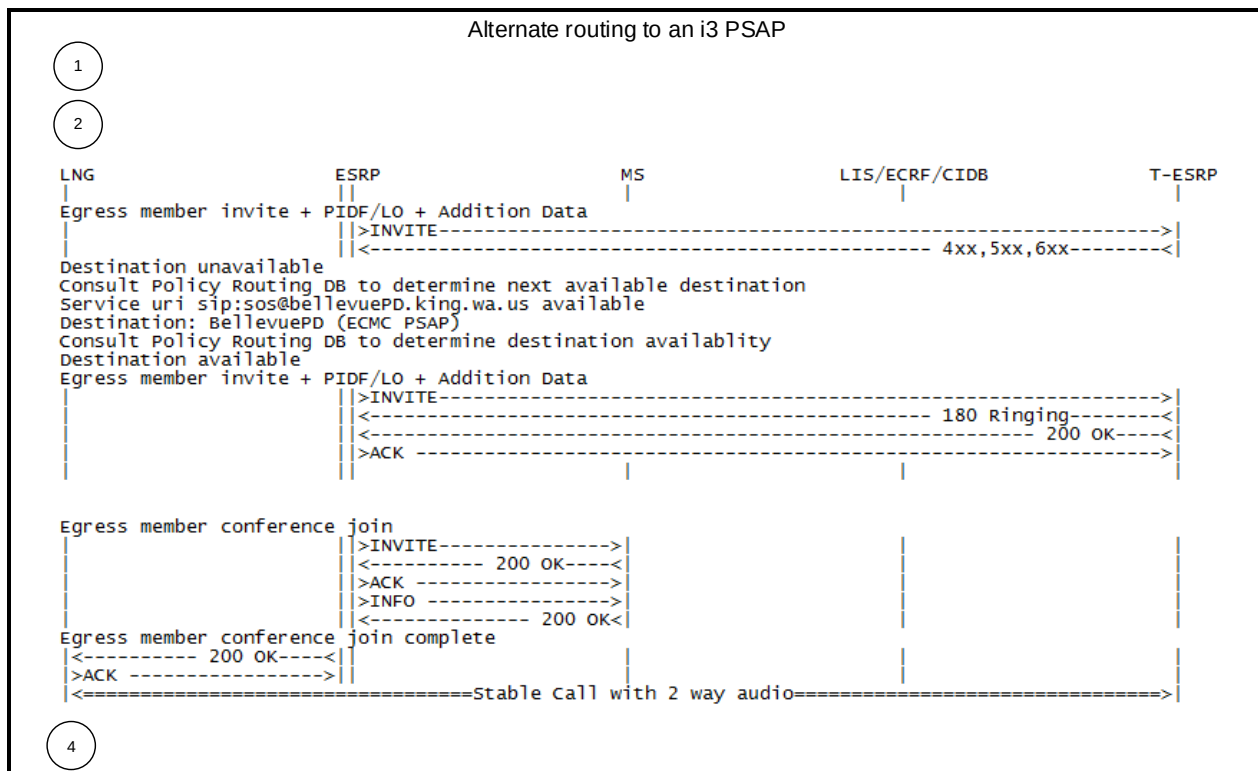


Figure 39: Call Flow B7 to B19—Alternate Routing to an i3 PSAP

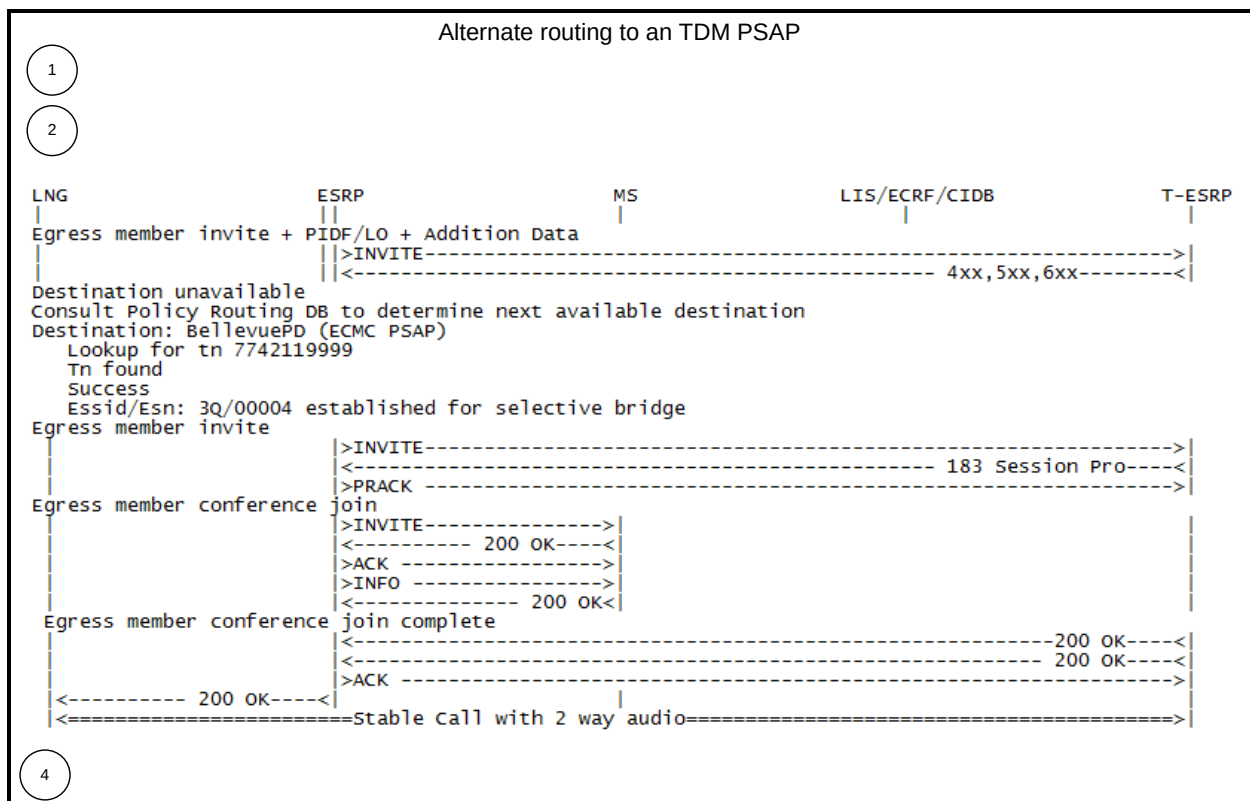


Figure 40: Call Flow B7 to B19—Alternate Routing to a TDM PSAP

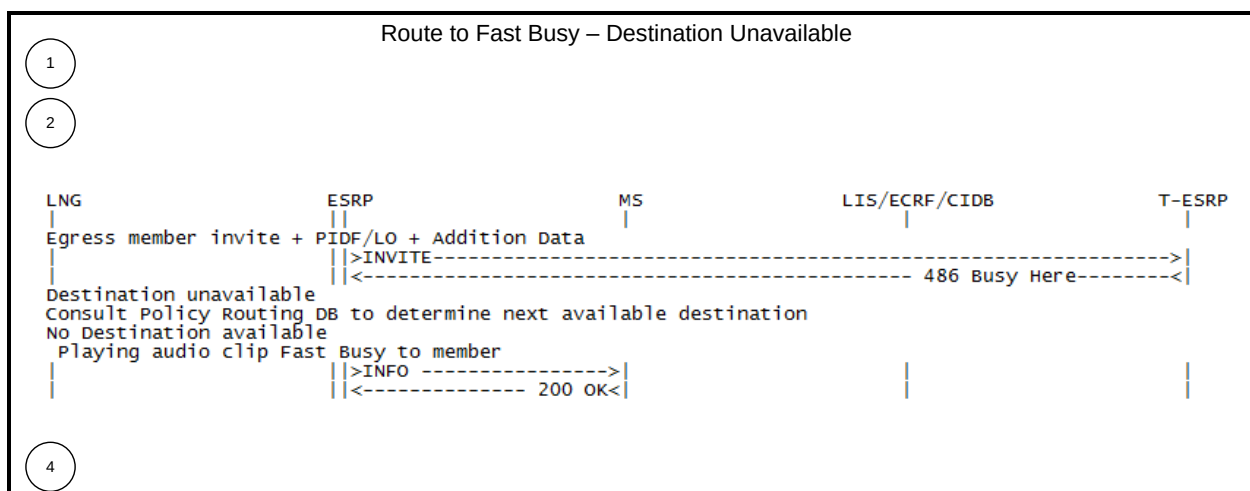


Figure 41: Call Flow B7 to B19—Route to Fast Busy—Destination Unavailable

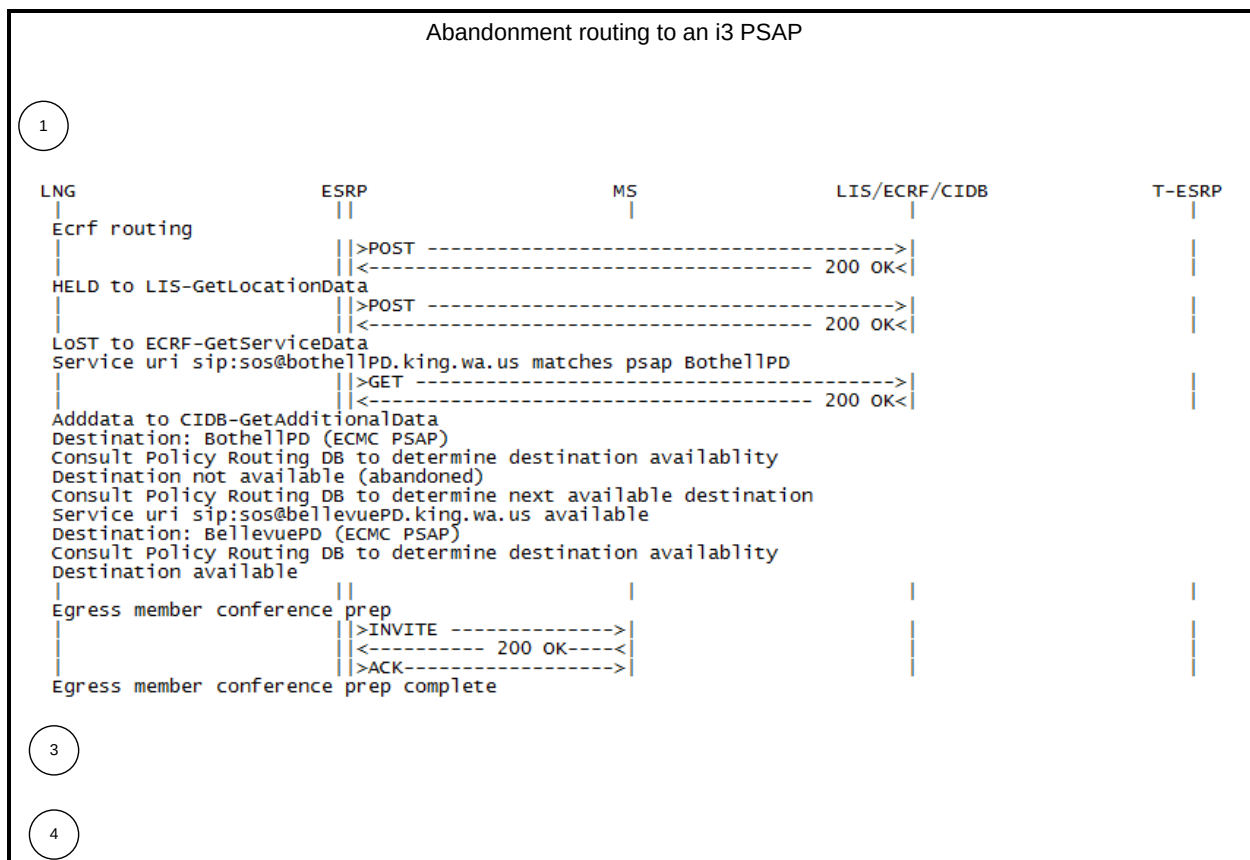


Figure 42: Call Flow B7 to B19—Abandonment Routing to an i3 PSAP

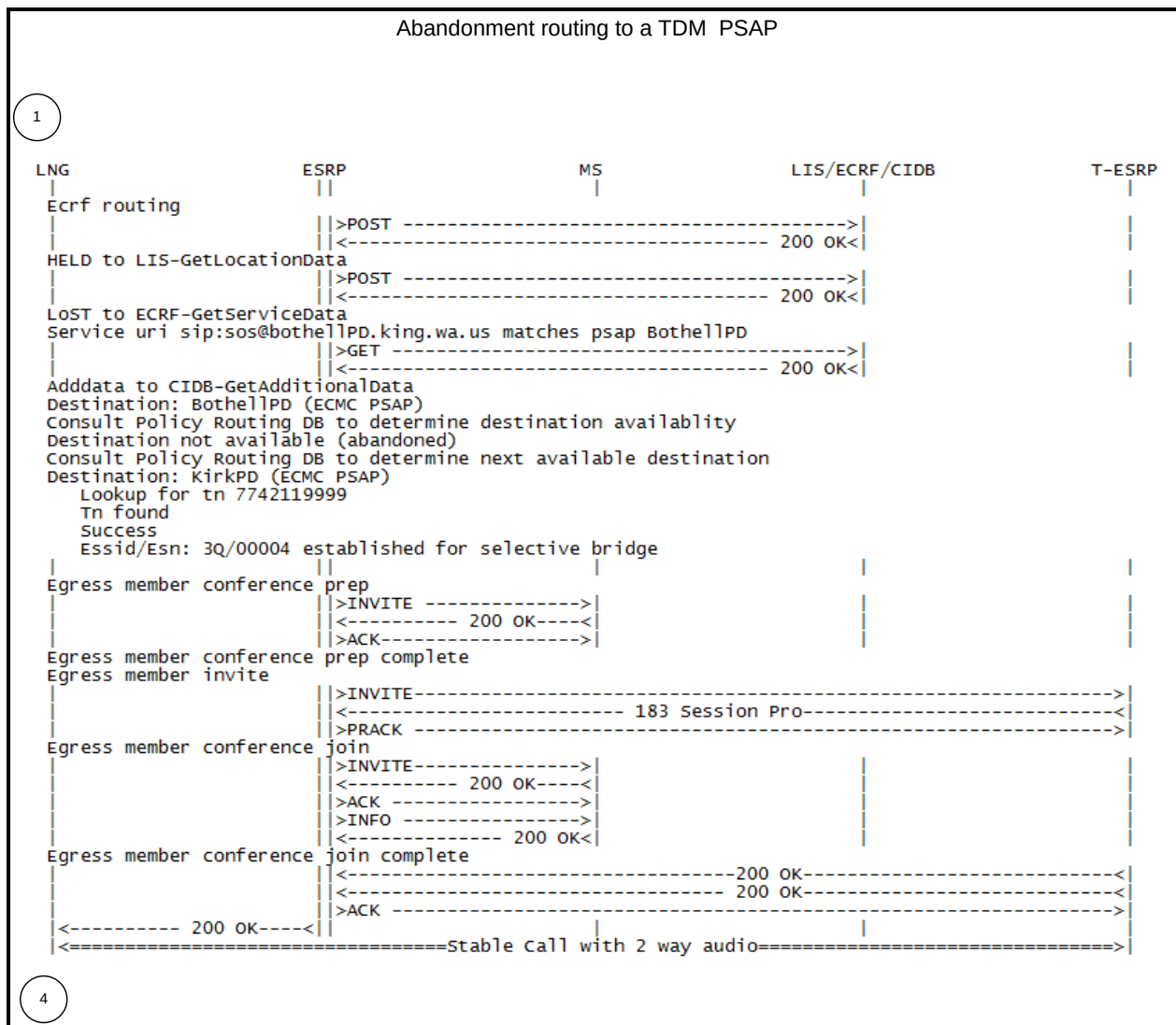


Figure 43: Call Flow B7 to B19—Abandonment Routing to a TDM PSAP

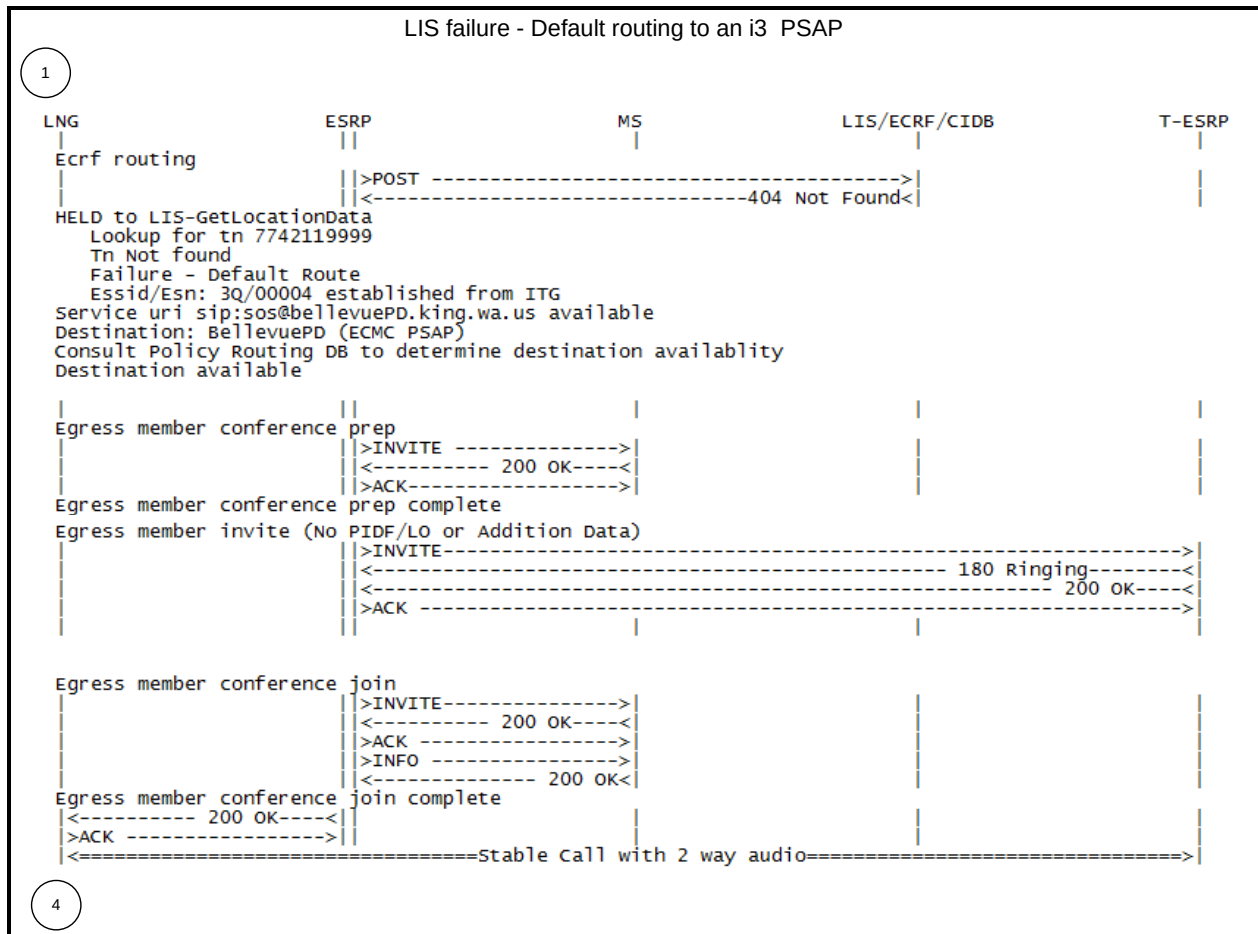


Figure 44: Call Flow B7 to B19—LIS Failure—Default Routing to an i3 PSAP

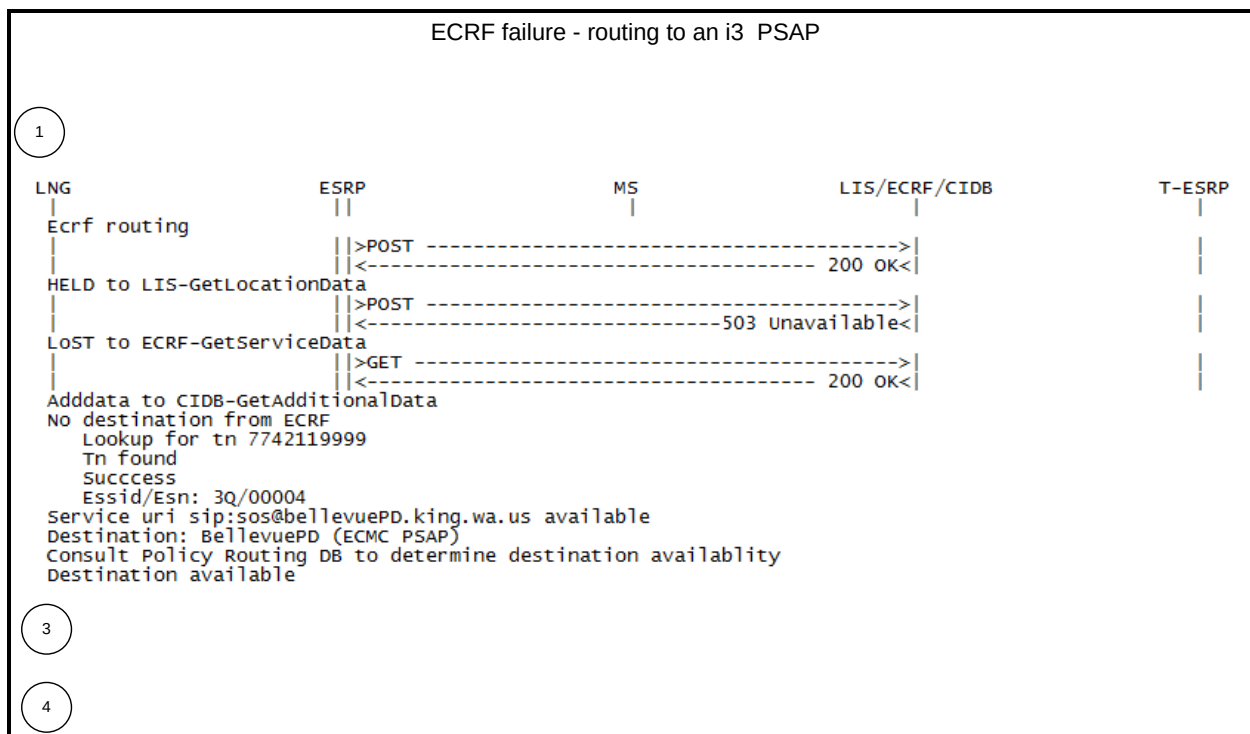


Figure 45: Call Flow B7 to B19—ECRF Failure—Routing to an i3 PSAP

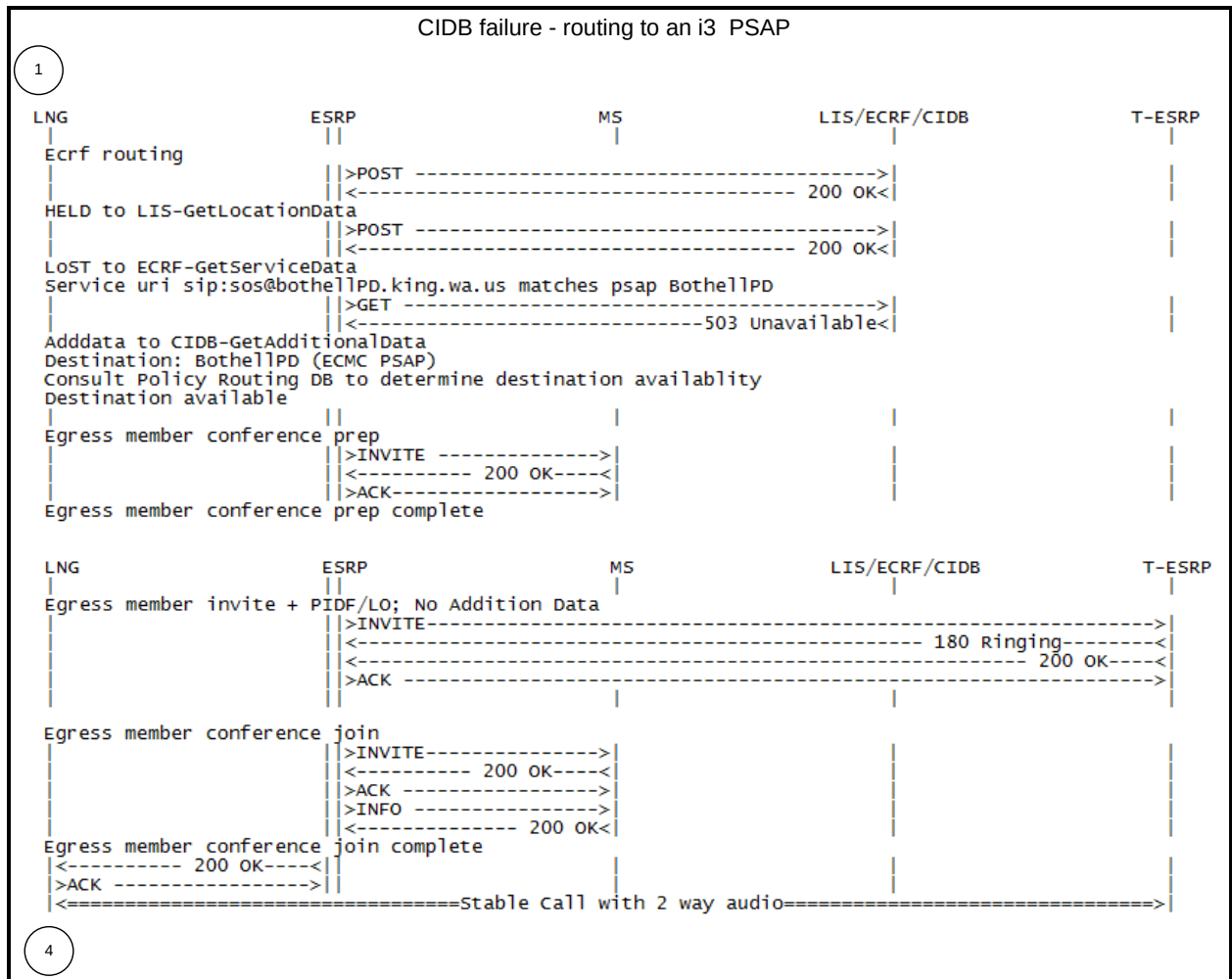


Figure 46: Call Flow B7 to B19—CIDB Failure—Routing to an i3 PSAP

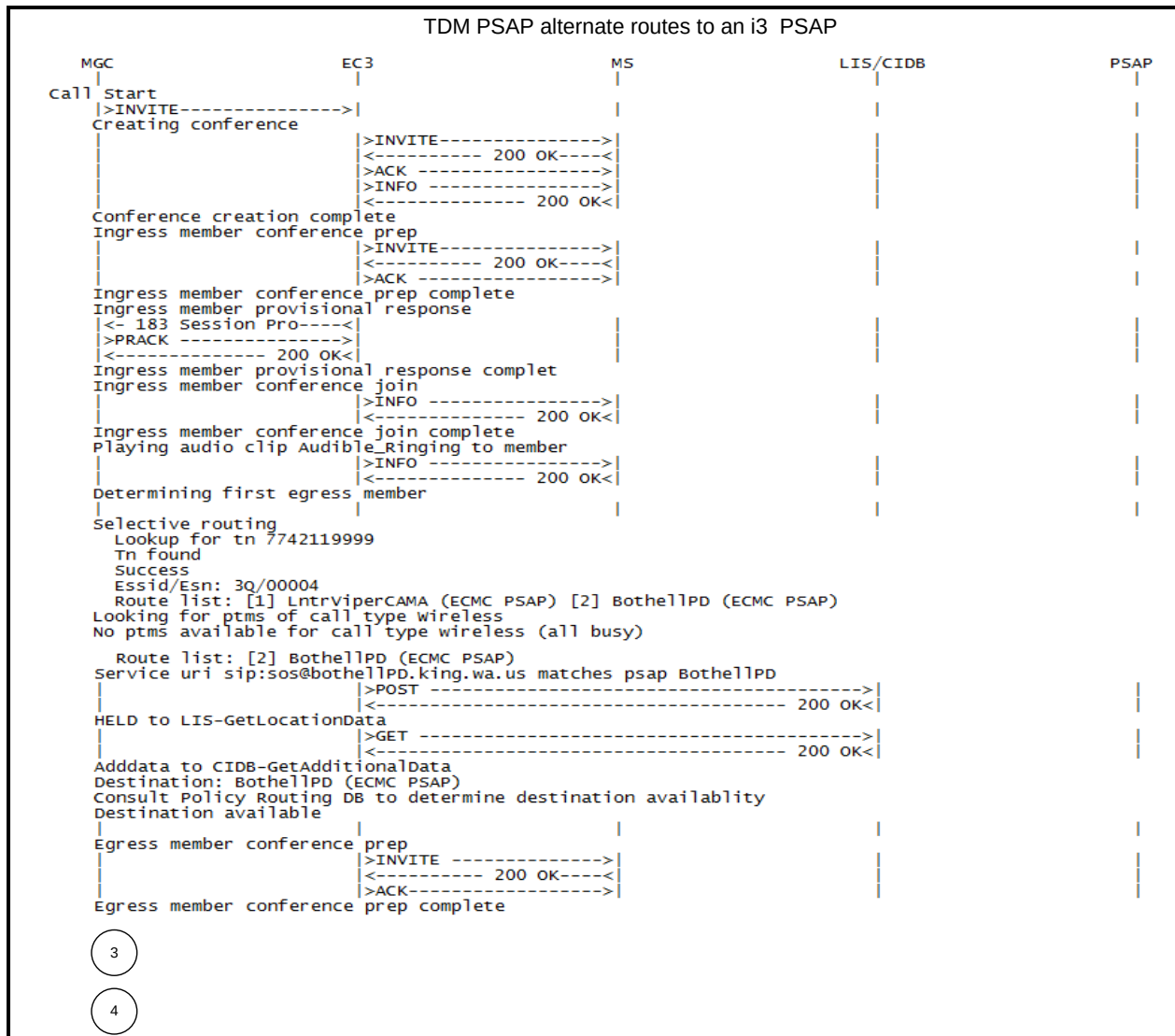


Figure 47: Call Flow B7 to B19—TDM PSAP Alternate Routes to an i3 PSAP

4.0 IP Ingress (not VSP)

In these call flows, the ingress is IP. The egress is to an IP PSAP, whether that PSAP is i3 capable or just RFAI. A TDM PSAP is also allowed, but no call flows are shown for it.

There are two kinds of IP ingress from an Originating Service Provider (OSP). The first is SIP Basic. The second is SIP i3. SIP Basic is TDM equivalency. So other than the interaction with the OSP SBC, the call flow interaction from the AT&T SBC thru the ECR to the PSAP is the same for a corresponding TDM call flow scenario. To illustrate this here is a generic SS7 ingress call.

OSP/9-1-1

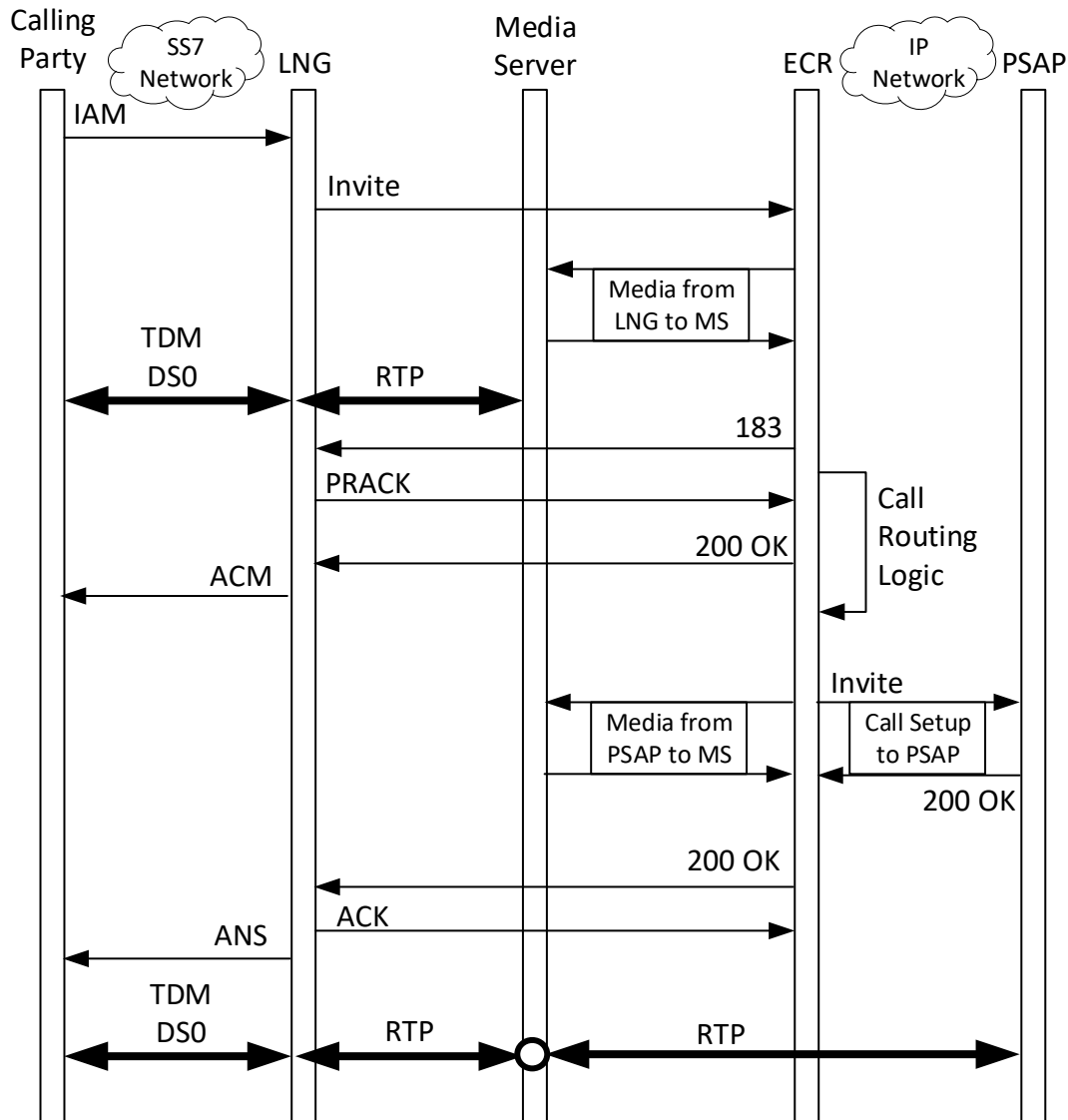


Figure 60: Generic SS7 ingress

For SIP Basic, here would be the generic call flow.:

OSP/9-1-1

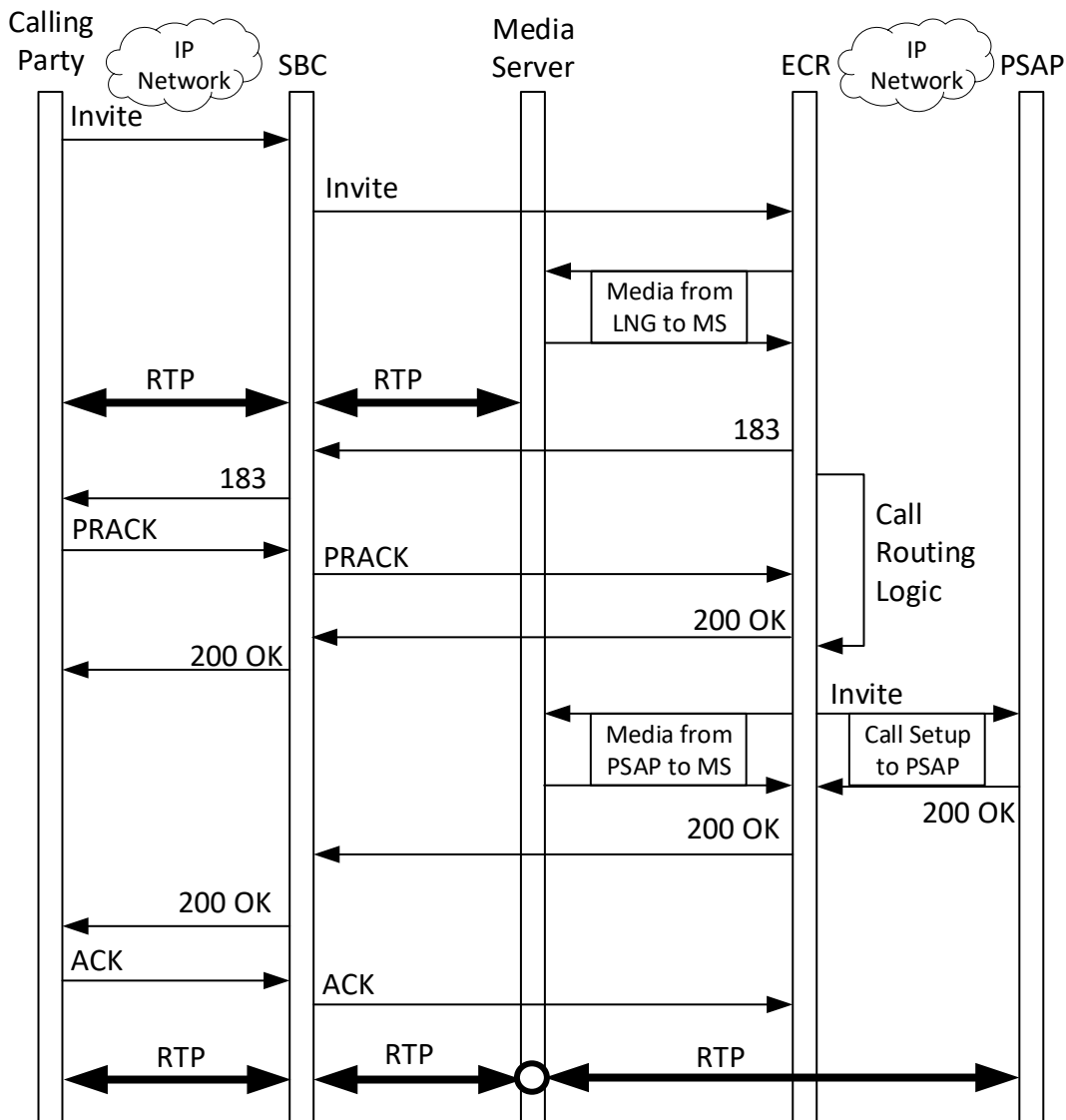


Figure 61: Generic IP SIP Basic Ingress

The only thing different in this call flow is the messaging from the far right side (the ingress method). The messaging from the LNG (for TDM) and SBC (for SIP Basic) is identical. Any of the call processing scenarios seen previously in this document are the same for TDM ingress versus IP SIP Basic ingress.

With IP SIP Basic ingress, if the call routing method is i3 (ECRF based call routing), the call flow uses i3 components to determine location, determine the routing, and provide additional data to format an i3 style SIP Invite to the T-ESRP (the PSAP). These components (LIS, ECRF, ADR) use HTTP(S) interfaces (POST or GET). In the call flows below, the POST/GET method has been replaced to show the i3 interface method (HELD, LoST, ADR) for clarity. AT&T uses an internal forest guide to determine the proper ECRF and GIS data set. This should not be confused with the National Forest Guide i3 component which currently does not exist. Again, even tho the ingress method is IP (SIP Basic), the call flows would be the same as with LNG ingress methods. Typically, for wireless and VoIP call types, the ANI is a pANI.

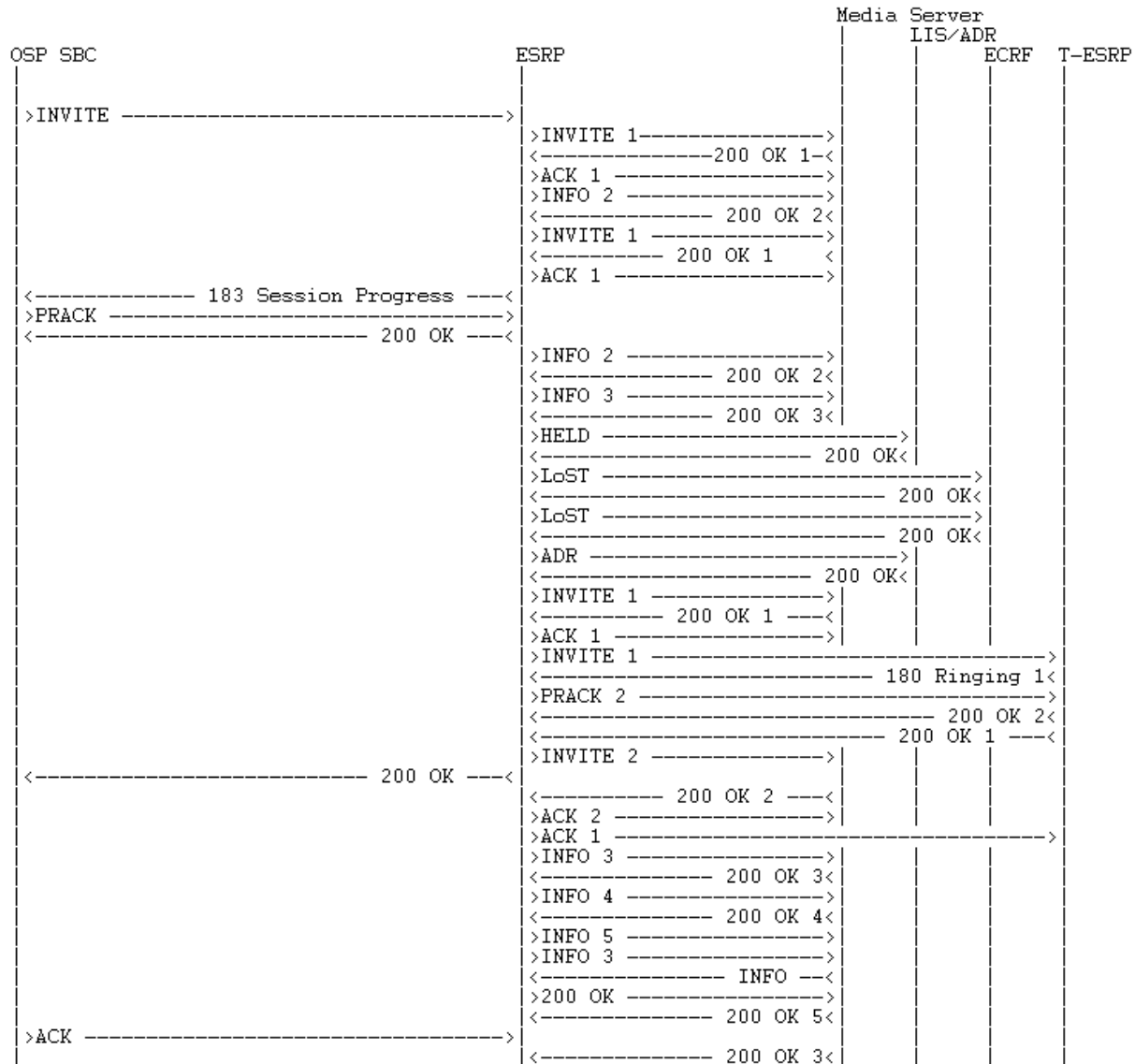


Figure 62: Standard i3 Call Flow

The ESRP to Media Server interactions are the same from previous call flows. The i3 part of the call flow is the HELD request to the LIS server to obtain location. The LoST requests to the ECRF (forest Guide to obtain AUS and resolution of the AUS to a PSAP URI). And finally an ADR request to obtain the additional data.

There are variations on the i3 call flows. One such call flow is where the location obtained from the LIS via HELD is not resolvable in the ECRF. An example of that would be a wireless call where the location could not be determined in the time allotted so information about the pANI shell record was returned. Shell records are not resolvable in an ECRF. Another example is where a location was returned but the accuracy of the location is not suitable for routing. At that point the ESRP falls back to alternative routing methods to determine a T-ESRP/PSAP. If the T-ESRP is an i3 T-ESRP, the the ADR query is made and the call then delivered to the T-ESRP. This call flow would look like this:

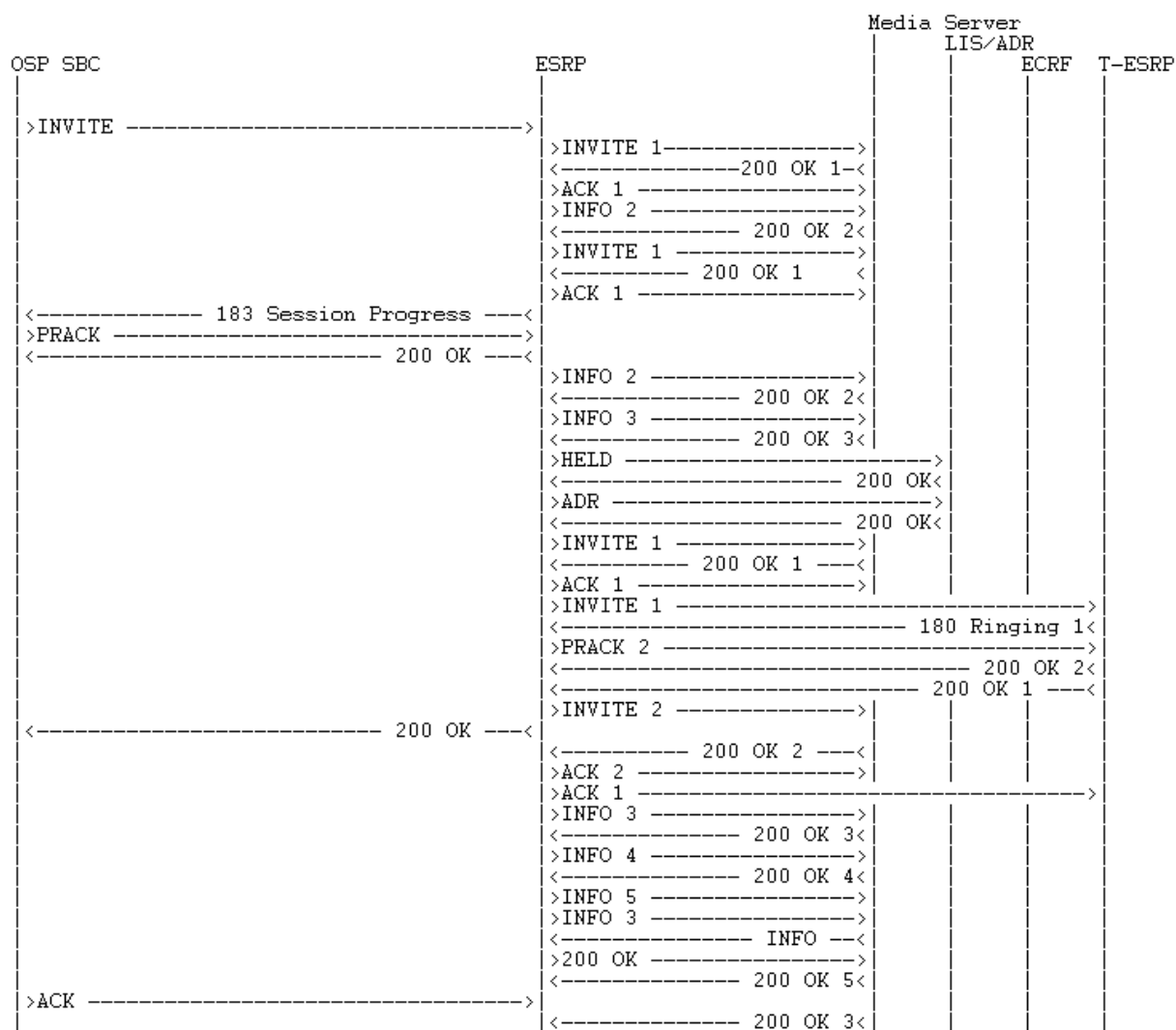


Figure 63: i3 Call Flow when location is unusable

Another call scenario in i3 call routing is after the HELD and LoSt queries, the resulting T-ESRP is not an i3 T-ESRP. At that point the ADR query would not be performed. This would look like this.

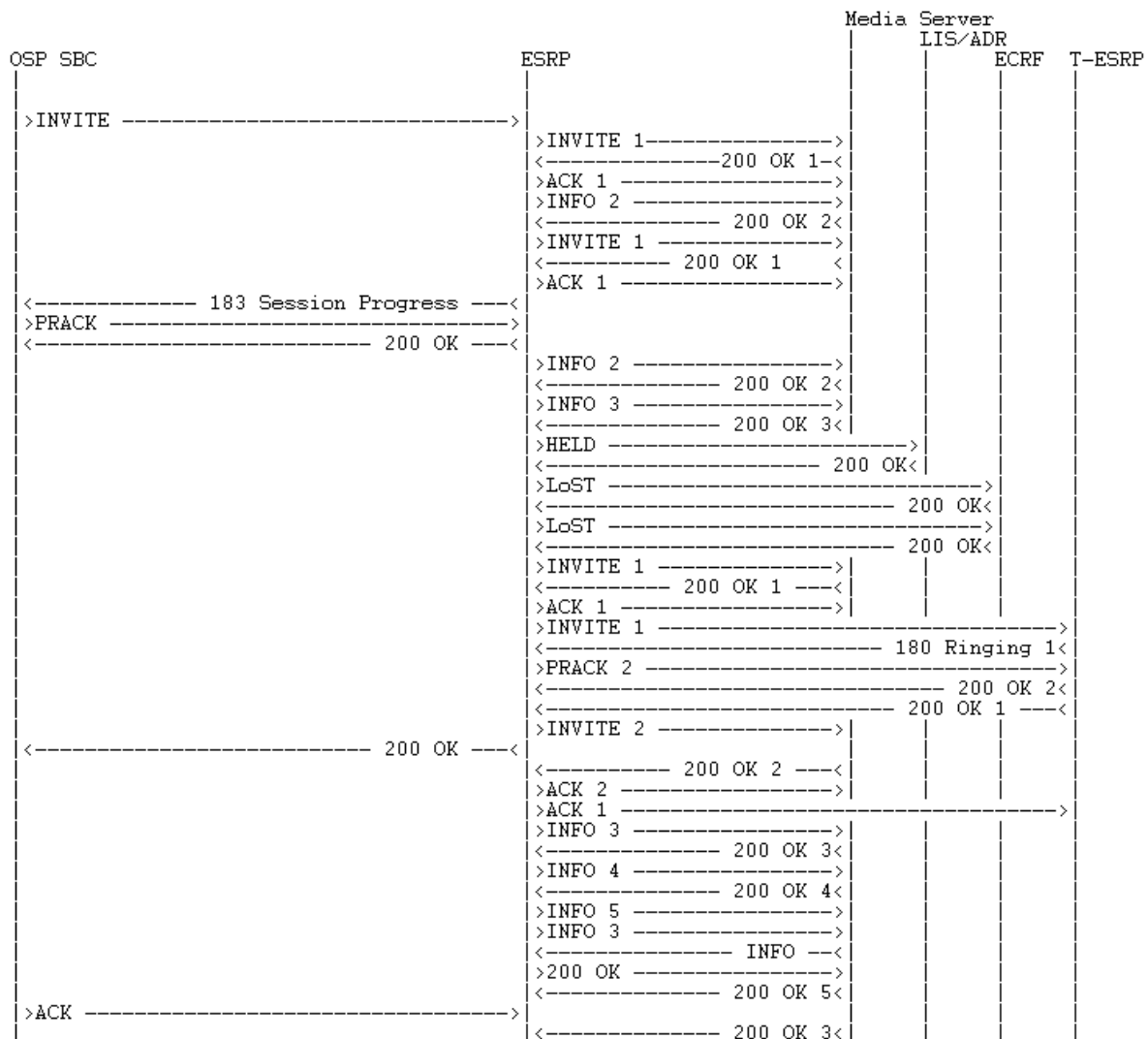


Figure 64: i3 Call Flow routing to non-i3 PSAP

i3 component failures: If an error is encountered with the HELD request to the LIS; at this point no location is available. The ESRP will fall back to alternative routing methods. The call is delivered to the T-ESRP without any location references. If an error is encountered with the LoST requests to the ECRF, no route information is available. The ESRP will fall back to alternative routing methods. The call is delivered to the T-ESRP with location references. These flows are variations on the previous flows and are not shown.

Once an i3 routed call lands on a T-ESRP, there are significant call flow interactions with the i3 components as part of call handling. The T-ESRP will interact with the LIS to obtain the current dispatch location, possibly use the ECRF to validate that the current dispatch location falls within their operating boundary, use the ECRF to obtain police, fire, and medical 1st responder information (labels and routing) and possibly update up to 3 ADR data sections. The other significant interaction is the DNS resolution of the FQDNs for each i3 component and the use of credentials for authentication for each i3 component. The T-ESRP may not use all of the component interfaces discussed previously. What is used is T-ESRP implementation dependent. The following call flow shows the T-ESRP using all of the available interfaces. Detailed call routing to the T-ESRP is not shown. Just the interactions from the T-ESRP to each of the i3 components.

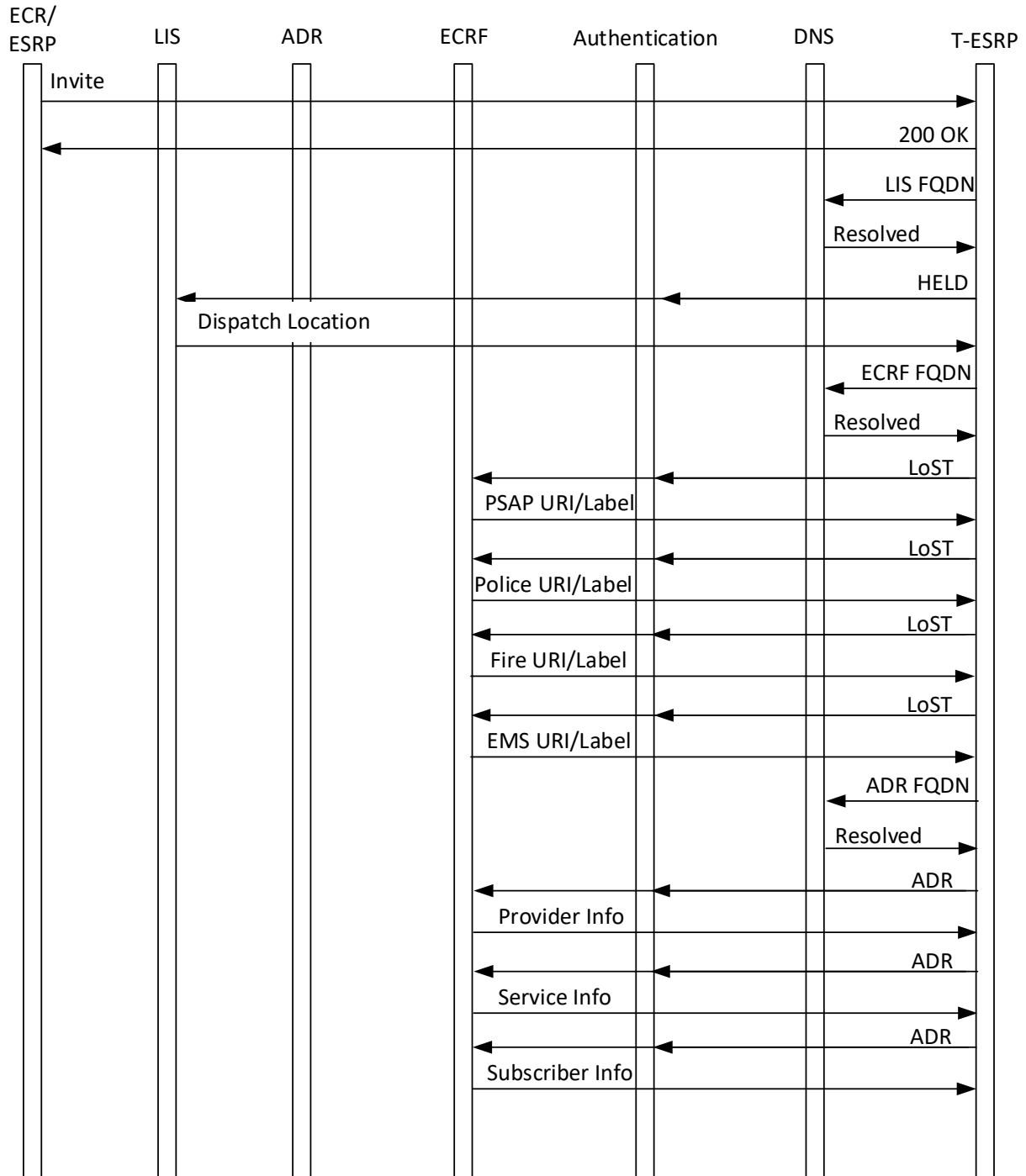
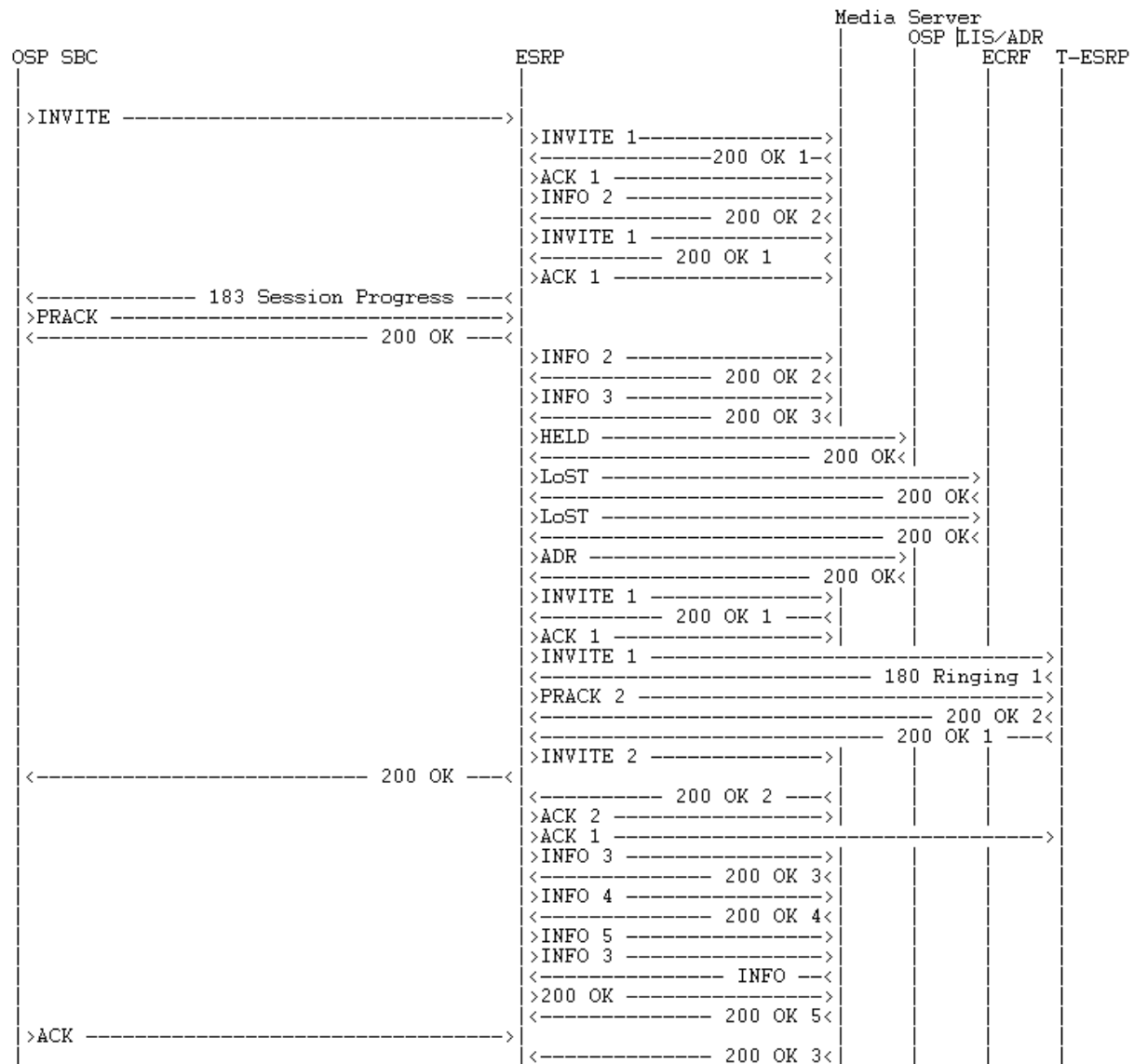


Figure 65: T-ESRP i3 component interaction

With IP ingress as i3 SIP, the call flows are basically the same. The difference is that the ingress i3 SIP invite contains references for LIS and ADR. The ESRP interaction with LIS and ADR is (off net) with the OSP's LIS and ADR. Note, there are not the AT&T LIS/ADR. Because the LIS and ADR requests are off-net, they are credentialed (just like the T-ESRP requests are).

Here is an example flow:



5.0 Loss of RTP Call Flow

5.1 Call Flow B: Generic ‘Loss of RTP’ Call Flow

The call flows in this section show the loss of RTP sequence of events and signaling at a high level. Figure 48, below, highlights the Loss of RTP (LOR) function.

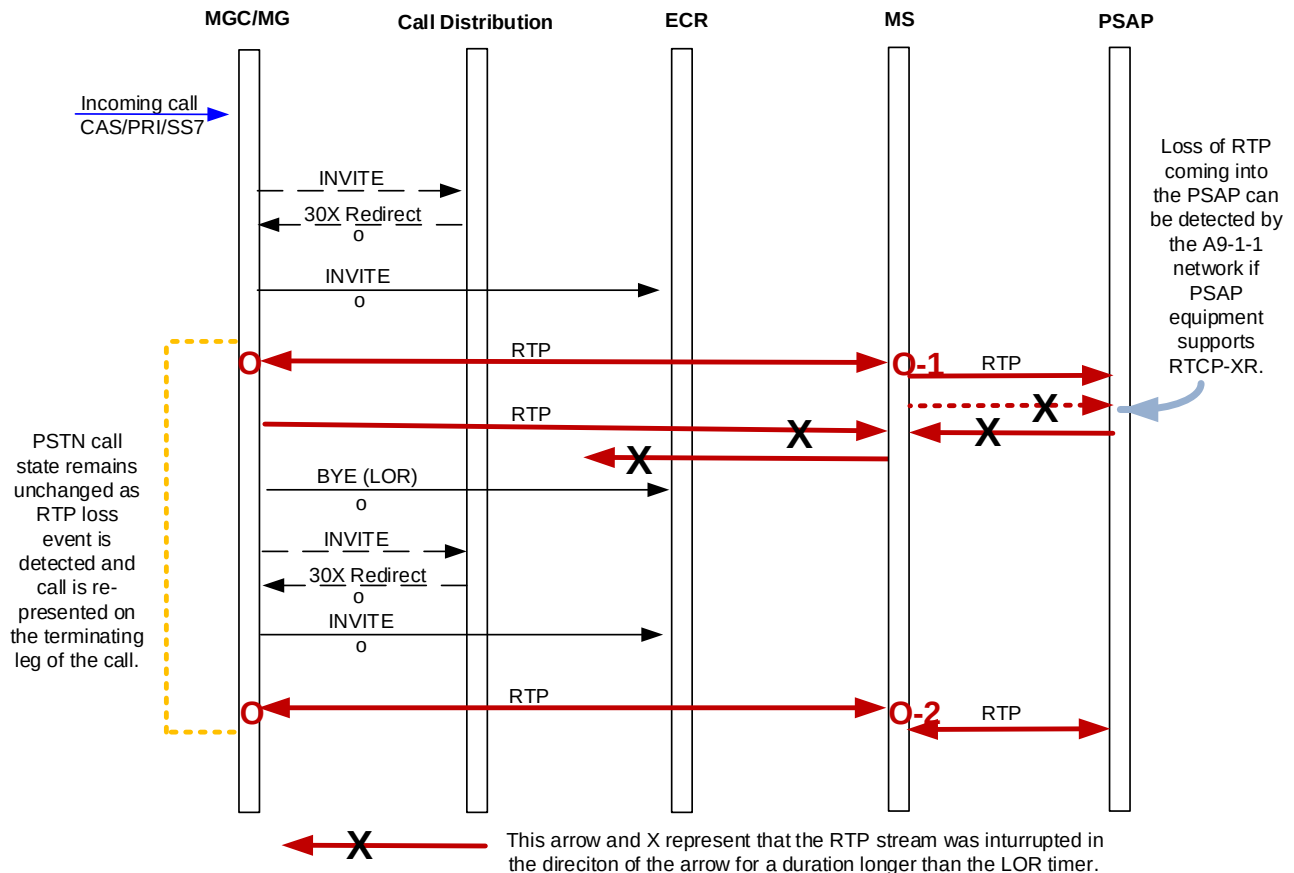


Figure 48 shows that, after a call is setup and stable, if the flow of RTP is interrupted for a number of seconds, the ingress MG will tear down the call associated with the failed RTP stream and then re-present the call to a new termination—all the while keeping the original 9-1-1 caller engaged in the call. So the caller would remain off-hook, and after a couple of seconds of silence would be ringing into a new termination for the call.

Note: The break in RTP can be detected on all legs of the call—and for both directions. The only constraint is that to detect loss of RTP being sent to the PSAP, the equipment at the PSAP network interface needs to support sending RTCP-XR packets into the ECRS network.

5.2 Section 1.2.3—Loss of RTP—Single LOR Re-Presentation—Sunny Day

This call flow shows the core function of the 'Loss of RTP' (LOR) feature. The call is initially setup between the 9-1-1 call originator and the first PSAP and is in a stable 2-way talk state. Then loss of RTP is detected (when a 3 second break in RTP was introduced – see trace at time 07:10:41.683) and the ingress MG drops the original PSAP leg and re-presents the call back to the same PSAP (but a different PTM). The entire time the originating 9-1-1 caller is kept up in the stable 2-way talk state.

Note: Important to this call flow is the detection of 'loss of RTP', which (by looking at the text description that follows the ladder diagrams) occurred at

2015-06-09 07:10:41.683- -IS has detected media inactivity.

This detection of the LOR event prompts the BYE shown in the ladder diagram (at 7:10:41.684).

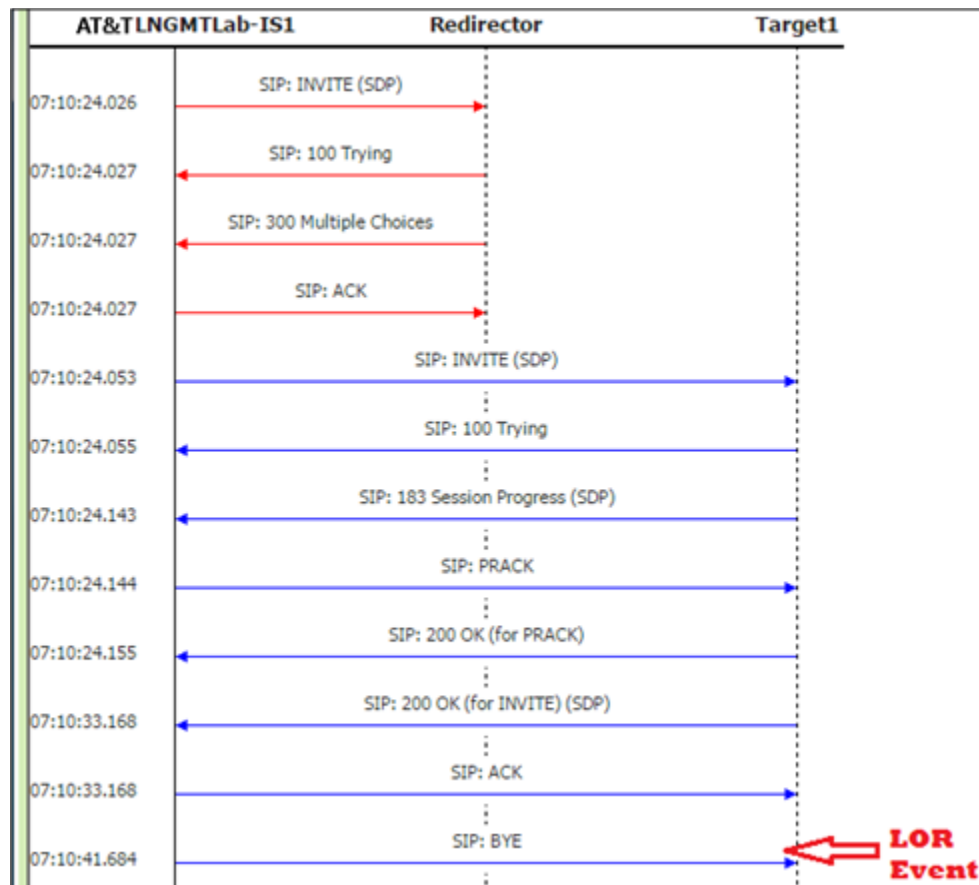


Figure 49: Detection of the LOR Event Prompts the BYE (Graphic 1 of 3)

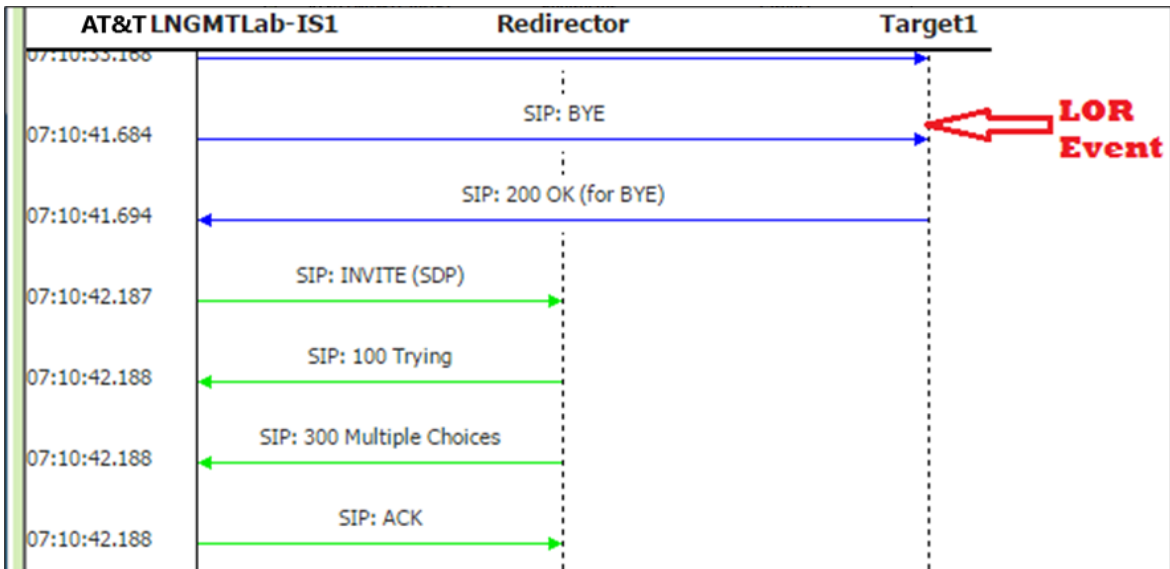


Figure 50: Detection of the LOR Event Prompts the BYE (Graphic 2 of 3)

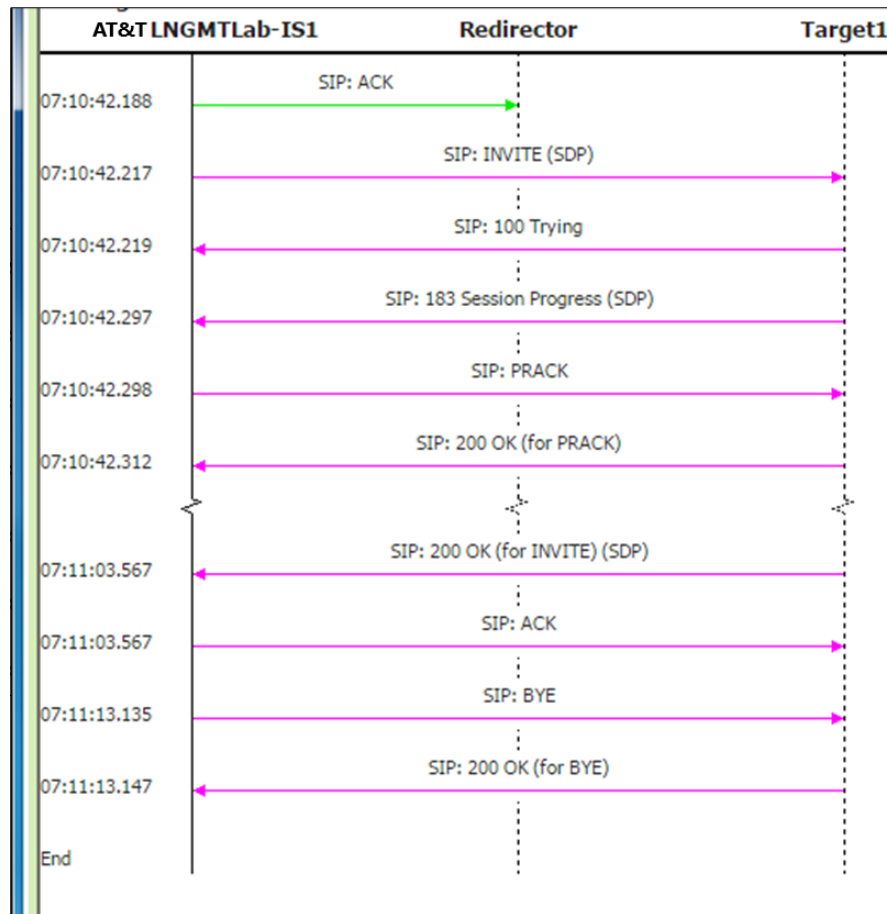


Figure 51: Detection of the LOR Event Prompts the BYE (Graphic 3 of 3)

2015-06-09 07:10:24.015- -Received ISDN message: Q.931 Message type = SETUP (5) CRV=0758

2015-06-09 07:10:24.015- -Received incoming ISDN call setup request.

2015-06-09 07:10:24.015- -Dialed digits detected on an ISDN interface (911).

2015-06-09 07:10:24.015- -Media will be cut through in both directions for Meta_PRI_ICL.

2015-06-09 07:10:24.015- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6526{ C=\$ { A=Facility/65543/1 { M { TS{...}, O{...}}}}}

2015-06-09 07:10:24.016- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6526{ C=10{ A=Facility/65543/1}}

2015-06-09 07:10:24.017- -RedirectorStarting number validation.

2015-06-09 07:10:24.017- -RedirectorNV succeeds.

2015-06-09 07:10:24.017- -RedirectorThis is an emergency call.

2015-06-09 07:10:24.017- -The calling numbers for this call have been determined.

2015-06-09 07:10:24.018- -RedirectorA local subscriber lookup is not required.

2015-06-09 07:10:24.018- -RedirectorRouting begins.

2015-06-09 07:10:24.018- -RedirectorRouting succeeds.

2015-06-09 07:10:24.018- -Sending call proceeding message for an incoming ISDN call.

2015-06-09 07:10:24.018- -Sending ISDN message: Q.931 Message type = CALL PROCEEDING (2)
CRV=8758

2015-06-09 07:10:24.019- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6527{ C=10{ A=RTP/\$ { M { TS{...}, O{...}, L{...}}, E=47{...}, EB}}}

2015-06-09 07:10:24.023- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6527{ C=10{ A=RTP/23{ M { L{...}}}}}

2015-06-09 07:10:24.023- -RedirectorMedia will be cut through in both directions for Redirector.

2015-06-09 07:10:24.023- -RedirectorSending outgoing SIP call setup request over a trunk.

2015-06-09 07:10:24.023- -RedirectorOTG and/or DTG parameters added to an outgoing SIP INVITE.

2015-06-09 07:10:24.023- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6528{ C=10{ MF=RTP/23{ M{ TS{...}, O{...}}}}}

2015-06-09 07:10:24.024- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6528{ C=10{ MF=RTP/23}}

2015-06-09 07:10:24.026- -RedirectorOutgoing SIP message sent : INVITE (SDP)
9187775505@10.105.190.136->911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:24.027- -RedirectorIncoming SIP message received : 100 Trying From:
<9187775505@10.105.190.136> To: <911@sip.lorrs.iclienv.a911net.net>

2015-06-09 07:10:24.027- -RedirectorIncoming SIP message received : 300 Multiple Choices From:
9187775505@10.105.190.136 To: 911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:24.027- -RedirectorOutgoing SIP message sent : ACK 9187775505@10.105.190.136-
>911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:24.028- -Redirector3 contacts have been extracted from a 3xx response to a SIP
INVITE message.

2015-06-09 07:10:24.028- -RedirectorA 300 Multiple Choices response was received for a SIP INVITE
message.

2015-06-09 07:10:24.028- -RedirectorMedia will be disconnected in both directions for Redirector.

2015-06-09 07:10:24.028- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6529{ C=10{ S=RTP/23}}

2015-06-09 07:10:24.029- -Target1Routing begins, using a contact header supplied in a 3xx response.

2015-06-09 07:10:24.029- -Target1Routing based on IP address or domain name.

2015-06-09 07:10:24.029- -Target1Routing succeeds using a contact header provided in a 3xx response.

2015-06-09 07:10:24.046- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6529{ C=10{ S=RTP/23{ SA{...}}}}

2015-06-09 07:10:24.047- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6530{ C=10{ A=RTP/\$ { M{ TS{...}, O{...}, L{...}}, E=48{...}, EB}}}

2015-06-09 07:10:24.049- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6530{ C=10{ A=RTP/24{ M{ L{...}}}}}

2015-06-09 07:10:24.049- -Target1Media will be cut through in both directions for Target1.

2015-06-09 07:10:24.049- -Target1Sending outgoing SIP call setup request over a trunk.

2015-06-09 07:10:24.049- -Target1OTG and/or DTG parameters added to an outgoing SIP INVITE.

2015-06-09 07:10:24.049- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6531{ C=10{ MF=RTP/24{ M{ TS{...}, O{...}}}}}

2015-06-09 07:10:24.051- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6531{ C=10{ MF=RTP/24}}

2015-06-09 07:10:24.053- -Target1Outgoing SIP message sent : INVITE (SDP)
9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:24.055- -Target1Incoming SIP message received : 100 Trying From:
<9187775505@10.105.190.136> To: <911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:10:24.143- -Target1Incoming SIP message received : 183 Session Progress (SDP) From:
9187775505@10.105.190.136 To: 911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:24.143- -Integrated Softswitch will generate a BAF record for billing leg 0.

2015-06-09 07:10:24.143- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6532{ C=10{ MF=RTP/24{ M{...}, E=49{...}}}}}

2015-06-09 07:10:24.144- -Target1Outgoing SIP message sent : PRACK 9187775505@10.105.190.136-
>911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:24.144- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6533{ C=10{ MF=Facility/65543/1{...}, O-MF=Facility/65543/1{...}}}

2015-06-09 07:10:24.146- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6532{ C=10{ MF=RTP/24{ M{ L{...}}}}}

2015-06-09 07:10:24.147- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6533{ C=10{ MF=Facility/65543/1, MF=Facility/65543/1}}

2015-06-09 07:10:24.147- -Sending ISDN message: Q.931 Message type = PROGRESS (3) CRV=8758

2015-06-09 07:10:24.155- -Target1Incoming SIP message received : 200 OK From:
<9187775505@10.105.190.136> To: <911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:10:33.168- -Target1Incoming SIP message received : 200 OK (SDP) From:
<9187775505@10.105.190.136> To: <911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:10:33.168- -Target1Outgoing call over a SIP trunk has been answered.

2015-06-09 07:10:33.168- -Target1SIP call setup has completed to SIP subscriber 911.

2015-06-09 07:10:33.168- -Target1Outgoing SIP message sent : ACK 9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:33.169- -Integrated Softswitch will generate a BAF record for billing leg 0.

2015-06-09 07:10:33.169- s-Incoming ISDN call has been answered.

2015-06-09 07:10:33.169- -Sending ISDN message: Q.931 Message type = CONNECT (7) CRV=8758

2015-06-09 07:10:33.245- -Received ISDN message: Q.931 Message type = CONNECT ACKNOWLEDGE (15) CRV=0758

2015-06-09 07:10:41.683- -Gateway controller received H.248 request from MG : !/2 [10.105.190.136]:2944 T=1074{ C=10{ N=RTP/24{ OE=49{20150609T13104168:ADID/IPSTOP}}}}

2015-06-09 07:10:41.683- -Gateway controller sending H.248 reply to MG : !/2 [10.105.190.136] P=1074{ C=10{ N=RTP/24}}

2015-06-09 07:10:41.683- -IS has detected media inactivity. ← LOR EVENT

2015-06-09 07:10:41.684- -Target1A call service has released a branch.

2015-06-09 07:10:41.684- -Target1The outbound SIP call branch is being recovered following a loss of media error.

2015-06-09 07:10:41.684- -Target1Sending outgoing SIP call release request.

2015-06-09 07:10:41.684- -Target1Media will be disconnected in both directions for Target1.

2015-06-09 07:10:41.684- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136] T=6545{ C=10{ S=RTP/24}}

2015-06-09 07:10:41.684- -Target1Outgoing SIP message sent : BYE 9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:41.684- -A call service has created a new branch.

2015-06-09 07:10:41.685- -RedirectorStarting number validation.

2015-06-09 07:10:41.685- -RedirectorNV succeeds.

2015-06-09 07:10:41.685- -RedirectorA local subscriber lookup is not required.

2015-06-09 07:10:41.686- -RedirectorRouting begins.

2015-06-09 07:10:41.686- -RedirectorRouting succeeds.

2015-06-09 07:10:41.693- -Gateway controller received H.248 reply from MG : !/2 [10.105.190.136]:2944 P=6545{ C=10{ S=RTP/24{ SA{...}}}}

2015-06-09 07:10:41.694- -Target1Incoming SIP message received : 200 OK From: <sip:9187775505@10.105.190.136 To: <sip:911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:10:42.184- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136] T=6546{ C=10{ A=RTP/\$ { M{ TS{...}, O{...}, L{...}}, E=50{...}, EB}}}

2015-06-09 07:10:42.187- -Gateway controller received H.248 reply from MG : !/2 [10.105.190.136]:2944 P=6546{ C=10{ A=RTP/25{ M{ L{...}}}}}

2015-06-09 07:10:42.187- -RedirectorMedia will be cut through in both directions for Redirector.

2015-06-09 07:10:42.187- -RedirectorSending outgoing SIP call setup request over a trunk.

2015-06-09 07:10:42.187- -RedirectorOTG and/or DTG parameters added to an outgoing SIP INVITE.

2015-06-09 07:10:42.187- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136] T=6547{ C=10{ MF=RTP/25{ M{ TS{...}, O{...}}}}}

2015-06-09 07:10:42.187- -RedirectorOutgoing SIP message sent : INVITE (SDP) 9187775505@10.105.190.136->911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:42.188- -RedirectorIncoming SIP message received : 100 Trying From: <sip:9187775505@10.105.190.136 To: <sip:911@sip.lorrs.iclienv.a911net.net>

2015-06-09 07:10:42.188- -RedirectorIncoming SIP message received : 300 Multiple Choices From: sip:9187775505@10.105.190.136 To: sip:911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:42.188- -RedirectorOutgoing SIP message sent : ACK 9187775505@10.105.190.136->911@sip.lorrs.iclienv.a911net.net

2015-06-09 07:10:42.188- -Redirector3 contacts have been extracted from a 3xx response to a SIP INVITE message.

2015-06-09 07:10:42.188- -RedirectorA 300 Multiple Choices response was received for a SIP INVITE message.

2015-06-09 07:10:42.189- -Gateway controller received H.248 reply from MG : !/2 [10.105.190.136]:2944 P=6547{ C=10{ MF=RTP/25}}

2015-06-09 07:10:42.189- -RedirectorMedia will be disconnected in both directions for Redirector.

2015-06-09 07:10:42.189- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6548{ C=10{ S=RTP/25}}

2015-06-09 07:10:42.190- -Target1Routing begins, using a contact header supplied in a 3xx response.

2015-06-09 07:10:42.190- -Target1Routing based on IP address or domain name.

2015-06-09 07:10:42.190- -Target1Routing succeeds using a contact header provided in a 3xx response.

2015-06-09 07:10:42.214- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6548{ C=10{ S=RTP/25{ SA{...}}}}

2015-06-09 07:10:42.215- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6549{ C=10{ A=RTP/\$ M{ TS{...}, O{...}, L{...}}, E=51{...}, EB}}}

2015-06-09 07:10:42.217- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6549{ C=10{ A=RTP/26{ M{ L{...}}}}}

2015-06-09 07:10:42.217- -Target1Media will be cut through in both directions for Target1.

2015-06-09 07:10:42.217- -Target1Sending outgoing SIP call setup request over a trunk.

2015-06-09 07:10:42.217- -Target1OTG and/or DTG parameters added to an outgoing SIP INVITE.

2015-06-09 07:10:42.217- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6550{ C=10{ MF=RTP/26{ M{ TS{...}, O{...}}}}}

2015-06-09 07:10:42.217- -Target1Outgoing SIP message sent : INVITE (SDP)
9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:42.219- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6550{ C=10{ MF=RTP/26}}

2015-06-09 07:10:42.219- -Target1Incoming SIP message received : 100 Trying From:
<9187775505@10.105.190.136> To: <911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:10:42.297- -Target1Incoming SIP message received : 183 Session Progress (SDP) From:
9187775505@10.105.190.136 To: 911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:42.298- -Target1Outgoing SIP message sent : PRACK 9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:10:42.298- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6551{ C=10{ MF=RTP/26{ M{...}, E=52{...}}}}

2015-06-09 07:10:42.300- -Gateway controller received H.248 reply from MG : !/2 [10.105.190.136]:2944 P=6551{ C=10{ MF=RTP/26{ M{ L{...}}}}}

2015-06-09 07:10:42.312- -Target1Incoming SIP message received : 200 OK From: <sip:9187775505@10.105.190.136 To: <sip:911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:11:03.567- -Target1Incoming SIP message received : 200 OK (SDP) From: <sip:9187775505@10.105.190.136 To: <sip:911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:11:03.567- -Target1Outgoing call over a SIP trunk has been answered.

2015-06-09 07:11:03.567- -Target1SIP call setup has completed to SIP subscriber 911.

2015-06-09 07:11:03.567- -Target1The recovery of a SIP call branch did not succeed.

2015-06-09 07:11:03.567- -Target1Outgoing SIP message sent : ACK 9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:11:13.133- -Received ISDN message: Q.931 Message type = DISCONNECT (69) CRV=0758

2015-06-09 07:11:13.133- -An ISDN call will be released. (Normal call clearing)

2015-06-09 07:11:13.134- -Writing XML billing record for leg 0 of : call from +19187775505 to +1911.

2015-06-09 07:11:13.134- -Writing call log for billing leg 0.

2015-06-09 07:11:13.134- -Beginning release of ISDN call.

2015-06-09 07:11:13.134- -Target1Sending outgoing SIP call release request.

2015-06-09 07:11:13.134- -Target1Media will be disconnected in both directions for Target1.

2015-06-09 07:11:13.135- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136] T=6554{ C=10{ S=RTP/26}}

2015-06-09 07:11:13.135- -Target1Outgoing SIP message sent : BYE 9187775505@10.105.190.136->911@sip.grflmt.iclienv.a911net.net

2015-06-09 07:11:13.143- -Gateway controller received H.248 reply from MG : !/2 [10.105.190.136]:2944 P=6554{ C=10{ S=RTP/26{ SA{...}}}}}

2015-06-09 07:11:13.147- -Target1Incoming SIP message received : 200 OK From: <sip:9187775505@10.105.190.136 To: <sip:911@sip.grflmt.iclienv.a911net.net>

2015-06-09 07:11:13.636- -Media will be disconnected in both directions for Meta_PRI_ICL.

2015-06-09 07:11:13.636- -Gateway controller sending H.248 request to MG : !/2 [10.105.190.136]
T=6555{ C=10{ S=Facility/65543/1}}

2015-06-09 07:11:13.645- -Gateway controller received H.248 reply from MG : !/2
[10.105.190.136]:2944 P=6555{ C=10{ S=Facility/65543/1}}

2015-06-09 07:11:13.646- -Sending ISDN message: Q.931 Message type = RELEASE (77) CRV=8758

2015-06-09 07:11:13.729- -Received ISDN message: Q.931 Message type = RELEASE COMPLETE (90)
CRV=0758

2015-06-09 07:11:13.729- -Release processing for an ISDN call is complete.

5.3 LoR with IP Ingress

In the case of TDM ingress, the MGC/MG has a custom feature that detects and re-generates a call when Loss of RTP is detected. In the case of IP ingress, the SBC can detect Loss of RTP, however it cannot (currently) regenerate the call. The call is terminated whenever RTP is detected as lost. Be aware that the IP network can detect RTP loss and switch networks in sub-second time. The SBC detecting a loss of RTP would be after the IP network had attempted a switchover and the switchover did not solve the problem. ***AT&T is working on a solution for Loss of RTP for IP Ingress.***

Currently, in 1 deployment (CT), a work around for LoR is in-place. That workaround is referred to as the LoR hairpin. The hairpin solution utilizes a MGC/MG to detect LoR. In this deployment which has 100% IP ingress and zero TDM trunks; a MGC/MG has been injected into the call path for LoR detection. In this scenario, the MGC/MG takes IP in and produces IP out. The following call flow shows that specific/custom call flow. Only the path of the SIP Invites are shown as fully detailing the entire flow would produce a very cluttered diagram. Just using the Invites, the reader can see (more easily) the path of the hairpin from a SIP signaling and RTP perspective.

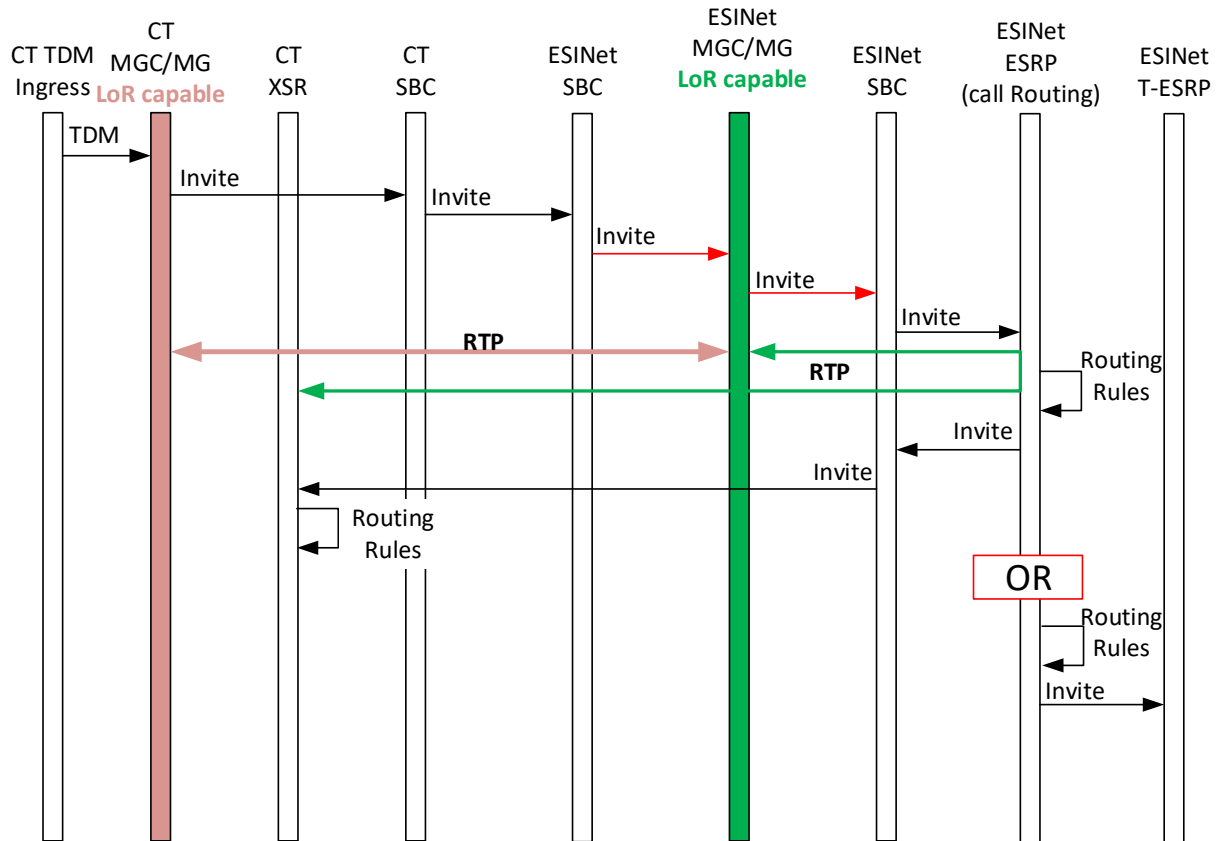


Figure 66; CT LoR Hairpin.

Some notes on the above diagram. Two ESINet SBCs are shown (on either side of the MGC/MG). This is because the ESINet SBC that receives the call from the CT network is not necessarily the SBC that gets the invite from the MGC/MG. That is, these SBCs can be in different Core Sites. The SBCs used will be Network Provisioning Group appropriate. Several MGC/MG aggregation sites are available. Selection of the site is load balanced. The SIP Invite coming from the CT network to the ESINet utilizes IP SIP basic. The ESINet network will make the egress SIP Invite back to the XSR look like (from a SIP Header perspective) it came from the CT MGC/MG. That is, all of the headers created by the CT MGC/MG are preserved as the call is processed thru the hairpin. As CT PSAP transition to ESINet, the ESRP will route to those PSAPs. Those PSAPs will then be on-net with ESINet. That was shown by the “OR” at the end of the call flow. The call flow from the ESRP to the T-ESRP is the same as any call flow previously shown. The call just has a more involved ingress.

6.0 Telephone Service Provider Interactions Call Flows

The following describes the call flow for SS7 signaling.

1. A caller dials 9-1-1 and the call is routed to the TSP switch.
2. The TSP switch sends an Initial Address Message (IAM) containing an ANI for wireline calls, or an ESRK pANI for NCAS wireless calls.
3. The TSP switch provides COT test tone in-band for the signaled trunk. AT&T loops the DS0 back to TSP.
4. The TSP switch sends COT message to indicate successful test.
5. Standard SS7 signaling occurs for the remainder of the call.
6. Either end of the call can initiate call tear down.
7. Release complete.

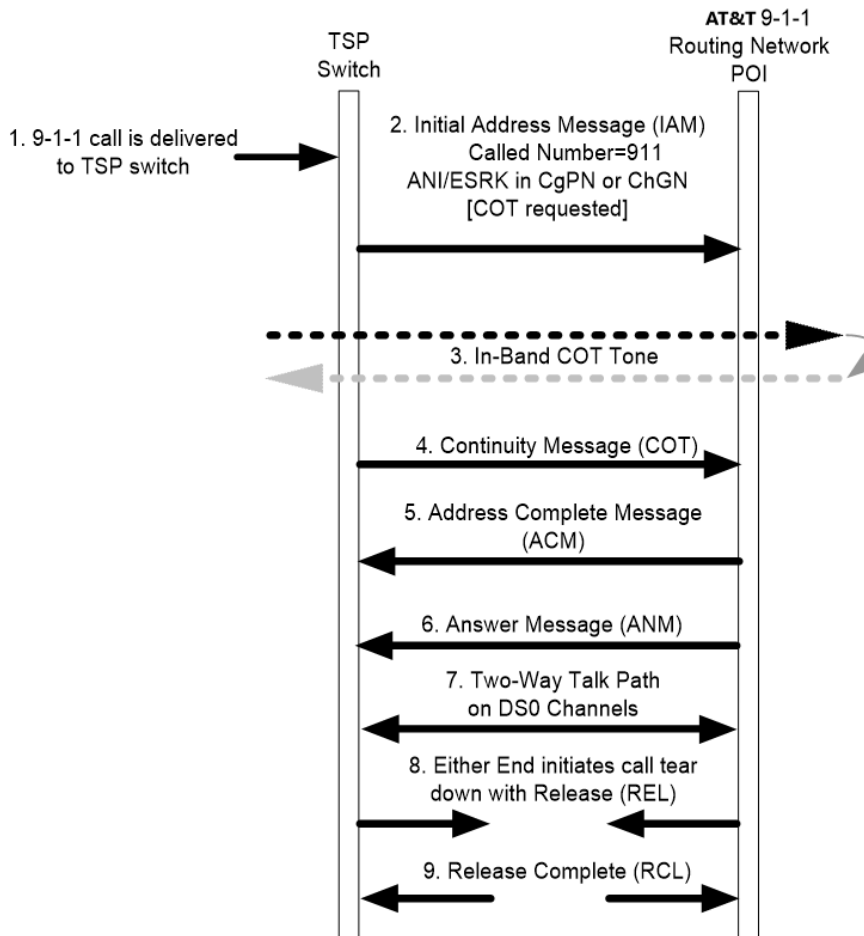


Figure 52: SS7 Signaling to Access AT&T Routing Network

6.1 ISDN/PRI Signaling to AT&T Routing Network

Along with SS7, ISDN/PRI facilities are preferred for their signaling accuracy and call setup speed, as compared to CAMA facilities.

It is expected that PBXs will be the most likely switch type sending 9-1-1 calls into the AT&T Routing Network using ISDN/PRI facilities. But there is no technical reason that an EO or an NCAS MSC could not also connect to the AT&T Routing Network using ISDN/PRI. The supported ISDN/PRI interface transports a single 10 digit number for each 9-1-1 call into the AT&T Routing Network, so wireless CAS or HCAS calls are not supported.

If a TSP attempts to route a call via PRI to the first AT&T Routing Network POI, and the call attempt fails, the TSP should attempt to route the call via the other PRI(s) to a different POI into the AT&T Routing Network.

6.1.1 ISDN/PRI Signaling Call Flow

The following describes the call flow for ISDN/PRI signaling.

1. A caller dials 9-1-1 and the call is routed to the TSP switch.
2. The TSP switch originates a call into AT&T 9-1-1 Routing with an ISDN PRI (Q.931) SETUP message, with the following Q.931 call attributes set

Called Number = 911¹

Calling Number = NPA-NXXYYYY (10 Digit ANI or ESRK)

3. The call setup continues using standard ISDN call processing. Either call end can initiate call tear-down.

¹ The Called Number should be 911, but may alternatively be 11, 1, or no digits.

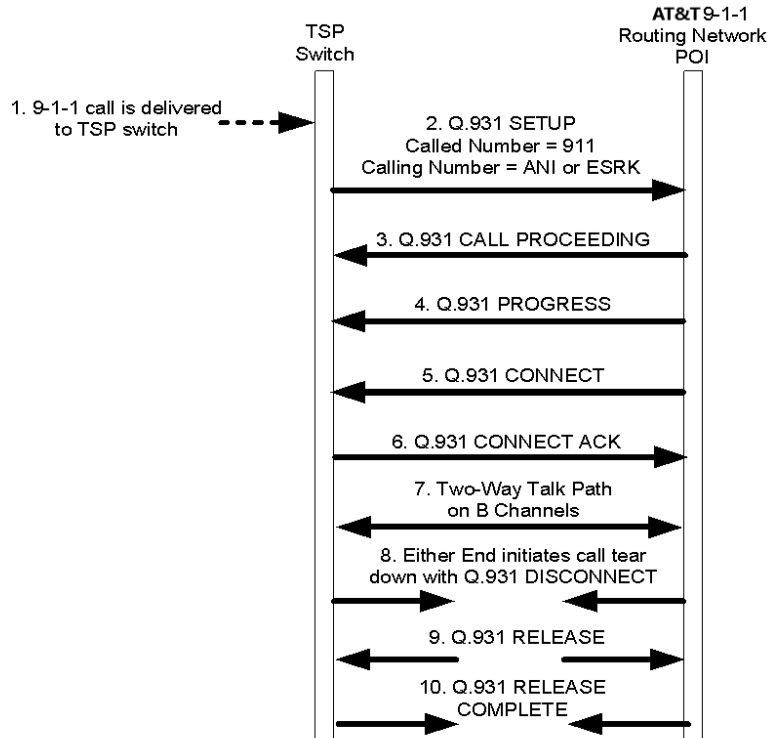


Figure 53: ISDN/PRI Signaling to Access AT&T Routing Network

6.2 CAMA Signaling to AT&T Routing Network

When the preferred signaling method of SS7 is not available, CAMA trunking is supported into the AT&T Routing Network. Two CAMA options are supported:

1. CAMA on DS0 based facilities (i.e., DS1) using 7 digit ANI plus an Information Digit (I Digit)
2. CAMA on DS0 based facilities using 7 digit ANI without an I Digit

For CAMA trunk groups, the Called Number is typically 9-1-1 (or alternatively 11, 1, or no digits). The Calling Number will consist of the 7 digit ANI of the call originator and will be missing the NPA (which is implied by the trunk group).

6.2.1 CAMA Signaling Call Flow

The following describes the call flow for CAMA signaling.

1. A caller dials 9-1-1 and the call is routed to the TSP switch. The TSP switch could be a wireline End Office, a wireless MSC, or a PBX.
2. The TSP switch seizes the CAMA trunk by going off-hook.
3. The AT&T Routing Network acknowledges the seizure and indicates readiness to accept Multi-Frequency (MF) address digits by replying with a wink, which is a temporary off-hook.

4. The TSP switch signals (using MF) the Called Number. The MF digit string sent is KP + 911 (or 11, 1, or no digits) + ST.
5. The response is a steady off-hook, which indicates readiness to accept additional MF address digits.
6. The TSP switch uses MF to signal the Calling Number in the form “KP + I + NXXXXXX + ST”, where “NXXXXXX” is the last seven digits of the ANI/Pani (ANI/Pani with the NPA removed), and “I” equals either:
 - A. Zero (0) if the ANI/Pani is valid
 - B. Two (2) if the ANI/Pani is invalid

Note: AT&T also supports an alternative configuration for DS0 based CAMA where the TSP sends no “I” digit and the TSP MF signals “KP + NXXXXXX + ST”.

7. At this point, there is a two way talk path between the call originator and the destination. Note that there is no answer supervision signaled from the AT&T Routing Network to the TSP switch.
8. Either end can disconnect the call by going on-hook.

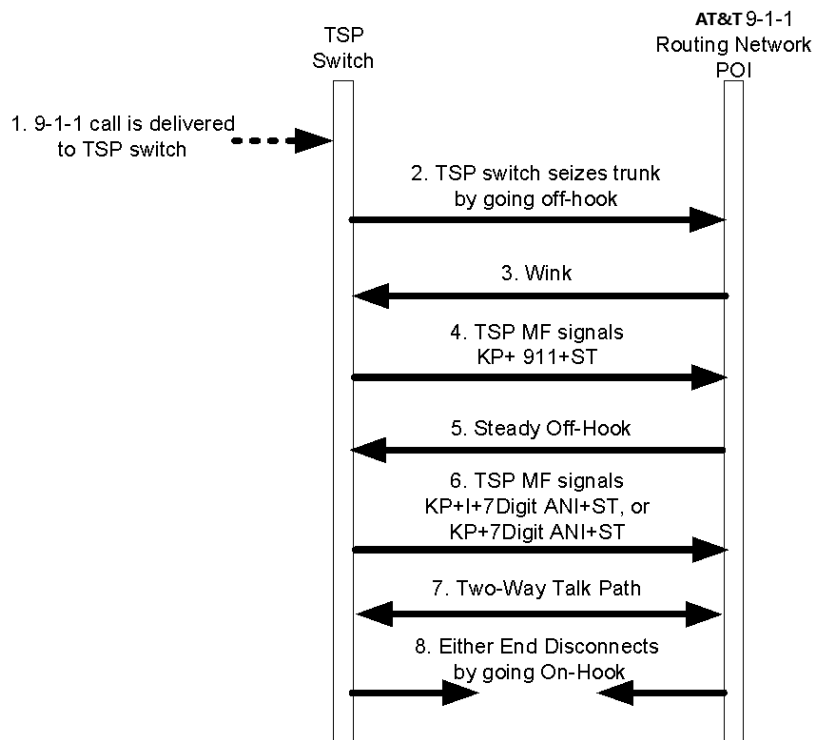


Figure 54: CAMA Signaling to Access AT&T Routing Network



Appendix K - AT&T ESInet-to-ESInet Interface Specification SIP Basic_v3.4.1



AT&T ESInet™
ESInet-to-ESInet Interface Specification
SIP Basic
Version 3.4.1

July 2023

Contents

1.0	Overview.....	3
1.2	Scope	3
1.3	Purpose and Applicability.....	4
1.4	Assumptions.....	4
2.0	Getting Ready for IP-to-IP NNI	5
2.1	Interconnection.....	5
2.2	Bandwidth Considerations	6
2.3	Interface Implementation	7
2.4	Encountering Errors and Route Advancement.	7
2.5	Real Time Text (RTT)	7
3.0	ESInet-to-ESInet SIP Basic (Pre-i3) Interface Option.....	9
3.1	SIP Messaging	9
4.0	Appendix A: ESInet-to-ESInet SIP Basic Implementation Guide.....	12
4.1	Interconnection and IP/Port Assignments.....	12
4.2	Handoff versus Transfer/Conference.....	12
4.3	Additional Examples.....	13
4.4	Trunk Group Names.....	14
4.5	Call Flow	14
5.0	Appendix B: Acronyms	15

List of Figures

Figure 1: Legacy SS7 Interconnection between Two Legacy Selective Routers	5
Figure 2: IP Interconnection between Two ESInet Providers	6
Figure 3: Handoff/Transfer/Conference Methods for Pre-i3 Interface	11
Figure 4: Handoff/Transfer/Conference Methods	12
Figure 5: Call Flow for Handoff and Transfer/Conference.....	14

Document History

Version	Date	Author	Description of Change
1.0	September 2016		Initial release
1.1	January 2019	Carl Smith	New Header: Interface
2.0	January 2019	Carl Smith	Added Appendix A: Pre-i3 ESInet to ESInet SIP Messaging.

Version	Date	Author	Description of Change
2.1	February 2019	Carl Smith	Updated value in the Interface header. Changes in format to the History-Info header value. Changes to Copyright page.
3.0	November 2019	Carl Smith Laurene Heinsohn L. Lett	Clarified pre-i3 and i3 interface options. Split document into two documents: 1) ESInet-to-ESInet Interface Specification SIP Basic (pre-i3), and 2) ESInet-to-ESInet Interface Specification - i3. This document is now the ESInet to ESInet Interface Specification SIP Basic v3. Rebranded to Intrado Life & Safety, Inc.
3.1	April 2020	Carl Smith	Updated to include discussions of Heartbeats, Error Codes/Route Advancement, and Loop Detection for Handoffs. The syntax and semantics of the interface have not changed.
3.2	June 2020	M. Hammond G. Chouinard J. Proctor	Reference to NNI Standard Section 2.5 added in Section 2.2.
3.3	June 2020	C. Smith	Real Time Text (RTT) added.
3.4	April 2021	C. Smith	Added the Interface Header which describes the version of the interface that the sender is using.
3.4.1	July 2023	L. Lett	Rebranded to AT&T.

1.0 Overview

This specification defines how Next Generation (NG) Service Providers can exchange emergency call traffic with AT&T's Next Generation Core Services (NGCS) and ESInets via a SIP/IP interface. This interface is referred to as ESInet-to-ESInet.

Emergency call traffic exchanged by NG Service Providers include handoffs and transfers. Transfers include bridging/conferencing.

A handoff is a call that is passed between ESInets as a 9-1-1 call (i.e., called=911). These calls initially land on a specific ESInet. After the ESInet examines the call it determines that the target PSAP is not in its domain (not supported on its ESInet) and it passes the call to the ESInet that serves the PSAP. An example for when this scenario occurs is in areas where two or more ESInets support split rate centers.

A transfer/conference is a call that has been routed to the Primary PSAP on one ESInet and the PSAP is initiating a transfer/conference with a PSAP on another ESInet. Currently, this is typically supported by both ESInets using a 10-digit TN as the called number. This concept is further defined later in the document.

Each Service Provider can send hand-offs and/or transfer calls to the other Service Provider. Each Service Provider can receive calls from the other Service Provider. The NENA documents referred to this as upstream ESInet (when an ESInet initiates a handoff/transfer/conference) and downstream ESInet (when an ESInet accepts a handoff/transfer/conference).

There are two primary options for a NG Service Provider to interface via SIP/IP to AT&T's NGCS/ESInets.

- *ESInet-to-ESInet SIP Basic*, which is a TDM replacement service that emulates SS7 connectivity.
- *ESInet-to-ESInet SIP i3*, which is a NENA i3-compliant service.

Many, if not all NG Service Providers are not yet prepared to pass a NENA i3 compliant call to another NG Service Provider. The primary driver for this state of preparedness is that NENA did not complete the ESInet-to-ESInet i3 framework in NENA-STA-010.2-2016 Version 2. Version 3 of the standard makes significant progress in completing the ESInet-to-ESInet i3 framework. AT&T anticipates that once Version 3 is published the industry will be able to move forward more assertively to support an i3-compliant exchange of traffic between NG Service Providers. Until then, AT&T offers a pre-i3 interface option named ESInet-to-ESInet SIP Basic.

Following is a description of the ESInet-to-ESInet SIP Basic interface option. The i3 interface option is available in a separate document titled; *ESInet to ESInet Interface Specification-i3*.

1.2 Scope

The evolution of emergency services is occurring within the core emergency service provider network(s) based upon applicable standards and business drivers. The National Emergency Number Association (NENA) is the predominate standards organization that defines standards for Next Generation Core Services, ESInets, and PSAP call handling domains.

There is a need to define an interconnection mechanism so that different NG emergency service provider networks interconnect uniformly. The the interface option described in this document defines both the IP network interconnection and the SIP methods interconnection.

The ESInet-to-ESInet SIP Basic interface option emulates a TDM interface by using legacy location and default route concepts; e.g. a hand-off call is passed with ANI which is used to retrieve an appropriate location with

routing instructions. Both legacy selective routing and NENA i3 compliant processes are employed to retrieve a caller's location based on the ANI. The NENA process is referred to as Legacy Network Gateway/Location Interwork Function (LNG/LIF).

1.3 Purpose and Applicability

The purpose of this specification is to define connectivity options, signaling, and parameter exchange between IP-based NG Service Provider networks.

This specification includes:

- Interconnection architecture
- SIP call/session control signalling

The following are not defined in this document:

- Provisioning of ANIs or p-ANIs in the databases
- Call admission and control (will be defined in the next version)

1.4 Assumptions

- Each NG Service provider must use a set of call control, call routing, and bearer functional entities to connect the ESInet.
- SIP is used for call control signalling.
- RTP is used for voice transport.
- G.711 uLaw encoding at 20ms packetization is used within the ESInet for best voice quality. Silence suppression is not supported due to PSAP requirements. In the future, higher performance codecs will be supported.
- DTMF will be transported as part of the voice band media in payload type 0 RTP packets. RFC 2833 is supported.
- The ESInet-to-ESInet SIP Basic interface option may include:
 - TN (ANI) for wireline calls
 - ESRK or ESQK for wireless or VoIP calls using Wireless Compatibility Mode (WCM). WCM calls are wireless or VoIP calls that emulate wireline in that they only pass the ESRK/ESQK and not a call back number.
 - The ESInet initiating the hand-off or transfer will anchor media.

2.0 Getting Ready for IP-to-IP NNI

There are two parts to the ESInet to ESInet interface specification; the IP network interconnection and the mechanics of the SIP messaging.

The interconnection methodology is independent of the SIP messaging. Therefore, the IP interconnection methodology is the same for both interface options: pre-i3 and i3.

2.1 Interconnection

The diagram below depicts a legacy SS7 interconnection between two Legacy Selective Routers (LSR).

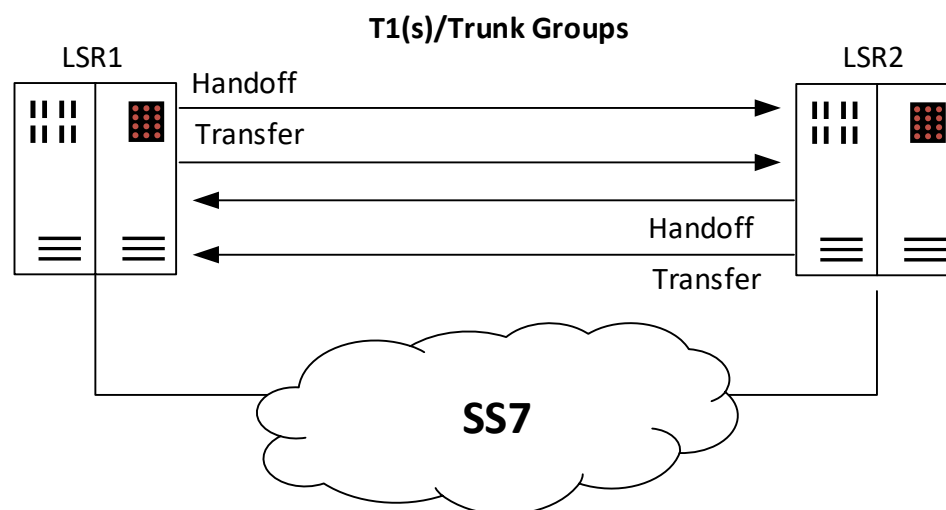


Figure 1: Legacy SS7 Interconnection between Two Legacy Selective Routers

LSR1 has an egress trunk group to LSR 2 for Handoffs and an egress trunk group for Transfers/Conferences. LSR 2 has a similar arrangement to LSR 1. These trunk groups are shown as 1-way. They could be 2-way trunk groups. Handoffs and Transfers could also be supported on the same trunk group. Different call types (wireline/wireless/VoIP) could be on separate or the same trunk groups.

The trunk groups could each have separate T1s or they could all be on a single T1, or even a DS3. The number of calls allowed for each type of trunk group is constrained by the number of DS0s in the trunk group. While not shown above, dual-homing arrangements could also be supported.

For the interconnection, one or more T1s with specific functional trunk groups (e.g. hand-offs or transfer/conference) are carried within the T1s to allow the two LSRs to connect and interoperate. The physical connection resources are the LSRs themselves. When LSR 1 ordered trunks to LSR 2; LSR1 and LSR2 would be the A and Z endpoints (using DLR/CLR terminology), respectively. Then vice versa for LSR2.

This interconnection scenario can be mapped to IP as:

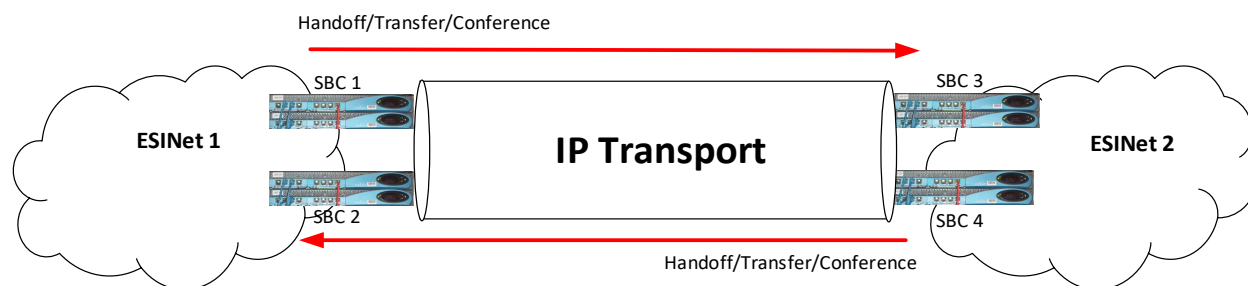


Figure 2: IP Interconnection between Two ESInet Providers

The interconnection end points are the SBCs each ESInet uses to terminate the IP transport. When ESInet 1 writes orders for IP Transport with ESInet 2, the A endpoints are SBC 1 and SBC 2 and the Z endpoints are SBC 3 and SBC 4. AT&T's standard connection type is private circuit. Requests for a VPN connection via public internet will be assessed on a case-by-case basis.

The IP transport can support handoffs and transfers/conferences in both directions or can be designed to support one-way traffic. AT&T will collaborate with the NG Service Provider to design the most appropriate arrangement.

A handoff is a call that is passed between ESInets as a 9-1-1 call (i.e. called=911). These calls initially land on a specific ESInet. After the ESInet examines the call it determines that the target PSAP is not in its domain (not supported on their ESInet) and it passes the call to the ESInet that serves the PSAP. An example for when this scenario occurs is in areas where two or more ESInets support split rate centers. **Note:** A handoff can end up routing in an infinite loop. Each ESInet must perform their own loop detection and break the loop. In the AT&T implementation an ingress handoff that routes as an egress handoff is not allowed. The originating ESInet will receive a SIP error code. That ESInet would be responsible for trying another route (route advance) or ultimately terminating the call to a treatment (i.e. fast busy or announcement).

A transfer/conference is a call that has been routed to the Primary PSAP on one ESInet and the PSAP is initiating a transfer/conference with a PSAP on another ESInet. Currently, this is typically supported by both ESInets using a 10-digit TN as the called number. This concept is further defined later in the document. This document may refer to a conference/transfer as a bridge.

2.2 Bandwidth Considerations

As with SS7 traffic, the NG Service Provider will traffic engineer their Emergency 9-1-1 traffic for IP connectivity. AT&T assumes the NG Service Provider will traffic engineer their service to meet appropriate Poisson thresholds (Poisson calculation to the appropriate blocking factor). In the legacy TDM world this would result in a DS0 count. In IP, this typically results in a concurrent call path (CCP) count.

To determine the bandwidth required, take the DS0 or CCP count and multiply by 100 kilobits/sec. Why 100kbps? AT&T uses the G.711 codec for voice. This codec typically operates at around 87 kbps. 100 kbps provides some buffer and allows for additional monitoring traffic. The NG Service Provider may want to add additional bandwidth for future growth (perhaps this is accounted for via the peaking factor in the Poisson calculation). IP bandwidth is typically very affordable so this should not add a significant amount of new costs. The appropriately sized IP transport is then used between the ESInets.

This establishes the IP connectivity between the ESInet providers.

Network considerations, including sizing, diversity, and transport can be found in the *AT&T Network to Network Interface Standards for OSP Networks and Foreign ESInets* document.

2.3 Interface Implementation

1.4.1 2.3.1 Heartbeats between ESInets

Heartbeat messaging can be used to determine route viability (i.e. is the route working?). This is best accomplished by using the capabilities of the BCF (Session Border Controller). There are methods built into the SBC that allow for SIP Options messages to be exchanged between each ESInets BCF. Should a pathway become unavailable, the loss of heartbeat will allow for the BCF to select another route. This selection occurs quickly (the route returns a 503 quickly; otherwise a 408 Timeout occurs after 4 to 5 seconds). The application programmer doesn't code a heartbeat message in the interface. The BCF (SBCs) take care of this function.

2.4 Encountering Errors and Route Advancement.

How each ESInet handles errors will be implementation specific. Two classes of errors can be encountered. They are:

- 1.) From the UpStream ESInet a network path does not exist (i.e., network down condition).
- 2.) The DownStream ESInet encounters an issue that doesn't allow it to complete the routing of the call to the DownStream ESRP/T-ESRP. These issues include traffic busy (486) or other 4xx, 5xx, or 6xx SIP error codes.

Each ESInet has multiple exit and entry points (i.e. multiple BCF IP addresses) to send/receive SIP messages. A BCF may be configured to route advance (i.e. try another entry point of the target ESInet). The BCF may send errors it receives to the application. And the BCF may do both. That is, the BCF tries route advancement and if all routes fail send the SIP error code to the ESInet's ESRP. The ESRP could then make a route advance decision and the routing attempt restarts. When all route advancement has been exhausted, the ESRP must then route to treatment (fast busy or announcement). The caller must be given an indication that the call is not being successful and be induced/influenced to hang up and try again.

In scenario 1, the UpStream ESInet has the responsibility to route advance and in the face of getting SIP error codes (486 Busy or otherwise) providing the treatment as the last resort.

In scenario 2, what happens is ESInet implementation specific. The DownStream ESInet may route to treatment when errors (486 busy or otherwise) are encountered or it may return the error code to the UpStream ESInet for the UpStream ESInet to try to route advance. If all routes are exhausted, then again it falls to the UpStream ESInet to apply treatment.

Again, all of this is ESInet implementation specific and may be scenario specific. That is, in certain error scenarios, the ESInet may route to treatment or for a different set of error codes return the error code to the other ESInet.

2.5 Real Time Text (RTT)

The indication that the call is an RTT call is only denoted in the SDP. There are no specific SIP headers associated with an RTT call. Here is an example of the SDP that indicates RTT.

```
a=rtpmap:0 PCMU/8000
a=rtpmap:120 telephone-event/8000
a=sendrecv
```

```
a=maxptime:240
a=ptime:20
m=text 27442 RTP/AVP 121
c=IP4 12.120.212.214
b=RS:128
b=RR:128
a=rtpmap:121 t140/1000
a=sendrecv
```

The highlighted headers show the `m=text` and the codec type of `t140` indicate RTT. Note that the G.711 (PCMU) is present as well. An RTT call has a voice component to the media as well as the RTT component of the media. The ESInet that receives an RTT call routes the call as they normally would. If the destination PSAP is not RTT capable, it is the responsibility of the ESInet that hosts the PSAP to transcode the RTT to Baudot (TDD).

Again, only handoffs can (currently) be passed between ESInets.

3.0 ESInet-to-ESInet SIP Basic (Pre-i3) Interface Option

3.1 SIP Messaging

With IP transport in place, we can now address the SIP messaging that each ESInet will use to exchange call traffic.

Note: as a pre-i3 (non-i3) interface, none of the i3 concepts of service URNs, location by reference or value, or additional data apply.

Regardless of whether the call is a handoff or transfer/ conference, the format of the SIP message (the headers required) is the same. The semantics of the call (handoff or transfer/conference) is conveyed in the Request URI. A handoff will have 911 as the user part of the SIP Request URI. A transfer/conference will have the 10-digit pilot TN of the target PSAP as the user part of the SIP Request URI.

There is an AT&T specific Interface header which communicates which version of the ESInet-to-ESInet-Basic interface is being used. AT&T is generally backwards compatible with the earlier version.

An example of this header is:

Interface: Intrado-ESInet-to-ESInet-Basic-3.0

3.1.1 Example: Handoff

```
INVITE sip:911@xxx.xxx.xxx.xxx:yyyy;dtg=TRUNKGROUPNAME SIP/2.0
Content-Type: application/sdp
To: <sip:911@xxx.xxx.xxx.xxx:yyyy>
Via: SIP/2.0/UDP xxxx.xxx.xxx.xxx:yyyy
Allow: INVITE, ACK, CANCEL, BYE, PRACK, OPTIONS
Accept: application/sdp
Call-ID: SDsnq0401-367e48c3b9fe610658ea66de87dab677-v3000v3
From: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
Max-Forwards: 64
Contact: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;transport=udp>
CSeq: 22686 INVITE
Content-Length: 178
Interface: Intrado-ESInet-to-ESInet-Basic-3.0
Supported: 100rel
P-Asserted-Identity: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
```

Note: The SIP software used by each NG Service Provider will most likely add a number of tags to various headers. Generally, the tags have no semantic meaning in processing the SIP message. The receiving ESInet must be able to handle these additional tags.

3.1.2 SIP Headers: Hand-off

3.1.2.1 Request URI for Hand-off Calls

The '911' in the user portion of the Request URI indicates that the call is a handoff.

The “dtg=” tag conveys the name of the handoff IP trunk group. The receiving ESInet can use this value to assign routing methodology for the handoff call. As an example, the routing methodologies used by AT&T follow.

- Main Routing
 - Selective Routing Database (SRDB) for ESN-based routing
 - ECRF for i3 Routing
 - Trunk Only Routing (TOR)
- Default Routing

The name of the ‘dtg=’ tag allows the receiving ESInet to assign semantics on how to handle the call. If the ESInet provider cannot handle the “dtg=” tag; AT&T will work with the ESInet provider to determine what semantics they can support.

3.1.2.2 From and P-Asserted-Identity:

These headers work in a hierarchy. P-Asserted-Identity (P-A-I) contains the true call-back number of the caller. If the sending ESInet does not know the true call-back number, the P-A-I header will not be present. Only the From header will be provided.

If the P-A-I is present, the P-A-I and From headers may contain the same values or different values. If both values are present and they are different, the receiving ESInet may have to try both values to find location. An example for when the values could be different is for a wireless call where the P-A-I may contain the true call-back and the From contains the p-ANI.

3.1.2.3 Support or Required:

The 100rel value indicates that a PRACK is required for 18x messages.

The rest of the headers are basic to a SIP message. They don’t have any specific semantics with respect to the ESInet-to-ESInet interface.

3.1.3 Example: Transfer/conference

```
INVITE sip:8601191234@xxx.xxx.xxx.xxx:yyyy;dtg=TRUNKGROUPNAME SIP/2.0
Content-Type: application/sdp
To: <sip:8601191234@xxx.xxx.xxx.xxx:yyyy>
Via: SIP/2.0/UDP xxx.xxx.xxx.xxx:yyyy
Allow: INVITE, ACK, CANCEL, BYE, PRACK, OPTIONS
Accept: application/sdp
Call-ID: SDsnq0401-367e48c3b9fe610658ea66de87dab677-v3000v3
From: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
Interface: Intrado-ESInet-to-ESInet-Basic-3.0
Max-Forwards: 64
Contact: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;transport=udp>
CSeq: 22686 INVITE
Content-Length: 178
Supported: 100rel
P-Asserted-Identity: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
```

3.1.4 SIP Headers: Transfers/Conferences

3.1.4.1 SIP URI for Transfers/Conferences

In this example, the Request URI indicates that the call is a transfer/conference. The user part of the Request URI indicates the Pilot TN of the target PSAP. The “dtg=” tag indicates the name of the transfer trunk group. The receiving ESInet can assign routing semantics associated with the trunk name.

3.1.4.2 P-A-I and From

The same semantics as in the handoff example above are used.

3.1.5 Summary

The following diagram summarizes the handoff/transfer/conference methods for the pre-i3 interface.

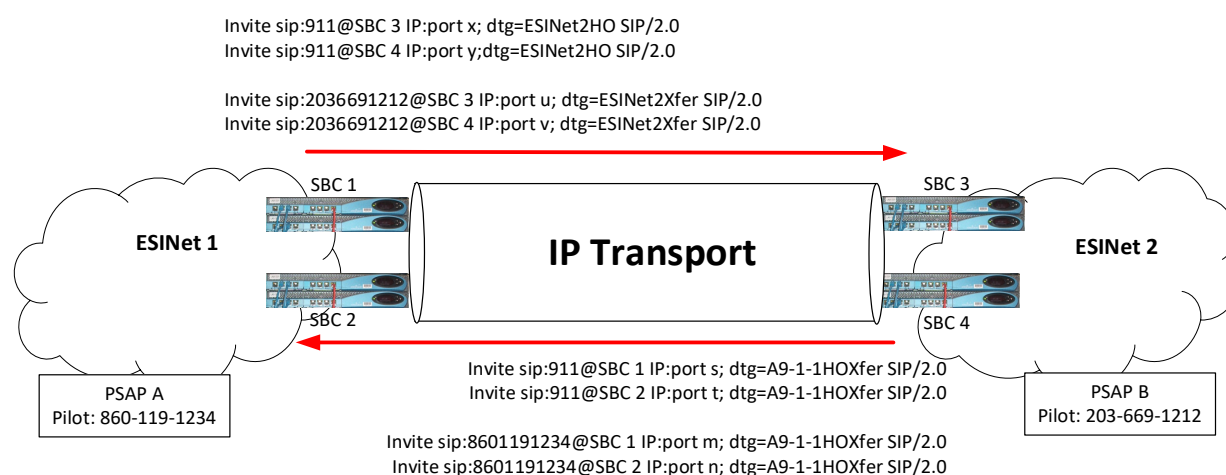


Figure 3: Handoff/Transfer/Conference Methods for Pre-i3 Interface

4.0 Appendix A: ESInet-to-ESInet SIP Basic Implementation Guide

The following diagram summarizes the handoff/transfer/conference methods.

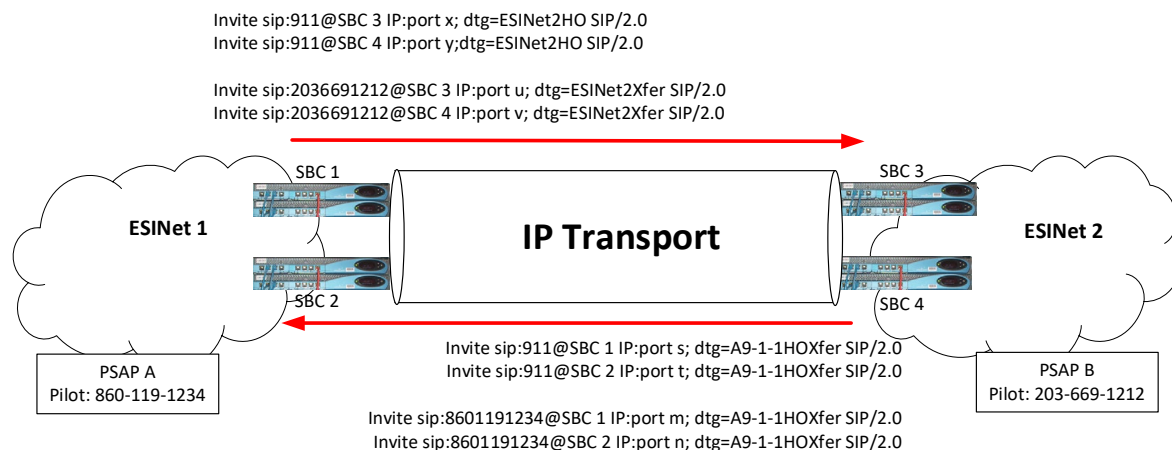


Figure 4: Handoff/Transfer/Conference Methods

4.1 Interconnection and IP/Port Assignments

AT&T is flexible with regard to destination IP addressing and SBC port assignments. The following combinations are supported.

- One IP and one port for all traffic – this option is effective when the NG Service Provider can support “dtg=” for routing semantics.
- Same IP address with different ports – this option is useful if the NG Service Provider is unable to support “dtg=”. The different ports are a proxy for this parameter and can be used to assign routing semantics.

4.2 Handoff versus Transfer/Conference

A handoff is a call that is passed between ESInets as a 9-1-1 call (i.e. called=911). These are calls that initially land on an ESInet and after routing analysis are deemed to not be in their domain (not supported on their ESInet). An example of this scenario is in areas where two or more ESInets support split rate centers.

A transfer/conference is a call that has been routed to the Primary PSAP on one ESInet and the PSAP is initiating a transfer/conference with a PSAP on another ESInet. With the SIP Basic pre-i3 interface option these calls are passed between ESInets with a called number that is a 10-digit TN. The TN is typically the pilot TN of the target PSAP. This requires that the PSAP pilot TNs are shared between the NG Service Providers; i.e., each ESInet knows the 10-digit pilot TNs of each other’s PSAPs. Each ESInet uses the 10-digit PSAP pilot TNs to signal to the other Service Provider to not do any route analysis, but to simply send the call to the PSAP indicated by the 10-digit TN.

4.3 Additional Examples

In the examples below, the IP interface is two-way. The examples contain what either ESInet provider should expect for handoff or transfers.

Note: AT&T supports UDP or TCP at the edge of our service. The examples below use UDP.

4.3.1 Example: Handoff (called = 911)

```
INVITE sip:911@xxx.xxx.xxx.xxx:yyyy;dtg=TRUNKGROUPNAME SIP/2.0
Content-Type: application/sdp
To: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
Via: SIP/2.0/UDP xxxx.xxx.xxx.xxx:yyyy;branch=z9hG4bKn5kel5007oc0seolc340.1
Allow: INVITE, ACK, CANCEL, BYE, REGISTER, REFER, INFO, SUBSCRIBE, NOTIFY, PRACK
Allow: UPDATE, OPTIONS_L
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay
Accept: multipart/mixed
Call-ID: SDsnq0401-367e48c3b9fe610658ea66de87dab677-v3000v3
From: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;tag=SDsnq0401-gK0777cc6b>
Interface: Intrado-ESInet-to-ESInet-Basic-3.0
Max-Forwards: 64
Contact: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;transport=udp>
CSeq: 22686 INVITE
Content-Length: 178
Supported: 100rel
Content-Disposition: session; handling=required
P-Asserted-Identity: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
```

In the example above:

- The P-Asserted-Identity header is included but is not required.
- Mandatory headers are in bold.
- Allow and Accept are specific to the respective ESInet environment.
- Supported: 100rel is required to PRACK 18x messages.

4.3.2 Example: Transfer/Conference (called=PSAP Pilot TN)

```
INVITE sip:3179113001@xxx.xxx.xxx.xxx:5060;dtg=TRUNKGROUPNAME SIP/2.0
Content-Type: application/sdp
To: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>
Via: SIP/2.0/UDP xxxx.xxx.xxx.xxx:yyyy;branch=z9hG4bKn5kel5007oc0seolc340.1
Allow: INVITE, ACK, CANCEL, BYE, REGISTER, REFER, INFO, SUBSCRIBE, NOTIFY, PRACK
Allow: UPDATE, OPTIONS_L
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay
Accept: multipart/mixed
Interface: Intrado-ESInet-to-ESInet-Basic-3.0
Call-ID: SDsnq0401-367e48c3b9fe610658ea66de87dab677-v3000v3
From: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;tag=SDsnq0401-gK0777cc6b>
Max-Forwards: 64
Contact: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy;transport=udp>
CSeq: 22686 INVITE
Content-Length: 178
```

Supported: 100rel

Content-Disposition: session; handling=required

P-Asserted-Identity: <sip:4255551212@xxx.xxx.xxx.xxx:yyyy>

In the example above, the 10-digit TN representing the pilot TN of the PSAP is a coordinated value between the Service Providers.

4.4 Trunk Group Names

The trunk group name must be coordinated between the NG Service providers.

A trunk group name has a maximum length of 24 characters. Valid characters are [A-Z][a-z][0-9][-].

The trunk group name must start with a letter (upper or lower case) or a number. Any combination of letters and numbers is allowed.

4.5 Call Flow

The call flow is the same between a handoff and a transfer/conference.

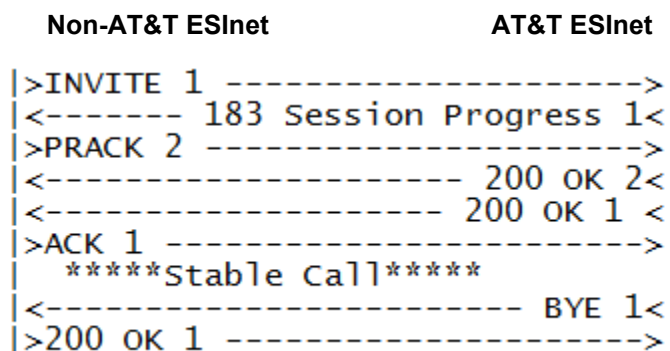


Figure 5: Call Flow for Handoff and Transfer/Conference

The call flow is the same when call origination is by the AT&T ESInet, e.g., AT&T ESInet → Non-AT&T ESInet.

5.0 Appendix B: Acronyms

Term	Definition
ADR	Additional Data Request
ANI	Automatic Number Identification
BCF	Border Control Function
CCP	Concurrent Call Paths
CLR	Circuit Layout Record
D-ESInet	Downstream ESInet
D-ESRP	Downstream ESRP
DLR	Design Layout Record
DNS	Domain Name System
DTMF	Dual Tone Multi Frequency
ECRF	Emergency Call Routing Function
EIDD	Emergency Information Data Document
EIDO	Emergency Incident Data Object
ESInet	Emergency Services IP network
ESQK	Emergency Services Query Key
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
FQDN	Fully Qualified Domain Name
HELD	HTTP Enabled Location Delivery
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
i3	The name given by NENA to a set of protocols used for next generation E9-1-1.
IETF	Internet Engineering Task Force
IP	Internet Protocol
LbyR	Location by Reference
LbyV	Location by Value
LIF	Location Interwork Function
LIS	Location Information Service
LNG	Legacy Network Gateway
LSR	Legacy Selective Router
NCAS	Non-Call Associated Signaling

Term	Definition
NENA	National Emergency Number Association
NG	Next Generation
NGCS	Next Generation Core Services
NIF	NG9-1-1 Interwork Function
OSP	Originating Service Provider
pANI	Pseudo-ANI (see ANI)
PIDF-LO	Presence Information Data Format - Location Object
PIF	Protocol Interwork Function
PSAP	Public Safety Answering Point
RFC	Request for Comments
RTP	Real Time Protocol
RTT	Real Time Text
SBC	Session Border Controller
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SS7	Signaling System 7
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
T-ESRP	Terminating Emergency Services Routing Proxy
TN	Telephone Number
U-ESInet	Upstream ESInet
U-ESRP	Upstream ESRP
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time (aka Greenwich Mean Time (GMT))
VoIP	Voice over Internet Protocol
XML	eXtensible Markup Language



Appendix L - AT&T 2025 Annual Report



LEADING THE NEXT ERA OF CONNECTIVITY

2025 ANNUAL REPORT

To our shareowners

2025 again proved the importance of the telecommunications industry. Our sector is undergoing a remarkable transformation driven by an increased desire for advanced connectivity to support growing demand for AI and the wave of innovation it enables.

Based on our view of how U.S. connectivity would evolve, we've been investing at the top of our industry in fiber and 5G — boosting American competitiveness and supporting local communities and economies. As a result of these investments, we own and operate America's best and largest converged fiber and 5G network. This uniquely positions AT&T to lead our industry forward.



John Stankey
Chairman and Chief Executive Officer,
AT&T Inc.

Growing with America's Best Network

Our founding innovator, Alexander Graham Bell, made the first phone call 150 years ago. Today, we're no longer a phone company. We're now an advanced networking company that moves secure workloads of data for consumers and businesses better than anyone else.

While we plan for the future, we are equally focused on delivering today. In 2025, we met or exceeded all consolidated full-year financial guidance driven by another solid year of 5G and fiber subscriber growth.

Broadband

We brought fiber to more places, and increased fixed wireless availability with deeper spectrum coverage. This resulted in our best consumer broadband subscriber growth in a decade and our 8th straight year of more than 1 million consumer fiber net adds.

Wireless

We delivered over 1.5 million postpaid phone net adds for the 5th consecutive year. We continued to attract new customers as we enhanced and modernized our wireless network and quickly put valuable spectrum from EchoStar to work.

Our investments in fiber and 5G — both organically and through acquisitions — have positioned us to accelerate and scale the execution of our converged strategy in 2026.

- With fiber, we'll do this in our traditional operating region, in acquired geographies from Lumen and with Gigapower. By the end of 2026, we expect to reach over 40 million fiber customer locations, up from 32 million locations at the end of 2025. This puts us well ahead of the competition, and on target to reach more than 60 million total fiber locations¹ by the end of 2030.
- And, with a base of more than 12 million total fiber subscribers growing at a pace of over 1 million customers per year, we still have plenty of runway to grow this durable franchise.
- We're also progressing on our vision to deliver always-on connectivity. In 2026, we plan to offer select AT&T customers, and public safety on FirstNet, beta satellite service through our work with AST SpaceMobile.

Putting Customers First

In 2025, we set a new precedent by launching the AT&T Guarantee, the first and only guarantee that covers both wireless and fiber networks.

With the industry's best assets, we're offering more customers what they want — the ability to purchase all their connectivity from one trusted provider.

- Our converged customers remain our most valuable. They display lower churn and a propensity to take higher Internet speeds, attach more wireless lines and stay with us longer.
- Growing our converged subscriber base helps us drive higher service revenue growth and deliver our long-term financial guidance.
- As we've expanded our convergence opportunity and the AT&T Guarantee, our brand affinity has strengthened. Brand love for AT&T has improved across every customer segment and every product. Additionally, AT&T has the highest net promoter score amongst converged customers.

We returned over

\$12B

to our shareholders through dividends and buybacks. This was more than a 50% increase from 2024.

Our convergence strategy is a winning play and these results give us confidence we are on the right track. Today, we're able to reach over 90 million customer locations with advanced Internet services — through fiber or 5G. This will only increase over the next several years. Through the execution of our convergence strategy, we expect to materially improve share in home Internet and wireless.

Focusing on Effective & Efficient Operations

As good stewards of your capital, we're always looking to reduce costs — allowing us to invest in future growth.

- In 2025, we achieved over \$1 billion of cost savings. We plan to achieve an additional \$4 billion in annual cost savings by the end of 2028 as we leverage AI, move more customer transactions to digital experiences, and achieve greater operating leverage from a growing customer base.
- Smart policies from FCC Chair Brendan Carr and his team have enabled us to accelerate our copper-based legacy network shutdown. In 2025, we fully powered down our first wire center. We have approval to discontinue copper-based services in more than 30% of our wire centers by the end of 2026, and we're on track to shut down a large majority of our copper-based services by the end of 2029.

As we transition to future-focused technologies, we're lowering operating costs and giving more customers advanced connectivity on a more efficient fiber and 5G network. The collective benefits of these cost-savings efforts are also showing up in our results, including improving consolidated adjusted EBITDA margins².

Winning Capital Allocation Strategy & Outlook

In 2025, we delivered on all the capital allocation commitments we set at the beginning of 2025.

- With full-year capital investment³ of \$22 billion, we continued our industry-leading fiber expansion efforts and worked to provide even better, more reliable wireless coverage.
- A strong balance sheet remained a key focus with AT&T reaching the target range of 2.5x net debt-to-adjusted EBITDA⁴ in the first half of 2025.
- We also expanded capital returns by implementing a share repurchase program. We returned over \$12 billion to our shareholders through dividends and buybacks. This was more than a 50% increase from 2024.

Over the past five years, we've significantly evolved how we talk about our company, and in the first quarter of 2026, we plan to adopt a new segment reporting structure with three financial reporting

segments: **Advanced Connectivity**, **Legacy** and **Latin America**. We believe this change reflects the company we have become and where our industry is headed.

The goal of this new structure is to show you, our shareholders, greater transparency into the returns we are generating on our growth investments in fiber and 5G, and how we're advancing with our legacy shutdown.

Overall, we remain on track to deliver ambitious multi-year growth targets and financial commitments. We believe we're positioned to drive improved growth now and well into the future.

- From 2026-2028, we expect leading investments in 5G and fiber to deliver strong returns and drive accelerated growth in adjusted EBITDA, double-digit adjusted EPS growth, and strong free cash flow⁵.
- Our three-year outlook also includes plans for greater shareholder returns. From 2026-2028, we anticipate \$45 billion-plus in shareholder returns thanks to an attractive dividend and share repurchases.
- We're confident that we'll lead our industry in advanced connectivity service revenue and adjusted EBITDA by the end of the decade.

Bringing Internet to More People

As we enter the next era of connectivity, we remain focused on playing our part in ensuring every American has access to reliable, high-speed Internet. We're proud to offer vital communications services that communities and first responders — through FirstNet — rely on across the United States.

AT&T is dedicated to doing its part to help close the digital divide. We committed a total of \$5 billion to help more people get and stay connected from 2021-2030. Overall, progress is being made. The latest data shows that fewer than 8 million U.S. households remain without Internet access. This achievement is due to private sector investment and smart public policy coming together to connect more communities and reduce the rolls of the unconnected by over 50% in four years.

Our three-year outlook

\$45B+

anticipated in shareholder returns — through dividends and share repurchases — from 2026-2028.

It's clear that leaders across all levels of government recognize the critical role advanced networks play in driving economic growth. Through initiatives like the Federal Government's BEAD program and pro-investment policies included in the One Big Beautiful Bill, we're closer than ever to closing the digital divide.

Ultimately, our goal is to make Internet access not only more easily available, but affordable to everyone. To do this, it's critical that we fix the funding mechanism for the pre-Internet era Universal Service Fund to align with how people connect today. This is the next great play for Congressional policy makers to create a digital future that benefits everyone.

We are the Best, Thanks to You

With the best network and telecommunications assets in America, we're more than ready to lead our industry forward as demand for AI and autonomous technologies grows on top of today's robust data and voice workloads. Our progress and performance in 2025 only further reinforces this belief.

To our customers:

We'll continue to put you first, always. The AT&T Guarantee is our promise to you. We'd like to thank you for trusting in AT&T as the one provider for all your important connectivity needs.

To our current and past employees:

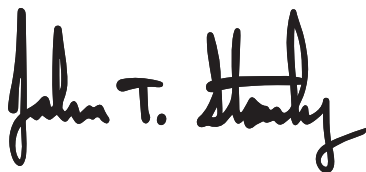
We owe the tremendous opportunity ahead of us to you. Providing good jobs and benefits for Americans remains critically important to us. We're proud to employ the largest unionized workforce in telecom. Our contributions to further fund our pension plans in 2025 only reinforces our commitment to you. Thank you for keeping our country connected.

To our shareowners:

We remain committed to the growth objectives we've laid out. We fully believe that our assets enable us to lead our industry and accelerate growth in our company. We expect to deliver healthy returns to you while positioning AT&T for a bright future.

Lastly, thank you to our Board of Directors and our talented management team for their continued support.

Sincerely,

A handwritten signature in black ink that reads "John T. Stankey". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

John Stankey

Chairman and Chief Executive Officer, AT&T Inc.

February 9, 2026

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

(Mark One)



**ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d)
OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2025

OR



**TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d)
OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission File Number: 001-8610

AT&T INC.

(Exact name of registrant as specified in its charter)

Delaware

(State or other jurisdiction
of incorporation or organization)

208 S. Akard St.

Dallas, Texas

(Address of principal executive office)

43-1301883

(I.R.S. Employer Identification No.)

75202

(Zip Code)

Registrant's telephone number, including area code: 210-821-4105

Securities registered pursuant to Section 12(b) of the Act:

<u>Title of each class</u>	<u>Trading Symbol(s)</u>	<u>Name of each exchange on which registered</u>
Common Shares (Par Value \$1.00 Per Share)	T	New York Stock Exchange NYSE Texas
Depository Shares, each representing a 1/1000th interest in a share of 5.000% Perpetual Preferred Stock, Series A	T PRA	New York Stock Exchange
Depository Shares, each representing a 1/1000th interest in a share of 4.750% Perpetual Preferred Stock, Series C	T PRC	New York Stock Exchange
AT&T Inc. 3.550% Global Notes due November 18, 2025	T 25B	New York Stock Exchange
AT&T Inc. 3.500% Global Notes due December 17, 2025	T 25	New York Stock Exchange
AT&T Inc. 0.250% Global Notes due March 4, 2026	T 26E	New York Stock Exchange
AT&T Inc. 1.800% Global Notes due September 5, 2026	T 26D	New York Stock Exchange
AT&T Inc. 2.900% Global Notes due December 4, 2026	T 26A	New York Stock Exchange
AT&T Inc. Floating Rate Global Notes due September 16, 2027	T 27C	New York Stock Exchange
AT&T Inc. 1.600% Global Notes due May 19, 2028	T 28C	New York Stock Exchange
AT&T Inc. 2.350% Global Notes due September 5, 2029	T 29D	New York Stock Exchange
AT&T Inc. 4.375% Global Notes due September 14, 2029	T 29B	New York Stock Exchange
AT&T Inc. 2.600% Global Notes due December 17, 2029	T 29A	New York Stock Exchange
AT&T Inc. 0.800% Global Notes due March 4, 2030	T 30B	New York Stock Exchange
AT&T Inc. 3.150% Global Notes due June 1, 2030	T 30C	New York Stock Exchange
AT&T Inc. 3.950% Global Notes due April 30, 2031	T 31F	New York Stock Exchange
AT&T Inc. 2.050% Global Notes due May 19, 2032	T 32A	New York Stock Exchange
AT&T Inc. 3.550% Global Notes due December 17, 2032	T 32	New York Stock Exchange
AT&T Inc. 3.600% Global Notes due June 1, 2033	T 33A	New York Stock Exchange
AT&T Inc. 5.200% Global Notes due November 18, 2033	T 33	New York Stock Exchange

Securities registered pursuant to Section 12(b) of the Act (continued):

<u>Title of each class</u>	<u>Trading Symbol(s)</u>	<u>Name of each exchange on which registered</u>
AT&T Inc. 3.375% Global Notes due March 15, 2034	T 34	New York Stock Exchange
AT&T Inc. 4.300% Global Notes due November 18, 2034	T 34C	New York Stock Exchange
AT&T Inc. 2.450% Global Notes due March 15, 2035	T 35	New York Stock Exchange
AT&T Inc. 3.150% Global Notes due September 4, 2036	T 36A	New York Stock Exchange
AT&T Inc. 4.050% Global Notes due June 1, 2037	T 37B	New York Stock Exchange
AT&T Inc. 2.600% Global Notes due May 19, 2038	T 38C	New York Stock Exchange
AT&T Inc. 1.800% Global Notes due September 14, 2039	T 39B	New York Stock Exchange
AT&T Inc. 7.000% Global Notes due April 30, 2040	T 40	New York Stock Exchange
AT&T Inc. 4.250% Global Notes due June 1, 2043	T 43	New York Stock Exchange
AT&T Inc. 4.875% Global Notes due June 1, 2044	T 44	New York Stock Exchange
AT&T Inc. 4.000% Global Notes due June 1, 2049	T 49A	New York Stock Exchange
AT&T Inc. 4.250% Global Notes due March 1, 2050	T 50	New York Stock Exchange
AT&T Inc. 3.750% Global Notes due September 1, 2050	T 50A	New York Stock Exchange
AT&T Inc. 5.350% Global Notes due November 1, 2066	TBB	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act: None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act.

Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company” and “emerging growth company” in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant has filed a report on and attestation to its management’s assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☒

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant’s executive officers during the relevant recovery period pursuant to §240.10D-1(b). ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Act).

Yes ☐ No ☒

Based on the closing price of \$28.94 per share on June 30, 2025, the aggregate market value of our voting and non-voting common stock held by non-affiliates was \$207 billion.

At January 28, 2026, common shares outstanding were 7,000,577,201.

DOCUMENTS INCORPORATED BY REFERENCE

- (1) Portions of AT&T Inc.’s Notice of 2026 Annual Meeting and Proxy Statement dated on or about March 23, 2026, to be filed within the period permitted under General Instruction G(3) (Part III).

TABLE OF CONTENTS

Item		Page
	PART I	
1.	Business	1
1A.	Risk Factors	7
1B.	Unresolved Staff Comments	15
1C.	Cybersecurity	15
2.	Properties	16
3.	Legal Proceedings	16
4.	Mine Safety Disclosures	16
	Information about our Executive Officers	17
	PART II	
5.	Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	18
6.	[Reserved]	19
7.	Management’s Discussion and Analysis of Financial Condition and Results of Operations	20
7A.	Quantitative and Qualitative Disclosures about Market Risk	37
8.	Financial Statements and Supplementary Data	42
9.	Changes in and Disagreements with Accountants on Accounting and Financial Disclosure	90
9A.	Controls and Procedures	90
9B.	Other Information	90
9C.	Disclosure Regarding Foreign Jurisdictions that Prevent Inspections	90
	PART III	
10.	Directors, Executive Officers and Corporate Governance	91
11.	Executive Compensation	91
12.	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	91
13.	Certain Relationships and Related Transactions, and Director Independence	92
14.	Principal Accountant Fees and Services	92
	PART IV	
15.	Exhibits and Financial Statement Schedules	92
16.	Form 10-K Summary	95

PART I

ITEM 1. BUSINESS

GENERAL

AT&T Inc. (“AT&T,” “we” or the “Company”) is a holding company incorporated under the laws of the State of Delaware in 1983 and has its principal executive offices at 208 S. Akard St., Dallas, Texas, 75202 (telephone number 210-821-4105). We maintain an internet website at www.att.com. (This website address is for information only and is not intended to be an active link or to incorporate any website information into this document.) We file electronically with the Securities and Exchange Commission (SEC) required reports on Form 8-K, Form 10-Q and Form 10-K; proxy materials; registration statements on Forms S-3 and S-8, as necessary; and other forms or reports as required. The SEC maintains a website (www.sec.gov) that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the SEC. We make available, free of charge, on our website our annual report on Form 10-K, our quarterly reports on Form 10-Q, current reports on Form 8-K and all amendments to those reports as soon as reasonably practicable after such reports are electronically filed with, or furnished to, the SEC. We also make available on that website, and in print, if any stockholder or other person so requests, our “Code of Ethics” applicable to all employees and Directors, our “Corporate Governance Guidelines,” and the charters for all committees of our Board of Directors, including Audit, Human Resources and Governance and Policy committees. Any changes to our Code of Ethics or waiver of our Code of Ethics for senior financial officers, executive officers or Directors will be posted on that website.

A reference to a “Note” refers to the Notes to Consolidated Financial Statements in Item 8.

History

AT&T, formerly known as SBC Communications Inc. (SBC), was formed as one of several regional holding companies created to hold AT&T Corp.’s (ATTC) local telephone companies. On January 1, 1984, we were spun-off from ATTC pursuant to an anti-trust consent decree, becoming an independent publicly traded telecommunications services provider.

Following our formation, we expanded our communications footprint and operations, most significantly:

- Our subsidiaries merged with incumbent local exchange carriers (ILEC) Pacific Telesis Group in 1997 and Ameritech Corporation in 1999.
- In 2005, we merged one of our subsidiaries with ATTC, creating one of the world’s leading telecommunications providers. In connection with the merger, we changed the name of our company from “SBC Communications Inc.” to “AT&T Inc.”
- In 2006, we acquired ILEC BellSouth Corporation (BellSouth), which included BellSouth’s 40% economic interest in AT&T Mobility LLC (AT&T Mobility), formerly Cingular Wireless LLC, resulting in 100% ownership of AT&T Mobility.
- In 2014, we completed the acquisition of wireless provider Leap Wireless International, Inc.
- In 2015, we acquired wireless properties in Mexico and acquired DIRECTV, a leading provider of digital television entertainment services in both the United States (included in our former Video business) and Latin America (referred to as Vrio, which was sold in November 2021).
- In July 2021, we closed our transaction with TPG Capital (TPG) to form a new company named DIRECTV Entertainment Holdings, LLC (DIRECTV). With the close of the transaction (DIRECTV Transaction), we separated our Video business, comprised of our U.S. video operations, and began accounting for our investment in DIRECTV under the equity method. In July 2025, we sold our remaining interest in DIRECTV to TPG.

General

We are a leading provider of telecommunications and technology services globally. The services and products that we offer vary by market and utilize various technology platforms in a range of geographies. Our reportable segments are organized as follows:

The **Communications segment** provides wireless and wireline telecom and broadband services to consumers located in the United States and businesses globally. Our business strategies reflect integrated product offerings that cut across product lines and utilize shared assets. This segment contains the following business units:

- **Mobility** provides nationwide wireless service and equipment.
- **Business Wireline** provides advanced ethernet-based fiber services, fixed wireless services, IP Voice and managed professional services, as well as legacy voice and data services and related equipment, to business customers.
- **Consumer Wireline** provides broadband services, including fiber connections that provide multi-gig services, and our fixed wireless access product (AT&T Internet Air or “AIA”) that provides internet services delivered over our 5G wireless network, to residential customers in select locations. Consumer Wireline also provides legacy telephony voice communication services.

The *Latin America segment* provides wireless service and equipment in Mexico.

Corporate support costs, including administrative support costs borne by AT&T where business units do not influence decision making, and results from business no longer integral to our operations are reported as *Corporate* and *Other*, which reconciles our segment results to consolidated operating income and income before income taxes.

Areas of Focus

We are a leader in providing connectivity services through our market focus areas of 5G and fiber. Fiber underpins the connectivity we deliver, both wired and wireless. Building on that fiber foundation is our solid spectrum portfolio, strengthened through Federal Communications Commission (FCC) auctions, other spectrum acquisitions and 5G deployment. We believe our fixed wireline and mobile approach will differentiate our services and provide us with additional convergence growth opportunities in the future as bandwidth demands continue to grow. We will continue to demonstrate our commitment to ensure management attention is sharply focused on growth areas and operational efficiencies.

Our integrated telecommunications network utilizes different technological platforms to provide instant connectivity at the higher speeds made possible by our fiber network expansion and wireless network enhancements. Streaming, augmented reality, “smart” technologies, user generated content and artificial intelligence (AI) are expected to continue to drive greater demand for broadband, which we believe will allow us to capitalize on our fiber and 5G deployments. During 2026, we are focused on the core capabilities of our products, our infrastructure and our network. We will also focus on accelerating our fiber expansion, organically and through our pending acquisition of substantially all of Lumen’s Mass Markets fiber business. We will continue to deploy low- and mid-band spectrum to improve speed and capacity, including spectrum to be acquired from our pending transactions with EchoStar Corporation (EchoStar) and other spectrum acquisitions. Our concentration is to aggregate the most traffic on the largest, lowest marginal cost, converged network through efficient spectrum deployment and construction of the largest high-capacity broadband solutions in the United States, while also working with regulators and customers to decommission high-cost legacy technologies over the next several years.

Wireless Service We continue to experience rapid growth in data usage as consumers are demanding seamless access across their wireless and wired devices, and businesses and municipalities are connecting an increasing number of equipment and facilities to the internet. The deployment of 5G, which allows for faster connectivity, lower latency and greater bandwidth, requires modifications of existing cell sites to add equipment supporting new frequencies, like the C-Band and the 3.45 GHz band. The increased speeds and network operating efficiency expected with 5G technology has enabled massive deployment of devices connected to the internet as well as faster delivery of data services. As the wireless industry has matured, with nearly full penetration of smartphones in the U.S. population, future wireless growth will depend on our ability to offer innovative services, plans and devices that bundle product offerings, add converged customer relationships and take advantage of our 5G wireless network.

To support higher mobile data usage, our priority is to best utilize a wireless network that has sufficient spectrum and capacity to support these innovations on as broad a geographic basis as possible. We expect to continue to invest significant capital in expanding our network capacity, as well as obtaining additional spectrum, when needed and available, that meets our long-term needs. We participate in FCC spectrum auctions, acquire spectrum licenses from third parties as it becomes available and redeploy existing spectrum previously used for more basic services to support more advanced mobile internet services.

In North America, our network covers over 441 million people with 4G LTE and over 322 million with 5G technology. In the United States, our network covers all major metropolitan areas and more than 337 million people with our LTE technology and more than 322 million people with our 5G technology.

Broadband Technology Fiber is a core priority for our business and over the last several years we have enhanced our focus to expand our fiber footprint and grow customers. At December 31, 2025, we had 10.4 million fiber consumer wireline broadband customers, adding 1.1 million during the year. The expansion builds on our recent investments to convert to a software-based network, managing the migration of wireline customers to services using our fiber infrastructure to provide broadband technology. Software-based technologies align with our global leadership in software defined network (SDN) and network function virtualization (NFV). This network approach delivers a demonstrable cost advantage in the deployment of next-generation technology over the traditional, hardware-intensive network approach. Our virtualized network supports next-generation applications like 5G and broadband-based services quickly and efficiently. At December 31, 2025, we had 16.0 million broadband connections, compared to 15.3 million broadband connections in the prior year.

In areas where fiber services are not available, in recent years we have offered fixed wireless access under our AT&T Internet Air (AIA) brand. At December 31, 2025, we had 1.5 million AIA connections, adding 875,000 during the year. With recent spectrum acquisitions, including our pending transaction with EchoStar we are expanding the capacity of the wireless network over which these services are provided to support this growth initiative.

Copper Decommissioning While building the network of the future, we are actively working to exit our legacy copper network operations across the large majority of our wireline footprint. Our exit strategy includes migrating customers to fiber and wireless alternatives, and working with policy-makers to decommission our inefficient and less reliable copper network. At December 31, 2025, we had 2.1 million customer location switched access lines in service and 2.8 million legacy consumer internet connections compared to 2.7 million customer location switched access lines in service and 4.1 million legacy consumer internet connections in the prior year.

BUSINESS OPERATIONS

OPERATING SEGMENTS

Our segments are strategic business units that offer different products and services over various technology platforms and/or in different geographies that are managed accordingly. We have two reportable segments: Communications and Latin America.

Additional information about our segments, including financial information, is included under the heading “Segment Results” in Item 7 and in Note 4 of Item 8.

COMMUNICATIONS

Our Communications segment provides wireless and wireline telecom and broadband services to consumers located in the United States and businesses globally. Our Communications services and products are marketed under the AT&T, AT&T Business, Cricket, AT&T PREPAIDSM, AT&T Fiber and AT&T Internet Air brand names. The Communications segment provided approximately 97% of 2025 segment operating revenues and accounted for substantially all of our 2025 total segment operating income. This segment contains the Mobility, Business Wireline and Consumer Wireline business units.

Mobility – Our Mobility business unit provides nationwide wireless service to consumers and wholesale and resale wireless subscribers located in the United States by utilizing our network to provide voice and data services, including high-speed internet over wireless devices. We classify our subscribers as either postpaid, prepaid or reseller. As of December 31, 2025, we served 120 million Mobility subscribers, including 91 million postpaid (74 million phone), 18 million prepaid and 11 million through resellers. Our Mobility business unit revenue includes the following categories: service and equipment.

Service

We offer a comprehensive range of high-quality nationwide wireless voice and data communications services in a variety of pricing plans to meet the communications needs of targeted customer categories. Through FirstNet[®] services, we also provide a nationwide wireless broadband network dedicated to public safety.

Consumers continue to require increasing availability of data-centric services and a network to connect and control wireless devices. An increasing number of our subscribers are using more advanced devices, including embedded computing systems and/or software, commonly called the Internet of Things (IoT). We offer unlimited plans that include features allowing for the sharing of voice, text and data across multiple devices, which attracts subscribers from other providers and helps minimize subscriber churn. We continue to upgrade our network and coordinate with equipment manufacturers and application developers to further capitalize on the continued growing demand for wireless data services.

We also offer nationwide wireless voice and data communications to certain customers who prefer to pay in advance. These services are offered under the Cricket and AT&T PREPAID brands and are typically monthly prepaid services.

Equipment

We sell a wide variety of handsets, wireless data cards and wireless computing devices manufactured by various suppliers for use with our voice and data services. We also sell accessories, such as carrying cases/protective covers and wireless chargers. We sell online and through our own company-owned stores, agents and third-party retail stores. We provide our customers the ability to purchase handsets on an installment basis and the opportunity to bring their own device. Subscribers that bring their own devices or retain handsets for longer periods impact upgrade activity. Like other wireless service providers, we also provide postpaid contract subscribers promotional equipment offers to initiate, renew or upgrade service.

Business Wireline – Our Business Wireline business unit provides services to business customers, including multinational corporations, small and mid-sized businesses, and governmental and wholesale customers. Our Business Wireline business unit revenue includes the following categories: legacy and other transitional services, fiber and advanced connectivity services, and equipment.

Legacy and Other Transitional Services

We offer legacy voice and other transitional services comprised of copper-based voice and data, Virtual Private Networks (VPN), wholesale, outsourcing and IP sales. Historically, a majority of our Business Wireline service revenues came from

legacy copper-based voice and data and traditional products; however, over recent years those services have been declining due to secular pressures. We plan to continue to focus on our owned and operated connectivity services powered by 5G and fiber as well as evaluating opportunities where we can turn down existing copper infrastructure.

Fiber and Advanced Connectivity Services

We offer fiber and other advanced connectivity services, such as AT&T Dedicated Internet, fiber ethernet and broadband, fixed wireless, and hosted and managed professional services. We continue to reconfigure our wireline network to take advantage of the latest technologies and services, and rely on our SDN and NFV to enhance business customers' digital agility in a rapidly evolving environment.

Equipment

Equipment revenues include customer premises equipment.

Consumer Wireline – Our Consumer Wireline business unit provides broadband services, including fiber connections, AIA and legacy telephony voice communication services, to customers in the United States by utilizing our IP-based and copper wired network. Our Consumer Wireline business unit revenue includes the following categories: broadband, legacy voice and data services and other service and equipment.

Broadband Service

We provide broadband and internet services to approximately 14.7 million customers, including 10.4 million fiber broadband connections and 1.5 million AIA connections at December 31, 2025. With the continued rise of data-intensive activities, like on-the-go video streaming, augmented reality, user generated content, AI-enabled applications, remote work and the widespread adoption of smart devices, we are experiencing increasing demand for high-speed broadband services. We believe our investment in expanding our industry-leading fiber network positions us to be a leader in wired connectivity. Our focus on fiber and AIA brings owner's economics and expected efficiencies while we continue to evaluate opportunities where we can turn down existing copper infrastructure.

We believe that our flexible platform, with a broadband and wireless connection, is the most efficient way to transport direct-to-consumer experiences both at home and on mobile devices. Through this integrated approach, we can optimize the use of storage in the home as well as in the cloud, while also providing a seamless service for consumers across screens and locations.

Legacy Voice and Data Services

Revenues from our traditional voice services continue to decline as customers switch to wireless or VoIP services provided by us, cable companies or other internet-based providers.

Other Service and Equipment

Other service revenues include VoIP services, customer fees and limited equipment.

Additional information on our Communications segment is contained in the "Overview" section of Item 7.

LATIN AMERICA

Our Latin America segment provides wireless service in Mexico. We utilize our regional and national wireless networks in Mexico to provide consumer and business customers with wireless data and voice communication services. The Latin America segment provided approximately 3% of 2025 segment operating revenues and less than 1% of our 2025 total segment operating income. We divide our revenue into the following categories: service and equipment.

Service

We provide postpaid and prepaid wireless services in Mexico to approximately 24.7 million subscribers under the AT&T and Unefon brands. Postpaid service allows for (1) no annual service contract for subscribers who bring their own device or purchase a device on installment and (2) service contracts for periods up to 36 months for subscribers who purchase their equipment under the traditional device subsidy model. We also offer prepaid plans.

Equipment

We sell a wide variety of handsets, including smartphones manufactured by various suppliers for use with our voice and data services. We sell through our own company-owned stores, agents and third-party retail stores.

Additional information on our Latin America segment is contained in the "Overview" section of Item 7.

MAJOR CLASSES OF SERVICE

The following table sets forth the percentage of total consolidated reported operating revenues by any class of service that accounted for 10% or more of our consolidated total operating revenues in any of the last three fiscal years:

	Percentage of Total Consolidated Operating Revenues		
	2025	2024	2023
Communications Segment			
Wireless service	54 %	53 %	52 %
Fiber and advanced connectivity ¹	13	12	11
Legacy and other transitional	8	10	13
Equipment	18	17	17
Latin America Segment			
Wireless service	2	2	2
Equipment	1	1	1

¹ Includes Fiber revenues reported in our Consumer Wireline business unit and Fiber and advanced connectivity services reported in our Business Wireline business unit.

Additional information on our geographical distribution of revenues is contained in Note 4 of Item 8.

GOVERNMENT REGULATION

Facilities-based wireless communications providers in the United States, like AT&T, must be licensed by the FCC to provide communications services at specified spectrum frequencies within defined geographic areas and must comply with FCC rules and policies governing the use of the spectrum. The FCC's rules have a direct impact on whether the wireless industry has sufficient spectrum available to support the high-quality, innovative services our customers demand. Wireless licenses are issued for a fixed time period, typically 10 to 15 years, and we must seek renewal of these licenses. While the FCC has generally renewed licenses, the FCC has authority to both revoke a license for cause and to deny a license renewal if a renewal is not in the public interest. Additionally, while wireless communications providers' prices and service offerings have historically not been subject to prescriptive regulation, the federal government and various states periodically consider new regulations and legislation relating to various aspects of wireless services.

The Communications Act of 1934 and other related laws give the FCC authority to regulate the U.S. operations of our interstate telecommunications services. In addition, our ILEC subsidiaries are subject to regulation by state governments, which may regulate intrastate services, provided such state regulation is consistent with federal law. Some states have eliminated or reduced regulations on our retail offerings. AT&T subsidiaries are also subject to the jurisdiction of the FCC with respect to intercarrier compensation, interconnection, and interstate and international services, including interstate access charges. Access charges are a form of intercarrier compensation designed to reimburse our wireline subsidiaries for the use of their networks by other carriers.

We continue to support regulatory and legislative measures and efforts at both the federal and state levels to minimize and/or moderate regulatory burdens that are no longer appropriate in a competitive communications market and that inhibit our ability to compete more effectively and offer services wanted and needed by our customers, including initiatives to transition services from traditional networks to all IP-based networks. At the same time, we also seek to ensure that legacy regulations are not further extended to broadband or wireless services, which are subject to vigorous competition.

Our subsidiaries operating outside the United States are subject to the jurisdiction of national and supranational regulatory authorities in the market where service is provided.

For a discussion of significant regulatory issues directly affecting our operations, please see the information contained under the headings "Operating Environment and Trends of the Business" and "Regulatory Landscape" of Item 7, which information is incorporated herein by reference.

IMPORTANCE, DURATION AND EFFECT OF LICENSES

Certain of our subsidiaries own or have licenses to various patents, copyrights, trademarks and other intellectual property necessary to conduct business. Many of our subsidiaries also hold government-issued licenses or franchises to provide wireline or wireless services. Additional information relating to regulations affecting those rights is contained under the heading "Regulatory Landscape" of Item 7. We actively pursue patents, trademarks and service marks to protect our intellectual property within the United States and abroad. We maintain a significant global portfolio of patents, trademarks and service mark registrations. We have also entered into licenses that permit other companies to utilize certain of our patents, trademarks,

service marks, and technologies, in exchange for payments and subject to appropriate safeguards and restrictions. As we transition our network from a switch-based network to an IP, software-based network, we have increasingly entered into licensing agreements with software developers.

We periodically license third-party patents and other intellectual rights in exchange for payments. We also receive claims from third parties asserting that our products, services or technologies infringe on their patents or other intellectual property rights. These claims could require us to pay damages or acquire license rights, stop offering the relevant products or services, and/or cease network functions or other activities. While the outcome of any litigation is uncertain, we do not believe that the resolution of any of these infringement claims or the expiration or non-renewal of any of our intellectual property rights would have a material adverse effect on our results of operations.

MAJOR CUSTOMERS

No customer accounted for 10% or more of our consolidated revenues in 2025, 2024 or 2023.

COMPETITION

Competition continues to increase for communications and digital services from traditional and nontraditional competitors. Technological advances have expanded the types and uses of services and products available. In addition, lack of or a reduced level of regulation of comparable legacy services has lowered costs for alternative communications service providers. As a result, we face continuing competition as well as some new opportunities in significant portions of our business.

Wireless We face substantial competition in our wireless businesses. Under current FCC rules, multiple licensees, who provide wireless services on the cellular, PCS, Advanced Wireless Services, 700 MHz and other spectrum bands, may operate in each of our U.S. service areas. Our competitors include two national wireless providers; a larger number of regional providers and resellers of each of those providers' services; and certain cable companies. In addition, we face competition from providers who offer voice, text messaging and other services as applications on data networks. We are one of three facilities-based providers in Mexico (retail and wholesale), with the most significant market share controlled by América Móvil. We may experience significant competition from companies that provide similar services using other communications technologies and services. While some of these technologies and services are now operational, others are being developed or may be developed. We compete for customers based principally on service/device offerings, price, network quality, coverage area and customer service.

Broadband The desire for high-speed data on demand, including data-intensive activities, is continuing to lead customers to terminate their traditional wired or copper-based services and use our fiber or fixed wireless services or competitors' fixed wireless, satellite and internet-based services. In most U.S. markets, we compete for customers with large cable companies and wireless broadband providers for high-speed internet and voice services.

Legacy Voice and Data We continue to lose legacy voice and data customers due to industry-wide secular declines and competitors (e.g., wireless, cable and VoIP providers) who can provide comparable services at lower prices because they are not subject to traditional telephone industry regulation (or the extent of regulation they are subject to is in dispute), utilize different technologies or promote a different business model. In most U.S. markets, we compete for customers with large cable companies and other smaller telecommunications companies.

Additionally, we provide local and interstate telephone and switched services to other service providers, primarily large internet service providers using the largest class of nationwide internet networks (internet backbone), wireless carriers, other telephone companies, cable companies and systems integrators. These services are subject to additional competitive pressures from the development of new technologies, the introduction of innovative offerings and increasing satellite, wireless, fiber-optic and cable transmission capacity for services.

RESEARCH AND DEVELOPMENT

AT&T scientists and engineers conduct research in a variety of areas, including IP networking, advanced network design and architecture, network and cybersecurity, network operations support systems and data analytics. The majority of the development activities are performed to create new services and to invent tools and systems to manage secure and reliable networks for us and our customers. Research and development expenses were \$843 in 2025, \$955 in 2024, and \$954 in 2023.

HUMAN CAPITAL

Number of Employees As of December 31, 2025, we employed approximately 133,030 persons.

Employee Development We believe our success depends on our employees' success and that all employees must have the skills they need to thrive. We offer training and elective courses that give employees the opportunity to enhance their skills. We also intend to help cultivate the next generation of talent that will lead our company into the future by providing employees with educational opportunities through our internal training organization.

Labor Contracts Approximately 43% of our employees are represented by the Communications Workers of America (CWA), the International Brotherhood of Electrical Workers (IBEW) or other unions. After expiration of collective bargaining agreements, work stoppages or labor disruptions may occur in the absence of new contracts or other agreements being reached. The main contracts set to expire in 2026 include the following:

- A contract covering approximately 9,000 employees across 36 states and the District of Columbia is set to expire in February.
- A contract covering approximately 4,300 employees across five states is set to expire in April.
- Two wireline contracts covering approximately 1,800 employees across all 50 states as well as the U.S. Virgin Islands and Puerto Rico are set to expire in April.

Compensation and Benefits In addition to salaries, we provide a variety of benefit programs to help meet the needs of our employees. These programs cover active and former employees and may vary by subsidiary and region. These programs include 401(k) plans, pension benefits, and health and welfare benefits, among many others. In addition to our active employee base, at December 31, 2025, we had approximately 477,000 retirees and dependents who were eligible to receive retiree benefits.

We review our benefit plans to maintain competitive packages that reflect the needs of our workforce. We also adapt our compensation model to provide fair and inclusive pay practices across our business. We are committed to pay equity for employees who hold the same jobs, work in the same geographic area, and have the same levels of experience and performance.

Employee Wellness We provide our employees access to flexible and convenient health and welfare programs and workplace accommodations. We have prioritized self-care and emphasized a focus on wellness and providing flexible scheduling or time-off options.

ITEM 1A. RISK FACTORS

In addition to the other information set forth in this document, including the matters contained under the heading “Cautionary Language Concerning Forward-Looking Statements,” you should carefully read the matters described below. We believe that each of these matters could materially affect our business. Most, if not all, of these factors are beyond our ability to control.

Macro-Economic Factors:

Adverse changes in the U.S. securities markets, a higher interest rate environment, rising inflation and medical costs could materially increase our benefit plan costs and future funding requirements.

Our costs to provide current benefits and funding for future benefits are subject to increases, primarily due to continuing increases in medical and prescription drug costs, in part due to inflation, and can be affected by lower returns on assets held by our pension and other benefit plans, which are reflected in our financial statements for that year. In calculating the recognized benefit costs, we have made certain assumptions regarding future investment returns, interest rates and medical costs. These assumptions could change significantly over time and could be materially different than originally projected. Lower than assumed investment returns, an increase in our benefit obligations, and higher than assumed medical and prescription drug costs will increase expenses.

The Financial Accounting Standards Board (FASB) requires companies to recognize the funded status of defined benefit pension and postretirement plans as an asset or liability in their statement of financial position and to recognize changes in that funded status in the year in which the changes occur. We have elected to reflect the annual adjustments to the funded status in our consolidated statement of income. Therefore, an increase in our costs or adverse market conditions will have a negative effect on our operating results.

Significant adverse changes in capital markets could result in the deterioration of our defined benefit plans’ funded status.

Inflationary pressures on costs, such as inputs for devices we sell and network components, labor and distribution costs, may impact our network construction, our financial condition or results of operations.

As a provider of telecommunications and technology services, we sell handsets, wireless data cards, wireless computing devices and customer premises equipment manufactured by various suppliers for use with our voice and data services and depend on suppliers to provide us, directly or through other suppliers, with items such as network equipment, customer premises equipment, and wireless-related equipment such as mobile hotspots, handsets, wirelessly enabled computers, wireless data cards and other connected devices for our customers. In recent years, the costs of these inputs and the costs of labor necessary to develop, deploy and maintain our networks and our products and services have increased. In addition, many of these inputs are subject to price fluctuations from a number of factors, including, but not limited to, market conditions, demand for raw

materials used in the production of these devices and network components, severe weather, energy costs, currency fluctuations, supplier capacities, governmental actions, import and export requirements (including tariffs), and other factors beyond our control. Recent spending by hyperscalers and others to support AI is beginning to pressure supply chains for goods such as semiconductors and other network components. Inflationary and supply pressures may continue into the future and could have an adverse impact on our ability to source materials.

Our attempts to offset these cost and supply pressures, such as through increases in the selling prices of some of our products and services, may not be successful. Higher product or service prices may result in reductions in sales volume or increases in subscriber churn. Consumers may be less willing to pay a price differential for our products and services and may increasingly purchase lower-priced offerings from us or our competitors, or may forego some purchases altogether, during a period of inflationary pressure or an economic downturn. To the extent that price increases are not sufficient to offset these increased costs adequately or in a timely manner, and/or if they result in significant decreases in sales volume, our business, financial condition or operating results may be adversely affected. Furthermore, we may not be able to offset any cost increases through productivity and cost-saving initiatives.

Adverse changes in global financial markets could limit our ability and our larger customers' and suppliers' ability to access capital or increase the cost of capital needed to fund business operations.

In recent years, uncertainty surrounding global growth rates, inflation and the interest rate environment produced volatility in the credit, currency and equity markets. Volatility may affect companies' access to the credit markets, leading to higher borrowing costs, or, in some cases, the inability to fund ongoing operations. In addition, we contract with large financial institutions to support our own treasury operations, including contracts to hedge our exposure to interest rates and foreign exchange and the funding of credit lines and other short-term debt obligations, including commercial paper. These financial institutions face stricter capital-related and other regulations in the United States and Europe, as well as ongoing legal and financial issues concerning their loan portfolios, which may hamper their ability to provide credit or raise the cost of providing such credit.

While we have been successful in continuing to access the credit and fixed income markets when needed, adverse changes in the financial markets could render us either unable to access these markets or able to access these markets only at higher interest costs and with restrictive financial or other conditions, severely affecting our business operations. Additionally, downgrades of our credit rating by the major credit rating agencies could increase our cost of borrowing and also impact the collateral we would be required to post under certain agreements we have entered into with our derivative counterparties, which could negatively impact our liquidity. Further, valuation changes in our derivative portfolio due to interest rates and foreign exchange rates could require us to post collateral and thus may negatively impact our liquidity.

Our international operations increase our exposure to political instability, to changes in the international economy and to regulation on our business, and these risks could offset our expected growth opportunities.

We have international operations, particularly in Mexico, and other countries worldwide where we need to comply with a wide variety of complex local laws, regulations and treaties, and are subject to evolving political environments. In addition, we are exposed to, among other factors, fluctuations in currency values, changes in relationships between U.S. and foreign governments, war or other hostilities, and other regulations that may materially affect our earnings. Involvement with foreign firms also exposes us to the risk of being unable to control the actions of those firms and therefore exposes us to risks associated with our obligation to comply with the Foreign Corrupt Practices Act (FCPA). Violations of the FCPA could have a material adverse effect on our operating results.

Industry-Wide Factors:

Changes to federal, state and foreign government regulations and decisions in regulatory proceedings, as well as private litigation, could further increase our operating costs and/or alter customer perceptions of our operations, which could materially adversely affect us.

Our subsidiaries providing wired services are subject to significant federal and state regulation, while many of our competitors are not. In addition, our subsidiaries and affiliates operating outside the United States are also subject to the jurisdiction of national and supranational regulatory authorities in the markets where service is provided. Our wireless subsidiaries are regulated to varying degrees by the FCC and in some instances, by state and local agencies. Adverse regulations and rulings by the courts, the FCC or states relating to broadband and wireless deployment could impede our ability to manage our networks and recover costs and lessen incentives to invest in our networks. The continuing growth of IP-based services, especially when accessed by wireless devices, has created or potentially could create conflicting regulation between the FCC and various state and local authorities, which may involve lengthy litigation to resolve and may result in outcomes unfavorable to us. In addition, increased public focus on a variety of issues related to our operations, such as privacy issues, government requests or orders for customer data, state rate regulation of broadband and concerns about global climate change, have led to proposals or new

legislation at state, federal and foreign government levels to change or increase regulation on our operations, which could result in additional costs of compliance or litigation. Enactment of new privacy laws and regulations could, among other things, adversely affect our ability to collect data and offer targeted advertisements or result in additional costs of compliance or litigation. Should customers decide that our competitors offer a more customer-friendly environment, our competitive position, results of operations or financial condition could be materially adversely affected.

Extreme weather events and other potential effects of climate change may impose risk of damage to our infrastructure, our ability to provide services, and may cause changes in federal, state and foreign government regulation, all of which may result in potential adverse impact to our financial results.

The potential physical effects of extreme weather events and other potential effects of climate change, such as increased frequency and severity of storms, floods, fires, freezing conditions, sea-level rise and other climate-related events, could damage our networks and cause disruptions in our services, which could adversely affect our operations, infrastructure and financial results. Operational impacts resulting from the potential physical effects of climate change, such as damage to our network infrastructure, could result in increased costs and loss of revenue. While we currently do not believe the potential losses or costs associated with the physical effects of climate change will be material, it is difficult to accurately and precisely calculate the future impacts of the physical effects of climate change given the dynamic nature of its impacts on the environment.

Continuing growth in and the converging nature of wireless and broadband services will require us to deploy significant amounts of capital and require ongoing access to spectrum in order to provide attractive services to customers.

Wireless and broadband services are undergoing rapid and significant technological changes and a dramatic increase in usage, including, in particular, the demand for faster and seamless usage of data across mobile and fixed devices. Recent world events and trends accelerated these changes and also resulted in higher network utilization, as more customers consumed bandwidth. Streaming, augmented reality, “smart” technologies, user generated content and AI are expected to continue to drive greater demand for broadband. We must continually invest in our networks in order to improve our wireless and broadband services to meet this increasing demand and changes in customer expectations while remaining competitive. Improvements in these services depend on many factors, including continued access to and deployment of adequate spectrum and the capital needed to expand our wireline network to support transport of these services. In order to stem broadband connectivity losses to cable competitors in our non-fiber wireline areas, we have been expanding our all-fiber wireline network and where we offer our fixed wireless access product. We must maintain and expand our network capacity and coverage for transport of data, including video, and voice between cell and fixed landline sites. To this end, we participate in spectrum auctions and continue to deploy software and other technology advancements in order to efficiently invest in our network.

We have spent, and plan to continue spending, significant capital and other resources on the ongoing development and deployment of our 5G and fiber networks. This deployment and other network service enhancements and product launches may not occur as scheduled or at the cost expected due to many factors, including unexpected inflation, delays in determining equipment and wireless handset operating standards, supplier delays, software issues, increases in network and handset component costs, regulatory permitting delays for tower sites or enhancements, or labor-related delays. Deployment of new technology also may adversely affect the performance of the network for existing services. If we cannot acquire needed spectrum, if our 5G and fiber standalone or converged offerings fail to gain acceptance in the marketplace or if we otherwise fail to deploy the services customers desire on a timely basis with acceptable quality and at reasonable costs, then our ability to attract and retain customers, and, therefore, maintain and improve our operating margins, could be materially adversely affected.

Increasing competition could materially adversely affect our operating results.

We have multiple wireless competitors in each of our service areas and compete for customers based principally on service/device offerings, price, network quality, reliability, speed, coverage area and customer service. In addition, we are facing growing competition from providers offering services using advanced wireless technologies and IP-based networks, among others. We expect market saturation to continue, which may cause the wireless industry’s customer growth rate to moderate in comparison with historical growth rates, leading to increased competition for customers, including from strategic alliances in converged connectivity. Our share of industry sales could be reduced due to aggressive pricing or promotional strategies pursued by competitors. We also expect that our customers’ growing demand for high-speed video and data services will place constraints on our network capacity. These competition and capacity constraints will continue to put pressure on pricing and margins as companies compete for potential customers. Additionally, we may not be able to accurately predict future consumer demands or the success of new services in markets. Our ability to address these issues will depend, among other things, on continued improvement in network quality and customer service and our ability to price our products and services competitively as well as effective marketing of attractive products and services. These efforts will involve significant expenses and require strategic management decisions on, and timely implementation of, equipment choices, network deployment and service offerings. In addition, a sustained decline in a reporting unit’s revenues and earnings has resulted in the past, and may

again result in the future, in a significant negative impact on its fair value, requiring us to record an impairment charge, which could have an adverse impact on our results of operations.

Intellectual property rights may be inadequate to take advantage of business opportunities, which may materially adversely affect our operations.

We may need to spend significant amounts of money to protect our intellectual property rights. Any impairment of our intellectual property rights, including due to changes in U.S. or foreign intellectual property laws or the absence of effective legal protections or enforcement measures, could materially adversely impact our operations.

Incidents or public assertions leading to damage to our reputation or questions about our business conduct, and any resulting lawsuits, claims or other legal proceedings, could have a material adverse effect on our business.

We believe that our brand image, awareness and reputation strengthen our relationship with consumers and contribute significantly to the success of our business. Our reputation and brand image could be negatively affected by a number of factors, including the safety, quality or reliability of our services, products and operations; cybersecurity incidents and data breaches, including our actual or perceived responses thereto; regulatory compliance; governance issues; our actual or perceived position or lack of position on social and other sensitive matters; and the conduct of our employees and former employees. Our ability to attract and retain employees is highly dependent upon our commitment to an inclusive workplace, ethical business practices and other qualities.

We currently are, and may in the future be, named as a defendant in lawsuits, claims and other legal proceedings that arise in or outside the ordinary course of our business based on alleged acts of misconduct by employees, contractors or other third parties. These actions seek, among other things, compensation for alleged personal injury (including claims for loss of life), workers' compensation, employment discrimination, sexual harassment, workplace misconduct, wage and hour claims and other employment-related damages, compensation for breach of contract, statutory or regulatory claims, negligence or gross negligence, punitive damages, consequential damages, and civil penalties or other losses or injunctive or declaratory relief. The outcome of any allegations, lawsuits, claims or legal proceedings is inherently uncertain and could result in significant costs, damage to our brands or reputation and diversion of management's attention from our business. In 2023, *The Wall Street Journal* published a series of articles alleging that lead-clad telecommunications cables are a public health hazard or may pose environmental risks. We are currently subject to litigation and have received inquiries from government authorities as a result of these assertions. We may be subject to additional litigation, government investigations and potentially new regulation or legislation relating to lead-clad cables. Any damage to our reputation or payments of significant amounts as a result of any of these issues, even if reserved, could materially and adversely affect our business, ability to serve customers, reputation, financial condition, results of operations and cash flows.

Our business is subject to risks related to public health crises.

Public health crises and resulting mitigation measures have in the past, and may in the future, cause a negative effect on our operating results. These effects include, but are not limited to, closure of retail stores; impact on our customers' ability to pay for our products and services; reduction in international roaming revenue; and reduced staffing levels in call centers and field operations. We also have in the past, and may in the future, incur significantly higher expenses attributable to infrastructure investments and increased labor costs due to public health crises.

Company-Specific Financial Factors:

Customer adoption of new software-based technologies may require higher-quality services from us, and meeting these demands could create supply chain issues and could increase capital costs.

The communications industry has experienced rapid changes in the past several years. An increasing number of our customers are using mobile devices for using AI-enabled applications and as their primary means of viewing video. In addition, businesses and government bodies are broadly shifting to wireless-based services for homes and infrastructure to improve services to their respective customers and constituencies. We have spent, and continue to spend, significant capital to shift our wired network to software-based technology and are expanding 5G wireless technology to address these demands. We have entered and continue to enter into a significant number of software licensing agreements and continue to work with software developers to provide network functions in lieu of installing switches or other physical network equipment in order to respond to rapid developments in wireless demand. While software-based functionality can be changed much more quickly than, for example, physical switches, the rapid pace of development means that we may increasingly need to rely on single-source and software solutions that have not previously been deployed in production environments. Should this software not function as intended or our license agreements provide inadequate protection from intellectual property infringement claims, we could be forced to either substitute (if available) or else spend time to develop alternative technologies at a much higher cost and incur harm to our reputation for reliability, and, as a result, our ability to remain competitive could be materially adversely affected.

We depend on various suppliers to provide equipment to operate our business and satisfy customer demand, and interruption or delay in supply can adversely impact our operating results.

We depend on suppliers to provide us, directly or through other suppliers, with items such as network equipment, customer premises equipment and wireless-related equipment such as mobile hotspots, handsets, wirelessly enabled computers, wireless data cards and other connected devices for our customers. In some instances, we depend on key single-source suppliers to provide important inputs where there are few alternative suppliers available. These suppliers could fail to provide equipment on a timely or cost-effective basis, or fail to meet our performance expectations, for a number of reasons, including difficulties in obtaining export licenses for certain technologies, inflationary pressures, inability to secure component parts, general business disruption, natural disasters, safety issues, economic and political instability, including the outbreak of war and other hostilities, and public health emergencies. In certain circumstances, we could be liable for the actions of our suppliers and other third parties we do business with. These factors have caused, and may again cause, delays in the development, manufacturing (including the sourcing of key components) and shipment of products to the extent that we or our suppliers are impacted. In certain limited circumstances, suppliers have been unable to supply products in a timely fashion, affecting our ability to provide products and services precisely as and when requested by our customers. It is possible that, in some circumstances, we could be forced to switch to a different key supplier or be unable to meet customer demand for certain products or services. Because of the cost and time lag that can be associated with transitioning from one supplier to another, our business could be substantially disrupted if we were required to, or chose to, replace the products of one or more key suppliers with products from another source, especially if the replacement became necessary on short notice. Any such disruption could increase our costs, decrease our operating efficiencies and have a negative effect on our operating results.

Increasing costs to provide services and failure to renew agreements on favorable terms, or at all, could adversely affect operating margins.

Our operating costs, including customer acquisition and retention costs, could continue to put pressure on margins and customer retention levels.

A number of our competitors offering comparable legacy services that rely on alternative technologies and business models are typically subject to less regulation, and therefore are able to operate with lower costs. These competitors generally can focus on discrete customer segments since they do not have regulatory obligations to provide universal service. Also, these competitors have cost advantages compared to us, due in part to operating on newer, more technically advanced and lower-cost networks with a nonunionized workforce, lower employee benefits and fewer retirees. We are transitioning services from our copper-based network and seeking regulatory approvals, where needed, at both the state and federal levels. If we do not obtain regulatory approvals for our network transition or obtain approvals with onerous conditions, we could experience significant cost and competitive disadvantages.

A significant portion of our workforce is represented by labor unions, and we could incur additional costs or experience work stoppages as a result of the renegotiation of our labor contracts.

As of December 31, 2025, approximately 43% of our workforce was represented by the Communications Workers of America (CWA), the International Brotherhood of Electrical Workers (IBEW) or other unions. While we have labor contracts in place with these unions, with subsequent negotiations we have in the past and could in the future incur additional costs and/or experience work stoppages, which could adversely affect our business operations.

We may not realize or sustain the expected benefits from acquisitions, joint ventures or our business transformation initiatives, including dispositions, which could have a material adverse effect on our business, operations, financial condition, results of operations and competitive position.

We have been and will be undertaking certain transformation initiatives and investments, which are designed to reduce costs, enable legacy rationalization, streamline and modernize distribution and customer service, improve our products and services, remove redundancies and simplify and improve processes and support functions. Our focus is on supporting added customer value with an improved customer experience. We intend for these efficiencies to enable increased investments in our strategic areas of focus, which include improving broadband connectivity (for example, fiber and 5G). We also expect these initiatives to drive efficiencies and improved margins. If we do not successfully manage and timely execute these initiatives and investments, which may include acquisitions, joint ventures, particularly those aimed at enhancing our fiber serviceable locations, and other strategic transactions, or if they are inadequate or ineffective, we may fail to meet our financial goals and achieve anticipated benefits, improvements may be delayed, not sustained or not realized, and our business, operations and competitive position could be adversely affected. In addition, any such initiative or investment entails certain risks and could present financial, managerial and operational challenges. Further, we are using and intend to further use AI-driven efficiencies in our network design and operations, software development, sales, marketing, customer support services and general and administrative costs. The models used in those products or operations, particularly generative AI models, may produce output or take action that is incorrect, release private or confidential information, reflect biases included in the data on which they are trained, infringe on the intellectual property rights of others, or be otherwise harmful. AI-related laws and regulations continue to remain uncertain and may vary from jurisdiction to jurisdiction. There can be no assurance that the usage of AI will meaningfully enhance our

products or operations, and any of these risks could expose us to liability or adverse legal or regulatory consequences and harm our reputation and the public perception of our business or the effectiveness of our security measures.

Unfavorable litigation or governmental investigation results could require us to pay significant amounts or lead to onerous operating procedures.

We are subject to a number of lawsuits both in the United States and in foreign countries, including, at any particular time, claims relating to antitrust, patent infringement, wage and hour, personal injury, environmental, customer data and privacy violations, cyberattacks, regulatory proceedings, breach of contract, and selling and collection practices. We also spend substantial resources complying with various government standards, which may entail related investigations and litigation. In the wireless and wireline area, we also face current and potential litigation relating to alleged adverse health effects on customers or employees who use such technologies including, for example, wireless devices. We may incur significant expenses defending such suits or government charges and may be subject to injunctions or required to pay amounts or otherwise change our operations in ways that could materially adversely affect our operations or financial results.

Cyberattacks impacting our networks, systems or data or those of our suppliers or vendors may have a material adverse effect on our operations or results of operations.

Cyberattacks – including through the use of malware, computer viruses, distributed denial of services attacks, ransomware attacks, credential harvesting, social engineering and other means for obtaining unauthorized access to or disrupting the operation of our networks and systems or accessing our data and those of our suppliers, vendors and other service providers – could have a material adverse effect on our operations or results of operations. As a critical infrastructure service provider, we believe that we are a particularly attractive target for such cyberattacks, including from nation states and highly sophisticated, state-sponsored, or otherwise well-funded actors, and we experience heightened risk from time to time as a result of geopolitical events.

Cyberattacks have caused, and may in the future cause, equipment or network failures, copying or loss of information, including sensitive personal information of customers or employees or proprietary information, as well as disruptions to our or our customers', suppliers' or vendors' operations, which have and in the future could result in significant expenses, potential investigations and legal liability, a loss of current or future customers and reputational damage. Additional resources and management attention may be necessary to respond to government inquiries and requirements, including potentially conflicting demands and requirements from multiple government agencies. Moreover, the amount and scope of insurance that we maintain against losses resulting from any such events or security breaches may not be sufficient to cover our losses or otherwise adequately compensate us for any disruptions to our business that may result. As our networks evolve, they are becoming increasingly reliant on software and cloud technologies to handle growing demands for data consumption. Cyberattacks against us and our suppliers and vendors have occurred in the past, including from highly sophisticated, state-sponsored actors as noted above, and will continue to occur in the future and are increasing in frequency, scope and potential harm over time. For example, in July 2024, we disclosed a cybersecurity incident on Item 1.05 of Form 8-K relating to the copying of mobile customer call data.

Due to the complexity and interconnectedness of our systems and those of our suppliers, vendors and other service providers, the process of enhancing our protective measures can itself create a risk of systems disruptions and security issues. Further, the use of artificial intelligence and machine learning by cybercriminals may increase the frequency and severity of cybersecurity attacks against us or our suppliers, vendors and other service providers. In addition, despite our efforts to detect unlawful intrusions, an attack may persist for an extended period of time before being detected, and, following detection, it may take considerable time for us to obtain sufficient information about the nature, scope and timing of the incident as well as the impact or reasonably likely impact on us. Indeed, as cyberattacks become increasingly sophisticated, a post-attack investigation may not be able to ascertain the entire scope of the attack's impact.

Extensive and costly efforts are undertaken to develop and test systems before deployment and to conduct ongoing monitoring and updating to prevent and withstand such attacks. While we may have contractual rights to assess the effectiveness of many of our suppliers' and vendors' systems and protocols, we cannot know or assess the effectiveness of all of our providers' systems and controls at all times. While, to date, we have not been subject to a cyberattack that has had a material adverse effect on our operations or results of operations, the preventive actions we take, or our suppliers or vendors take, to reduce the risks associated with cyberattacks may be insufficient to repel or mitigate the effects of a major cyberattack in the future.

Natural disasters, extreme weather conditions or terrorist or other hostile acts could cause damage to our infrastructure and result in significant disruptions to our operations.

Our business operations could be subject to interruption by equipment or network failures caused by human error, system failures, unauthorized access to our network and critical infrastructure, power outages, terrorist or other hostile acts, including acts of war, and natural disasters, such as flooding, hurricanes and forest fires. Such events could cause significant damage to the infrastructure upon which our business operations rely, resulting in degradation or disruption of service to our customers, as well as significant recovery time and expenditures to resume operations. Our system redundancy and other measures we take to

protect our infrastructure and operations from the impacts of such events may be ineffective or inadequate to sustain our operations through all such events. Any of these occurrences could result in lost revenues from business interruption, damage to our reputation and reduced profits.

Increases in our debt levels to fund spectrum purchases, or other strategic decisions could adversely affect our ability to finance future debt at attractive rates and reduce our ability to respond to competition and adverse economic trends.

We intend to and have incurred debt to fund significant acquisitions, as well as spectrum purchases needed to compete in our industry. While we believe such decisions were prudent and necessary to take advantage of both growth opportunities and respond to industry developments, we did experience credit rating downgrades from historical levels. Banks and potential purchasers of our publicly traded debt may decide that these strategic decisions and similar actions we may take in the future, as well as expected trends in the industry, will continue to increase the risk of investing in our debt and may demand a higher rate of interest, impose restrictive covenants or otherwise limit the amount of potential borrowing. Additionally, our capital allocation plan is focused on, among other things, managing our debt level. Any failure to successfully execute this plan could adversely affect our cost of funds, liquidity, competitive position and access to capital markets.

Our business may be impacted by changes in tax laws and regulations, judicial interpretations of the same or administrative actions by federal, state, local and foreign taxing authorities.

Tax laws are dynamic and subject to change as new laws are passed and new interpretations of the law are issued or applied. In many cases, the application of existing, newly enacted or amended tax laws may be uncertain and subject to differing interpretations, especially when evaluated against ever-changing products and services provided by our global telecommunications and technology businesses. In addition, tax legislation has been introduced or is being considered in various jurisdictions that could significantly impact our tax rate, tax liabilities and carrying value of deferred tax assets or deferred tax liabilities. Any of these changes could materially impact our financial performance and our tax provision, net income and cash flows.

We are also subject to ongoing examinations by taxing authorities in various jurisdictions. Although we regularly assess the likelihood of an adverse outcome resulting from these examinations to determine the adequacy of provisions for taxes, there can be no assurance as to the outcome of these examinations. In the event that we have not accurately or fully described, disclosed or determined, calculated or remitted amounts that were due to taxing authorities or if the ultimate determination of our taxes owed is for an amount in excess of amounts previously accrued, we could be subject to additional taxes, penalties and interest, which could materially impact our business, financial condition and operating results.

CAUTIONARY LANGUAGE CONCERNING FORWARD-LOOKING STATEMENTS

Information set forth in this report contains forward-looking statements that are subject to risks and uncertainties, and actual results could differ materially. Many of these factors are discussed in more detail in the “Risk Factors” section. We claim the protection of the safe harbor for forward-looking statements provided by the Private Securities Litigation Reform Act of 1995.

The following factors could cause our future results to differ materially from those expressed in the forward-looking statements:

- Adverse economic and political changes, public health emergencies and our ability to access financial markets on favorable terms.
- Increases in our benefit plans’ costs, including due to worse-than-assumed investment returns and discount rates, mortality assumptions, medical cost trends, or healthcare laws or regulations.
- The final outcome of FCC and other federal, state or foreign government agency proceedings (including judicial review of such proceedings) and legislative and regulatory efforts involving issues important to our business, including, without limitation, results of pending governmental investigations; the transition from legacy technologies to IP-based infrastructure, including the withdrawal of legacy TDM-based services; universal service; broadband deployment; wireless equipment siting regulations; E911 services; rules concerning digital discrimination; competition policy; privacy; net neutrality; copyright protection; availability of new spectrum on fair and reasonable terms; and wireless and satellite license awards and renewals, and our response to such legislative and regulatory efforts.
- Enactment of or changes to state, local, federal and/or foreign tax laws and regulations, and actions by tax agencies and judicial authorities, and the resolution of disputes with any taxing jurisdictions.
- U.S. and foreign laws and regulations regarding intellectual property rights protection and privacy, personal data protection and user consent.
- Our ability to compete in a competitive industry and against competitors that can offer product/service offerings at lower prices due to lower cost structures and regulatory and legislative actions adverse to us, including non-regulation of comparable alternative technologies and/or government-owned or subsidized networks, and our response to such competition and emerging technologies, including artificial intelligence.
- Disruptions in our supply chain that have a material impact on our ability to acquire needed goods and services.
- The development and delivery of attractive and profitable wireless and broadband offerings and devices, including our ability to match speeds offered by competitors; and the availability, cost and/or reliability of technologies required to provide such offerings.
- Our ability to adequately fund additional wireless spectrum and network development, deployment and maintenance; and regulations and conditions relating to spectrum use, licensing, obtaining additional spectrum, technical standards and deployment and usage, including network management rules.
- Our ability to manage growth in wireless data services, including network quality.
- The outcome of pending, threatened or potential litigation and arbitration.
- The impact from major equipment, software or other failures or errors that disrupt our networks or cyber incidents; the effect of security breaches related to the network or customer information; our inability to obtain handsets, equipment/software or have handsets, equipment/software serviced in a timely and cost-effective manner; severe weather conditions or other natural disasters including earthquakes and forest fires; public health emergencies; energy shortages; or wars or terrorist attacks.
- The issuance by the FASB or other accounting oversight bodies of new or revised accounting standards.
- The imposition of tariffs and their duration and uncertainty surrounding further tariffs and congressional action regarding spending and taxation, which may result in changes in government spending and affect business and consumer spending trends.
- Our ability to realize or sustain the expected benefits of our business transformation initiatives, which are designed to reduce costs, enable legacy rationalization, streamline distribution, remove redundancies and simplify and improve processes and support functions.
- Our ability to successfully complete acquisitions, divestitures and joint venture transactions, as well as achieve our expectations regarding the financial impact of completed and/or pending transactions.

Readers are cautioned that other factors discussed in this report, although not enumerated here, also could materially affect our future earnings.

ITEM 1B. UNRESOLVED STAFF COMMENTS

Not applicable.

ITEM 1C. CYBERSECURITY

Governance

Board and Audit Committee Oversight

Our Board of Directors has delegated to the Audit Committee the oversight responsibility to review and discuss with management the Company's privacy and data security, including cybersecurity, risk exposures, policies and practices, and the steps management has taken to detect, monitor and control such risks and the potential impact of those exposures on our business, financial results, operations and reputation. The full Board and Audit Committee regularly receive reports and presentations on privacy and data security, which address relevant cybersecurity issues and risks and span a wide range of topics. These reports and presentations are provided by officers with responsibility for privacy and data security, who include our Chief Information Security Officer (CISO), Chief Technology Officer (CTO) and AT&T's Legal team. In addition to regular reports to the Audit Committee, we have protocols by which certain security incidents are escalated within the Company and, where appropriate, reported in a timely manner to the Audit Committee.

Chief Security Office/CISO

We maintain a Chief Security Office (CSO), which is charged with management-level responsibility for all aspects of network and information security within the Company. Led by our CISO and comprised of a large team of highly trained security professionals across multiple countries, the CSO is responsible for:

- a. establishing the policies, standards and requirements for the security of AT&T's computing and network environments;
- b. protecting AT&T-owned and -managed assets and resources against unauthorized access by monitoring potential security threats, correlating network events and overseeing the execution of corrective actions;
- c. promoting compliance with AT&T's security policies and network and information security program in a consistent manner on network systems and applications; and
- d. providing security thought leadership in the global security arena.

Our CISO plays the key management role in assessing and managing our material risks from cybersecurity threats. The CISO also works closely with AT&T Legal to oversee compliance with legal, regulatory and contractual security requirements. The CISO has extensive technical leadership experience and cybersecurity expertise, gained from over 20 years of experience, including serving as the Chief Information Security Officer and Director of the Office of Cybersecurity at a U.S. government agency, in addition to serving as the Chief Information Security Officer of two large public companies. Prior to that, he served for 20 years in the U.S. military, in various information technology roles of increasing seniority. The security professionals in the CSO have cybersecurity backgrounds and expertise relevant to their roles, including, in certain circumstances, relevant industry certifications.

Risk Management and Strategy

We maintain a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity or availability. Our program encompasses the CSO and its policies, platforms, procedures and processes for assessing, identifying and managing risks from cybersecurity threats, including third-party risk from vendors and suppliers. The program is integrated into our overall risk management framework and is generally designed to identify and respond to security incidents and threats in a timely manner to minimize the loss or compromise of information assets and to facilitate incident resolution.

We maintain continuous and near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. This security monitoring leverages tools, where available, such as near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trend analysis and predictive security alerting. We assess, identify and manage risks from cybersecurity threats through various mechanisms, which from time to time may include tabletop exercises to test our preparedness and incident response process, business unit assessments, control gap analyses, threat modeling, impact analyses, internal audits, external audits, penetration tests and engaging third parties to conduct analyses of our information security program. When circumstances warrant, we also retain external cybersecurity experts to assist the CSO. We conduct vulnerability testing and assess identified vulnerabilities for severity, the potential impact to AT&T and our customers, and likelihood of occurrence. We regularly evaluate security controls to maintain their functionality in accordance with security policy. We also obtain cybersecurity threat intelligence from recognized forums, third parties and other sources as part of our risk assessment process. In addition, as a critical infrastructure entity, we collaborate

with numerous agencies in the U.S. government to help protect U.S. communications networks and critical infrastructure, which, in turn, informs our cybersecurity threat intelligence.

With respect to incident response, the Company has adopted a Cybersecurity Incident Response Plan, as well as a Data Privacy Incident Response Plan that applies if customer information has been compromised (together, the “IRPs”), to provide a common framework for responding to security incidents. This framework establishes procedures for identifying, validating, categorizing, documenting and responding to security events that are identified by or reported to the CSO. The IRPs apply to all AT&T personnel (including contractors and partners) that perform functions or services that require securing AT&T information and computing assets, and to all devices and network services that are owned or managed by the Company.

The IRPs set out a coordinated, multi-functional approach for investigating, containing and mitigating incidents, including reporting findings to senior management and other key stakeholders and keeping them informed and involved as appropriate. In general, our incident response process follows the NIST (National Institute of Standards and Technology) framework and focuses on four phases: preparation; detection and analysis; containment, eradication and recovery; and post-incident remediation.

Impact of Cybersecurity Risk

In 2025, we did not identify and were not aware of any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, that we believe have materially affected or are reasonably likely to materially affect our business strategy, results of operations or financial condition. For a discussion of cybersecurity risk, please see the information contained under the heading “Cyberattacks impacting our networks, systems or data or those of our suppliers or vendors may have a material adverse effect on our operations or results of operations” of Item 1A.

ITEM 2. PROPERTIES

Our properties do not lend themselves to description by character and location of principal units. At December 31, 2025, of our total property, plant and equipment, outside plant (including cable, wiring and other non-central office network equipment) represented 29%; other equipment, comprised principally of wireless network equipment attached to towers, furniture and office equipment and vehicles and other work equipment, represented 26%; central office equipment represented 25%; land, building and wireless communications towers represented 12%; and other miscellaneous property represented 8%.

For our Communications segment, substantially all of the installations of central office equipment are located in buildings and on land we own. Many garages, administrative and business offices, wireless towers, telephone centers and retail stores are leased. Property on which communications towers are located may be either owned or leased.

ITEM 3. LEGAL PROCEEDINGS

We are a party to numerous lawsuits, regulatory proceedings and other matters arising in the ordinary course of business. As of the date of this report, we do not believe any pending legal proceedings to which we or our subsidiaries are subject are required to be disclosed as material legal proceedings pursuant to this item.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

INFORMATION ABOUT OUR EXECUTIVE OFFICERS

As of February 1, 2026

Name	Age	Position	Held Since
John T. Stankey	63	Chairman of the Board, Chief Executive Officer and President	2/2025
Darcie (Henry) Cakaric	54	Senior Executive Vice President and Chief Human Resources Officer	10/2025
Pascal Desroches	61	Senior Executive Vice President and Chief Financial Officer	4/2021
Edward W. Gillespie	64	Senior Executive Vice President - External and Legislative Affairs, AT&T Services, Inc.	4/2020
Kellyn S. Kenny	48	Chief Marketing and Growth Officer	5/2022
Lori M. Lee	60	Global Marketing Officer and Senior Executive Vice President - International	12/2022
Jeremy Legg	56	Chief Technology Officer, AT&T Services, Inc.	5/2022
David R. McAtee II	57	Senior Executive Vice President and General Counsel	10/2015
Jeffery S. McElfresh	55	Chief Operating Officer	5/2022

The above executive officers have held high-level managerial positions with AT&T or its subsidiaries for more than the past five years, except for Ms. Cakaric. Executive officers are not appointed to a fixed term of office.

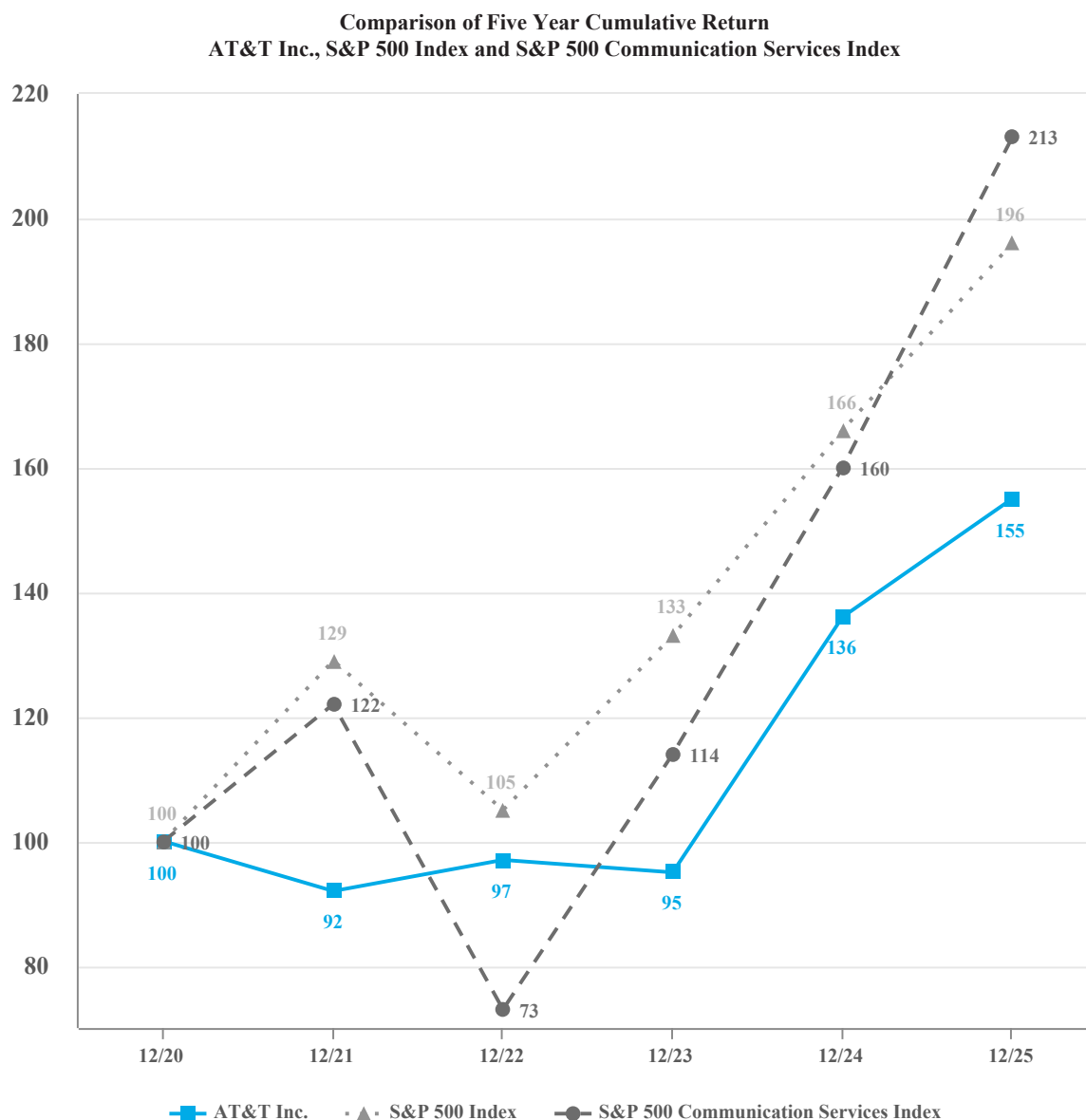
Ms. Cakaric was previously Chief People Officer of StackAdapt from July 2024 to October 2025, Chief People Officer of Flexport from September 2023 to July 2024, Chief People Officer of Snap from October 2022 to September 2023, Chief Human Resources Officer of Amazon.com from July 2021 to October 2022 and Vice President of Human Resources of Amazon.com from June 2016 to June 2021.

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Our common stock is listed on the New York Stock Exchange and NYSE Texas under the ticker symbol "T". The number of stockholders of record as of December 31, 2025 and 2024 was 671,341 and 712,700. The number of stockholders of record as of January 28, 2026, was 668,838. We declared dividends on common stock, on a quarterly basis, totaling \$1.11 per share in 2025 and 2024.

STOCK PERFORMANCE GRAPH



The comparison above assumes \$100 invested on December 31, 2020, in AT&T common stock and the following Standard & Poor's (S&P) Indices: S&P 500 Index and S&P 500 Communication Services Index. Total return equals stock price appreciation plus reinvestment of dividends.

A summary of our repurchases of common stock during the fourth quarter of 2025 is as follows:

ISSUER PURCHASES OF EQUITY SECURITIES

Period	(a)	(b)	(c)	(d)
	Total Number of Shares (or Units) Purchased ^{1,2}	Average Price Paid Per Share (or Unit)	Total Number of Shares (or Units) Purchased as Part of Publicly Announced Plans or Programs ¹	Maximum Number (or Approximate Dollar Value) of Shares (or Units) That May Yet Be Purchased Under The Plans or Programs ¹
October 1, 2025 –				
October 31, 2025	25,877,433	\$ 26.09	25,875,113	\$ 6,881
November 1, 2025 –				
November 30, 2025	20,730,081	\$ 25.23	20,700,000	\$ 6,359
December 1, 2025 –				
December 31, 2025	25,622,121	\$ 24.70	25,421,711	\$ 5,731
Total	72,229,635	\$ 25.35	71,996,824	

¹ In December 2024, our Board of Directors approved, and we announced, an authorization to repurchase up to \$10,000 of common stock (the “2024 Authorization”). Amounts in Column (d) represent amounts remaining under the 2024 Authorization. In January 2026, our Board of Directors approved, and we announced, an authorization to repurchase an additional \$10,000 of common stock. The authorizations have no expiration date.

² Of the shares purchased, 232,811 shares were acquired through the withholding of taxes on the vesting of restricted stock and performance shares or in respect of the exercise price of options.

ITEM 6. [RESERVED]

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

OVERVIEW

AT&T Inc. is referred to as “we,” “AT&T” or the “Company” throughout this document. AT&T products and services are provided or offered by subsidiaries and affiliates of AT&T Inc. under the AT&T brand and not by AT&T Inc., and the names of the particular subsidiaries and affiliates providing the services generally have been omitted. AT&T is a holding company whose subsidiaries and affiliates operate worldwide in the telecommunications and technology industries. You should read this discussion in conjunction with the consolidated financial statements and accompanying notes (Notes).

Our Management's Discussion and Analysis of Financial Condition and Results of Operations included in this document generally discusses 2025 and 2024 items and year-to-year comparisons between 2025 and 2024. Discussions of 2023 items and year-to-year comparisons between 2024 and 2023 that are not included in this document can be found in “Management's Discussion and Analysis of Financial Condition and Results of Operations” in Part II, Item 7 of our Annual Report on Form 10-K for the fiscal year ended December 31, 2024.

We have two reportable segments: Communications and Latin America. Our segment results presented in Note 4 and discussed below follow our internal management reporting. Each segment's percentage calculation of total segment operating revenue is derived from our segment results table in Note 4. Segment operating income is primarily attributable to our Communications segment due to prior-years operating losses in Latin America. Percentage increases and decreases that are not considered meaningful are denoted with a dash.

	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Operating Revenues					
Communications	\$ 120,896	\$ 117,652	\$ 118,038	2.8 %	(0.3)%
Latin America	4,379	4,232	3,932	3.5	7.6
Corporate	373	452	458	(17.5)	(1.3)
AT&T Operating Revenues	\$ 125,648	\$ 122,336	\$ 122,428	2.7 %	(0.1)%
Operating Income (Loss)					
Communications	\$ 27,927	\$ 27,095	\$ 27,801	3.1 %	(2.5)%
Latin America	145	40	(141)	—	—
Segment Operating Income	28,072	27,135	27,660	3.5	(1.9)
Corporate	(2,559)	(2,902)	(2,961)	11.8	2.0
Certain significant items	(1,351)	(5,184)	(1,238)	73.9	—
AT&T Operating Income	\$ 24,162	\$ 19,049	\$ 23,461	26.8 %	(18.8)%

The **Communications segment** accounted for approximately 97% of our 2025 and 2024 total segment operating revenues and accounted for substantially all segment operating income in 2025 and 2024. This segment provides services to businesses and consumers located in the United States and businesses globally. Our business strategies reflect integrated product offerings that cut across product lines and utilize shared assets. This segment contains the following business units:

- **Mobility** provides nationwide wireless service and equipment.
- **Business Wireline** provides advanced ethernet-based fiber services, fixed wireless services, IP Voice and managed professional services, as well as legacy voice and data services and related equipment, to business customers.
- **Consumer Wireline** provides broadband services, including fiber connections that provide multi-gig services, and AT&T Internet Air (AIA) services, to residential customers in select locations. Consumer Wireline also provides legacy telephony voice communication services.

The **Latin America segment** accounted for approximately 3% of our 2025 and 2024 total segment operating revenues and less than 1% of segment operating income in 2025 and 2024. This segment provides wireless service and equipment in Mexico.

RESULTS OF OPERATIONS

Consolidated Results Our financial results are summarized in the following table. We then discuss factors affecting our overall results. Additional analysis is discussed in our “Segment Results” section. We also discuss our expected revenue and expense trends for 2026 in the “Operating Environment and Trends of the Business” section.

	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Operating revenues					
Service	\$ 101,158	\$ 100,135	\$ 99,649	1.0 %	0.5 %
Equipment	24,490	22,201	22,779	10.3	(2.5)
Total Operating Revenues	125,648	122,336	122,428	2.7	(0.1)
Operating expenses					
Operations and support	79,762	77,632	78,997	2.7	(1.7)
Asset impairments and abandonments and restructuring	838	5,075	1,193	(83.5)	—
Depreciation and amortization	20,886	20,580	18,777	1.5	9.6
Total Operating Expenses	101,486	103,287	98,967	(1.7)	4.4
Operating Income	24,162	19,049	23,461	26.8	(18.8)
Interest expense	6,804	6,759	6,704	0.7	0.8
Equity in net income of affiliates	1,895	1,989	1,675	(4.7)	18.7
Other income (expense) – net	7,754	2,419	1,416	—	70.8
Income Before Income Taxes	27,007	16,698	19,848	61.7	(15.9)
Net Income	23,386	12,253	15,623	90.9	(21.6)
Net Income Attributable to AT&T	21,953	10,948	14,400	—	(24.0)
Net Income Attributable to Common Stock	\$ 21,889	\$ 10,746	\$ 14,192	— %	(24.3) %

OVERVIEW

Operating revenues increased in 2025, reflecting higher Mobility and Consumer Wireline revenues, partially offset by declines in Business Wireline. Operating revenues in Mexico were also higher, overcoming unfavorable foreign exchange impacts during the first half of 2025.

Operations and support expenses increased in 2025, reflecting higher sales volumes in our Mobility business unit, which drove higher equipment, advertising, selling and bad debt expenses. Also contributing to higher costs were approximately \$440 of apportioned legal settlements during 2025, higher network-related expenses and advertising costs due to the launch of a new campaign in 2025. Increases were partially offset by declines from our continued transformation efforts and lower content licensing fees.

Asset impairments and abandonments and restructuring decreased in 2025, with higher impairments in 2024. Noncash charges in 2024 primarily related to a goodwill impairment charge of \$4,422 associated with our Business Wireline reporting unit as well as restructuring charges, including termination fees associated with our network modernization program to deploy commercial scale open radio access network (Open RAN). Expenses in 2025 primarily relate to restructuring severance charges.

Depreciation and amortization expense increased in 2025, primarily due to ongoing capital spending for strategic initiatives such as fiber and network upgrades, partially offset by lower depreciation from fully depreciated legacy assets and impacts from our Open RAN network modernization efforts.

Operating income increased in 2025 and decreased in 2024. Our operating margin was 19.2% in 2025, compared to 15.6% in 2024, and 19.2% in 2023.

Interest expense increased in 2025, primarily due to lower capitalized interest associated with spectrum acquisitions. The increase was partially offset by lower average commercial paper balances.

Equity in net income of affiliates decreased in 2025, reflecting our sale of DIRECTV in July 2025. The decrease was partially offset by cash distributions received by AT&T in excess of the carrying amount of our investment in DIRECTV prior to disposition (see Notes 10 and 19).

Other income (expense) – net increased in 2025. The increase was primarily due to a gain of approximately \$5,600 recognized on the sale of our interest in DIRECTV (see Note 10). The increase was also driven by a gain on a prior disposition and noncash impairment charges for a held-for-sale business and our SKY Mexico equity investment. Partially offsetting the increases were lower pension and postretirement benefit credits and lower returns on other benefit-related investments.

Income tax expense decreased in 2025, primarily due to a lower effective tax rate driven by a tax-free gain on sale of DIRECTV in 2025 and a goodwill impairment in 2024, which is not deductible for tax purposes.

Our effective tax rate was 13.4% in 2025, 26.6% in 2024, and 21.3% in 2023, reflecting the nonrecognition of income taxes on the DIRECTV gain and larger discrete tax benefits in 2025, and the goodwill impairment in 2024, which was not deductible for tax purposes.

Segment Results Our segments are comprised of strategic business units or other operations that offer products and services to different customer segments over various technology platforms and/or in different geographies that are managed accordingly. We evaluate segment performance based on operating income as well as EBITDA and/or EBITDA margin. See “Discussion and Reconciliation of Non-GAAP Measures” for a reconciliation of EBITDA and EBITDA margin to the most comparable financial measures calculated and presented in accordance with U.S. generally accepted accounting principles (GAAP).

COMMUNICATIONS SEGMENT				Percent Change	
	2025	2024	2023	2025 vs. 2024	2024 vs. 2023
Segment Operating Revenues					
Mobility	\$ 89,482	\$ 85,255	\$ 83,982	5.0 %	1.5 %
Business Wireline	17,231	18,819	20,883	(8.4)	(9.9)
Consumer Wireline	14,183	13,578	13,173	4.5	3.1
Total Segment Operating Revenues	\$ 120,896	\$ 117,652	\$ 118,038	2.8 %	(0.3) %
Segment Operating Income (Loss)					
Mobility	\$ 27,196	\$ 26,314	\$ 25,861	3.4 %	1.8 %
Business Wireline	(816)	(88)	1,289	—	—
Consumer Wireline	1,547	869	651	78.0	33.5
Total Segment Operating Income	\$ 27,927	\$ 27,095	\$ 27,801	3.1 %	(2.5) %

Operating revenues increased in 2025, driven by increases in Mobility service revenue and our Consumer Wireline business unit, driven by gains in wireless and broadband services. Partially offsetting these increases were declines in our Business Wireline business unit, which reflects lower demand for legacy services.

Operating income increased in 2025 and decreased in 2024. The 2025 operating income reflects an increase in operating income from our Mobility and Consumer Wireline business units, partially offset by a decrease in our Business Wireline business unit. Our Communications segment operating income margin was 23.1% in 2025, 23.0% in 2024 and 23.6% in 2023. Our Communications segment EBITDA margin was 39.6% in 2025, 39.5% in 2024 and 38.3% in 2023.

Communications Business Unit Discussion**Mobility Results**

	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Operating revenues					
Service	\$ 67,384	\$ 65,373	\$ 63,175	3.1 %	3.5 %
Equipment	22,098	19,882	20,807	11.1	(4.4)
Total Operating Revenues	89,482	85,255	83,982	5.0	1.5
Operating expenses					
Operations and support	51,864	48,724	49,604	6.4	(1.8)
Depreciation and amortization	10,422	10,217	8,517	2.0	20.0
Total Operating Expenses	62,286	58,941	58,121	5.7	1.4
Operating Income	\$ 27,196	\$ 26,314	\$ 25,861	3.4 %	1.8 %

The following tables highlight other key measures of performance for Mobility:

Subscribers

(in 000s)	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Postpaid	90,879	89,200	87,104	1.9 %	2.4 %
Postpaid phone	74,214	72,749	71,255	2.0	2.1
Prepaid	18,294	19,023	19,236	(3.8)	(1.1)
Reseller	10,932	9,628	7,468	13.5	28.9
Total Mobility Subscribers¹	120,105	117,851	113,808	1.9 %	3.6 %

¹ Wireless subscribers and net additions exclude customers with free lines provided under promotional pricing until such lines are converted to paying lines.

Mobility Net Additions

(in 000s)	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Postpaid Phone Net Additions	1,551	1,653	1,744	(6.2) %	(5.2) %
Total Phone Net Additions	1,159	1,525	1,801	(24.0)	(15.3)
Postpaid ¹	1,738	2,250	2,315	(22.8)	(2.8)
Prepaid	(536)	(102)	128	—	—
Reseller	1,112	2,020	1,279	(45.0)	57.9
Mobility Net Subscriber Additions^{2,3}	2,314	4,168	3,722	(44.5) %	12.0 %
Postpaid Churn ⁴	1.05 %	0.92 %	0.98 %	13 BP	(6) BP
Postpaid Phone Churn ⁴	0.90 %	0.76 %	0.81 %	14 BP	(5) BP

¹ In addition to postpaid phones, includes tablets and wearables and other. Tablet net adds (losses) were 143, 167 and (68) for the years ended December 31, 2025, 2024 and 2023, respectively. Wearables and other net adds were 44, 430 and 639 for the years ended December 31, 2025, 2024 and 2023, respectively.

² Excludes migrations between wireless subscriber categories, including connected devices, and acquisition-related activity during the period.

³ Wireless subscribers and net additions exclude customers with free lines provided under promotional pricing until such lines are converted to paying lines.

⁴ Calculated by dividing the aggregate number of wireless subscribers who canceled service during a month by the total number of wireless subscribers at the beginning of that month. The churn rate for the period is equal to the average of the churn rate for each month of that period.

Service revenue increased during 2025, largely due to growth from subscriber gains, partially offset by promotional activity.

ARPU

Postpaid ARPU increased in 2025 reflecting pricing actions that were largely offset by increased promotional activity, growth in our converged customer relationships, and our success in attracting customers in underpenetrated segments with lower ARPUs but attractive lifetime values, such as age 55-plus in our “value customers.”

Churn

The effective management of subscriber churn is critical to our ability to maximize revenue growth and to maintain and improve margins. Postpaid churn and postpaid phone churn were higher in 2025, partially driven by an increase in our customer base that reached the end of device financing periods, which normalized in the second half of 2025.

Equipment revenue increased in 2025, primarily driven by higher wireless device sales volumes.

Operations and support expenses increased in 2025, primarily due to higher sales volumes, which drove higher equipment, advertising, selling and bad debt expenses. The increase also reflected higher advertising due to the launch of a new campaign, and higher network costs that were partially offset by lower content licensing fees and expense declines from transformation efforts.

Depreciation expense increased in 2025, primarily due to ongoing capital spending for network upgrades and expansion, partially offset by lower depreciation impacts from our network modernization efforts.

Operating income increased in 2025 and 2024. Our Mobility operating income margin was 30.4% in 2025, 30.9% in 2024 and 30.8% in 2023. Our Mobility EBITDA margin was 42.0% in 2025, 42.8% in 2024 and 40.9% in 2023.

Business Wireline Results

	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Operating revenues					
Legacy and other transitional services	\$ 9,170	\$ 11,095	\$ 13,680	(17.4)%	(18.9)%
Fiber and advanced connectivity services	7,333	6,969	6,594	5.2	5.7
Equipment	728	755	609	(3.6)	24.0
Total Operating Revenues	17,231	18,819	20,883	(8.4)	(9.9)
Operating expenses					
Operations and support	12,213	13,352	14,217	(8.5)	(6.1)
Depreciation and amortization	5,834	5,555	5,377	5.0	3.3
Total Operating Expenses	18,047	18,907	19,594	(4.5)	(3.5)
Operating Income (Loss)	\$ (816)	\$ (88)	\$ 1,289	— %	— %

Legacy and other transitional services revenues decreased in 2025, driven by lower demand for legacy and VPN services, which we expect to continue as we decommission our copper-based legacy network. These revenue declines were partially offset by targeted pricing actions in the first quarter of 2025.

Fiber and advanced connectivity services revenues increased in 2025, driven by higher fiber and fixed wireless revenues.

Equipment revenues decreased in 2025, driven by lower customer premises equipment sales, which can vary from year to year based on the nature of services purchased.

Operations and support expenses decreased in 2025, primarily driven by lower personnel and customer support costs associated with ongoing transformation initiatives. Expense declines also include lower network and advertising costs.

Depreciation expense increased in 2025, primarily due to ongoing capital investment for strategic initiatives such as fiber, partially offset by fully depreciated legacy assets.

Operating income decreased in 2025 and 2024. Our Business Wireline operating income margin was (4.7)% in 2025, (0.5)% in 2024 and 6.2% in 2023. Our Business Wireline EBITDA margin was 29.1% in 2025, 29.1% in 2024 and 31.9% in 2023.

Consumer Wireline Results

	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Operating revenues					
Broadband	\$ 12,187	\$ 11,212	\$ 10,455	8.7 %	7.2 %
Legacy voice and data services	1,013	1,265	1,508	(19.9)	(16.1)
Other service and equipment	983	1,101	1,210	(10.7)	(9.0)
Total Operating Revenues	14,183	13,578	13,173	4.5	3.1
Operating expenses					
Operations and support	8,933	9,048	9,053	(1.3)	(0.1)
Depreciation and amortization	3,703	3,661	3,469	1.1	5.5
Total Operating Expenses	12,636	12,709	12,522	(0.6)	1.5
Operating Income	\$ 1,547	\$ 869	\$ 651	78.0 %	33.5 %

The following tables highlight other key measures of performance for Consumer Wireline:

Broadband Connections

(in 000s)	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Broadband ¹	14,704	13,987	13,729	5.1 %	1.9 %
Fiber Broadband Connections	10,406	9,331	8,307	11.5 %	12.3 %

¹ Includes AIA.

Broadband Net Additions

(in 000s)	2025	2024	2023	Percent Change	
				2025 vs. 2024	2024 vs. 2023
Broadband Net Additions ^{1,2}	729	258	(24)	— %	— %
Fiber Broadband Net Additions	1,075	1,024	1,092	5.0 %	(6.2)%

¹ Includes AIA.

² Excludes the impact of customer disconnections resulting from the termination of AIA services in areas with unfavorable regulatory requirements in the first quarter of 2025.

Broadband revenues increased in 2025, driven by an increase in fiber revenues of 17.0%. Higher fiber revenues reflect an increase in fiber customers, which we expect to continue as we invest further in building our fiber footprint, and higher ARPU. This increase also includes growth in AIA revenues and was partially offset by declines in copper-based broadband services.

Legacy voice and data service revenues decreased in 2025, reflecting the continued decline in demand for these services in favor of other technologies, such as wireless and fiber services.

Other service and equipment revenues decreased in 2025, reflecting the continued decline in the number of VoIP customers.

Operations and support expenses decreased in 2025, driven by lower customer support costs and content licensing fees, offset by higher network-related expenses and marketing costs.

Depreciation expense increased in 2025, primarily due to ongoing capital spending for strategic initiatives such as fiber and network upgrades and expansion, partially offset by fully depreciated legacy assets.

Operating income increased in 2025 and 2024. Our Consumer Wireline operating income margin was 10.9% in 2025, 6.4% in 2024 and 4.9% in 2023. Our Consumer Wireline EBITDA margin was 37.0% in 2025, 33.4% in 2024 and 31.3% in 2023.

LATIN AMERICA SEGMENT				Percent Change	
	2025	2024	2023	2025 vs. 2024	2024 vs. 2023
Segment Operating revenues					
Service	\$ 2,715	\$ 2,668	\$ 2,569	1.8 %	3.9 %
Equipment	1,664	1,564	1,363	6.4	14.7
Total Segment Operating Revenues	4,379	4,232	3,932	3.5	7.6
Segment Operating expenses					
Operations and support	3,563	3,535	3,349	0.8	5.6
Depreciation and amortization	671	657	724	2.1	(9.3)
Total Segment Operating Expenses	4,234	4,192	4,073	1.0	2.9
Operating Income (Loss)	\$ 145	\$ 40	\$ (141)	— %	— %

The following tables highlight other key measures of performance for Mexico:

Subscribers

				Percent Change	
(in 000s)	2025	2024	2023	2025 vs. 2024	2024 vs. 2023
Postpaid	6,751	5,837	5,236	15.7 %	11.5 %
Prepaid	17,730	17,486	16,663	1.4	4.9
Reseller	199	253	417	(21.3)	(39.3)
Mexico Wireless Subscribers	24,680	23,576	22,316	4.7 %	5.6 %

Mexico Wireless Net Additions

				Percent Change	
(in 000s)	2025	2024	2023	2025 vs. 2024	2024 vs. 2023
Postpaid	914	601	311	52.1 %	93.2 %
Prepaid	244	823	459	(70.4)	79.3
Reseller	(54)	(164)	(57)	67.1	—
Mexico Wireless Net Additions	1,104	1,260	713	(12.4)%	76.7 %

Service revenues increased in 2025, reflecting growth in subscribers and ARPU, partially offset by unfavorable foreign exchange impacts.

Equipment revenues increased in 2025, driven by higher equipment sales, partially offset by unfavorable foreign exchange impacts.

Operations and support expenses increased in 2025, driven by increased sales volume, resulting in higher equipment, selling and bad debt expense, partially offset by favorable impact of foreign exchange.

Depreciation expense increased in 2025, primarily due to accelerated depreciation on certain network assets and higher in-service assets, partially offset by favorable impact of foreign exchange.

Operating income improved in 2025 and 2024. Our Mexico operating income margin was 3.3% in 2025, 0.9% in 2024 and (3.6)% in 2023. Our Mexico EBITDA margin was 18.6% in 2025, 16.5% in 2024 and 14.8% in 2023.

OPERATING ENVIRONMENT AND TRENDS OF THE BUSINESS

2026 Revenue Trends We expect revenue growth in our wireless and broadband businesses as customers demand instant connectivity and higher speeds made possible by wireless network enhancements through 5G deployment and our fiber network expansion. We believe that our simplified go-to-market strategy for 5G in underpenetrated markets will continue to contribute

to wireless subscriber and service revenue growth and that expansion of our fiber and AIA serviceable locations will drive greater demand for broadband services. We expect that an increasing portion of our revenues will come from converged customers with seamless connectivity through an innovative product portfolio and strong customer relationships.

As we expand our fiber reach, we will be orienting our business portfolio to leverage this opportunity to offset continuing declines in legacy Business Wireline products by growing connectivity with small to mid-sized businesses. We plan to use our strong fiber and wireless assets, broad distribution and integrated product offerings to strengthen our overall market position. We will continue to rationalize our product portfolio with a longer-term shift of the business to fiber and wireless connectivity, and growth in value-added services. As customers are demanding faster and more reliable services, we are decommissioning our legacy copper network and enhancing our offerings to include services that provide better experiences over newer technologies, such as AT&T Internet Air.

2026 Expense Trends During 2026, we expect expense trends consistent with the prior year, and that we will continue to focus on efficiency, led by our cost transformation initiative. We expect the spending required to support growth and efficiency initiatives, primarily our continued deployment of fiber and 5G, to pressure expense trends in 2026. These investments will help prepare us to meet the continued increase in customer demand for enhanced wireless and broadband services, including on-the-go video streaming, augmented reality, “smart” technologies, user generated content and AI. Our network modernization efforts should result in a more efficient use of capital and lower network-related expenses in the coming years. Furthermore, access to our network and newer technology may drive customers to upgrade devices and equipment, the expenses associated with those equipment sales are expected to contribute to higher costs.

We continue to transform our operations to be more efficient and effective. We are restructuring businesses, working with regulators and customers to sunset legacy networks, improving customer service and ordering functions through digital transformation, sizing our support costs and staffing with current activity levels, and reassessing overall benefit costs. We also expect cost savings through AI-driven efficiencies in network design and operations, software development, sales, marketing, customer support services and general and administrative costs.

Market Conditions In recent years, uncertainty surrounding global growth rates, tariffs, inflation and a higher interest rate environment continued to produce volatility in the credit, currency and equity markets. We expect ongoing pressure on pricing during 2026 as we respond to the geopolitical and macroeconomic environment and our competitive marketplace, especially in wireless services.

Included on our consolidated balance sheets are assets held by benefit plans for the payment of future benefits. Our pension plans are subject to funding requirements of the Employee Retirement Income Security Act of 1974, as amended (ERISA). We plan to voluntarily contribute approximately \$350 to our pension plans in 2026 and expect only minimal ERISA contribution requirements. Investment returns on these assets depend largely on trends in the economy, and a weakness in the equity, fixed income and real asset markets could require us to make future contributions to the pension plans. In addition, our policy of recognizing actuarial gains and losses related to our pension and other postretirement plans in the period in which they arise subjects us to earnings volatility caused by changes in market conditions; however, these actuarial gains and losses do not impact segment performance as they are required to be recorded in “Other income (expense) – net.” Changes in our discount rate, which are tied to changes in the bond market, and changes in the performance of equity markets, may have significant impacts on the valuation of our pension and other postretirement obligations at the end of 2026 (see “Critical Accounting Policies and Estimates”).

Expected Growth Areas Over the next few years, we expect our growth to come from wireless and IP-based fiber broadband services. We provide integrated services to diverse groups of customers in the United States, on a converged telecommunications network utilizing different technological platforms. In 2026, our key initiatives include:

- Continuing our wireless subscriber momentum and 5G deployment, with expansion of wireless subscribers in underpenetrated markets and converged connectivity.
- Continuing our fiber deployment, improving fiber penetration, growing AT&T Internet Air services, accelerating connectivity growth and increasing broadband revenues, inclusive of impact of integrating recent acquisitions of spectrum and fiber assets.
- Continuing our deployment of Open RAN to build a more robust ecosystem of network infrastructure providers and suppliers, fostering lower network costs, improved operational efficiencies and allowing for continued investment in our fast-growing broadband network.
- Continuing to drive efficiencies and a competitive advantage through cost transformation initiatives, including modernization of our IT infrastructure and product simplification.

Wireless We expect to continue to deliver revenue growth in the coming years. We are in a period of rapid growth in wireless video and data usage and believe that there are substantial opportunities available for next-generation integrated services that

combine technologies and services. As of December 31, 2025, we served 145 million wireless subscribers in North America, with 120 million in the United States.

Our LTE technology covers over 441 million people in North America, and in the United States, we cover all major metropolitan areas and over 337 million people. At December 31, 2025, our network covers more than 322 million people with 5G technology in the United States and North America. When combined with our upgraded backhaul network, we provide enhanced network capabilities and superior mobile broadband speeds for data and video services.

Our networks covering both the United States and Mexico have enabled our customers to use wireless services without roaming on other companies' networks. At December 31, 2025, we provided LTE coverage to over 104 million people in Mexico.

Integration of Wireless and Fiber Services The communications industry has evolved into internet-based technologies capable of converging the offering of wireline and wireless services. As the owner and operator of scaled wireless and fiber networks, we plan to continue to focus on expanding our wireless network capabilities and providing broadband offerings that allow customers to integrate their home or business fixed services with their mobile service. We intend to continue to develop and provide unique integrated mobile and broadband/fiber solutions.

REGULATORY LANDSCAPE

AT&T subsidiaries operating within the United States are subject to federal and state regulatory authorities. While these issues may apply only to certain subsidiaries, the words "we," "AT&T" and "our" are used to simplify the discussion. The following discussions are intended as a condensed summary of the issues rather than as a comprehensive legal analysis and description of all of these specific issues.

International Regulation

Our subsidiaries operating outside the United States are subject to the jurisdiction of regulatory authorities in the territories in which the subsidiaries operate. Our licensing, compliance and advocacy initiatives in foreign countries primarily enable the provision of enterprise (i.e., large business) services globally and wireless services in Mexico.

The General Data Protection Regulation went into effect in Europe in May of 2018. This regulation created a range of new compliance obligations and significantly increased financial penalties for noncompliance. AT&T processes and handles personal data of its customers and subscribers, employees of its enterprise customers and its employees.

U.S. Regulation

In the Telecommunications Act of 1996 (Telecom Act), Congress established a national policy framework intended to bring the benefits of competition and investment in advanced telecommunications facilities and services to all Americans by opening all telecommunications markets to competition and reducing or eliminating regulatory burdens that harm consumer welfare. Nonetheless, since then, the FCC and some state regulatory commissions have maintained, re-imposed or expanded certain regulatory requirements that were imposed decades ago on our traditional wireline subsidiaries when they operated as legal monopolies. Recently, the FCC's regulatory approach has depended on control of the executive branch, eliminating a variety of antiquated and unnecessary regulations in a number of areas, while imposing or re-imposing regulations in other areas. We continue to support regulatory and legislative measures and efforts, at both the state and federal levels, to reduce inappropriate regulatory burdens that inhibit our ability to compete effectively and offer needed services to our customers, including initiatives to transition services from traditional networks to all IP-based networks. At the same time, we also seek to ensure that legacy regulations are not further extended to broadband or wireless services, which are subject to vigorous competition. We have organized the following discussion by service impacted.

Internet Until 2015, the FCC classified fixed and mobile consumer broadband internet access services as information services subject to minimal regulation. In 2015, the FCC reclassified such services as telecommunications services subject to broader regulation by the FCC and imposed "net neutrality rules." Since then, the FCC has twice reversed course, most recently again reclassifying such services as telecommunications services subject to broader regulation by the FCC in an order adopted on April 25, 2024. Multiple trade associations and other parties challenged the FCC's reclassification decision in appeals consolidated in the U.S. Court of Appeals for the Sixth Circuit. The trade associations petitioned the Sixth Circuit to stay the FCC's order. On August 1, 2024, the Sixth Circuit issued a stay of the FCC order pending review of the appeals, holding that broadband providers are likely to succeed on the merits. On January 2, 2025, the Sixth Circuit issued an order granting the petition for review and setting aside the FCC net neutrality order, holding that broadband internet access service is an information service.

In 2021, New York enacted the Affordable Broadband Act (ABA), requiring ISPs offering "fixed" mass-market broadband service, including fixed wireless, to offer discounted plans to low-income customers. In June 2021, the ABA was enjoined by a federal district court, which found the ABA preempted by federal law. In April 2024, the Second Circuit overruled and vacated the district court order. The Supreme Court subsequently denied the trade association's request for review. Under an agreement

with the New York Attorney General, the law began to be enforced on January 15, 2025. A number of state legislatures have since considered legislation regulating the rates of fixed broadband service, with Connecticut adopting a law requiring wireline ISPs that are state contractors to stand up a discounted broadband offering to low-income customers.

Since 2018, some states have adopted legislation or issued executive orders that established state net neutrality rules, including California, Maine, Minnesota, Vermont and Washington. Additional states may seek to impose net neutrality requirements in the future.

On November 15, 2023, the FCC adopted rules to “facilitate” equal access to broadband and prevent digital discrimination in broadband access. The rules, which became effective March 22, 2024, prohibit covered entities from implementing policies or practices not justified by genuine issues of technical or economic feasibility, that differentially impact consumers’ access to broadband internet access service based on prohibited characteristics (including income level, race and ethnicity) or that have such differential impact, whether intentional or not. The rules broadly apply prospectively to all aspects of an ISP’s service that could impact a consumer’s ability to access broadband, including deployment, marketing and credit checks, among other things. We may be required to answer complaints alleging that the company has violated the FCC rules, and those complaints may seek relief, including changes to our business practices or civil forfeitures that could result in significant costs or reputational harm. It is currently uncertain how the FCC will enforce these new rules. Several business associations have filed appeals challenging the rules and several of those appeals have been consolidated in the Eighth Circuit, which held oral argument on September 25, 2024.

Privacy-related legislation continues to be adopted or considered in a number of jurisdictions. Legislative, regulatory and litigation actions could result in increased costs of compliance, further regulation or claims against broadband internet access service providers and others, and increased uncertainty in the value and availability of data.

Infrastructure Investment On November 15, 2021, the Infrastructure Investment and Jobs Act (IIJA) was signed into law. The legislation appropriates \$65,000 to support broadband deployment and adoption. The National Telecommunications and Information Agency (NTIA) is responsible for distributing more than \$48,000 of this funding, including \$42,500 in state grants for broadband deployment projects in unserved and underserved areas through the Broadband, Equity, Access and Deployment (BEAD) Programs. NTIA and states are in the process of administering these grants. Where appropriate, AT&T has applied for, and in some cases has been awarded, and may continue to apply for grants under this or other government infrastructure programs.

Wireless Industry-wide network densification and 5G technology expansion efforts, which are needed to satisfy extensive demand for video and internet access, will involve significant deployment of “small cell” equipment. This increases the importance of local permitting processes that allow for the placement of small cell equipment in the public right-of-way on reasonable timelines and terms. The FCC has adopted multiple Orders streamlining federal, state and local wireless structure review processes that had the tendency to delay and impede deployment of small cell and related infrastructure used to provide telecommunications and broadband services. Additional spectrum will be needed industrywide for 5G and future services. On July 4, 2025, as part of the omnibus reconciliation package (One Big Beautiful Bill (OB BB)), the President signed into law a provision that reauthorized, for 10 years, FCC statutory authority to conduct spectrum auctions and further required auction of 800 MHz of spectrum within eight years. The FCC’s implementation of this legislation will have a direct impact on whether the wireless industry has sufficient spectrum to support future wireless services. As a first step, in November 2025, the FCC opened a rulemaking to consider the auctioning of spectrum in the upper C-Band, as required by OB BB.

ACCOUNTING POLICIES AND STANDARDS

Critical Accounting Policies and Estimates Because of the size of the financial statement line items they relate to or the extent of judgment required by our management, some of our accounting policies and estimates have a more significant impact on our consolidated financial statements than others.

Pension and Postretirement Benefits Our actuarial estimates of retiree benefit expense and the associated significant weighted-average assumptions are discussed in Note 14. Our assumed weighted-average discount rates for pension and postretirement benefits of 5.50% and 5.30%, respectively, at December 31, 2025, reflect the hypothetical rate at which the projected benefit obligations could be effectively settled or paid out to participants. We determined our discount rate based on a range of factors, including a yield curve composed of the rates of return on several hundred high-quality, fixed income corporate bonds available at the measurement date and corresponding to the related expected durations of future cash outflows for the obligations. These bonds had an average rating of at least Aa3 or AA- by the nationally recognized statistical rating organizations, denominated in U.S. dollars, and generally not callable, convertible or index linked. For the year ended December 31, 2025, when compared to the year ended December 31, 2024, we decreased our pension discount rate by 0.20%, resulting in an increase in our pension plan benefit obligation of \$680, and decreased our postretirement discount rate by 0.30%, resulting in an increase in our postretirement benefit obligation of \$167.

Our expected long-term rate of return is 7.75% on pension plan assets and 4.00% on postretirement plan assets for 2025 and 2026. Our expected return on plan assets is calculated using the actual fair value of plan assets. If all other factors were to remain unchanged, we expect that a 0.50% decrease in the expected long-term rate of return would cause 2026 combined pension and postretirement cost to increase \$139, which under our accounting policy would be adjusted to actual returns in the current year upon remeasurement of our retiree benefit plans.

We recognize gains and losses on pension and postretirement plan assets and obligations immediately in “Other income (expense) – net” in our consolidated statements of income. These gains and losses are generally measured annually as of December 31, and accordingly, will normally be recorded during the fourth quarter, unless an earlier remeasurement is required. Should actual experience differ from actuarial assumptions, the projected pension benefit obligation and net pension cost and accumulated postretirement benefit obligation and postretirement benefit cost would be affected in future years. See Note 14 for additional discussions regarding our assumptions.

Asset Valuations and Impairments Goodwill and other indefinite-lived intangible assets are not amortized but tested at least annually on October 1 for impairment. For impairment testing, we estimate fair values using models that predominantly rely on the expected cash flows to be derived from the reporting unit or use of the asset. Long-lived assets are reviewed for impairment whenever events or circumstances indicate that the book value may not be recoverable over the remaining life. Inputs underlying the expected cash flows include, but are not limited to, subscriber counts, revenue per user, capital investment and acquisition costs per subscriber, and ongoing operating costs. We based our assumptions on a combination of our historical results, trends, business plans and marketplace participant data.

Annual Goodwill Testing

Goodwill is tested on a reporting unit basis by comparing the estimated fair value of each reporting unit to its book value. If the fair value exceeds the book value, then no impairment is measured. We estimate fair values using an income approach (also known as a discounted cash flow model) and market multiple approaches. The income approach utilizes our future cash flow projections with a perpetuity value discounted at an appropriate weighted average cost of capital. The market multiple approach uses the multiples of publicly traded companies whose services are comparable to those offered by the reporting units.

As of October 1, 2025, the calculated fair values of the reporting units with remaining goodwill exceeded their book values in all circumstances in excess of 10%. If either the projected long-term growth rates declined by 0.5%, if the projected long-term EBITDA margin declined by 0.5%, or if the weighted average cost of capital increased by 0.5%, the fair values would still be higher than the book value of the reporting units.

The fair values of our remaining reporting units could be negatively impacted by future sustained declines in macroeconomic or business conditions, higher discount rates or declines in the value of AT&T stock and could result in goodwill impairment charges in future periods.

U.S. Wireless Licenses

We have the option to first perform a qualitative assessment to determine whether it is more likely than not that the book value of our wireless licenses exceeds the fair value. On a periodic basis, or if the qualitative assessment indicates potential impairment, we will perform a quantitative impairment test.

Our quantitative assessment involves assessing the fair value of U.S. wireless licenses using a discounted cash flow model (the Greenfield Approach) and a qualitative corroborative market approach based on auction prices, depending upon auction activity. The Greenfield Approach assumes a company initially owns only the wireless licenses and makes investments required to build an operation comparable to current use. These licenses are tested annually for impairment on an aggregated basis, consistent with their use on a national scope for the United States. For impairment testing, we assume subscriber and revenue growth will trend up to projected levels, with a long-term growth rate reflecting expected long-term inflation trends. We assume churn rates will initially exceed our current experience but decline to rates that are in line with industry-leading churn.

During 2025, we performed a qualitative impairment assessment that considered several factors, including macroeconomic conditions, industry and regulatory considerations, recent and projected performance of the reporting unit and the prior quantitative impairment testing results. The qualitative assessment indicated it is more likely than not that the fair value of our wireless licenses exceeded the book value; thus, a quantitative assessment was not performed.

For our most recent quantitative assessment, which was performed in 2024, we used a discount rate of 8.75%, based on the optimal long-term capital structure of a market participant and its associated cost of debt and equity for the licenses, to calculate the present value of the projected cash flows. The quantitative impairment assessment indicated the fair value of our wireless licenses exceeded their book value by more than 10%. If either the projected rate of long-term growth of cash flows or revenues

declined by 0.5%, or if the discount rate increased by 0.5%, the fair values of these wireless licenses would still be higher than the book value.

Income Taxes Our estimates of income taxes and the significant items giving rise to the deferred assets and liabilities are shown in Note 13 and reflect our assessment of actual future taxes to be paid on items reflected in the financial statements, giving consideration to both timing and probability of these estimates. Actual income taxes could vary from these estimates due to future changes in income tax law or the final review of our tax returns by federal, state or foreign tax authorities.

We use our judgment to determine whether it is more likely than not that we will sustain positions that we have taken on tax returns and, if so, the amount of benefit to initially recognize within our financial statements. We regularly review our uncertain tax positions and adjust our unrecognized tax benefits (UTBs) in light of changes in facts and circumstances, such as changes in tax law, interactions with taxing authorities and developments in case law. These adjustments to our UTBs may affect our income tax expense. Settlement of uncertain tax positions may require use of our cash.

New Accounting Standards

See Note 1 for discussion of recently issued or adopted accounting standards.

OTHER BUSINESS MATTERS

Environmental We are subject from time to time to judicial and administrative proceedings brought by various governmental authorities under federal, state or local environmental laws. We reference in our Forms 10-Q and 10-K certain environmental proceedings that could result in monetary sanctions (exclusive of interest and costs) of three hundred thousand dollars or more. However, we do not believe that any of those currently pending will have a material adverse effect on our results of operations.

LIQUIDITY AND CAPITAL RESOURCES

For the years ended December 31,	2025	2024	2023
Cash provided by operating activities	\$ 40,284	\$ 38,771	\$ 38,314
Cash used in investing activities	(18,777)	(17,490)	(19,660)
Cash used in financing activities	(6,386)	(24,708)	(15,614)

At December 31,	2025	2024
Cash and cash equivalents	\$ 18,234	\$ 3,298
Total debt	136,100	123,532

We had \$18,234 in cash and cash equivalents available at December 31, 2025, increasing \$14,936 since December 31, 2024. Cash and cash equivalents included cash of \$3,521 and money market funds and other cash equivalents of \$14,713. Approximately \$1,330 of our cash and cash equivalents were held in accounts outside of the United States and may be subject to restrictions on repatriation. Our cash and cash equivalents at December 31, 2025 was elevated in anticipation of the consummation of announced transactions. (See Note 6)

In 2025, cash inflows were primarily provided by cash receipts from operations, including cash from our sale and transfer of our receivables to third parties, and the disposition of our investment in DIRECTV. These inflows exceeded cash used to meet the needs of the business, including, but not limited to, payment of operating expenses, including higher device payments from higher sales volumes. The cash generated from operating activities was primarily used to fund capital improvements, make dividend payments to stockholders, repurchase preferred and common stock, and repay long-term debt. We maintain availability under our credit facilities and our commercial paper program to meet our short-term liquidity requirements.

Refer to “Contractual Obligations” discussion below for additional information regarding our cash requirements.

Cash Provided by Operating Activities

During 2025, cash provided by operating activities was \$40,284, compared to \$38,771 in 2024, driven by operational growth and lower cash tax payments. Partially offsetting this increase and lowering cash from operations during 2025 were voluntarily pension contributions of approximately \$1,150 and advanced cash payments of about \$900 to Frontier Communications, a subsidiary of Verizon Communications Inc.

We actively manage the timing of our supplier payments for operating items to optimize the use of our cash. Among other things, we seek to make payments on 90-day or greater terms, while providing the suppliers with access to bank facilities that

permit earlier payments at their cost (referred to as supplier financing program). In addition, for payments to suppliers of handset inventory, as part of our working capital initiatives, we have arrangements that allow us to extend the stated payment terms by up to 90 days at an additional cost to us (referred to as direct supplier financing). The net impact of direct supplier financing, including principal and interest payments, was to improve cash from operating activities \$443 in 2025 and \$661 in 2024. All supplier financing payments are due within one year. (See Note 22)

Cash Used in Investing Activities

During 2025, cash used in investing activities totaled \$18,777, consisting primarily of \$20,842 (including interest during construction) for capital expenditures. During 2025, investing activities also included \$148 of FirstNet sustainability receipts net of investment and \$620 for our investment in a new strategic partner, DriveNets, related to wireline network transformation accounted for under the equity method of accounting.

On July 2, 2025, we completed the sale of our interest in DIRECTV to TPG and recorded a current note receivable of approximately \$3,600, of which we had received \$3,100 by the end of 2025, and a long-term note receivable of \$500. (See Note 10)

We enter into multi-year software licensing arrangements, which are typically paid over the license terms of two to five years and referred to as vendor financing. Additionally, for capital improvements, we have negotiated favorable vendor payment terms of 120 days or more with some of our vendors, which are also referred to as vendor financing. Vendor financing is excluded from capital expenditures and reported as financing activities. Vendor financing payments were \$1,181 in 2025, compared to \$1,792 in 2024. Capital expenditures in 2025 were \$20,842, and when including \$1,181 cash paid for vendor financing, capital investment was \$22,023 (\$32 lower than the prior year).

The vast majority of our capital expenditures are spent on our networks, including product development and related support systems. In 2025, we placed \$1,594 of productive assets in service under vendor financing arrangements (compared to \$700 in 2024).

In November 2024, we agreed to purchase select spectrum licenses from United States Cellular Corporation (UScellular) for approximately \$1,000, subject to closing conditions, including the consummation of UScellular's sale of its wireless operations and select spectrum assets to T-Mobile US, Inc. We completed our acquisition of these licenses on January 13, 2026, with a cash payment of \$1,018.

On May 21, 2025, we agreed to acquire substantially all of Lumen's Mass Markets fiber business for \$5,750 in cash, subject to purchase price adjustments. At the time of signing, the pending acquisition covered approximately one million fiber customers, and also included fiber network assets that reached more than four million fiber locations. On February 2, 2026, we completed the transaction and expect to manage the customer relationships in our Consumer Wireline business and place the fiber network assets in a new, wholly owned subsidiary. We plan to sell a controlling interest in the subsidiary to an equity partner that will co-invest in the ongoing business, and, as such, it is expected to meet the criteria for discontinued operations.

On August 25, 2025, we agreed to purchase FCC licenses in the 600 MHz and 3.45 GHz bands from EchoStar for approximately \$23,000, subject to certain adjustments. The transaction is expected to close in early 2026 and is subject to regulatory approval and other closing conditions. The FCC licenses will be used to expand our 5G network, meet future capacity demands and support future wireless communications services. We signed a short-term spectrum manager lease on the 3.45 GHz spectrum, which was deployed in cell sites covering nearly two-thirds of the U.S. population.

The amount of capital expenditures is influenced by demand for services and products, capacity needs and network enhancements. In 2026, we expect that our capital investment, which includes capital expenditures and cash paid for vendor financing, will be in the \$23,000 to \$24,000 range.

Cash Provided by or Used in Financing Activities

In 2025, cash used in financing activities totaled \$6,386 and was comprised of dividend payments, common and preferred stock repurchases, debt repayments and vendor financing payments, partially offset by issuances of long-term debt and issuances of preferred interests in a subsidiary.

A tabular summary of our debt activity during 2025 is as follows:

	First Quarter	Second Quarter	Third Quarter	Fourth Quarter	Full Year 2025
Issuance of notes and debentures:					
USD notes	\$ —	\$ 3,473	\$ 4,959	\$ —	\$ 8,432
EUR notes	2,956	—	2,639	—	5,595
Debt issuances	\$ 2,956	\$ 3,473	\$ 7,598	\$ —	\$ 14,027
Repayments:					
USD notes	\$ —	\$ —	\$ —	\$ (145)	\$ (145)
EUR notes	(1,321)	(32)	—	(2,441)	(3,794)
CAD notes	—	—	—	(960)	(960)
Other	(205)	(62)	(229)	(133)	(629)
Repayments of long-term debt	\$ (1,526)	\$ (94)	\$ (229)	\$ (3,679)	\$ (5,528)

The weighted average interest rate of our long-term debt portfolio, including credit agreement borrowings and the impact of derivatives, was approximately 4.2% as of December 31, 2025 and 2024. We had \$134,718 of total notes and debentures outstanding at December 31, 2025. This also included Euro, British pound sterling, Canadian dollar, Australian dollar and Swiss franc denominated debt that totaled approximately \$35,307.

At December 31, 2025, we had \$9,011 of long-term debt maturing within one year. We had no outstanding commercial paper borrowings or other short-term borrowings on December 31, 2025.

During 2025, we paid \$1,181 of cash under our vendor financing program, compared to \$1,792 in 2024. Total vendor financing payables included in our December 31, 2025 consolidated balance sheet were \$1,892, with \$956 due within one year (in “Accounts payable and accrued liabilities”) and the remainder predominantly due within five years (in “Other noncurrent liabilities”).

During 2025, we repurchased approximately 159 million shares totaling \$4,269 under our \$10,000 common stock repurchase authorization approved by the Board of Directors in December 2024, excluding brokerage fees and the one percent excise tax imposed by the Inflation Reduction Act of 2022. At December 31, 2025, we had approximately \$5,731 remaining under this 2024 repurchase authorization. On January 27, 2026, the Board approved an authorization to repurchase an additional \$10,000 of common stock.

We paid dividends on common and preferred shares of \$8,180 in 2025, compared with \$8,208 in 2024. Dividends on common stock declared by our Board of Directors totaled \$1.11 per share in 2025 and in 2024. Our dividend policy considers the expectations and requirements of stockholders, capital funding requirements of AT&T and long-term growth opportunities.

Financing activities in 2025 also included the issuance of \$2,250 of nonconvertible cumulative preferred interests in Telco LLC, with the funds used to redeem all outstanding Series B preferred stock for \$2,075 (see Note 16). We also received approximately \$850 in upfront cash proceeds from a structured sale-leaseback of real estate.

On February 5, 2026, we issued \$6,500 principal amount of global notes due 2031 to 2056 with a weighted average coupon of 5.2%. We intend to use the net proceeds from this issuance for general corporate purposes, which may include debt repayments and pending acquisitions.

Our 2026 financing activities will focus on managing our debt level, funding pending acquisitions, paying dividends, subject to approval by our Board of Directors, and repurchasing common stock when deemed appropriate. We plan to fund our financing

uses of cash through a combination of cash from operations, issuance of debt and asset sales. The timing and mix of any debt issuance and/or refinancing will be guided by credit market conditions and interest rate trends.

Credit Facilities

The following summary of our various credit and loan agreements does not purport to be complete and is qualified in its entirety by reference to each agreement filed as exhibits to our Annual Report on Form 10-K.

We use credit facilities as a tool in managing our liquidity status. On November 3, 2025, we entered into (i) a \$12,000 Second Amended and Restated Credit Agreement (Revolving Credit Agreement), with Citibank, N.A., as agent, amending and restating our existing \$12,000 Amended and Restated Credit Agreement, dated as of November 18, 2022, and (ii) a \$17,500 Delayed Draw Term Loan Credit Agreement (Term Loan), with Bank of America, N.A., as agent. No amount was outstanding under the Revolving Credit Agreement or the Term Loan as of December 31, 2025. (See Note 11)

We also utilize other external financing sources, which include various credit arrangements supported by government agencies to support network equipment purchases as well as a commercial paper program.

The Revolving Credit Agreement and the Term Loan contain covenants that are customary for an issuer with investment grade senior debt credit ratings, including a net debt-to-EBITDA financial ratio covenant requiring us to maintain, as of the last day of each fiscal quarter, a ratio of not more than 3.75-to-1. As of December 31, 2025, we were in compliance with the covenants for our credit facilities.

Collateral Arrangements

Most of our counterparty collateral arrangements require cash collateral posting by AT&T only when derivative market values exceed certain thresholds. Under these arrangements, which cover the majority of our \$35,741 derivative portfolio, counterparties are still required to post collateral. During 2025, we posted \$11 of cash collateral, on a net basis. Cash postings under these arrangements vary with changes in credit ratings and netting agreements. (See Note 12)

Other

Our total capital consists of debt (long-term debt and debt maturing within one year), redeemable noncontrolling interest and stockholders' equity. Our capital structure does not include debt issued by our equity method investments. At December 31, 2025, our debt ratio was 51.4%, compared to 50.7% at December 31, 2024 and 53.5% at December 31, 2023. The debt ratio is affected by the same factors that affect total capital, and reflects our recent debt issuances, repayments and reclassifications related to redemption of noncontrolling interests.

A significant amount of our cash outflows is related to tax items, acquisition of spectrum and benefits paid for current and former employees:

- Total taxes incurred, collected and remitted by AT&T during 2025 and 2024 were \$16,326 and \$16,968. These taxes include income, franchise, property, sales, excise, payroll, gross receipts and various other taxes and fees.
- Total domestic spectrum acquired primarily through FCC auctions, including cash, exchanged spectrum, auction deposits and spectrum relocation and clearing costs, was approximately \$379 in 2025, \$380 in 2024 and \$2,940 in 2023.
- Total health and welfare benefits provided to certain active and retired employees and their dependents totaled approximately \$2,490 in 2025 and \$2,550 in 2024, with \$483 paid from plan assets in 2025, compared to \$736 in 2024. Of those benefits, approximately \$2,220 related to medical and prescription drug benefits in 2025, compared to \$2,290 in 2024. We paid \$2,957 of pension benefits out of plan assets in 2025, compared to \$2,447 in 2024.

Contractual Obligations

Our contractual obligations as of December 31, 2025, and the estimated timing of payment, are in the following table:

	Payments Due By Period				
	Total	Less than 1 Year	1-3 Years	3-5 Years	More than 5 Years
Long-term debt obligations ¹	\$ 144,664	\$ 8,652	\$ 15,858	\$ 13,938	\$ 106,216
Interest payments on long-term debt ²	94,373	6,067	11,059	9,992	67,255
Purchase obligations ³	24,638	8,545	10,698	2,505	2,890
Operating lease obligations ⁴	27,556	4,956	8,360	5,432	8,808
FirstNet sustainability payments ⁵	16,029	896	3,224	2,589	9,320
Unrecognized tax benefits (UTB) ⁶	10,282	45	—	—	10,237
Other finance obligations ⁷	11,626	1,843	2,699	1,928	5,156
Total Contractual Obligations⁸	\$ 329,168	\$ 31,004	\$ 51,898	\$ 36,384	\$ 209,882

¹ Represents principal or payoff amounts of notes, debentures and credit agreement borrowings at maturity (see Note 11). Foreign debt includes the impact from hedges, when applicable.

² Includes credit agreement borrowings.

³ We expect to fund the purchase obligations with cash on hand, which may include cash provided by operations or through incremental borrowings. The minimum commitment for certain obligations is based on termination penalties that could be paid to exit the contracts. (See Note 21)

⁴ Represents operating lease payments (see Note 8).

⁵ Represents contractual commitment to make sustainability payments over the 25-year contract. These sustainability payments represent our commitment to fund FirstNet's operating expenses and future reinvestment in the network, which we own and operate. FirstNet has a statutory requirement to reinvest funds that exceed the agency's operating expenses, which we anticipate to be \$15,000. (See Note 20)

⁶ The noncurrent portion of the UTBs is included in the "More than 5 Years" column, as we cannot reasonably estimate the timing or amounts of additional cash payments, if any, at this time (see Note 13).

⁷ Represents future minimum payments under the Crown Castle and other arrangements (see Note 18), payables subject to extended payment terms (see Note 22) and finance lease payments (see Note 8).

⁸ Excludes debt transactions, pending acquisitions and other investment funding completed after December 31, 2025 (see Note 6).

Certain items were excluded from this table because the year of payment is unknown and could not be reliably estimated, we believe the obligations are immaterial, or the settlement of the obligation will not require the use of cash. These items include: deferred income tax liability of \$58,312 (see Note 13); net postemployment benefit obligations of \$9,113 (including current portion); and other noncurrent liabilities of \$7,155.

DISCUSSION AND RECONCILIATION OF NON-GAAP MEASURES

We also evaluate segment and business unit performance based on EBITDA, which is defined as operating income excluding depreciation and amortization, and/or EBITDA margin, which is defined as EBITDA divided by total revenue. EBITDA is used as part of our management reporting, and we believe EBITDA to be a relevant and useful measurement to our investors as it measures the cash generation potential of our business units. EBITDA does not give effect to depreciation and amortization expenses incurred in operating income nor is it burdened by cash used for debt service requirements and thus does not reflect available funds for distributions, reinvestment or other discretionary uses. There are material limitations to using these non-GAAP financial measures. EBITDA and EBITDA margin, as we have defined them, may not be comparable to similarly titled measures reported by other companies.

	2025	2024	2023
Communications Segment			
Operating income	\$ 27,927	\$ 27,095	\$ 27,801
Add: Depreciation and amortization	19,959	19,433	17,363
EBITDA	\$ 47,886	\$ 46,528	\$ 45,164
Operating income margin	23.1 %	23.0 %	23.6 %
EBITDA margin	39.6 %	39.5 %	38.3 %
Mobility			
Operating income	\$ 27,196	\$ 26,314	\$ 25,861
Add: Depreciation and amortization	10,422	10,217	8,517
EBITDA	\$ 37,618	\$ 36,531	\$ 34,378
Operating income margin	30.4 %	30.9 %	30.8 %
EBITDA margin	42.0 %	42.8 %	40.9 %
Business Wireline			
Operating income (loss)	\$ (816)	\$ (88)	\$ 1,289
Add: Depreciation and amortization	5,834	5,555	5,377
EBITDA	\$ 5,018	\$ 5,467	\$ 6,666
Operating income margin	(4.7)%	(0.5)%	6.2 %
EBITDA margin	29.1 %	29.1 %	31.9 %
Consumer Wireline			
Operating income	\$ 1,547	\$ 869	\$ 651
Add: Depreciation and amortization	3,703	3,661	3,469
EBITDA	\$ 5,250	\$ 4,530	\$ 4,120
Operating income margin	10.9 %	6.4 %	4.9 %
EBITDA margin	37.0 %	33.4 %	31.3 %
Latin America Segment			
Operating income (loss)	\$ 145	\$ 40	\$ (141)
Add: Depreciation and amortization	671	657	724
EBITDA	\$ 816	\$ 697	\$ 583
Operating income margin	3.3 %	0.9 %	(3.6)%
EBITDA margin	18.6 %	16.5 %	14.8 %

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We are exposed to market risks primarily from changes in interest rates and foreign currency exchange rates. These risks, along with other business risks, impact our cost of capital. It is our policy to manage our debt structure and foreign exchange exposure in order to manage capital costs, control financial risks and maintain financial flexibility over the long term. In managing market risks, we employ derivatives according to documented policies and procedures, including interest rate swaps, interest rate locks, foreign currency exchange contracts and combined interest rate foreign currency contracts (cross-currency swaps). We do not use derivatives for trading or speculative purposes. We do not foresee significant changes in the strategies we use to manage market risk in the near future.

One of the most significant assumptions used in estimating our postretirement benefit obligations is the assumed weighted-average discount rate, which is the hypothetical rate at which the projected benefit obligations could be effectively settled or paid out to participants. We determined our discount rate based on a range of factors, including a yield curve composed of the rates of return on several hundred high-quality, fixed income corporate bonds available at the measurement date and corresponding to the related expected durations of future cash outflows for the obligations. In recent years, the discount rates have been increasingly volatile, and on average have been lower than in historical periods. Lower discount rates used to measure our pension and postretirement plans result in higher obligations. Future increases in these rates could result in lower obligations, improved funded status and actuarial gains.

Interest Rate Risk

The majority of our financial instruments are medium- and long-term fixed-rate notes and debentures. Changes in interest rates can lead to significant fluctuations in the fair value of these instruments. The principal amounts by expected maturity, average interest rate and fair value of our liabilities that are exposed to interest rate risk are described in Notes 11 and 12. In managing interest expense, we control our mix of fixed- and floating-rate debt through term loans, floating-rate notes, and interest rate swaps. We have established interest rate risk limits that we closely monitor by measuring interest rate sensitivities in our debt and interest rate derivatives portfolios.

Our foreign-denominated long-term debt has been swapped from fixed-rate or floating-rate foreign currencies to fixed-rate U.S. dollars at issuance through cross-currency swaps, removing interest rate risk and foreign currency exchange risk associated with the underlying interest and principal payments. Likewise, periodically we enter into interest rate locks to partially hedge the risk of increases in the benchmark interest rate during the period leading up to the probable issuance of fixed-rate debt. We expect gains or losses on our cross-currency swaps and interest rate locks to offset the losses and gains in the financial instruments they hedge.

We had no interest rate swaps and no interest rate locks at December 31, 2025.

Foreign Exchange Risk

We principally use foreign exchange contracts to hedge costs and debt denominated in foreign currencies. We are also exposed to foreign currency exchange risk through our foreign affiliates and equity investments in foreign companies.

Through cross-currency swaps, our foreign-denominated debt has been swapped from fixed-rate or floating-rate foreign currencies to fixed-rate U.S. dollars at issuance, removing interest rate and foreign currency exchange risk associated with the underlying interest and principal payments. We expect gains or losses in our cross-currency swaps to offset the gains and losses in the financial instruments they hedge. We had cross-currency swaps with a notional value of \$35,741 and a fair value of \$(1,174) outstanding at December 31, 2025.

For the purpose of assessing specific risks, we use a sensitivity analysis to determine the effects that market risk exposures may have on the fair value of our financial instruments and results of operations. We had no foreign exchange forward contracts at December 31, 2025.

REPORT OF MANAGEMENT

The consolidated financial statements have been prepared in conformity with U.S. generally accepted accounting principles. The integrity and objectivity of the data in these financial statements, including estimates and judgments relating to matters not concluded by year end, are the responsibility of management, as is all other information included in the Annual Report, unless otherwise indicated.

The financial statements of AT&T Inc. (AT&T) have been audited by Ernst & Young LLP, Independent Registered Public Accounting Firm. Management has made available to Ernst & Young LLP all of AT&T's financial records and related data, as well as the minutes of stockholders' and directors' meetings. Furthermore, management believes that all representations made to Ernst & Young LLP during its audit were valid and appropriate.

Management maintains disclosure controls and procedures that are designed to ensure that information required to be disclosed by AT&T is recorded, processed, summarized, accumulated and communicated to its management, including its principal executive and principal financial officers, to allow timely decisions regarding required disclosure, and reported within the time periods specified by the Securities and Exchange Commission's rules and forms.

Management also seeks to ensure the objectivity and integrity of its financial data by the careful selection of its managers, by organizational arrangements that provide an appropriate division of responsibility and by communication programs aimed at ensuring that its policies, standards and managerial authorities are understood throughout the organization.

The Audit Committee of the Board of Directors meets periodically with management, the internal auditors and the independent auditors to review the manner in which they are performing their respective responsibilities and to discuss auditing, internal accounting controls and financial reporting matters. Both the internal auditors and the independent auditors periodically meet alone with the Audit Committee and have access to the Audit Committee at any time.

Assessment of Internal Control

The management of AT&T is responsible for establishing and maintaining adequate internal control over financial reporting, as defined in Rule 13a-15(f) or 15d-15(f) under the Securities Exchange Act of 1934. AT&T's internal control system was designed to provide reasonable assurance to the company's management and Board of Directors regarding the preparation and fair presentation of published financial statements.

AT&T management assessed the effectiveness of the company's internal control over financial reporting as of December 31, 2025. In making this assessment, it used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in *Internal Control – Integrated Framework* (2013 framework). Based on its assessment, AT&T management believes that, as of December 31, 2025, the company's internal control over financial reporting is effective based on those criteria.

Ernst & Young LLP, the independent registered public accounting firm that audited the financial statements included in this Annual Report, has issued an attestation report on the company's internal control over financial reporting.

/s/John T. Stankey

John T. Stankey
Chairman of the Board,
Chief Executive Officer and President

/s/Pascal Desroches

Pascal Desroches
Senior Executive Vice President
and Chief Financial Officer

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the Stockholders and the Board of Directors of AT&T Inc.

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of AT&T Inc. (the Company) as of December 31, 2025 and 2024, the related consolidated statements of income, comprehensive income, cash flows and changes in stockholders' equity for each of the three years in the period ended December 31, 2025, and the related notes and financial statement schedule listed in the Index at Item 15(a) (collectively referred to as the "consolidated financial statements"). In our opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the Company at December 31, 2025 and 2024, and the results of its operations and its cash flows for each of the three years in the period ended December 31, 2025, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the Company's internal control over financial reporting as of December 31, 2025, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) and our report dated February 9, 2026 expressed an unqualified opinion thereon.

Basis for Opinion

These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's financial statements based on our audits. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud. Our audits included performing procedures to assess the risks of material misstatement of the financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that our audits provide a reasonable basis for our opinion.

Critical Audit Matters

The critical audit matters communicated below are matters arising from the current period audit of the financial statements that were communicated or required to be communicated to the audit committee and that: (1) relate to accounts or disclosures that are material to the financial statements and (2) involved our especially challenging, subjective or complex judgments. The communication of critical audit matters does not alter in any way our opinion on the consolidated financial statements, taken as a whole, and we are not, by communicating the critical audit matters below, providing separate opinions on the critical audit matters or on the accounts or disclosures to which they relate.

Discount rates used in determining pension and postretirement benefit obligations

Description of the Matter

At December 31, 2025, the Company's defined benefit pension obligation was \$30,627 million and exceeded the fair value of pension plan assets of \$28,677 million, resulting in an unfunded benefit obligation of \$1,950 million. Additionally, at December 31, 2025, the Company's postretirement benefit obligation was \$6,477 million and exceeded the fair value of postretirement plan assets of \$722 million, resulting in an unfunded benefit obligation of \$5,755 million. As explained in Note 14 to the consolidated financial statements, the Company updates the assumptions used to measure the defined benefit pension and postretirement benefit obligations, including discount rates, at December 31 or upon a remeasurement event. The Company determines the discount rates used to measure the obligations based on the development of a yield curve using high-quality corporate bonds selected to yield cash flows that correspond to the expected timing and amount of the expected future benefit payments.

Auditing the defined benefit pension and postretirement benefit obligations was complex due to the judgmental nature of the actuarial assumptions made by management, primarily the discount rates, used in the Company's measurement process. The discount rates have a significant effect on the measurement of the defined benefit pension and postretirement benefit obligations, and auditing the discount rates was complex because it required an evaluation of the credit quality of the corporate bonds used to develop the discount rates and the correlation of those bonds' cash inflows to the timing and amount of future expected benefit payments.

*How We
Addressed the
Matter in Our
Audit*

We obtained an understanding, evaluated the design and tested the operating effectiveness of certain controls over management's review of the determination of the discount rates used in the defined benefit pension and postretirement benefit obligations calculations.

To test the determination of the discount rates used in the calculation of the defined benefit pension and postretirement benefit obligations, we performed audit procedures that focused on evaluating, with the assistance of our actuarial specialists, the determination of the discount rates, among other procedures. For example, we evaluated the selected yield curve used to determine the discount rates applied in measuring the defined benefit pension and postretirement benefit obligations. As part of this assessment, we considered the credit quality of the corporate bonds that comprised the yield curve and compared the timing and amount of cash flows at maturity with the expected amounts and duration of the related benefit payments.

Evaluation of goodwill for impairment

*Description of
the Matter*

At December 31, 2025, the Company's goodwill balance was \$63,425 million. As discussed in Note 1 to the consolidated financial statements, reporting unit goodwill is tested at least annually for impairment. Estimating fair value in connection with the impairment evaluation involves the utilization of discounted cash flow and market multiple approaches.

Auditing management's annual goodwill impairment test for the Consumer Wireline reporting unit was complex because the estimation of fair value involves subjective management assumptions, such as the projected long-term EBITDA margin and weighted average cost of capital, and complex valuation methodologies, such as the discounted cash flow and market multiple approaches. Assumptions used in these valuation models are forward-looking, and changes in these assumptions can have a material effect on the determination of fair value.

*How We
Addressed the
Matter in Our
Audit*

We obtained an understanding, evaluated the design and tested the operating effectiveness of certain controls over the Company's impairment evaluation processes. Our procedures included testing controls over management's review of the valuation models and its determination of the significant assumptions described above.

Our audit procedures to test management's impairment evaluation included, among others, assessing the valuation methodologies and significant assumptions discussed above and the underlying data used to develop such assumptions. For example, we compared the significant assumptions to current industry, market and economic trends, and other guideline companies in the same industry. Where appropriate, we evaluated whether changes to the Company's business and other factors would affect the significant assumptions. We also assessed the historical accuracy of management's estimates and performed independent sensitivity analyses. We involved our valuation specialists to assist us in evaluating the methodologies and auditing the assumptions used to calculate the estimated fair value of the Consumer Wireline reporting unit.

/s/ Ernst & Young LLP

We have served as the Company's auditor since 1999.

Dallas, Texas
February 9, 2026

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the Stockholders and the Board of Directors of AT&T Inc.

Opinion on Internal Control Over Financial Reporting

We have audited AT&T Inc.'s internal control over financial reporting as of December 31, 2025, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) (the COSO criteria). In our opinion, AT&T Inc. (the Company) maintained, in all material respects, effective internal control over financial reporting as of December 31, 2025, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the 2025 consolidated financial statements of the Company and our report dated February 9, 2026 expressed an unqualified opinion thereon.

Basis for Opinion

The Company's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Report of Management. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audit in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects.

Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

Definition and Limitations of Internal Control Over Financial Reporting

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

/s/ Ernst & Young LLP

Dallas, Texas
February 9, 2026

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA**Consolidated Statements of Income**

	2025	2024	2023
Operating Revenues			
Service	\$ 101,158	\$ 100,135	\$ 99,649
Equipment	24,490	22,201	22,779
Total operating revenues	125,648	122,336	122,428
Operating Expenses			
Cost of revenues			
Equipment	25,396	22,249	23,136
Other cost of revenues (exclusive of depreciation and amortization shown separately below)	25,424	26,972	26,987
Selling, general and administrative	28,942	28,411	28,874
Asset impairments and abandonments and restructuring	838	5,075	1,193
Depreciation and amortization	20,886	20,580	18,777
Total operating expenses	101,486	103,287	98,967
Operating Income	24,162	19,049	23,461
Other Income (Expense)			
Interest expense	(6,804)	(6,759)	(6,704)
Equity in net income of affiliates	1,895	1,989	1,675
Other income (expense) – net	7,754	2,419	1,416
Total other income (expense)	2,845	(2,351)	(3,613)
Income Before Income Taxes	27,007	16,698	19,848
Income tax expense	3,621	4,445	4,225
Net Income	23,386	12,253	15,623
Less: Net Income Attributable to Noncontrolling Interest	(1,433)	(1,305)	(1,223)
Net Income Attributable to AT&T	\$ 21,953	\$ 10,948	\$ 14,400
Less: Preferred Stock Dividends and Redemption Gain	(64)	(202)	(208)
Net Income Attributable to Common Stock	\$ 21,889	\$ 10,746	\$ 14,192
Basic Earnings Per Share Attributable to Common Stock	\$ 3.04	\$ 1.49	\$ 1.97
Diluted Earnings Per Share Attributable to Common Stock	\$ 3.04	\$ 1.49	\$ 1.97

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Comprehensive Income

	2025	2024	2023
Net income	\$ 23,386	\$ 12,253	\$ 15,623
Other comprehensive income (loss), net of tax:			
Foreign Currency:			
Translation adjustment, net of taxes of \$117, \$(175) and \$143	354	(545)	463
Reclassification adjustment included in net income, net of taxes of \$0, \$(14) and \$0	—	127	—
Securities:			
Net unrealized gains (losses), net of taxes of \$5, \$(5) and \$8	15	(19)	22
Reclassification adjustment included in net income, net of taxes of \$1, \$10 and \$4	3	30	11
Derivative Instruments:			
Net unrealized gains (losses), net of taxes of \$(216), \$121 and \$228	(650)	380	922
Reclassification adjustment included in net income, net of taxes of \$14, \$14 and \$12	45	45	47
Defined benefit postretirement plans:			
Net prior service (cost) credit arising during period, net of taxes of \$0, \$0 and \$10	—	—	32
Amortization of net prior service credit included in net income, net of taxes of \$(457), \$(492) and \$(642)	(1,427)	(1,523)	(1,963)
Reclassification adjustment realized in net income, net of taxes of \$(4), \$0 and \$0	5	—	—
Other comprehensive income (loss)	(1,655)	(1,505)	(466)
Total comprehensive income	21,731	10,748	15,157
Less: Total comprehensive income attributable to noncontrolling interest	(1,433)	(1,305)	(1,223)
Total Comprehensive Income Attributable to AT&T	\$ 20,298	\$ 9,443	\$ 13,934

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Balance Sheets

	December 31,	
	2025	2024
Assets		
Current Assets		
Cash and cash equivalents	\$ 18,234	\$ 3,298
Accounts receivable – net of related allowance for credit loss of \$429 and \$375	8,843	9,638
Inventories	2,420	2,270
Prepaid and other current assets	19,235	15,962
Total current assets	48,732	31,168
Property, Plant and Equipment – Net	131,559	128,871
Goodwill – Net	63,425	63,432
Licenses – Net	128,148	127,035
Other Intangible Assets – Net	5,254	5,255
Investments in and Advances to Equity Affiliates	1,106	295
Operating Lease Right-Of-Use Assets	22,642	20,909
Other Assets	19,332	17,830
Total Assets	\$ 420,198	\$ 394,795
Liabilities and Stockholders' Equity		
Current Liabilities		
Debt maturing within one year	\$ 9,011	\$ 5,089
Accounts payable and accrued liabilities	38,514	35,657
Advanced billings and customer deposits	4,266	4,099
Dividends payable	1,989	2,027
Total current liabilities	53,780	46,872
Long-Term Debt	127,089	118,443
Deferred Credits and Other Noncurrent Liabilities		
Noncurrent deferred tax liabilities	58,312	58,939
Postemployment benefit obligation	8,478	9,025
Operating lease liabilities	18,943	17,391
Other noncurrent liabilities	25,104	23,900
Total deferred credits and other noncurrent liabilities	110,837	109,255
Redeemable Noncontrolling Interest	2,001	1,980
Stockholders' Equity		
Preferred stock (\$1 par value, 10,000,000 authorized at December 31, 2025 and December 31, 2024):		
Series A (48,000 issued and outstanding at December 31, 2025 and December 31, 2024)	—	—
Series B (20,000 issued and 0 outstanding at December 31, 2025 and 20,000 issued and outstanding at December 31, 2024)	—	—
Series C (70,000 issued and outstanding at December 31, 2025 and December 31, 2024)	—	—
Common stock (\$1 par value, 14,000,000,000 authorized at December 31, 2025 and December 31, 2024: issued 7,620,748,598 at December 31, 2025 and December 31, 2024)	7,621	7,621
Additional paid-in capital	106,533	109,108
Retained earnings	15,768	1,871
Treasury stock (583,246,242 at December 31, 2025 and 444,853,148 at December 31, 2024, at cost)	(18,529)	(15,023)
Accumulated other comprehensive income (loss)	(860)	795
Noncontrolling interest	15,958	13,873
Total stockholders' equity	126,491	118,245
Total Liabilities and Stockholders' Equity	\$ 420,198	\$ 394,795

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Cash Flows

	2025	2024	2023
Operating Activities			
Net Income	\$ 23,386	\$ 12,253	\$ 15,623
Adjustments to reconcile net income to net cash provided by operating activities:			
Depreciation and amortization	20,886	20,580	18,777
Provision for uncollectible accounts	2,271	1,969	1,969
Asset impairments and abandonments and restructuring	838	5,075	1,193
Pension and postretirement benefit expense (credit)	(1,588)	(1,883)	(2,552)
Actuarial and settlement (gain) loss on pension and postretirement benefits – net	519	56	1,594
Net (gain) loss on investments	(5,889)	80	441
Changes in operating assets and liabilities:			
Receivables	(1,526)	123	82
Equipment installment receivables and related sales	324	(1,846)	(133)
Contract asset and cost deferral	(1,208)	160	(1,006)
Inventories, prepaid and other current assets	(460)	70	747
Accounts payable and other accrued liabilities	884	(1,104)	(1,574)
Changes in income taxes	2,226	1,978	2,618
Postretirement claims and contributions	(1,436)	(166)	(735)
Other – net	1,057	1,426	1,270
Total adjustments	16,898	26,518	22,691
Net Cash Provided by Operating Activities	40,284	38,771	38,314
Investing Activities			
Capital expenditures	(20,842)	(20,263)	(17,853)
Acquisitions, net of cash acquired	(379)	(380)	(2,942)
Dispositions	3,218	75	72
Distributions from DIRECTV in excess of cumulative equity in earnings	—	928	2,049
(Purchases), sales and settlements of securities – net	181	2,575	(902)
Other – net	(955)	(425)	(84)
Net Cash Used in Investing Activities	(18,777)	(17,490)	(19,660)
Financing Activities			
Net change in short-term borrowings with original maturities of three months or less	—	—	(914)
Issuance of other short-term borrowings	—	491	5,406
Repayment of other short-term borrowings	—	(2,487)	(3,415)
Issuance of long-term debt	14,027	19	10,004
Repayment of long-term debt	(5,528)	(10,297)	(12,044)
Note payable to DIRECTV, net of payments	—	—	(130)
Payment of vendor financing	(1,181)	(1,792)	(5,742)
Redemption of preferred stock	(2,075)	—	—
Purchase of treasury stock	(4,500)	(215)	(194)
Issuance of treasury stock	21	15	3
Issuance of preferred interests in subsidiary	2,221	—	7,151
Redemption of preferred interests in subsidiary	(65)	—	(5,333)
Dividends paid	(8,180)	(8,208)	(8,136)
Other – net	(1,126)	(2,234)	(2,270)
Net Cash Used in Financing Activities	(6,386)	(24,708)	(15,614)
Net increase (decrease) in cash and cash equivalents and restricted cash	15,121	(3,427)	3,040
Cash and cash equivalents and restricted cash beginning of year	3,406	6,833	3,793
Cash and Cash Equivalents and Restricted Cash End of Year	\$ 18,527	\$ 3,406	\$ 6,833

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Changes in Stockholders' Equity

	2025		2024		2023	
	Shares	Amount	Shares	Amount	Shares	Amount
<i>Preferred Stock – Series A</i>						
Balance at beginning of year	—	\$ —	—	\$ —	—	\$ —
Balance at end of year	—	\$ —	—	\$ —	—	\$ —
<i>Preferred Stock – Series B</i>						
Balance at beginning of year	—	\$ —	—	\$ —	—	\$ —
Balance at end of year	—	\$ —	—	\$ —	—	\$ —
<i>Preferred Stock – Series C</i>						
Balance at beginning of year	—	\$ —	—	\$ —	—	\$ —
Balance at end of year	—	\$ —	—	\$ —	—	\$ —
<i>Common Stock</i>						
Balance at beginning of year	7,621	\$ 7,621	7,621	\$ 7,621	7,621	\$ 7,621
Balance at end of year	7,621	\$ 7,621	7,621	\$ 7,621	7,621	\$ 7,621
<i>Additional Paid-In Capital</i>						
Balance at beginning of year		\$ 109,108		\$ 114,519		\$ 123,610
Redemption of preferred stock		(2,165)		—		—
Preferred stock dividends		—		(134)		(205)
Common stock dividends (\$1.11, \$1.11 and \$1.11 per share in 2025, 2024 and 2023)		—		(4,020)		(7,991)
Issuance of treasury stock		(469)		(516)		(379)
Share-based compensation		59		(184)		(109)
Redemption or reclassification of interests held by noncontrolling owners		—		(557)		(407)
Balance at end of year		\$ 106,533		\$ 109,108		\$ 114,519
<i>Retained Earnings (Deficit)</i>						
Balance at beginning of year		\$ 1,871		\$ (5,015)		\$ (19,415)
Net income attributable to AT&T		21,953		10,948		14,400
Preferred stock redemption gain		90		—		—
Preferred stock dividends		(194)		(71)		—
Common stock dividends (\$1.11, \$1.11 and \$1.11 per share in 2025, 2024 and 2023)		(7,952)		(3,991)		—
Balance at end of year		\$ 15,768		\$ 1,871		\$ (5,015)

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Changes in Stockholders' Equity – continued

	2025		2024		2023	
	Shares	Amount	Shares	Amount	Shares	Amount
<i>Treasury Stock</i>						
Balance at beginning of year	(445)	\$ (15,023)	(471)	\$ (16,128)	(493)	\$ (17,082)
Repurchase and acquisition of common stock	(168)	(4,539)	(12)	(215)	(10)	(194)
Reissuance of treasury stock	30	1,033	38	1,320	32	1,148
Balance at end of year	(583)	\$ (18,529)	(445)	\$ (15,023)	(471)	\$ (16,128)
<i>Accumulated Other Comprehensive Income (Loss)</i>						
<i>Attributable to AT&T, net of tax</i>						
Balance at beginning of year		\$ 795		\$ 2,300		\$ 2,766
Other comprehensive income (loss) attributable to AT&T		(1,655)		(1,505)		(466)
Balance at end of year		\$ (860)		\$ 795		\$ 2,300
<i>Noncontrolling Interest¹</i>						
Balance at beginning of year		\$ 13,873		\$ 14,145		\$ 8,957
Net income attributable to noncontrolling interest		1,276		1,163		1,146
Issuance and acquisition (disposition) of noncontrolling owners		2,221		(29)		5,180
Redemption of noncontrolling interest		(144)		(76)		(53)
Distributions		(1,268)		(1,330)		(1,085)
Balance at end of year		\$ 15,958		\$ 13,873		\$ 14,145
Total Stockholders' Equity at beginning of year		\$ 118,245		\$ 117,442		\$ 106,457
Total Stockholders' Equity at end of year		\$ 126,491		\$ 118,245		\$ 117,442

¹ Excludes redeemable noncontrolling interest.

The accompanying notes are an integral part of the consolidated financial statements.

Notes to Consolidated Financial Statements

NOTE 1. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Presentation Throughout this document, AT&T Inc. is referred to as “AT&T,” “we” or the “Company.” The consolidated financial statements include the accounts of the Company and subsidiaries and affiliates which we control. AT&T is a holding company whose subsidiaries and affiliates operate worldwide in the telecommunications and technology industries.

The consolidated financial statements include our controlled subsidiaries, as well as variable interest entities (VIE) where we are deemed to be the primary beneficiary. All significant intercompany transactions are eliminated in consolidation. Investments in entities that we do not control but have significant influence are accounted for under the equity method. We also record our proportionate share of our equity method investees’ other comprehensive income (OCI) items, including translation adjustments. We treat distributions received from equity method investees as returns on investment and classify them as cash flows from operating activities until those distributions exceed our cumulative equity in the earnings of that investment. We treat the excess amount as a return of investment and classify it as cash flows from investing activities. In the event we receive dividends in excess of the carrying amount of the investment, and we have no obligation to provide financial support to the equity method investee, we treat those dividends as returns on investment and classify them as cash flows from operating activities.

The preparation of financial statements in conformity with U.S. generally accepted accounting principles (GAAP) requires management to make estimates and assumptions, including other estimates of fair value, probable losses and expenses, that affect the amounts reported in the financial statements and accompanying notes. Actual results could differ from those estimates. Moreover, unfavorable changes in market conditions, including interest rates, could adversely impact those estimates and result in asset impairments. Certain prior-period amounts have been conformed to the current period’s presentation, providing further disaggregation of activities within Cash from Operations in our consolidated statements of cash flows and additional revenue categories for our Business Wireline and Consumer Wireline business units.

Adopted and New Accounting Standards

Income Taxes In December 2023, the Financial Accounting Standards Board (FASB) issued ASU No. 2023-09, “Income Taxes (Topic 740): Improvements to Income Tax Disclosures” (ASU 2023-09). Beginning with our 2025 annual reporting, we adopted, through retrospective application, ASU 2023-09, which requires that a public entity disclose specific categories in its annual income tax rate reconciliation table and provide additional qualitative information for reconciling items representing at least 5% of pre-tax income or loss from continuing operations, using the federal statutory tax rate. The standard also requires an annual breakdown of income taxes paid by jurisdiction (i.e., federal, state and foreign), with further disaggregation by jurisdictions representing at least 5% of total income taxes paid.

Segment Reporting In November 2023, the FASB issued ASU No. 2023-07, “Segment Reporting (Topic 280): Improvements to Reportable Segment Disclosures” (ASU 2023-07). Beginning with our 2024 annual reporting, we adopted, through retrospective application, ASU 2023-07, which requires that a public entity disclose, on an interim and annual basis, significant segment expense categories and amounts that are regularly provided to its chief operating decision maker (CODM) and included in each reported measure of segment profit or loss. An entity must also disclose, by reportable segment, the amount and composition of other expenses. The standard requires an entity disclose the title and position of its CODM and explain how the CODM uses these reported measures in assessing segment performance and determining how to allocate resources.

Convertible Instruments Beginning with 2022 interim reporting, we adopted, through retrospective application, ASU No. 2020-06, “Debt - Debt with Conversion and Other Options (Subtopic 470-20) and Derivatives and Hedging - Contracts in Entity’s Own Equity (Subtopic 815-40): Accounting for Convertible Instruments and Contracts in an Entity’s Own Equity” (ASU 2020-06). ASU 2020-06 requires that instruments which may be settled in cash or stock are presumed settled in stock in calculating diluted earnings per share. Prior to the April 2023 repurchase, settlement of our Series A Cumulative Perpetual Membership Interests in AT&T Mobility II LLC (Mobility preferred interests) could have resulted in additional dilutive impact, the magnitude of which was influenced by the fair value of the Mobility preferred interests and the average AT&T common stock price during the reporting period, which varied from period-to-period (see Note 16).

Disaggregation of Income Statement Expenses In November 2024, the FASB issued ASU No. 2024-03, “Income Statement - Reporting Comprehensive Income - Expense Disaggregation Disclosures (Subtopic 220-40): Disaggregation of Income Statement Expenses” (ASU 2024-03), which requires that a public entity disclose the amounts of (a) purchases of inventory, (b) employee compensation, (c) depreciation and (d) intangible asset amortization included in each relevant expense caption presented on the face of the income statement. The standard also requires an entity to disclose a qualitative description of the amounts remaining in relevant expense captions that are not separately disaggregated quantitatively as well as disclose the total

amount of selling expenses and, annually, the entity's definition of selling expenses. ASU 2024-03 will be effective for annual periods beginning after December 15, 2026, with either retrospective or prospective application. The standard allows for early adoption of these requirements; we are currently evaluating the disclosure impacts of our adoption.

Internal-Use Software In September 2025, the FASB issued ASU No. 2025-06, Intangibles - Goodwill and Other - Internal-Use Software (Subtopic 350-40): Targeted Improvements to the Accounting for Internal-Use Software (ASU 2025-06). ASU 2025-06 removes references to prescriptive and sequential software development stages and requires software cost capitalization when management has authorized and committed to funding, and it is probable that the project will be completed, and the software used for its intended function. ASU 2025-06 will be effective for annual reporting periods beginning after December 15, 2027. We are evaluating the impacts of our adoption of ASU 2025-06 and currently do not expect that it will have a material impact on our financial statements.

Accounting Policies

Income Taxes We record deferred income taxes for temporary differences between the carrying amounts of assets and liabilities for financial reporting purposes and the computed tax basis of those assets and liabilities. We record valuation allowances against the deferred tax assets (included, together with our deferred income tax assets, as part of our reportable net deferred income tax liabilities on our consolidated balance sheets), for which the realization is uncertain. We review these items regularly in light of changes in federal, state and foreign tax laws and changes in our business.

On July 4, 2025, the One Big Beautiful Bill Act was enacted, which restores or makes permanent certain expiring business tax provisions from the Tax Cuts and Jobs Act of 2017. As a result of the legislation, we reduced our taxable income position in 2025. The legislation did not materially impact our income tax expense, but we expect it will result in a material decrease to cash taxes paid relative to our expectations. (See Note 13)

Cash and Cash Equivalents Cash and cash equivalents include all highly liquid investments with original maturities of three months or less. The carrying amounts approximate fair value. At December 31, 2025, we held \$3,521 in cash and \$14,713 in money market funds and other cash equivalents. Of our total cash and cash equivalents, \$1,330 resided in foreign jurisdictions, some of which is subject to restrictions on repatriation.

Allowance for Credit Losses We record expense to maintain an allowance for credit losses for estimated losses that result from the failure or inability of our customers to make required payments deemed collectible from the customer when the service was provided or product was delivered. When determining the allowances for trade receivables and loans, we consider the probability of recoverability of accounts receivable based on past experience, taking into account current collection trends and general economic factors, including bankruptcy rates. We also consider future economic trends to estimate expected credit losses over the lifetime of the asset. Credit risks are assessed based on historical write-offs, net of recoveries, as well as an analysis of the aged accounts receivable balances with allowances generally increasing as the receivable ages. Accounts receivable may be fully reserved for when specific collection issues are known to exist, such as catastrophes or pending bankruptcies.

Inventories Inventories primarily consist of wireless devices and accessories and are valued at the lower of cost or net realizable value.

Property, Plant and Equipment Property, plant and equipment is stated at cost, except for assets acquired through business combinations, which are initially recorded at fair value. The cost of additions and substantial improvements to property, plant and equipment is capitalized, and includes internal compensation costs for these projects. The cost of maintenance and repairs of property, plant and equipment is charged to operating expenses. Property, plant and equipment costs are depreciated using straight-line methods over their estimated economic lives. Certain subsidiaries follow composite group depreciation methodology. Accordingly, when a portion of their depreciable property, plant and equipment is retired in the ordinary course of business, the gross book value is reclassified to accumulated depreciation, and no gain or loss is recognized on the disposition of these assets.

Property, plant and equipment is reviewed for recoverability whenever events or changes in circumstances indicate that the carrying amount of an asset group may not be recoverable. We recognize an impairment loss when the carrying amount of a long-lived asset is not recoverable. The carrying amount of a long-lived asset is not recoverable if it exceeds the sum of the undiscounted cash flows expected to result from the use and eventual disposition of the asset. (See Note 7)

The liability for the fair value of an asset retirement obligation is recorded in the period in which it is incurred if a reasonable estimate of fair value can be made. In periods subsequent to initial measurement, we recognize period-to-period changes in the

liability resulting from the passage of time and revisions to either the timing or the amount of the original estimate. The increase in the carrying value of the associated long-lived asset is depreciated over the corresponding estimated economic life.

Software Costs We capitalize certain costs incurred in connection with developing or obtaining internal-use software. Capitalized software costs are included in “Property, Plant and Equipment – Net” on our consolidated balance sheets.

We amortize our capitalized software costs over a three-year to seven-year period, reflecting the estimated period during which these assets will remain in service.

Goodwill and Other Intangible Assets We have the following major classes of intangible assets: goodwill; licenses, which include Federal Communications Commission (FCC) and other wireless licenses; customer lists and relationships; and trademarks, trade names and various other finite-lived intangible assets (see Note 9).

Goodwill represents the excess of consideration paid over the fair value of identifiable net assets acquired in business combinations.

Wireless licenses provide us with the exclusive right to utilize certain radio frequency spectrum to provide wireless communications services. While wireless licenses are issued for a fixed period of time (generally 10 years), renewals of domestic wireless licenses have occurred routinely and at nominal cost. We have determined that there are currently no legal, regulatory, contractual, competitive, economic or other factors that limit the useful lives of our FCC wireless licenses. Cash paid, including spectrum deposits (net of refunds), capitalized interest, and any payments for incentive and relocation costs are included in “Acquisitions, net of cash acquired” in our consolidated statements of cash flows. Interest is capitalized until the spectrum is ready for its intended use.

We amortize our wireless licenses in Mexico over their average remaining economic life of 25 years.

We acquired the rights to the AT&T and other trade names in previous acquisitions, classifying certain of those trade names as indefinite-lived. We have the effective ability to retain these exclusive rights permanently at a nominal cost.

Goodwill, FCC wireless licenses and other indefinite-lived intangible assets are not amortized but are tested at least annually for impairment (see Note 9). The testing for Goodwill and other indefinite-lived intangible assets is performed on the value as of October 1 each year and compares the book values of the assets to their fair values. Goodwill is tested by comparing the carrying amount of each reporting unit, deemed to be our principal operating segments or one level below them, to the fair value using both discounted cash flow as well as market multiple approaches. Trade names are tested by comparing their book values to their fair values calculated using a discounted cash flow approach on a presumed royalty rate derived from the revenues related to each brand name.

For FCC wireless licenses, we have the option to first perform a qualitative assessment to determine whether it is more likely than not that the book value exceeds their fair value. We consider several factors under the qualitative assessment, including macroeconomic conditions, industry and regulatory considerations, recent and projected performance of the business and the prior quantitative impairment testing results. On a periodic basis, or if the qualitative assessment indicates potential impairment, we perform a quantitative impairment test on the value as of October 1. FCC wireless licenses are tested on an aggregate basis, consistent with our use of the licenses on a national scope, using a discounted cash flow approach. We last performed a quantitative test in 2024.

Intangible assets that have finite useful lives are amortized over their estimated economic lives (see Note 9). Customer lists and relationships are amortized using primarily the sum-of-the-months-digits method of amortization over the period in which those relationships are expected to contribute to our future cash flows. Finite-lived trademarks and trade names are amortized using the straight-line method over the estimated useful life of the assets. The remaining finite-lived intangible assets are generally amortized using the straight-line method. These assets, along with other long-lived assets, are reviewed for recoverability whenever events or changes in circumstances indicate that the carrying amount of an asset group may not be recoverable.

Advertising Costs We expense advertising costs for products and services or for promoting our corporate image as incurred (see Note 23).

Foreign Currency Translation Our foreign subsidiaries and foreign investments generally report their earnings in their local currencies. We translate their foreign assets and liabilities at exchange rates in effect at the balance sheet dates. We translate their revenues and expenses using average rates during the year. The resulting foreign currency translation adjustments are recorded as a separate component of accumulated OCI on our consolidated balance sheets (see Note 3).

Pension and Other Postretirement Benefits See Note 14 for a comprehensive discussion of our pension and postretirement benefits, including a discussion of the actuarial assumptions, our policy for recognizing the associated gains and losses and our method used to estimate service and interest cost components.

NOTE 2. EARNINGS PER SHARE

A reconciliation of the numerators and denominators of basic and diluted earnings per share is shown in the table below:

Year Ended December 31,	2025	2024	2023
Numerators			
Numerator for basic earnings per share:			
Net Income Attributable to Common Stock	\$ 21,889	\$ 10,746	\$ 14,192
Dilutive potential common shares:			
Mobility preferred interests	—	—	72
Share-based compensation	12	—	13
Numerator for diluted earnings per share	\$ 21,901	\$ 10,746	\$ 14,277
Denominators (000,000)			
Denominator for basic earnings per share:			
Weighted average number of common shares outstanding	7,169	7,199	7,181
Dilutive potential common shares:			
Mobility preferred interests (in shares)	—	—	71
Share-based compensation (in shares)	10	5	6
Denominator for diluted earnings per share	7,179	7,204	7,258

On April 5, 2023, we repurchased all of our Mobility preferred interests (see Note 16). For periods prior to repurchase, under ASU 2020-06, the ability to settle the Mobility preferred interests in stock was reflected in our diluted earnings per share calculation (see Note 1).

NOTE 3. OTHER COMPREHENSIVE INCOME

Changes in the balances of each component included in accumulated OCI are presented below. All amounts are net of tax and exclude noncontrolling interest.

	Foreign Currency Translation Adjustment	Net Unrealized Gains (Losses) on Securities	Net Unrealized Gains (Losses) on Derivative Instruments	Defined Benefit Postretirement Plans	Accumulated Other Comprehensive Income
Balance as of December 31, 2022	\$ (1,800)	\$ (90)	\$ (1,998)	\$ 6,654	\$ 2,766
Other comprehensive income (loss) before reclassifications	463	22	922	32	1,439
Amounts reclassified from accumulated OCI	— ¹	11 ¹	47 ²	(1,963) ³	(1,905)
Net other comprehensive income (loss)	463	33	969	(1,931)	(466)
Balance as of December 31, 2023	(1,337)	(57)	(1,029)	4,723	2,300
Other comprehensive income (loss) before reclassifications	(545)	(19)	380	—	(184)
Amounts reclassified from accumulated OCI	127 ¹	30 ¹	45 ²	(1,523) ³	(1,321)
Net other comprehensive income (loss)	(418)	11	425	(1,523)	(1,505)
Balance as of December 31, 2024	(1,755)	(46)	(604)	3,200	795
Other comprehensive income (loss) before reclassifications	354	15	(650)	—	(281)
Amounts reclassified from accumulated OCI	— ¹	3 ¹	45 ²	(1,422) ³	(1,374)
Net other comprehensive income (loss)	354	18	(605)	(1,422)	(1,655)
Balance as of December 31, 2025	\$ (1,401)	\$ (28)	\$ (1,209)	\$ 1,778	\$ (860)

¹ (Gains) losses are included in “Other income (expense) – net” in the consolidated statements of income.

² (Gains) losses are primarily included in “Interest expense” in the consolidated statements of income (see Note 12).

³ The amortization of prior service credits associated with postretirement benefits is included in “Other income (expense) – net” in the consolidated statements of income (see Note 14).

NOTE 4. SEGMENT INFORMATION

Our segments are comprised of strategic business units or other operations that offer products and services to different customer segments over various technology platforms and/or in different geographies that are managed accordingly. We have two reportable segments: Communications and Latin America.

Our chief operating decision maker (CODM) is our Chief Executive Officer and President. Our CODM uses operating income to evaluate performance and allocate resources, including capital allocations, when managing the business. Our CODM manages operations through the review of actual and forecasted “Operations and Support Expenses” information at a segment and business unit level, with Communications and Latin America segments primarily evaluated on a direct cost basis and comprised of equipment, compensation, network and technology, sales, advertising and other costs.

Additionally, business unit expenses within the Communications segment include direct and shared costs. Direct costs are incurred in support of products and services offered by the business units, such as equipment costs (predominantly wireless devices), network access, rents, leases, sales support, customer provisioning and commission expenses. Shared costs amongst the business units generally include information technology, network engineering and construction costs, advertising and other general and administrative expense.

The **Communications segment** provides wireless and wireline telecom and broadband services to consumers located in the United States and businesses globally. Our business strategies reflect integrated product offerings that cut across product lines and utilize shared assets. This segment contains the following business units:

- **Mobility** provides nationwide wireless service and equipment.
- **Business Wireline** provides advanced ethernet-based fiber services, fixed wireless services, IP Voice and managed professional services, as well as legacy voice and data services and related equipment, to business customers.
- **Consumer Wireline** provides broadband services, including fiber connections that provide multi-gig services, and our fixed wireless access product (AT&T Internet Air or “AIA”) that provides internet services delivered over our 5G wireless network, to residential customers in select locations. Consumer Wireline also provides legacy telephony voice communication services.

The **Latin America segment** provides wireless service and equipment in Mexico.

Corporate and *Other* reconciles our segment results to consolidated operating income and income before income taxes.

Corporate includes:

- *DTV-related retained costs*, which are costs previously allocated to the Video business that were retained after the transaction, net of reimbursements from DIRECTV Entertainment Holdings, LLC (DIRECTV) under transition service agreements. With the sale of our remaining interest in DIRECTV, we will no longer report these costs in 2026 (see Note 10).
- *Parent administration support*, which includes costs borne by AT&T where the business units do not influence decision making.
- *Securitization fees* associated with our sales of receivables (see Note 17).
- *Value portfolio*, which are businesses no longer integral to our operations or which we no longer actively market.

Other items consist of:

- *Certain significant items*, which includes items associated with the merger and integration of acquired or divested businesses, including amortization of intangible assets, employee separation charges associated with voluntary and/or strategic offers, asset impairments and abandonments and restructuring, and other items for which the segments are not being evaluated.

“Interest expense” and “Other income (expense) – net” are managed only on a total company basis and are, accordingly, reflected only in consolidated results.

For the year ended December 31, 2025

	Revenues	Operations and Support Expenses	Depreciation and Amortization	Operating Income (Loss)
Communications				
Mobility	\$ 89,482	\$ 51,864	\$ 10,422	\$ 27,196
Business Wireline	17,231	12,213	5,834	(816)
Consumer Wireline	14,183	8,933	3,703	1,547
Total Communications	120,896	73,010	19,959	27,927
Latin America	4,379	3,563	671	145
Segment Total	125,275	76,573	20,630	28,072
Corporate and Other				
Corporate:				
DTV-related retained costs	—	225	200	(425)
Parent administration support	(1)	1,737	18	(1,756)
Securitization fees	115	702	—	(587)
Value portfolio	259	50	—	209
Total Corporate	373	2,714	218	(2,559)
Certain significant items	—	1,313	38	(1,351)
Total Corporate and Other	373	4,027	256	(3,910)
AT&T Inc.	\$ 125,648	\$ 80,600	\$ 20,886	\$ 24,162

AT&T Inc.

Dollars in millions except per share amounts

For the year ended December 31, 2024

	Revenues	Operations and Support Expenses	Depreciation and Amortization	Operating Income (Loss)
Communications				
Mobility	\$ 85,255	\$ 48,724	\$ 10,217	\$ 26,314
Business Wireline	18,819	13,352	5,555	(88)
Consumer Wireline	13,578	9,048	3,661	869
Total Communications	117,652	71,124	19,433	27,095
Latin America	4,232	3,535	657	40
Segment Total	121,884	74,659	20,090	27,135
Corporate and Other				
Corporate:				
DTV-related retained costs	—	465	414	(879)
Parent administration support	(2)	1,722	6	(1,730)
Securitization fees	116	628	—	(512)
Value portfolio	338	102	17	219
Total Corporate	452	2,917	437	(2,902)
Certain significant items	—	5,131	53	(5,184)
Total Corporate and Other	452	8,048	490	(8,086)
AT&T Inc.	\$ 122,336	\$ 82,707	\$ 20,580	\$ 19,049

For the year ended December 31, 2023

	Revenues	Operations and Support Expenses	Depreciation and Amortization	Operating Income (Loss)
Communications				
Mobility	\$ 83,982	\$ 49,604	\$ 8,517	\$ 25,861
Business Wireline	20,883	14,217	5,377	1,289
Consumer Wireline	13,173	9,053	3,469	651
Total Communications	118,038	72,874	17,363	27,801
Latin America	3,932	3,349	724	(141)
Segment Total	121,970	76,223	18,087	27,660
Corporate and Other				
Corporate:				
DTV-related retained costs	—	686	586	(1,272)
Parent administration support	(7)	1,416	6	(1,429)
Securitization fees	85	604	—	(519)
Value portfolio	380	99	22	259
Total Corporate	458	2,805	614	(2,961)
Certain significant items	—	1,162	76	(1,238)
Total Corporate and Other	458	3,967	690	(4,199)
AT&T Inc.	\$ 122,428	\$ 80,190	\$ 18,777	\$ 23,461

The following table is a reconciliation of Segment Operating Income to “Income Before Income Taxes” reported in our consolidated statements of income:

For the years ended December 31,	2025	2024	2023
Communications	\$ 27,927	\$ 27,095	\$ 27,801
Latin America	145	40	(141)
Segment Operating Income	28,072	27,135	27,660
Reconciling Items:			
Corporate	(2,559)	(2,902)	(2,961)
Transaction, legal and other costs	(627)	(123)	(98)
Amortization of intangibles acquired	(38)	(53)	(76)
Asset impairments and abandonments and restructuring	(838)	(5,075)	(1,193)
Benefit-related gains (losses)	152	67	129
AT&T Operating Income	24,162	19,049	23,461
Interest expense	6,804	6,759	6,704
Equity in net income of affiliates	1,895	1,989	1,675
Other income (expense) – net	7,754	2,419	1,416
Income Before Income Taxes	\$ 27,007	\$ 16,698	\$ 19,848

The following table sets forth revenues earned from customers, and property, plant and equipment located in different geographic areas:

At or for the years ended December 31,	2025		2024		2023	
	Revenues	Net Property, Plant & Equipment	Revenues	Net Property, Plant & Equipment	Revenues	Net Property, Plant & Equipment
United States	\$ 120,219	\$ 128,181	\$ 116,882	\$ 125,573	\$ 117,097	\$ 124,387
Mexico	4,428	3,097	4,286	2,981	3,993	3,750
Asia/Pacific Rim	395	68	462	82	521	99
Europe	382	126	441	139	504	166
Latin America	110	54	149	60	194	67
Other	114	33	116	36	119	20
Total	\$ 125,648	\$ 131,559	\$ 122,336	\$ 128,871	\$ 122,428	\$ 128,489

The following table presents assets, investments in equity affiliates and capital expenditures by segment:

At or for the years ended December 31,	2025			2024		
	Investments in Equity Method Capital			Investments in Equity Method Capital		
	Assets	Investees	Expenditures	Assets	Investees	Expenditures
Communications	\$ 500,244	\$ —	\$ 19,588	\$ 481,757	\$ —	\$ 19,335
Latin America	9,460	—	276	7,808	—	269
Corporate and eliminations	(89,506)	1,106	978	(94,770)	295	659
Total	\$ 420,198	\$ 1,106	\$ 20,842	\$ 394,795	\$ 295	\$ 20,263

NOTE 5. REVENUE RECOGNITION

We report our revenues net of sales taxes and record certain regulatory fees, primarily Universal Service Fund (USF) fees, on a net basis. No customer accounted for more than 10% of consolidated revenues in 2025, 2024 or 2023.

We offer service-only contracts and contracts that bundle equipment used to access the services and/or with other service offerings. Some contracts have fixed terms and others are cancelable on a short-term basis (i.e., month-to-month arrangements).

Examples of service revenues include wireless, fiber and other advanced connectivity, transitional and legacy voice and data. These services represent a series of distinct services that is considered a separate performance obligation. Service revenue is recognized when services are provided, based upon either period of time (e.g., monthly service fees) or usage (e.g., bytes of data processed).

Some of our services require customer premises equipment that, when combined and integrated with AT&T's specific network infrastructure, facilitates the delivery of service to the customer. In evaluating whether the equipment is a separate performance obligation, we consider the customer's ability to benefit from the equipment on its own or together with other readily available resources and if so, whether the service and equipment are separately identifiable (i.e., is the service highly dependent on, or highly interrelated with the equipment). When equipment is a separate performance obligation, we record the sale of equipment when title has passed and the products are accepted by the customer. For devices sold through indirect channels (e.g., national retailers), revenue is recognized when the retailer accepts the device, not upon activation.

Our equipment and service revenues are predominantly recognized on a gross basis, as most of our services do not involve a third party and we typically control the equipment that is sold to our customers.

Revenue recognized from fixed-term contracts that bundle services and/or equipment is allocated based on the standalone selling price of all required performance obligations of the contract (i.e., each item included in the bundle). Promotional discounts are attributed to each required component of the arrangement, resulting in recognition over the contract term. Standalone selling prices are determined by assessing prices paid for service-only contracts (e.g., arrangements where customers bring their own devices) and standalone device pricing.

We offer the majority of our customers the option to purchase certain wireless devices in installments over a specified period of time, and, in many cases, they may be eligible to trade in the original equipment for a new device and have the remaining unpaid balance paid or settled. For customers that elect these equipment installment payment programs, at the point of sale, we recognize revenue for the entire amount of revenue allocated to the customer receivable net of fair value of the trade-in right guarantee, when applicable. The difference between the revenue recognized and the consideration received is recorded as a note receivable when the devices are not discounted and our right to consideration is unconditional. When installment sales include promotional discounts that are earned by customers over the contract term (e.g., "buy one get one free" or equipment discounts with trade-in of a device), notes receivable are recognized net of discounts and the difference between revenue recognized and consideration received is recorded as a contract asset to be amortized over the contract term.

Less commonly, we offer certain customers highly discounted devices when they enter into a minimum service agreement term. For these contracts, we recognize equipment revenue at the point of sale based on a standalone selling price allocation. The difference between the revenue recognized and the cash received is recorded as a contract asset that will amortize over the contract term.

Our contracts allow for customers to frequently modify their arrangement, without incurring penalties in many cases. When a contract is modified, we evaluate the change in scope or price of the contract to determine if the modification should be treated as a new contract or if it should be considered a change of the existing contract. We generally do not have significant impacts from contract modifications.

Revenues from transactions between us and our customers are recorded net of revenue-based regulatory fees and taxes. Cash incentives given to customers are recorded as a reduction of revenue. Nonrefundable, upfront service activation and setup fees associated with service arrangements are deferred and recognized over the associated service contract period or customer relationship life.

Revenue Categories

The following tables set forth reported revenue by category and by business unit:

For the year ended December 31, 2025

	Communications			Latin America	Corporate & Other	Total
	Mobility	Business Wireline	Consumer Wireline			
Wireless service	\$ 67,384	\$ —	\$ —	\$ 2,715	\$ —	\$ 70,099
Fiber and advanced connectivity ¹	—	7,333	8,645	—	—	15,978
Non-fiber consumer broadband	—	—	3,542	—	—	3,542
Legacy and other transitional	—	9,170	1,013	—	179	10,362
Other	—	—	983	—	194	1,177
Total Service	67,384	16,503	14,183	2,715	373	101,158
Equipment	22,098	728	—	1,664	—	24,490
Total	\$ 89,482	\$ 17,231	\$ 14,183	\$ 4,379	\$ 373	\$ 125,648

¹ Advanced connectivity services reported in Business Wireline.

For the year ended December 31, 2024

	Communications			Latin America	Corporate & Other	Total
	Mobility	Business Wireline	Consumer Wireline			
Wireless service	\$ 65,373	\$ —	\$ —	\$ 2,668	\$ —	\$ 68,041
Fiber and advanced connectivity ¹	—	6,969	7,391	—	—	14,360
Non-fiber consumer broadband	—	—	3,821	—	—	3,821
Legacy and other transitional	—	11,095	1,265	—	253	12,613
Other	—	—	1,101	—	199	1,300
Total Service	65,373	18,064	13,578	2,668	452	100,135
Equipment	19,882	755	—	1,564	—	22,201
Total	\$ 85,255	\$ 18,819	\$ 13,578	\$ 4,232	\$ 452	\$ 122,336

¹ Advanced connectivity services reported in Business Wireline.

For the year ended December 31, 2023

	Communications			Latin America	Corporate & Other	Total
	Mobility	Business Wireline	Consumer Wireline			
Wireless service	\$ 63,175	\$ —	\$ —	\$ 2,569	\$ —	\$ 65,744
Fiber and advanced connectivity ¹	—	6,594	6,267	—	—	12,861
Non-fiber consumer broadband	—	—	4,188	—	—	4,188
Legacy and other transitional	—	13,680	1,508	—	294	15,482
Other	—	—	1,210	—	164	1,374
Total Service	63,175	20,274	13,173	2,569	458	99,649
Equipment	20,807	609	—	1,363	—	22,779
Total	\$ 83,982	\$ 20,883	\$ 13,173	\$ 3,932	\$ 458	\$ 122,428

¹ Advanced connectivity services reported in Business Wireline.

Deferred Customer Contract Acquisition and Fulfillment Costs

Costs to acquire and fulfill customer contracts, including commissions on service activations, for our Mobility, Business Wireline and Consumer Wireline services, are deferred and amortized over the contract period or expected customer relationship life, which typically ranges from three years to five years.

The following table presents the deferred customer contract acquisition and fulfillment costs included on our consolidated balance sheets at December 31:

<i>Consolidated Balance Sheets</i>	2025	2024
Deferred Acquisition Costs		
Prepaid and other current assets	\$ 3,550	\$ 3,239
Other Assets	4,778	4,177
Total deferred customer contract acquisition costs	\$ 8,328	\$ 7,416
Deferred Fulfillment Costs		
Prepaid and other current assets	\$ 1,862	\$ 2,101
Other Assets	2,864	3,289
Total deferred customer contract fulfillment costs	\$ 4,726	\$ 5,390

The following table presents deferred customer contract acquisition and fulfillment cost amortization, which are primarily included in "Selling, general and administrative" and "Other cost of revenues," respectively, for the years ended December 31:

<i>Consolidated Statements of Income</i>	2025	2024
Deferred acquisition cost amortization	\$ 3,837	\$ 3,667
Deferred fulfillment cost amortization	2,279	2,525

Contract Assets and Liabilities

A contract asset is recorded when revenue is recognized in advance of our right to bill and receive consideration. The contract asset will decrease as services are provided and billed. For example, when installment sales include promotional discounts (e.g., trade-in device credits) the difference between revenue recognized and consideration received is recorded as a contract asset to be amortized over the contract term.

Our contract assets primarily relate to our wireless businesses. Promotional equipment sales where we offer handset credits, which are allocated between equipment and service in proportion to their standalone selling prices, when customers commit to a specified service period result in additional contract assets recognized. These contract assets will amortize over the service contract period, resulting in lower future service revenue.

When consideration is received in advance of the delivery of goods or services, a contract liability is recorded. Reductions in the contract liability will be recorded as we satisfy the performance obligations.

The following table presents contract assets and liabilities on our consolidated balance sheets at December 31:

<i>Consolidated Balance Sheets</i>	2025	2024
Contract asset	\$ 7,816	\$ 6,855
Current portion in "Prepaid and other current assets"	4,131	3,845
Contract liability	4,409	4,272
Current portion in "Advanced billings and customer deposits"	4,136	3,981

Our beginning of period contract liabilities recorded as customer contract revenue during 2025 was \$3,981.

Remaining Performance Obligations

Remaining performance obligations represent services we are required to provide to customers under bundled or discounted arrangements, which are satisfied as services are provided over the contract term. In determining the transaction price allocated, we do not include non-recurring charges and estimates for usage, nor do we consider arrangements with an original expected duration of less than one year, which are primarily prepaid wireless and residential internet agreements.

Remaining performance obligations associated with business contracts reflect recurring charges billed, adjusted to reflect estimates for sales incentives and revenue adjustments. Performance obligations associated with wireless contracts are estimated using a portfolio approach in which we review all relevant promotional activities, calculating the remaining performance obligation using the average service component for the portfolio and the average device price. As of December 31,

2025, the aggregate amount of the transaction price allocated to remaining performance obligations was \$43,989, of which we expect to recognize approximately 88% by the end of 2027, with the balance recognized thereafter.

NOTE 6. ACQUISITIONS, DISPOSITIONS AND OTHER ADJUSTMENTS

Spectrum Auctions In February 2021, the FCC announced that AT&T was the winning bidder for 1,621 C-Band licenses, comprised of a total of 80 MHz nationwide, including 40 MHz in Phase I. We received the licenses in July 2021 and classified the auction deposits, related capitalized interest and billed relocation costs as “Licenses – Net” on our December 31, 2021 consolidated balance sheet. In December 2021, we paid \$955 of Incentive Payments upon clearing of Phase I spectrum and paid \$2,112 upon clearing of Phase II spectrum in 2023.

Pending Acquisitions

Spectrum On August 25, 2025, we agreed to purchase FCC licenses in the 600 MHz and 3.45 GHz bands from EchoStar Corporation for approximately \$23,000, subject to certain adjustments. The transaction is expected to close in early 2026 and is subject to regulatory approval and other closing conditions. The FCC licenses will be used to expand our 5G network, meet future capacity demands and support future wireless communications services. We signed a short-term spectrum manager lease on the 3.45 GHz spectrum, which was deployed in cell sites covering nearly two-thirds of the U.S. population.

Fiber On May 21, 2025, we agreed to acquire substantially all of Lumen’s Mass Markets fiber business for \$5,750 cash, subject to purchase price adjustments. At the time of signing, the pending acquisition covered approximately one million fiber customers, and also included fiber network assets that reached more than four million fiber locations. On February 2, 2026, we completed the transaction and expect to manage the customer relationships in our Consumer Wireline business and place the fiber network assets in a new, wholly owned subsidiary. We plan to sell a controlling interest in the subsidiary to an equity partner that will co-invest in the ongoing business, and, as such, it is expected to meet the criteria for discontinued operations.

NOTE 7. PROPERTY, PLANT AND EQUIPMENT

Property, plant and equipment is summarized as follows at December 31:

	Lives (years)	2025	2024
Land	-	\$ 1,370	\$ 1,372
Buildings and improvements	2-44	40,674	39,947
Central office equipment ¹	3-10	87,496	101,607
Cable, wiring and conduit	15-50	101,530	95,217
Other equipment	3-20	90,853	87,656
Software	3-7	17,942	17,663
Under construction	-	7,705	7,452
		347,570	350,914
Accumulated depreciation and amortization		216,011	222,043
Property, plant and equipment – net		\$ 131,559	\$ 128,871

¹ Includes certain network software.

Our depreciation expense was \$20,746 in 2025, \$20,421 in 2024 and \$18,593 in 2023. Depreciation expense included amortization of software totaling \$3,209 in 2025, \$3,076 in 2024 and \$3,023 in 2023.

In conjunction with the decommissioning of our copper-based legacy network, we retired approximately \$16,600 of fully depreciated assets that were no longer in use. These assets were primarily related to our network and central offices.

NOTE 8. LEASES

We have operating and finance leases for certain facilities and equipment used in our operations. Our leases generally have remaining lease terms of up to 15 years. Some of our operating leases (e.g., for towers and real estate) contain renewal options that may be exercised, and some of our leases include options to terminate the leases within one year.

We have recognized a right-of-use asset for both operating and finance leases, and a corresponding lease liability that represents the present value of our obligation to make payments over the lease term. The present value of the lease payments is calculated using the incremental borrowing rate for operating and finance leases, which was determined using a portfolio approach based

on the rate of interest that we would have to pay to borrow an amount equal to the lease payments on a collateralized basis over a similar term. We use the unsecured borrowing rate and risk-adjust that rate to approximate a collateralized rate in the currency of the lease, which will be updated on a quarterly basis for measurement of new lease liabilities.

The components of lease expense were as follows:

	2025	2024	2023
Operating lease cost	\$ 5,927	\$ 5,776	\$ 5,577
Finance lease cost:			
Amortization of leased assets in property, plant and equipment	\$ 182	\$ 205	\$ 232
Interest on lease obligation	142	171	184
Total finance lease cost	\$ 324	\$ 376	\$ 416

The following table provides supplemental cash flows information related to leases:

	2025	2024	2023
Cash Flows from Operating Activities			
Cash paid for amounts included in lease obligations:			
Operating cash flows from operating leases	\$ 4,830	\$ 4,757	\$ 4,588
Supplemental Lease Cash Flow Disclosures			
Operating lease right-of-use assets obtained in exchange for new operating lease obligations	5,517	3,762	2,693

The following tables set forth supplemental balance sheet information related to leases at December 31:

	2025	2024
Operating Leases		
Operating lease right-of-use assets	\$ 22,642	\$ 20,909
Accounts payable and accrued liabilities	\$ 3,581	\$ 3,533
Operating lease obligation	18,943	17,391
Total operating lease obligation	\$ 22,524	\$ 20,924
Finance Leases		
Property, plant and equipment, at cost	\$ 2,476	\$ 2,449
Accumulated depreciation and amortization	(1,484)	(1,378)
Property, plant and equipment – net	\$ 992	\$ 1,071
Current portion of long-term debt	\$ 190	\$ 179
Long-term debt	1,192	1,237
Total finance lease obligation	\$ 1,382	\$ 1,416
Weighted-Average Remaining Lease Term (years)		
Operating leases	7.6	7.6
Finance leases	5.3	6.7
Weighted-Average Discount Rate		
Operating leases	4.6 %	4.5 %
Finance leases	8.7 %	8.5 %

The following table provides the expected future minimum maturities of lease obligations:

	Operating Leases	Finance Leases
At December 31, 2025		
2026	\$ 4,956	\$ 309
2027	4,489	316
2028	3,871	324
2029	3,141	333
2030	2,291	275
Thereafter	8,808	204
Total lease payments	27,556	1,761
Less: Imputed interest	(5,032)	(379)
Total	\$ 22,524	\$ 1,382

NOTE 9. GOODWILL AND OTHER INTANGIBLE ASSETS

We test goodwill for impairment at a reporting unit level, which is deemed to be our principal operating segments or one level below, using the methodology described in Note 1. With our annual impairment testing as of October 1, the calculated fair value of each reporting unit exceeded its book value.

Changes to our goodwill in 2024 resulted from a third-quarter noncash goodwill impairment charge of \$4,422 in our consolidated statements of income, which represented the entirety of our Business Wireline reporting unit goodwill. The decline in fair value was primarily due to the change in the long-term strategic plan of our Business Wireline reporting unit, which reflected lower long-term projected future cash flows associated with the industry-wide secular decline, including a faster-than-previously anticipated decline of legacy services.

Our Communications segment has three reporting units: Mobility, Consumer Wireline and Business Wireline. Business Wireline goodwill was fully impaired in 2024. The reporting unit is deemed to be the operating segment for Latin America and its goodwill was fully impaired in 2022. At December 31, 2025, accumulated goodwill impairments totaled \$29,234.

The following table sets forth the changes in the carrying amounts of goodwill for the Communications segment:

	2025			2024		
	Balance at Jan. 1	Dispositions and other	Balance at Dec. 31	Balance at Jan. 1	Impairment	Balance at Dec. 31
Communications						
Goodwill	\$ 91,840	\$ (7)	\$ 91,833	\$ 91,840	\$ —	\$ 91,840
Accumulated Impairments	(28,408)	—	(28,408)	(23,986)	(4,422)	(28,408)
Total	\$ 63,432	\$ (7)	\$ 63,425	\$ 67,854	\$ (4,422)	\$ 63,432

We review amortizing intangible assets for impairment whenever events or circumstances indicate that the carrying amount may not be recoverable over the remaining life of the asset or asset group.

In 2025, we performed a qualitative impairment assessment, which indicated it was more likely than not that the fair value of our FCC wireless licenses exceeded the book value and did not result in an impairment. In 2024, we performed a quantitative impairment assessment, which reflected the fair value of our FCC wireless licenses exceeded their book value.

FCC wireless licenses increased in 2025 primarily due to spectrum acquisitions and capitalized interest. FCC wireless licenses increased in 2024 primarily due to compensable relocation and incentive payments and \$199 of capitalized interest. (See Notes 6 and 23)

Our other intangible assets at December 31 are summarized as follows:

Other Intangible Assets	2025				2024			
	Weighted-Average Life	Gross Carrying Amount	Accumulated Amortization	Currency Translation Adjustment	Gross Carrying Amount	Accumulated Amortization	Currency Translation Adjustment	
Amortized intangible assets:								
Wireless licenses	21.3 years	\$ 3,582	\$ 831	\$ (73)	\$ 2,999	\$ 696	\$ (343)	
Customer lists and relationships	N/A	—	—	—	349	275	(74)	
Trademarks, trade names and other	13.2 years	42	23	(6)	43	23	(6)	
Total	21.2 years	\$ 3,624	\$ 854	\$ (79)	\$ 3,391	\$ 994	\$ (423)	

Indefinite-lived intangible assets not subject to amortization:

Wireless licenses	\$ 125,470	\$ 125,075
Trade names	5,241	5,241
Total	\$ 130,711	\$ 130,316

Amortized intangible assets are definite-life assets, and, as such, we record amortization expense based on a method that most appropriately reflects our expected cash flows from these assets. Amortization expense for definite-life intangible assets was \$140 for the year ended December 31, 2025, \$159 for the year ended December 31, 2024 and \$184 for the year ended December 31, 2023. Estimated amortization expense for the next five years is: \$178 for 2026, \$178 for 2027, \$178 for 2028, \$178 for 2029 and \$176 for 2030.

NOTE 10. EQUITY METHOD INVESTMENTS

Investments in partnerships, joint ventures and less than majority-owned subsidiaries in which we have significant influence are accounted for under the equity method.

Our investments in equity affiliates at December 31, 2025, primarily included our interests in DriveNets and Gigapower. On July 2, 2025, we sold our interest in DIRECTV to TPG Capital (TPG).

DIRECTV Prior to its sale, we accounted for our investment in DIRECTV under the equity method of accounting. DIRECTV was considered a VIE for accounting purposes. As DIRECTV was jointly governed by a board with representation from both AT&T and TPG, with TPG having tie-breaking authority on certain key decisions, most significantly the appointment and removal of the CEO, we concluded that we were not the primary beneficiary of DIRECTV.

Our ownership interest in DIRECTV included \$4,250 of junior preferred interests, an additional distribution preference of \$4,200 and a 70% economic interest in common units.

In third-quarter 2024, our investment in DIRECTV was reduced to zero on our consolidated balance sheet, as a result of aggregate cash receipts exceeding our initial investment balance plus our cumulative equity in DIRECTV earnings. As we were not committed, implicitly or explicitly, to provide financial or other support to DIRECTV, we recorded cash distributions received in excess of our share of DIRECTV's earnings in "Equity in net income of affiliates" in the consolidated statements of income and as cash provided by operations in the consolidated statements of cash flows.

Prior to sale, during 2025, 2024 and 2023, we recognized \$1,926, \$2,027 and \$1,666 of equity in net income of affiliates and received total distributions of \$1,926, \$2,955 and \$3,715, respectively, from DIRECTV. The book value of our investment in DIRECTV was \$0 at December 31, 2025 and 2024.

Upon the sale of our interests in DIRECTV in July 2025, we recorded a current note receivable of approximately \$3,600 and a long-term receivable of \$500. The disposition of DIRECTV also resulted in the release of approximately \$2,900 of historical deferred tax liabilities. We recorded a gain on the sale of DIRECTV of approximately \$5,600, which includes the impact of the transfer of deferred tax liabilities, indemnification liabilities and unfavorable contracts, in "Other income (expense) – net" in the

consolidated statements of income in 2025. As of December 31, 2025, we have received \$3,100 of cash on the current note receivable, which was included in “Dispositions” in the consolidated statements of cash flows.

DriveNets We hold a 16.6% interest in DriveNets, which designs and builds high-scale networking solutions for service providers and AI infrastructures.

Gigapower We hold a 50% interest in our joint venture Gigapower, LLC (Gigapower), which provides a fiber network in select areas to internet service providers and other businesses across the United States.

SKY Mexico In June 2024, we sold our 41.3% interest in SKY Mexico, a leading pay-TV provider in Mexico.

The following table is a reconciliation of our investments in equity affiliates as presented on our consolidated balance sheets:

	2025	2024
Beginning of year	\$ 295	\$ 1,251
Additional investments	819	117
Distributions from DIRECTV in excess of cumulative equity in earnings	—	(928)
Dividends and distributions of cumulative earnings received	(1,937)	(2,033)
Equity in net income of affiliates	1,895	1,989
Impairments	—	(155)
Other adjustments	34	54
End of year	\$ 1,106	\$ 295

NOTE 11. DEBT

Long-term debt of AT&T and its subsidiaries, including interest rates and maturities, is summarized as follows at December 31:

	2025	2024
Notes and debentures		
Interest Rates ¹		
0.00% – 2.99%	2025 – 2033	
	\$ 22,240	\$ 21,860
3.00% – 4.99%	2025 – 2061	
	89,379	83,725
5.00% – 6.99%	2025 – 2095	
	29,165	22,679
7.00% – 8.75%	2025 – 2097	
	3,524	3,565
Fair value of interest rate swaps recorded in debt	3	6
	144,311	131,835
Unamortized (discount) premium – net	(9,193)	(9,340)
Unamortized issuance costs	(400)	(379)
Total notes and debentures	134,718	122,116
Finance lease obligations	1,382	1,416
Total long-term debt, including current maturities	136,100	123,532
Current maturities of long-term debt	(9,011)	(5,089)
Total long-term debt	\$ 127,089	\$ 118,443

¹ Foreign debt includes the impact from hedges, when applicable.

We had outstanding Euro, British pound sterling, Canadian dollar, Australian dollar and Swiss franc denominated debt of approximately \$35,307 and \$30,685 at December 31, 2025 and 2024, respectively.

The weighted-average interest rate of our long-term debt portfolio, including credit agreement borrowings and the impact of derivatives, was approximately 4.2% as of December 31, 2025 and 2024.

Our long-term debt maturing within one year was \$9,011 and \$5,089 at December 31, 2025 and 2024, respectively. We had no outstanding commercial paper or other short-term borrowings as of December 31, 2025 and 2024.

Financing Activities

During 2025, we received net proceeds of \$14,027 on the issuance of \$14,111 in long-term debt, with an average weighted maturity of approximately 12.3 years and a weighted average interest rate of 5.0%. We repaid \$5,399 of long-term debt with a weighted average interest rate of 4.7%. Our debt activity during 2025 primarily consisted of the following:

	First Quarter	Second Quarter	Third Quarter	Fourth Quarter	Full Year 2025
Issuance of notes and debentures:					
USD notes	\$ —	\$ 3,473	\$ 4,959	\$ —	\$ 8,432
EUR notes	2,956	—	2,639	—	5,595
Debt issuances	\$ 2,956	\$ 3,473	\$ 7,598	\$ —	\$ 14,027
Repayments:					
USD notes	\$ —	\$ —	\$ —	\$ (145)	\$ (145)
EUR notes	(1,321)	(32)	—	(2,441)	(3,794)
CAD notes	—	—	—	(960)	(960)
Other	(205)	(62)	(229)	(133)	(629)
Repayments of long-term debt	\$ (1,526)	\$ (94)	\$ (229)	\$ (3,679)	\$ (5,528)

As of December 31, 2025 and 2024, we were in compliance with all covenants and conditions of instruments governing our debt. Substantially all of our outstanding long-term debt is unsecured. Maturities of outstanding long-term notes and debentures, as of December 31, 2025, and the corresponding weighted-average interest rate scheduled for repayment are as follows:

	2026	2027	2028	2029	2030	Thereafter
Debt repayments ^{1,2}	\$ 8,652	\$ 8,953	\$ 6,905	\$ 6,918	\$ 7,020	\$106,216
Weighted-average interest rate ²	3.1%	3.8%	3.2%	4.6%	4.3%	4.3%

¹ Debt repayments represent maturity value. Foreign debt includes the impact from hedges, when applicable.

² Includes credit agreement borrowings.

On February 5, 2026, we issued \$6,500 principal amount of global notes due 2031 to 2056 with a weighted average coupon of 5.2%. We intend to use the net proceeds from this issuance for general corporate purposes, which may include debt repayments and pending acquisitions.

Credit Facilities*General*

On November 3, 2025, we entered into (i) a \$12,000 Second Amended and Restated Credit Agreement (Revolving Credit Agreement), with Citibank, N.A., as agent, amending and restating our existing \$12,000 Amended and Restated Credit Agreement, dated as of November 18, 2022, and (ii) a \$17,500 Delayed Draw Term Loan Credit Agreement (Term Loan), with Bank of America, N.A., as agent. No amount was outstanding under either the Revolving Credit Agreement or the Term Loan as of December 31, 2025.

The Revolving Credit Agreement and the Term Loan contain covenants that are customary for an issuer with investment grade senior debt credit ratings, including a net debt-to-EBITDA financial ratio covenant requiring us to maintain, as of the last day of each fiscal quarter, a ratio of not more than 3.75 to 1.

The events of default under the Revolving Credit Agreement and the Term Loan are customary for agreements of this type and such events would result in the acceleration of, or permit the requisite lenders to accelerate, as applicable, required payments under the relevant agreement and could increase the applicable margin under the relevant agreement by 2.00% per annum.

Revolving Credit Agreement

Advances under the Revolving Credit Agreement denominated in U.S. dollars will bear interest, at our option, either:

- at a variable annual rate equal to: (1) the highest of (but not less than zero) (a) the rate of interest announced publicly by Citibank in New York, New York, from time to time, as Citibank's base rate, (b) 0.5% per annum above the federal funds rate, and (c) the forward-looking term rate based on the secured overnight financing rate (Term SOFR) for a period of one

month plus 1.00%, plus (2) an applicable margin, as set forth in the Revolving Credit Agreement (Applicable Margin for Base Advances); or

- at a rate equal to: (i) Term SOFR for a period of one, three or six months, as applicable, plus (ii) an applicable margin, as set forth in the Revolving Credit Agreement (Applicable Margin for Benchmark Rate Revolving Advances).

Advances under the Revolving Credit Agreement denominated in Euro will bear interest at the Euro Interbank Offered Rate (EURIBOR) plus the Applicable Margin for Benchmark Rate Revolving Advances.

Advances under the Revolving Credit Agreement denominated in Sterling will bear interest at the Sterling Overnight Index Average (SONIA) plus the Applicable Margin for Benchmark Rate Revolving Advances.

The Applicable Margin for Benchmark Rate Revolving Advances will be equal to 0.690%, 0.805%, 0.920% or 1.045% per annum depending on our senior unsecured long-term debt ratings. The Applicable Margin for Base Rate Revolving Advances will be equal to the greater of (x) 0.00% and (y) the relevant Applicable Margin for Benchmark Rate Revolving Advances minus 1.00% per annum, depending on our senior unsecured long-term debt ratings.

We will also pay a facility fee of 0.06%, 0.07% or 0.08% per annum of the amount of the lender commitments, depending on AT&T's credit rating under the Revolving Credit Agreement.

The obligations of the lenders under the Revolving Credit Agreement to provide advances to us will terminate on November 3, 2030, unless the commitments are terminated in whole prior to that date. All advances must be repaid no later than the date on which lenders are no longer obligated to make any advances under the Revolving Credit Agreement.

The Revolving Credit Agreement provides that we and the lenders representing more than 50% of the facility amount may agree to extend their commitments under the Revolving Credit Agreement for two one-year periods beyond the initial termination date. We have the right to terminate, in whole or in part, amounts committed by the lenders under the Revolving Credit Agreement in excess of any outstanding advances; however, any such terminated commitments may not be reinstated.

The proceeds of the advances shall be solely for general corporate purposes.

Delayed Draw Term Loan Credit Agreement

The Term Loan is comprised of (i) a \$6,000 364-day delayed draw term loan facility (364-Day Term Loan Facility) and (ii) a \$11,500 two-year delayed draw term loan facility (Two-Year Term Loan Facility). Each of the 364-Day Term Loan Facility and Two-Year Term Loan Facility is available for a single draw at any time before November 3, 2026. The proceeds of the Term Loan will be used for general corporate purposes, which may include financing acquisitions of additional spectrum.

Advances will bear interest, at our option, either:

- at a variable annual rate (Base Rate) equal to: (1) the highest of (but not less than zero) (a) the prime rate quoted by Bank of America, N.A., (b) 0.5% per annum above the federal funds rate, and (c) the forward-looking SOFR term rate administered by the Chicago Mercantile Exchange (or any successor administrator) and published on the applicable Reuters screen page (or such other commercially available source providing such quotations) (Term SOFR Screen Rate) for a period of one month plus 1.00%, plus (2) an applicable margin, as set forth in the Term Loan (Applicable Margin for Base Rate Term Advances); or
- at a variable annual rate based upon Term SOFR (SOFR Rate) equal to: (1) the Term SOFR Screen Rate with a term equivalent to the applicable interest period of the advance plus (2) an applicable margin, as set forth in the Term Loan (Applicable Margin for SOFR Rate Term Advances).

The Applicable Margin for SOFR Rate Term Advances will be equal to 0.450%, 0.575%, 0.825%, 0.950% and 1.075% per annum for the 364-Day Term Loan Facility and 0.550%, 0.675%, 0.925%, 1.050% and 1.175% per annum for the Two-Year Term Loan Facility, in each case, depending on our senior unsecured long-term debt ratings. The Applicable Margin for Base Rate Term Advances under the Term Loan will be equal to the greater of (x) 0.00% and (y) the relevant Applicable Margin for SOFR Rate Term Advances minus 1.00% per annum, depending on our unsecured long-term debt ratings.

Commencing March 3, 2026, we will also pay a fee of 0.05%, 0.06%, 0.07%, 0.08% or 0.10% per annum of the amount of unused lender commitments, depending on our senior unsecured long-term debt ratings.

The Term Loan is not subject to amortization, and the entire principal amount of (i) the 364-Day Term Loan Facility will be due and payable 364 days after the date on which the borrowing is made and (ii) the Two-Year Term Loan Facility will be due and payable two years after the date on which the borrowing is made.

NOTE 12. FAIR VALUE MEASUREMENTS AND DISCLOSURE

The Fair Value Measurement and Disclosure framework in ASC 820, “Fair Value Measurement,” provides a three-tiered fair value hierarchy based on the reliability of the inputs used to determine fair value. Level 1 refers to fair values determined based on quoted prices in active markets for identical assets. Level 2 refers to fair values estimated using significant other observable inputs, and Level 3 includes fair values estimated using significant unobservable inputs.

The level of an asset or liability within the fair value hierarchy is based on the lowest level of any input that is significant to the fair value measurement. Our valuation techniques maximize the use of observable inputs and minimize the use of unobservable inputs.

The valuation methodologies described above may produce a fair value calculation that may not be indicative of future net realizable value or reflective of future fair values. We believe our valuation methods are appropriate and consistent with other market participants. The use of different methodologies or assumptions to determine the fair value of certain financial instruments could result in a different fair value measurement at the reporting date. There have been no changes in the methodologies used since December 31, 2024.

Long-Term Debt and Other Financial Instruments

The carrying amounts and estimated fair values of our long-term debt, including current maturities, and other financial instruments are summarized as follows:

	December 31, 2025		December 31, 2024	
	Carrying Amount	Fair Value	Carrying Amount	Fair Value
Notes and debentures ¹	\$ 134,718	\$ 127,852	\$ 122,116	\$ 114,167
Investment securities ²	1,609	1,609	1,603	1,603

¹ Includes credit agreement borrowings.

² Excludes investments accounted for under the equity method.

The carrying amount of debt with an original maturity of less than one year approximates fair value. The fair value measurements used for notes and debentures are considered Level 2 and are determined using various methods, including quoted prices for identical or similar securities in both active and inactive markets.

Following is the fair value leveling for investment securities that are measured at fair value and derivatives as of December 31, 2025 and December 31, 2024. Derivatives designated as hedging instruments are reflected as “Prepaid and other current assets,”

“Other Assets,” “Accounts payable and accrued liabilities,” and “Other noncurrent liabilities” on our consolidated balance sheets.

	December 31, 2025			
	Level 1	Level 2	Level 3	Total
Equity Securities				
Domestic equities	\$ 566	\$ —	\$ —	\$ 566
International equities	8	—	—	8
Fixed income equities	217	—	—	217
Available-for-Sale Debt Securities	—	587	—	587
Asset Derivatives				
Cross-currency swaps	—	876	—	876
Liability Derivatives				
Cross-currency swaps	—	(2,050)	—	(2,050)
	December 31, 2024			
	Level 1	Level 2	Level 3	Total
Equity Securities				
Domestic equities	\$ 484	\$ —	\$ —	\$ 484
International equities	8	—	—	8
Fixed income equities	178	—	—	178
Available-for-Sale Debt Securities	—	689	—	689
Asset Derivatives				
Cross-currency swaps	—	87	—	87
Liability Derivatives				
Cross-currency swaps	—	(4,163)	—	(4,163)

Investment Securities

Our investment securities include both equity and debt securities that are measured at fair value, as well as equity securities without readily determinable fair values. A substantial portion of the fair values of our investment securities is estimated based on quoted market prices. Investments in equity securities not traded on a national securities exchange are valued at cost, less any impairment, and adjusted for changes resulting from observable, orderly transactions for identical or similar securities. Investments in debt securities not traded on a national securities exchange are valued using pricing models, quoted prices of securities with similar characteristics or discounted cash flows.

The components comprising total gains and losses in the period on equity securities are as follows:

For the years ended December 31,	2025	2024	2023
Total gains (losses) recognized on equity securities	\$ 85	\$ 209	\$ 257
Gains (losses) recognized on equity securities sold	1	(52)	89
Unrealized gains (losses) recognized on equity securities held at end of period	\$ 84	\$ 261	\$ 168

At December 31, 2025, available-for-sale debt securities totaling \$587 have maturities as follows - less than one year: \$13; one to three years: \$125; three to five years: \$183; five or more years: \$266.

Our cash equivalents (money market securities) and short-term investments (certificate and time deposits) are recorded at amortized cost, and the respective carrying amounts approximate fair values. Short-term investments are recorded in “Prepaid and other current assets,” and our investment securities are recorded in “Other Assets” on the consolidated balance sheets.

Derivative Financial Instruments

We enter into derivative transactions to manage certain market risks, primarily interest rate risk and foreign currency exchange risk. This includes the use of interest rate swaps, interest rate locks, foreign exchange forward contracts and combined interest rate foreign exchange contracts (cross-currency swaps). We do not use derivatives for trading or speculative purposes. We

record derivatives on our consolidated balance sheets at fair value that is derived from observable market data, including yield curves and foreign exchange rates (all of our derivatives are Level 2). Cash flows associated with derivative instruments are presented in the same category in the consolidated statements of cash flows as the item being hedged.

Fair Value Hedging Periodically, we enter into and designate fixed-to-floating interest rate swaps as fair value hedges. The purpose of these swaps is to manage interest rate risk by managing our mix of fixed-rate and floating-rate debt. These swaps involve the receipt of fixed-rate amounts for floating interest rate payments over the life of the swaps without exchange of the underlying principal amount.

We also designate most of our cross-currency swaps and foreign exchange contracts as fair value hedges. The purpose of these contracts is to hedge foreign currency risk associated with changes in spot rates on foreign-denominated debt. For cross-currency hedges, we have elected to exclude the change in fair value of the swap related to both time value and cross-currency basis spread from the assessment of hedge effectiveness. For foreign exchange contracts, we have elected to exclude the change in fair value of forward points from the assessment of hedge effectiveness.

Unrealized and realized gains or losses from fair value hedges impact the same category on the consolidated statements of income as the item being hedged, including the earnings impact of excluded components. In instances where we have elected to exclude components from the assessment of hedge effectiveness related to fair value hedges, unrealized gains or losses on such excluded components are recorded as a component of accumulated OCI and recognized into earnings over the life of the hedging instrument. Unrealized gains on derivatives designated as fair value hedges are recorded at fair value as assets, and unrealized losses are recorded at fair market value as liabilities. Except for excluded components, changes in the fair value of derivative instruments designated as fair value hedges are offset against the change in fair value of the hedged assets or liabilities through earnings. In the years ended December 31, 2025 and 2024, no ineffectiveness was measured on fair value hedges.

Cash Flow Hedging We designate some of our cross-currency swaps as cash flow hedges to hedge our exposure to variability in expected future cash flows that are attributable to foreign currency risk and interest rate risk generated from our foreign-denominated debt. These agreements include initial and final exchanges of principal from fixed foreign denominated amounts to fixed U.S. dollar denominated amounts, to be exchanged at a specified rate that is usually determined by the market spot rate upon issuance. They also include an interest rate swap of a fixed or floating foreign denominated interest rate to a fixed U.S. dollar denominated interest rate.

On September 30, 2022, we de-designated most of our cross-currency swaps from cash flow hedges and re-designated these swaps as fair value hedges. The amount remaining in accumulated other comprehensive loss related to cash flow hedges on the de-designation date was \$1,857. The amount will be reclassified to earnings when the hedged item is recognized in earnings or when it becomes probable that the forecasted transactions will not occur. The election of fair value hedge designation for cross-currency swaps does not have an impact on our financial results.

Unrealized gains on derivatives designated as cash flow hedges are recorded at fair value as assets, and unrealized losses are recorded at fair value as liabilities. For derivative instruments designated as cash flow hedges, changes in fair value are reported as a component of accumulated OCI and are reclassified into the consolidated statements of income in the same period the hedged transaction affects earnings.

Periodically, we enter into and designate interest rate locks to partially hedge the risk of changes in interest payments attributable to increases in the benchmark interest rate during the period leading up to the probable issuance of fixed-rate debt. We designate our interest rate locks as cash flow hedges. Gains and losses when we settle our interest rate locks are amortized into income over the life of the related debt. Over the next 12 months, we expect to reclassify \$59 from accumulated OCI to "Interest expense" due to the amortization of net losses on historical interest rate locks.

Collateral and Credit-Risk Contingency We have entered into agreements with our derivative counterparties establishing collateral thresholds based on respective credit ratings and netting agreements. At December 31, 2025, we had posted collateral of \$513 (a deposit asset) and held collateral of \$314 (a receipt liability). Under the agreements, if AT&T's credit rating had been downgraded two ratings levels by Fitch Ratings, one level by S&P and one level by Moody's, before the final collateral exchange in December, we would have been required to post additional collateral of \$49. If AT&T's credit rating had been downgraded three ratings levels by Fitch Ratings, two levels by S&P and two levels by Moody's, we would have been required to post additional collateral of \$1,405. At December 31, 2024, we had posted collateral of \$188 (a deposit asset) and held collateral of \$0 (a receipt liability). We do not offset the fair value of collateral, whether the right to reclaim cash collateral (a receivable) or the obligation to return cash collateral (a payable) exists, against the fair value of the derivative instruments.

Following are the notional amounts of our outstanding derivative positions at December 31:

	2025	2024
Cross-currency swaps	\$ 35,741	\$ 34,884
Total	\$ 35,741	\$ 34,884

Following are the related hedged items affecting our financial position and performance:

Effect of Derivatives in the Consolidated Statements of Income

Fair Value Hedging Relationships			
For the years ended December 31,	2025	2024	2023
Interest rate swaps ("Interest expense"):			
Gain (loss) on interest rate swaps	\$ (3)	\$ (1)	\$ (6)
Gain (loss) on long-term debt	3	1	6
Cross-currency swaps:			
Gain (loss) on cross-currency swaps	3,741	(1,347)	1,121
Gain (loss) on long-term debt	(3,741)	1,347	(1,121)
Gain (loss) recognized in accumulated OCI	(866)	501	1,126
Foreign exchange contracts:			
Gain (loss) on foreign exchange contracts	—	—	12
Gain (loss) on long-term debt	—	—	(12)
Gain (loss) recognized in accumulated OCI	—	—	12

In addition, the net swap settlements that accrued and settled in the periods above were offset against "Interest expense."

Cash Flow Hedging Relationships			
For the years ended December 31,	2025	2024	2023
Cross-currency swaps:			
Gain (loss) recognized in accumulated OCI	\$ —	\$ —	\$ 12
Interest rate locks:			
Interest income (expense) reclassified from accumulated OCI into income	(59)	(59)	(59)

Nonrecurring Fair Value Measurements

In addition to assets and liabilities that are recorded at fair value on a recurring basis, impairment indicators may subject goodwill and long-lived assets to nonrecurring fair value measurements. The implied fair values of the Business Wireline, Consumer Wireline and Mexico reporting units were estimated using both the discounted cash flow as well as market multiple approaches (see Note 9). The inputs to these models are considered Level 3.

NOTE 13. INCOME TAXES

Significant components of our deferred tax liabilities (assets) are as follows at December 31:

	2025	2024
Depreciation and amortization	\$ 37,570	\$ 36,531
Licenses and nonamortizable intangibles	21,742	20,660
Lease right-of-use assets	5,494	5,103
Lease liabilities	(5,464)	(5,107)
Employee benefits	(2,585)	(3,017)
Deferred fulfillment costs	1,657	1,788
Equity in partnership	14	2,716
Net operating loss and other carryforwards	(5,567)	(5,619)
Other – net	1,401	1,466
Subtotal	54,262	54,521
Deferred tax assets valuation allowance	3,978	4,338
Net deferred tax liabilities	\$ 58,240	\$ 58,859
Noncurrent deferred tax liabilities	\$ 58,312	\$ 58,939
Less: Noncurrent deferred tax assets	(72)	(80)
Net deferred tax liabilities	\$ 58,240	\$ 58,859

At December 31, 2025, we had combined net operating and capital loss carryforwards (tax effected) for federal income tax purposes of \$695, state of \$545 and foreign of \$2,227, expiring through 2045. Additionally, we had federal credit carryforwards of \$645 and state credit carryforwards of \$1,454, expiring primarily through 2045.

We recognize a valuation allowance if, based on the weight of available evidence, it is more likely than not that some portion, or all, of a deferred tax asset will not be realized. Our valuation allowances at December 31, 2025 and 2024 related primarily to state and foreign net operating losses and state credit carryforwards.

We consider post-1986 unremitted foreign earnings subjected to the one-time transition tax not to be indefinitely reinvested as such earnings can be repatriated without any significant incremental tax costs. We consider other types of unremitted foreign earnings to be indefinitely reinvested. U.S. income and foreign withholding taxes have not been recorded on temporary differences related to investments in certain foreign subsidiaries as such differences are considered indefinitely reinvested. The amount of unrecognized deferred tax liability does not have a material impact on the financial statements.

We recognize the financial statement effects of a tax return position when it is more likely than not, based on the technical merits, that the position will ultimately be sustained. For tax positions that meet this recognition threshold, we apply our judgment, taking into account applicable tax laws, our experience in managing tax audits and relevant GAAP, to determine the amount of tax benefits to recognize in our financial statements. For each position, the difference between the benefit realized on our tax return and the benefit reflected in our financial statements is recorded on our consolidated balance sheets as an unrecognized tax benefit (UTB). We update our UTBs at each financial statement date to reflect the impacts of audit settlements and other resolutions of audit issues, the expiration of statutes of limitation, developments in tax law and ongoing discussions with taxing authorities.

A reconciliation of the change in our UTB balance from January 1 to December 31 for 2025, 2024 and 2023 is as follows:

Federal, State and Foreign Tax	2025	2024	2023
Balance at beginning of year	\$ 12,533	\$ 11,924	\$ 9,657
Increases for tax positions related to the current year	521	369	1,026
Increases for tax positions related to prior years	294	1,017	448
Decreases for tax positions related to prior years	(124)	(772)	(212)
Lapse of statute of limitations	(13)	(8)	(16)
Settlements	96	3	1,021
Balance at end of year	13,307	12,533	11,924
Accrued interest and penalties	2,604	2,223	1,785
Gross unrecognized income tax benefits	15,911	14,756	13,709
Less: Deferred federal and state income tax benefits	(966)	(849)	(687)
Less: Tax attributable to timing items included above	(7,401)	(6,964)	(6,438)
Total UTB that, if recognized, would impact the effective income tax rate as of the end of the year	\$ 7,544	\$ 6,943	\$ 6,584

Periodically we make deposits to taxing jurisdictions which reduce our UTB balance but are not included in the reconciliation above. The amount of deposits that reduced our UTB balance was \$2,894 at December 31, 2025, \$2,282 at December 31, 2024 and \$2,361 at December 31, 2023. Current tax assets on our consolidated balance sheets were \$2,772 at December 31, 2025, \$2,236 at December 31, 2024 and \$2,079 at December 31, 2023.

Accrued interest and penalties included in UTBs were \$2,604 as of December 31, 2025, \$2,223 as of December 31, 2024 and \$1,785 as of December 31, 2023. We record interest and penalties related to federal, state and foreign UTBs in income tax expense. The net interest and penalty expense included in income tax expense was \$476 for 2025, \$474 for 2024 and \$324 for 2023.

We file income tax returns in the U.S. federal jurisdiction and various state, local and foreign jurisdictions. As a large taxpayer, our income tax returns are regularly audited by the Internal Revenue Service (IRS) and other taxing authorities.

The IRS has completed field examinations of our tax returns through 2015. All audit periods prior to 2006 are closed for federal examination purposes, and we have effectively resolved all outstanding audit issues for years through 2010 with the IRS Appeals Division.

The components of income tax expense (benefit) are as follows:

	2025	2024	2023
Federal:			
Current	\$ 970	\$ 2,769	\$ 2,280
Deferred	2,524	1,289	2,250
	3,494	4,058	4,530
State and local:			
Current	(269)	859	423
Deferred	331	(512)	(832)
	62	347	(409)
Foreign:			
Current	44	68	66
Deferred	21	(28)	38
	65	40	104
Total	\$ 3,621	\$ 4,445	\$ 4,225

“Income Before Income Taxes” in the consolidated statements of income included the following components for the years ended December 31:

	2025	2024	2023
U.S. income before income taxes	\$ 26,993	\$ 16,674	\$ 20,506
Foreign income (loss) before income taxes	14	24	(658)
Total	\$ 27,007	\$ 16,698	\$ 19,848

A reconciliation of income tax expense (benefit) and the amount computed by applying the statutory federal income tax rate of 21% to income before income taxes is as follows:

	2025		2024		2023	
	Amount	Percent	Amount	Percent	Amount	Percent
U.S. federal statutory tax rate	\$ 5,671	21.0 %	\$ 3,507	21.0 %	\$ 4,168	21.0 %
State and local income taxes – net of federal tax effect ^{1,2}	(155)	(0.6)	276	1.6	262	1.3
Foreign tax effects	40	0.2	22	0.1	98	0.5
Effect of change in tax laws or rates enacted current period	—	—	—	—	—	—
Effect of cross-border tax laws	—	—	(19)	(0.1)	(1)	—
Tax credits						
Research and development credit	(139)	(0.5)	(183)	(1.1)	(180)	(0.9)
Other	(5)	—	(7)	—	(5)	—
Changes in valuation allowance	53	0.2	2	—	53	0.3
Nontaxable or nondeductible items:						
Goodwill impairment	—	—	929	5.6	9	—
Noncontrolling interest	(301)	(1.1)	(274)	(1.6)	(259)	(1.3)
Divestiture of DIRECTV	(1,311)	(4.9)	—	—	—	—
Other	(124)	(0.5)	(43)	(0.3)	(157)	(0.8)
Changes in unrecognized tax benefits ²	578	2.1	388	2.3	467	2.4
Other adjustments						
Tax basis adjustments	(592)	(2.2)	—	—	—	—
Other	(94)	(0.3)	(153)	(0.9)	(230)	(1.2)
Effective income tax rate	\$ 3,621	13.4 %	\$ 4,445	26.6 %	\$ 4,225	21.3 %

¹ The states that contribute to the majority (greater than 50%) of the tax effect in this category include California for 2025; Florida, Illinois, Michigan, New York and Texas for 2024; and California and Illinois for 2023. State taxes are impacted by current year earnings, book-tax differences, apportionment methodologies, legislative changes, divestitures, return to accrual adjustments and other permanent book-tax differences.

² Effective January 1, 2025, we adopted ASU 2023-09, which requires the effective tax rate reconciliation to include a distinct category for changes in UTBs. This category must include the tax effects of changes in judgment related to prior-period tax positions, settlements and statute of limitations expirations, aggregated across all tax jurisdictions. Furthermore, in accordance with ASU 2023-09, we have elected to present tax positions taken in the current annual reporting period, aggregated across all tax jurisdictions, within “Changes in unrecognized tax benefits.”

The amounts of cash income taxes paid, net of amounts refunded, are as follows at December 31:

	2025	2024	2023
Federal	\$ 1,219	\$ 2,452	\$ 1,319
State	91	(49)	193
Foreign	43	53	87
Total	\$ 1,353	\$ 2,456	\$ 1,599

NOTE 14. PENSION AND POSTRETIREMENT BENEFITS

We offer noncontributory pension programs covering the majority of domestic nonmanagement employees in our Communications business. Nonmanagement employees' pension benefits are generally calculated using one of two formulas: a flat dollar amount applied to years of service according to job classification, or a cash balance plan with negotiated annual pension band credits as well as interest credits. Most employees can elect to receive their pension benefits in either a lump sum payment or an annuity.

Pension programs covering U.S. management employees are closed to new entrants. These programs continue to provide benefits to participants that were generally hired before January 1, 2015, who receive benefits under either cash balance pension programs that include annual or monthly credits based on salary as well as interest credits, or a traditional pension formula (i.e., a stated percentage of employees' adjusted career income).

We also provide a variety of medical, dental and life insurance benefits to certain retired employees under various plans and accrue actuarially determined postretirement benefit costs as active employees earn these benefits.

In 2023, AT&T and State Street Global Advisors Trust Company, as independent fiduciary of the AT&T Pension Benefit Plan (Plan), entered into a commitment agreement with subsidiaries of Athene Holding Ltd. (Athene) under which AT&T agreed to purchase nonparticipating single premium group annuity contracts that would transfer to Athene \$8,067 of the Plan's defined benefit pension obligations related to certain retirees, participants and beneficiaries under the Plan. This transaction with Athene was considered a settlement for accounting purposes and required us to remeasure our pension plan assets and obligations at quarter-end for the second and third quarters of 2023.

Obligations and Funded Status

For defined benefit pension plans, the benefit obligation is the projected benefit obligation, the actuarial present value, as of our December 31 measurement date, of all benefits attributed by the pension benefit formula to employee service rendered to that date. The amount of benefit to be paid depends on a number of future events incorporated into the pension benefit formula, including estimates of the average life of employees and their beneficiaries and average years of service rendered. It is measured based on assumptions concerning future interest rates and future employee compensation levels as applicable.

For postretirement benefit plans, the benefit obligation is the accumulated postretirement benefit obligation, the actuarial present value as of the measurement date of all future benefits attributed under the terms of the postretirement benefit plans to employee service.

The following table presents the change in the projected benefit obligation for the years ended December 31:

	Pension Benefits		Postretirement Benefits	
	2025	2024	2025	2024
Benefit obligation at beginning of year	\$ 30,944	\$ 33,227	\$ 6,339	\$ 6,693
Service cost - benefits earned during the period	427	487	18	22
Interest cost on projected benefit obligation	1,601	1,586	318	310
Actuarial (gain) loss	629	(1,909)	394	84
Benefits paid, including settlements	(2,957)	(2,447)	(609)	(770)
Plan transfers	(17)	—	17	—
Benefit obligation at end of year	\$ 30,627	\$ 30,944	\$ 6,477	\$ 6,339

The following table presents the change in the fair value of plan assets for the years ended December 31 and the plans' funded status at December 31:

	Pension Benefits		Postretirement Benefits	
	2025	2024	2025	2024
Fair value of plan assets at beginning of year	\$ 27,919	\$ 30,098	\$ 1,144	\$ 1,763
Actual return on plan assets	2,562	265	61	117
Benefits paid, including settlements ¹	(2,957)	(2,447)	(483)	(736)
Contributions	1,153	3	—	—
Fair value of plan assets at end of year	28,677	27,919	722	1,144
Unfunded status at end of year ²	\$ (1,950)	\$ (3,025)	\$ (5,755)	\$ (5,195)

¹ At our discretion, certain postretirement benefits may be paid from our cash accounts, which does not reduce Voluntary Employee Benefit Association (VEBA) assets. Future benefit payments may be made from VEBA trusts and thus reduce those asset balances.

² Funded status is not indicative of our ability to pay ongoing pension benefits or of our obligation to fund retirement trusts. Required pension funding is determined in accordance with the Employee Retirement Income Security Act of 1974, as amended (ERISA), and applicable regulations.

Amounts recognized on our consolidated balance sheets at December 31 are listed below:

	Pension Benefits		Postretirement Benefits	
	2025	2024	2025	2024
Current portion of employee benefit obligation ¹	\$ —	\$ —	\$ (499)	\$ (455)
Employee benefit obligation ²	(1,950)	(3,025)	(5,256)	(4,740)
Net amount recognized	\$ (1,950)	\$ (3,025)	\$ (5,755)	\$ (5,195)

¹ Included in "Accounts payable and accrued liabilities."

² Included in "Postemployment benefit obligation," combined with international pension obligations and other postemployment obligations of \$212 and \$1,060 at December 31, 2025, and \$157 and \$1,103 at December 31, 2024, respectively.

The accumulated benefit obligation for our pension plans represents the actuarial present value of benefits based on employee service and compensation as of a certain date and does not include an assumption about future compensation levels. The accumulated benefit obligation for our pension plans was \$30,069 at December 31, 2025, and \$30,322 at December 31, 2024.

Net Periodic Benefit Cost and Other Amounts Recognized in Other Comprehensive Income

Periodic Benefit Costs

The service cost component of net periodic pension cost (credit) is recorded in operating expenses in the consolidated statements of income while the remaining components are recorded in "Other income (expense) – net." Our combined net pension and postretirement cost (credit) recognized in our consolidated statements of income was \$(1,121), \$(1,817) and \$(1,017) for the years ended December 31, 2025, 2024 and 2023.

The following table presents the components of net periodic benefit cost (credit):

	Pension Benefits			Postretirement Benefits		
	2025	2024	2023	2025	2024	2023
Service cost – benefits earned during the period	\$ 427	\$ 487	\$ 477	\$ 18	\$ 22	\$ 23
Interest cost on projected benefit obligation	1,601	1,586	1,876	318	310	340
Expected return on assets	(2,029)	(2,212)	(2,533)	(38)	(61)	(130)
Amortization of prior service credit	(48)	(87)	(133)	(1,837)	(1,928)	(2,472)
Net periodic benefit cost (credit) before remeasurement	(49)	(226)	(313)	(1,539)	(1,657)	(2,239)
Actuarial (gain) loss	96	38	1,717	371	28	181
Settlement (gain) loss	—	—	(363)	—	—	—
Net pension and postretirement cost (credit)	\$ 47	\$ (188)	\$ 1,041	\$ (1,168)	\$ (1,629)	\$ (2,058)

Other Changes in Benefit Obligations Recognized in Other Comprehensive Income

The following table presents the after-tax changes in benefit obligations recognized in OCI and the after-tax prior service credits that were amortized from OCI into net periodic benefit costs:

	Pension Benefits			Postretirement Benefits		
	2025	2024	2023	2025	2024	2023
Balance at beginning of year	\$ 150	\$ 216	\$ 316	\$ 3,066	\$ 4,523	\$ 6,354
Prior service (cost) credit	—	—	—	—	—	32
Amortization of prior service credit	(36)	(66)	(100)	(1,392)	(1,457)	(1,863)
Total recognized in other comprehensive (income) loss	(36)	(66)	(100)	(1,392)	(1,457)	(1,831)
Balance at end of year	\$ 114	\$ 150	\$ 216	\$ 1,674	\$ 3,066	\$ 4,523

Assumptions

In determining the projected benefit obligation and the net pension and postretirement benefit cost, we used the following significant weighted-average assumptions:

	Pension Benefits			Postretirement Benefits		
	2025	2024	2023	2025	2024	2023
Weighted-average discount rate for determining benefit obligation at December 31	5.50%	5.70%	5.00%	5.30%	5.60%	5.00%
Discount rate in effect for determining service cost ¹	5.80%	5.10%	5.40%	5.80%	5.10%	5.20%
Discount rate in effect for determining interest cost ¹	5.40%	4.90%	5.30%	5.30%	4.90%	5.10%
Weighted-average interest credit rate for cash balance pension programs ²	4.60%	4.60%	4.20%	—%	—%	—%
Long-term rate of return on plan assets	7.75%	7.75%	7.50%	4.00%	4.00%	6.50%
Composite rate of compensation increase for determining benefit obligation	3.00%	3.00%	3.00%	3.00%	3.00%	3.00%
Composite rate of compensation increase for determining net cost (credit)	3.00%	3.00%	3.00%	3.00%	3.00%	3.00%

¹ Weighted-average discount rates shown for years with interim remeasurements: 2023 for pension benefits.

² Weighted-average interest crediting rates for cash balance pension programs relate only to the cash balance portion of total pension benefits. A 0.50% increase in the weighted-average interest crediting rate would increase the pension benefit obligation by \$140.

We recognize gains and losses on pension and postretirement plan assets and obligations immediately in “Other income (expense) – net” in our consolidated statements of income. These gains and losses are generally measured annually as of December 31 and accordingly, will normally be recorded during the fourth quarter, unless an earlier remeasurement is required. Should actual experience differ from actuarial assumptions, the projected pension benefit obligation and net pension cost and accumulated postretirement benefit obligation and postretirement benefit cost would be affected in future years.

Discount Rate Our assumed weighted-average discount rates for pension and postretirement benefits of 5.50% and 5.30% respectively, at December 31, 2025, reflect the hypothetical rate at which the projected benefit obligation could be effectively settled or paid out to participants. We determined our discount rates based on a range of factors, including a yield curve composed of the rates of return on several hundred high-quality, fixed income corporate bonds available at the measurement date and corresponding to the related expected durations of future cash outflows. These bonds had an average rating of at least Aa3 or AA- by the nationally recognized statistical rating organizations, denominated in U.S. dollars, and generally not callable, convertible or index linked. For the year ended December 31, 2025, when compared to the year ended December 31, 2024, we decreased our pension discount rate by 0.20%, resulting in an increase in our pension plan benefit obligation of \$680, and decreased our postretirement discount rate by 0.30%, resulting in an increase in our postretirement benefit obligation of \$167. For the year ended December 31, 2024, when compared to the year ended December 31, 2023, we increased our pension

discount rate by 0.70%, resulting in a decrease in our pension plan benefit obligation of \$1,994, and increased our postretirement discount rate by 0.60%, resulting in a decrease in our postretirement benefit obligation of \$317.

We utilize a full yield curve approach in the estimation of the service and interest components of net periodic benefit costs for pension and other postretirement benefits. Under this approach, we apply discounting using individual spot rates from a yield curve composed of the rates of return on several hundred high-quality, fixed income corporate bonds available at the measurement date. These spot rates align to each of the projected benefit obligations and service cost cash flows. The service cost component relates to the active participants in the plan, so the relevant cash flows on which to apply the yield curve are considerably longer in duration on average than the total projected benefit obligation cash flows, which also include benefit payments to retirees. Interest cost is computed by multiplying each spot rate by the corresponding discounted projected benefit obligation cash flows. The full yield curve approach reduces any actuarial gains and losses based upon interest rate expectations (e.g., built-in gains in interest cost in an upward-sloping yield curve scenario), or gains and losses merely resulting from the timing and magnitude of cash outflows associated with our benefit obligations. Neither the annual measurement of our total benefit obligations nor annual net benefit cost is affected by the full yield curve approach.

Expected Long-Term Rate of Return In 2026, our expected long-term rate of return is 7.75% on pension plan assets and 4.00% on postretirement plan assets. Our long-term rates of return reflect the average rate of earnings expected on the funds invested, or to be invested, to provide for the benefits included in the projected benefit obligations. In setting the long-term assumed rate of return, management considers capital markets' future expectations, the asset mix of the plans' investment and average historical asset return. Actual long-term returns can, in relatively stable markets, also serve as a factor in determining future expectations. We consider many factors that include, but are not limited to, historical returns on plan assets, current market information on long-term returns (e.g., long-term bond rates) and current and target asset allocations between asset categories. The target asset allocation is determined based on consultations with external investment advisers. If all other factors were to remain unchanged, we expect that a 0.50% decrease in the expected long-term rate of return would cause 2026 combined pension and postretirement cost to increase \$139. However, any differences in the rate and actual returns will be included with the actuarial gain or loss recorded in the fourth quarter when our plans are remeasured.

Composite Rate of Compensation Increase Our expected composite rate of compensation increase cost of 3.00% in 2025 and 2024 reflects the long-term average rate of salary increases.

Healthcare Cost Trend Our healthcare cost trend assumptions are developed based on historical cost data, the near-term outlook and an assessment of likely long-term trends. Based on our assessment of expectations of healthcare industry inflation, our 2026 assumed annual healthcare prescription drug cost trend and medical cost trend for eligible participants is 8.25%, grading down to an ultimate trend rate of 4.25% in 2035. For 2025, our assumed annual healthcare prescription drug cost trend and medical cost trend for eligible participants was 8.25%, grading down to an ultimate trend rate of 4.25% in 2032.

Plan Assets

Plan assets consist primarily of private and public equity, government and corporate bonds, and real assets (real estate and natural resources). The asset allocations of the pension plans are maintained to meet ERISA requirements. Any plan contributions, as determined by ERISA regulations, are made to a pension trust for the benefit of plan participants. We do not have significant ERISA required contributions to our pension plans for 2026. We voluntarily contributed \$1,150 to our pension plans during 2025, and intend to voluntarily contribute \$350 during 2026.

We maintain VEBA trusts to partially fund postretirement benefits; however, there are no ERISA or regulatory requirements that these postretirement benefit plans be funded annually.

The principal investment objectives are to ensure the availability of funds to pay pension and postretirement benefits as they become due under a broad range of future economic scenarios, maximize long-term investment return with an acceptable level of risk based on our pension and postretirement obligations, and diversify broadly across and within the capital markets to insulate asset values against adverse experience in any one market. Each asset class has broadly diversified characteristics. Substantial biases toward any particular investing style or type of security are sought to be avoided by managing the aggregation of all accounts with portfolio benchmarks. Asset and benefit obligation forecasting studies are conducted periodically, generally every two to three years, or when significant changes have occurred in market conditions, benefits, participant demographics or funded status. Decisions regarding investment policy are made with an understanding of the effect of asset allocation on funded status, future contributions and projected expenses. During 2025, the pension trust entered into a series of derivative contracts as part of an additional interest rate hedging strategy. This hedging strategy better aligns the pension asset duration with the liability duration and improves the interest rate hedge ratio. The notional amount of the contracts was approximately \$7,300 as of December 31, 2025.

AT&T Inc.

Dollars in millions except per share amounts

The plans' weighted-average asset targets and actual allocations as a percentage of plan assets, including the exposure of future contracts by asset categories, at December 31 are as follows:

	Pension Assets ¹					Postretirement (VEBA) Assets				
	Target		2025	2024		Target		2025	2024	
Equity securities:										
Domestic	8 %	-	18 %	14 %	12 %	8 %	-	18 %	13 %	10 %
International	5 %	-	15 %	11	9	— %	-	10 %	5	4
Fixed income securities	39 %	-	49 %	43	44	— %	-	14 %	9	12
Real assets	11 %	-	21 %	13	15	— %	-	6 %	1	1
Private equity	13 %	-	23 %	17	19	— %	-	6 %	1	1
Other	— %	-	3 %	2	1	66 %	-	76 %	71	72
Total			100 %		100 %			100 %		100 %

¹ Excludes interest rate hedging strategy notional value of \$7,300.

At December 31, 2025, AT&T securities represented less than 1% of assets held by our pension trust. The VEBA trusts do not hold AT&T securities.

Investment Valuation

Investments are stated at fair value. Fair value is the price that would be received to sell an asset or paid to transfer a liability at the measurement date.

Investments in securities traded on a national securities exchange are valued at the last reported sales price on the final business day of the year. If no sale was reported on that date, they are valued at the last reported bid price. Investments in securities not traded on a national securities exchange are valued using pricing models, quoted prices of securities with similar characteristics or discounted cash flows. Shares of registered investment companies are valued based on quoted market prices, which represent the net asset value of shares held at year-end.

Other commingled investment entities are valued at quoted redemption values that represent the net asset values of units held at year-end, which management has determined approximates fair value.

Real estate and natural resource direct investments are valued at amounts based upon appraisal reports. Fixed income securities valuation is based upon observable prices for comparable assets, broker/dealer quotes (spreads or prices), or a pricing matrix that derives spreads for each bond based on external market data, including the current credit rating for the bonds, credit spreads to Treasuries for each credit rating, sector add-ons or credits, issue-specific add-ons or credits as well as call or other options.

Purchases and sales of securities are recorded as of the trade date. Realized gains and losses on sales of securities are determined on the basis of average cost. Interest income is recognized on the accrual basis. Dividend income is recognized on the ex-dividend date.

Non-interest bearing cash and overdrafts are valued at cost, which approximates fair value.

Fair Value Measurements

See Note 12 for a discussion of the fair value hierarchy that prioritizes the inputs to valuation techniques used to measure fair value.

The following tables set forth by level, within the fair value hierarchy, the pension and postretirement assets and liabilities at fair value as of December 31, 2025:

Pension Assets and Liabilities at Fair Value				
	Level 1	Level 2	Level 3	Total
Non-interest bearing cash	\$ 92	\$ —	\$ —	\$ 92
Interest bearing cash	4	—	—	4
Foreign currency contracts	—	3	—	3
Equity securities:				
Domestic equities	2,797	—	2	2,799
International equities	1,593	—	—	1,593
Fixed income securities:				
Corporate bonds and other investments	—	7,007	14	7,021
Government and municipal bonds	26	3,675	—	3,701
Mortgage-backed securities	—	198	—	198
Real estate and real assets	—	—	2,403	2,403
Securities lending collateral ¹	688	1,484	—	2,172
Receivable for variation margin	2	—	—	2
Assets at fair value	5,202	12,367	2,419	19,988
Investments sold short and other liabilities at fair value	(48)	(3)	—	(51)
Total plan net assets at fair value	\$ 5,154	\$ 12,364	\$ 2,419	\$ 19,937
Assets held at net asset value practical expedient				
Private equity funds				5,029
Real estate funds				1,198
Commingled funds				5,076
Total assets held at net asset value practical expedient				11,303
Other assets (liabilities) ²				(2,563)
Total Plan Net Assets				\$ 28,677

¹ Securities lending collateral primarily includes cash and government and municipal bonds.

² Other assets (liabilities) include amounts receivable, accounts payable and net adjustment for securities lending payable.

Postretirement Assets and Liabilities at Fair Value				
	Level 1	Level 2	Level 3	Total
Interest bearing cash	\$ 505	\$ —	\$ —	\$ 505
Equity securities:				
Domestic equities	3	—	—	3
Total plan net assets at fair value	\$ 508	\$ —	\$ —	\$ 508
Assets held at net asset value practical expedient				
Private equity funds				6
Real estate funds				9
Commingled funds				197
Total assets held at net asset value practical expedient				212
Other assets (liabilities) ¹				2
Total Plan Net Assets				\$ 722

¹ Other assets (liabilities) include amounts receivable and accounts payable.

The following tables set forth by level, within the fair value hierarchy, the pension and postretirement assets and liabilities at fair value as of December 31, 2024:

Pension Assets and Liabilities at Fair Value				
	Level 1	Level 2	Level 3	Total
Non-interest bearing cash	\$ 146	\$ —	\$ —	\$ 146
Interest bearing cash	23	—	—	23
Foreign currency contracts	—	2	—	2
Equity securities:				
Domestic equities	2,608	—	2	2,610
International equities	1,145	—	—	1,145
Fixed income securities:				
Corporate bonds and other investments	—	6,925	1	6,926
Government and municipal bonds	—	4,274	—	4,274
Mortgage-backed securities	—	267	—	267
Real estate and real assets	—	—	2,311	2,311
Securities lending collateral ¹	643	961	—	1,604
Receivable for variation margin	4	—	—	4
Assets at fair value	4,569	12,429	2,314	19,312
Investments sold short and other liabilities at fair value	(152)	(12)	—	(164)
Total plan net assets at fair value	\$ 4,417	\$ 12,417	\$ 2,314	\$ 19,148
Assets held at net asset value practical expedient				
Private equity funds				5,138
Real estate funds				1,957
Commingled funds				3,895
Total assets held at net asset value practical expedient				10,990
Other assets (liabilities) ²				(2,219)
Total Plan Net Assets				\$ 27,919

¹ Securities lending collateral primarily includes cash and government and municipal bonds.

² Other assets (liabilities) include amounts receivable, accounts payable and net adjustment for securities lending payable.

Postretirement Assets and Liabilities at Fair Value				
	Level 1	Level 2	Level 3	Total
Interest bearing cash	\$ 816	\$ 6	\$ —	\$ 822
Equity securities:				
Domestic equities	1	—	—	1
Total plan net assets at fair value	\$ 817	\$ 6	\$ —	\$ 823
Assets held at net asset value practical expedient				
Private equity funds				9
Real estate funds				9
Commingled funds				299
Total assets held at net asset value practical expedient				317
Other assets (liabilities) ¹				4
Total Plan Net Assets				\$ 1,144

¹ Other assets (liabilities) include amounts receivable and accounts payable.

For the years ended December 31, 2025 and 2024, our postretirement assets did not include significant investments in Level 3 assets, nor were there significant changes in fair value of those assets during the period. The tables below set forth a summary of changes in the fair value of the Level 3 pension assets:

	Equities	Fixed Income Funds	Real Estate and Real Assets	Total
Balance as of December 31, 2024	\$ 2	\$ 1	\$ 2,311	\$ 2,314
Realized gains (losses)	—	—	(315)	(315)
Unrealized gains (losses)	—	—	325	325
Transfers in	—	—	319	319
Purchases	—	13	102	115
Sales	—	—	(339)	(339)
Balance as of December 31, 2025	\$ 2	\$ 14	\$ 2,403	\$ 2,419

	Equities	Fixed Income Funds	Real Estate and Real Assets	Total
Balance as of December 31, 2023	\$ 2	\$ 1	\$ 2,954	\$ 2,957
Realized gains (losses)	—	—	159	159
Unrealized gains (losses)	—	—	(510)	(510)
Purchases	—	—	291	291
Sales	—	—	(583)	(583)
Balance as of December 31, 2024	\$ 2	\$ 1	\$ 2,311	\$ 2,314

Estimated Future Benefit Payments

Expected benefit payments are estimated using the same assumptions used in determining our benefit obligation at December 31, 2025. Because benefit payments will depend on future employment and compensation levels; average years employed; average life spans; and payment elections, among other factors, changes in any of these assumptions could significantly affect these expected amounts. The following table provides expected benefit payments under our pension and postretirement plans:

	Pension Benefits	Postretirement Benefits
2026	\$ 3,460	\$ 664
2027	2,955	641
2028	2,893	623
2029	2,830	520
2030	2,765	538
Years 2031 - 2035	12,516	2,536

Supplemental Retirement Plans

We also provide certain senior- and middle-management employees with nonqualified, unfunded supplemental retirement and savings plans. While these plans are unfunded, we have assets in a designated non-bankruptcy remote trust that are independently managed and used to provide for certain of these benefits. These plans include supplemental pension benefits as well as compensation-deferral plans, some of which include a corresponding match by us based on a percentage of the compensation deferral. For our supplemental retirement plans, the projected benefit obligation was \$1,199 and the net supplemental retirement pension cost was \$92 at and for the year ended December 31, 2025. The projected benefit obligation was \$1,305 and the net supplemental retirement pension cost was \$18 at and for the year ended December 31, 2024.

We use the same significant assumptions for the composite rate of compensation increase in determining our projected benefit obligation and the net pension and postemployment benefit cost. Our discount rates of 5.10% at December 31, 2025 and 5.50% at December 31, 2024 were calculated using the same methodologies used in calculating the discount rates for our qualified pension and postretirement benefit plans.

Deferred compensation expense was \$96 in 2025, \$152 in 2024 and \$101 in 2023.

Contributory Savings Plans

We maintain contributory savings plans that cover substantially all employees. Under the savings plans, we match in cash or company stock a stated percentage of eligible employee contributions, subject to a specified ceiling. There are no debt-financed shares held by the Employee Stock Ownership Plans, allocated or unallocated.

Our match of employee contributions to the savings plans is fulfilled with purchases of our stock on the open market or company cash. Benefit cost, which is based on the cost of shares or units allocated to participating employees' accounts or the cash contributed to participant accounts, was \$546, \$565 and \$570 for the years ended December 31, 2025, 2024 and 2023.

NOTE 15. SHARE-BASED COMPENSATION

Under our various share-based compensation plans, senior and other management employees and nonemployee directors have received performance stock units and other nonvested stock units.

As of December 31, 2025, we were authorized to issue up to approximately 41 million shares of common stock (including shares that may be issued upon exercise of outstanding options or upon vesting of performance stock units or other nonvested stock units) pursuant to these various plans:

- Performance stock units, which are nonvested stock units, which are valued based upon the market price of our common stock at the date of grant and performance expectations. These distribute in the form of AT&T common stock and cash at the end of a three-year period, subject to the achievement of certain performance goals. We treat the cash-settled portion of these awards as a liability.
- Restricted stock and restricted stock units are valued at the market price of our common stock at the date of grant and do not have any performance conditions. Restricted stock predominantly vests over a three- to ten-year period and restricted stock units predominantly vest over a three-year period.

We account for our share-based compensation arrangements based on the fair value of the awards on their respective grant date, which may affect our ability to fully realize the value shown on our consolidated balance sheets of deferred tax assets associated with compensation expense. We record a valuation allowance when our future taxable income is not expected to be sufficient to recover the asset. Accordingly, there can be no assurance that the current stock price of our common shares will rise to levels sufficient to realize the entire tax benefit currently reflected on our consolidated balance sheets. However, to the extent we generate excess tax benefits (i.e., those additional tax benefits in excess of the deferred taxes associated with compensation expense previously recognized) the potential future impact on income would be reduced.

Our consolidated statements of income include the share-based compensation cost recognized for the plans described above as "Selling, general and administrative" expense. Those expenses, as well as the associated tax benefits, are reflected in the table below:

	2025	2024	2023
Performance stock units	\$ 152	\$ 127	\$ 79
Restricted stock and stock units	384	378	400
Total	\$ 536	\$ 505	\$ 479
Income tax benefit	\$ 130	\$ 123	\$ 118

A summary of the status of our nonvested stock units as of December 31, 2025, and changes during the year then ended is presented as follows (shares in millions):

Nonvested Stock Units	Shares	Weighted-Average Grant-Date Fair Value
Nonvested at January 1, 2025	37	\$ 19.88
Granted	18	26.04
Vested	(22)	20.87
Forfeited	(4)	21.13
Nonvested at December 31, 2025	29	\$ 22.74

As of December 31, 2025, there was \$584 of total unrecognized compensation cost related to nonvested share-based compensation arrangements outstanding. That cost is expected to be recognized over a weighted-average period of 1.89 years. The total fair value of shares vested during the year was \$464 for 2025, compared to \$452 for 2024 and \$592 for 2023.

NOTE 16. STOCKHOLDERS' AND MEZZANINE EQUITY

Authorized Shares We have authorized 14 billion common shares of AT&T stock and 10 million preferred shares of AT&T stock, each with a par value of \$1.00 per share. Cumulative perpetual preferred shares consist of the following:

- Series A: 48 thousand shares outstanding at December 31, 2025 and December 31, 2024, with a \$25,000 per share liquidation preference and a dividend rate of 5.000%.
- Series B: no shares outstanding at December 31, 2025 and 20 thousand shares outstanding at December 31, 2024, with a €100,000 per share liquidation preference, and an initial rate of 2.875%. We redeemed all outstanding Series B cumulative preferred shares on March 3, 2025. The shares had a total liquidation preference of €2.0 billion and were redeemed for \$2,075.
- Series C: 70 thousand shares outstanding at December 31, 2025 and December 31, 2024, with a \$25,000 per share liquidation preference, and a dividend rate of 4.75%.

So long as the quarterly preferred dividends are declared and paid on a timely basis on each series of preferred shares, there are no limitations on our ability to declare a dividend on or repurchase AT&T common shares. The preferred shares are optionally redeemable by AT&T at the liquidation price on or after five years from the issuance date, or upon certain other contingent events.

Stock Repurchase Program From time to time, we repurchase shares of common stock. Over the past few years, these repurchases have generally been for distribution through our employee benefit plans or in connection with certain acquisitions. In December 2024, the Board approved an authorization to repurchase up to \$10,000 of common stock (the "2024 Authorization") and terminated the March 2014 authorization. During 2025, we repurchased approximately 159 million shares totaling \$4,269 under this authorization, excluding brokerage fees and the one percent excise tax imposed by the Inflation Reduction Act of 2022. On January 27, 2026, the Board approved an authorization to repurchase an additional \$10,000 of common stock (the "2026 Authorization").

To implement repurchase authorizations, we have used open market repurchases, relying on Rule 10b5-1 of the Securities Exchange Act of 1934, where feasible. We have also used accelerated share repurchase agreements with large financial institutions to repurchase our stock. During 2024, we repurchased approximately 36 thousand shares totaling \$1 under the March 2014 authorization.

Dividend Declarations In December 2025 and December 2024, AT&T declared a quarterly preferred dividend of \$36. In December 2025 and December 2024, AT&T declared a quarterly common dividend of \$0.2775 per share of common stock.

Preferred Interests Issued by Subsidiaries We have issued cumulative perpetual preferred membership interests in certain subsidiaries. The preferred interests are entitled to cash distributions, subject to declaration.

Mobility II Preferred Interests

In 2018, we issued 320 million Series A Cumulative Perpetual Preferred Membership Interests in Mobility II (Mobility preferred interests), which paid cash distributions of 7% per annum, subject to declaration. So long as the distributions were declared and paid, the terms of the Mobility preferred interests did not impose any limitations on cash movements between affiliates, or our ability to declare a dividend on or repurchase AT&T shares. All Mobility preferred interests were repurchased as of April 2023.

Prior to repurchase, a holder of the Mobility preferred interests could put the interests to Mobility II, or Mobility II could have redeemed the interests upon a change in control of Mobility II or on or after September 9, 2022, with either option only allowed to be exercised during certain periods. The redemption price was to be paid with cash, AT&T common stock, or a combination of cash and AT&T common stock, at Mobility II's sole election.

Tower Holdings Preferred Interests

In 2019, we issued \$6,000 nonconvertible cumulative preferred interests in a wireless subsidiary (Tower Holdings) that holds interests in various tower assets and has the right to receive approximately \$6,000 if the purchase options from the tower companies are exercised.

The membership interests in Tower Holdings consist of (1) common interests, which are held by a consolidated subsidiary of AT&T, and (2) two series of preferred interests (collectively the "2019 Tower preferred interests"). The 2019 Tower preferred

interests were subject to reset in December 2024 and included a September series (Tower Class A-1) totaling \$1,500 that paid an initial preferred distribution of 5.0%, and a December series (Tower Class A-2) totaling \$4,500 that paid an initial preferred distribution of 4.75%.

In August 2024, we amended the 2019 Tower preferred interests, effective November 2024, to reset the rate and restructure the membership interests whereby all of the 2019 Tower preferred interests are now designated Fixed Rate Class A Limited Membership Interests (Tower Fixed Rate Interests). A portion of the Tower Fixed Rate Interests will move to Floating Rate Class A Limited Membership Interests (Tower Floating Rate Interests) each year over a five-year period. The Tower Fixed Rate Interests pay a preferred distribution of 5.90%, and the Tower Floating Rate Interests pay a preferred distribution equal to the Secured Overnight Financing Rate (SOFR) plus 250 basis points, as defined in the agreement. Distributions are paid quarterly, subject to declaration, and reset every five years. Any failure to declare or pay distributions on the Tower Fixed Rate Interests or Tower Floating Rate Interests (collectively, the “Tower preferred interests”) would not impose any limitation on cash movements between affiliates, or our ability to declare a dividend on or repurchase AT&T shares. We can call the Tower preferred interests at the issue price beginning in November 2029, and we can call the Tower Floating Rate Interests at any time. We redeemed \$65 of the Tower Floating Rate Interests in November 2025. If not called, the remaining Tower Floating Rate Interests could equal \$460 by 2028. The Tower preferred interests are included in “Noncontrolling interest” on the consolidated balance sheets.

The holders of the Tower preferred interests have the option to require redemption upon the occurrence of certain contingent events, such as the failure of AT&T to pay the preferred distribution for two or more periods or to meet certain other requirements, including a minimum credit rating. If notice is given upon such an event, all other holders of equal or more subordinate classes of membership interests in Tower Holdings are entitled to receive the same form of consideration payable to the holders of the preferred interests, resulting in a deemed liquidation for accounting purposes.

Telco LLC Preferred Interests

In September 2020, we issued \$2,000 nonconvertible cumulative preferred interests (Telco Class A-1) out of a newly created limited liability company (Telco LLC) that was formed to hold telecommunications-related assets. In April 2023, we expanded our September 2020 transaction and issued an additional \$5,250 of nonconvertible cumulative preferred interests (Telco Class A-2 and A-3). In March 2025, we issued an additional \$2,250 of nonconvertible cumulative preferred interests in Telco LLC (Telco Class A-4). The Telco Class A-4 interests will pay an initial preferred distribution of 5.94% annually, subject to declaration, and subject to reset on November 1, 2028, and every four years thereafter. The Telco Class A-4 interests can be called at issue price beginning on November 1, 2028, and are subject to the same redemption and liquidation rights as the Telco Class A-1, A-2 and A-3 interests. As of December 31, 2025 and 2024, cumulative preferred interests in our Telco LLC totaled \$9,500 and \$7,250 (collectively the “Telco preferred interests”).

Members’ equity in Telco LLC consists of (1) members’ interests, which are held by a consolidated subsidiary of AT&T, (2) Telco Class A-1 preferred interests, which pay an initial preferred distribution of 4.25% annually, subject to declaration, and subject to reset every seven years, and (3) Telco Class A-2 and A-3 preferred interests, which pay an initial preferred distribution of 6.85% annually, subject to declaration, and subject to reset on November 1, 2027, and every seven years thereafter. Failure to pay distributions on the Telco preferred interests would not limit cash movements between affiliates, or our ability to declare a dividend on or repurchase AT&T shares. We can call the Telco preferred interests at the issue price beginning seven years from the issuance date. The Telco preferred interests are included in “Noncontrolling interest” on the consolidated balance sheets.

The holders of the Telco preferred interests have the option to require redemption upon the occurrence of certain contingent events, such as the failure of Telco LLC to pay the preferred distribution for two or more periods or to meet certain other requirements, including a minimum credit rating. If notice is given, all other holders of equal or more subordinate classes of members’ equity are entitled to receive the same form of consideration payable to the holders of the preferred interests, resulting in a deemed liquidation for accounting purposes.

Mobility II Redeemable Noncontrolling Interests

In June 2023, we issued two million Series B Cumulative Perpetual Preferred Membership Interests in Mobility II LLC (Mobility noncontrolling interests), which pay cash distributions of 6.8% per annum, subject to declaration. So long as the distributions are declared and paid, the terms of the Mobility noncontrolling interests will not impose any limitations on cash movements between affiliates, or our ability to declare a dividend on or repurchase AT&T shares.

The Mobility noncontrolling interests are required to be initially recorded at fair value less issuance costs and will accrete to redemption value of \$2,000 through “Net Income Attributable to Noncontrolling Interest.” The Mobility noncontrolling interests are considered Level 3 under the Fair Value Measurement and Disclosures framework (see Note 12) and included in “Redeemable Noncontrolling Interest” on the consolidated balance sheets.

A holder of the Mobility noncontrolling interests may put the interests to Mobility II on or after the earliest of certain events or each June 15 and December 15, beginning on June 15, 2028. Mobility II may redeem the interests on each March 15 and September 15, beginning on March 15, 2028. The price at which a put option or a redemption option can be exercised is the sum of (a) \$1,000 per Mobility noncontrolling interest plus (b) any accrued and unpaid distributions. The redemption price must be paid in cash.

NOTE 17. SALES OF RECEIVABLES

We have agreements with various third-party financial institutions pertaining to the sales of certain types of our accounts receivable. The most significant of these programs are discussed in detail below and generally consist of (1) receivables arising from equipment installment plans, which are sold for cash and beneficial interests, such as deferred purchase price, when applicable, and (2) revolving trade receivables, which are sold for cash. Under the terms of our agreements for these programs, we continue to service the transferred receivables on behalf of the financial institutions.

The following table sets forth a summary of cash proceeds received, net of remittances paid, from sales of receivables for the years ended December 31:

	2025	2024	2023
Net cash received (paid) from equipment installment receivables program ¹	\$ 1,318	\$ (1,358)	\$ 648
Net cash received (paid) from revolving receivables program	16	1,147	1,456
Net cash received (paid) from other programs	—	—	(632)
Total net cash impact to cash flows from operating activities ²	\$ 1,334	\$ (211)	\$ 1,472

¹ Cash from initial sales of \$12,391, \$10,587 and \$10,980 for the years ended December 31, 2025, 2024 and 2023, respectively.

² Net of facility fees.

The sales of receivables did not have a material impact on our consolidated statements of income or to “Total Assets” reported on our consolidated balance sheets. We reflect cash receipts on sold receivables as cash flows from operations in our consolidated statements of cash flows. In the event cash is received on the beneficial interests, those receipts are classified as cash flows from investing activities, when applicable.

Our equipment installment and revolving receivables programs are discussed in detail below. The following table sets forth a summary of the receivables and accounts being serviced at December 31:

	2025		2024	
	Equipment Installment	Revolving	Equipment Installment	Revolving
Gross receivables:	\$ 3,725	\$ 425	\$ 3,504	\$ 553
<i>Balance sheet classification</i>				
Accounts receivable				
Notes receivable	1,886	—	1,817	—
Trade receivables	304	425	237	553
Other Assets				
Noncurrent notes and trade receivables	1,535	—	1,450	—
Outstanding portfolio of receivables derecognized from our consolidated balance sheets	\$ 11,987	\$ 2,940	\$ 11,909	\$ 2,770
Cash proceeds received, net of remittances ¹	9,617	2,940	8,243	2,770

¹ Represents amounts to which financial institutions remain entitled, excluding the beneficial interests.

Equipment Installment Receivables Program

We offer our customers the option to purchase certain wireless devices in installments over a specified period of time and, in many cases, once certain conditions are met, they may be eligible to trade in the original equipment for a new device and have the remaining unpaid balance paid or settled.

We maintain a program under which we transfer a portion of these receivables through our bankruptcy-remote subsidiary in exchange for cash and beneficial interests. In the event a customer trades in a device prior to the end of the installment contract period, we agree to make a payment to the financial institutions equal to any outstanding remaining installment receivable balance. Accordingly, we record a guarantee obligation for this estimated amount at the time the receivables are transferred.

The following table sets forth a summary of equipment installment receivables sold under this program:

	2025	2024	2023
Gross receivables sold ¹	\$ 12,513	\$ 10,696	\$ 11,104
Net receivables sold ²	11,991	10,160	10,603
Cash proceeds received	12,391	10,587	10,980
Guarantee obligation recorded	925	930	932

¹ Receivables net of promotion credits.

² Receivables net of allowance and other reserves.

Beneficial interests, when applicable, and guarantee obligations are initially recorded at estimated fair value and subsequently adjusted for changes in present value of expected cash flows. The estimation of their fair values is based on remaining installment payments expected to be collected and the expected timing and value of device trade-ins. The estimated value of the device trade-ins considers prices offered to us by independent third parties and contemplates changes in value after the launch of a device model. The fair value measurements used for the beneficial interests and the guarantee obligation are considered Level 3 under the Fair Value Measurement and Disclosure framework (see Note 12).

The following table presents the previously transferred equipment installment receivables, which we repurchased in exchange for the associated beneficial interests:

	2025	2024	2023
Fair value of repurchased receivables	\$ 4,786	\$ 3,185	\$ 2,997
Carrying value of beneficial interests	4,774	3,199	3,013
Gain (loss) on repurchases ¹	\$ 12	\$ (14)	\$ (16)

¹ These gains (losses) are included in "Selling, general and administrative" expense in the consolidated statements of income.

At December 31, 2025 and December 31, 2024, our beneficial interests were \$2,067 and \$3,185, respectively, of which \$1,338 and \$1,906 are included in "Prepaid and other current assets" on our consolidated balance sheets, with the remainder in "Other Assets." The guarantee obligation at December 31, 2025 and December 31, 2024 was \$410 and \$301, respectively, of which \$216 and \$150 are included in "Accounts payable and accrued liabilities" on our consolidated balance sheets, with the remainder in "Other noncurrent liabilities." Our maximum exposure to loss as a result of selling these equipment installment receivables is limited to the total amount of our beneficial interests and guarantee obligation.

Revolving Receivables Program

During 2025, we expanded our revolving agreement to transfer up to \$2,940 of certain receivables through our bankruptcy-remote subsidiaries to various financial institutions on a recurring basis in exchange for cash equal to the gross receivables transferred. This agreement is subject to renewal on an annual basis and the transfer limit may be expanded or reduced from time to time. As customers pay their balances, we transfer additional receivables into the program, resulting in our gross receivables sold exceeding net cash flow impacts (e.g., collect and reinvest). The transferred receivables are fully guaranteed by our bankruptcy-remote subsidiaries, which hold additional receivables in the amount of \$425 that are pledged as collateral under this agreement. The transfers are recorded at fair value of the proceeds received and obligations assumed less derecognized receivables. Our maximum exposure to loss related to these receivables transferred is limited to the derecognized amount outstanding.

The following table sets forth a summary of the revolving receivables sold:

	2025	2024	2023
Gross receivables sold/cash proceeds received ¹	\$ 30,311	\$ 21,632	\$ 8,882
Total collections under revolving agreement	30,141	20,362	7,382
Net cash proceeds received	\$ 170	\$ 1,270	\$ 1,500
Net receivables sold ²	\$ 29,480	\$ 21,039	\$ 8,679

¹ Includes initial sales of receivables of \$170, \$1,270 and \$1,500 for the years ended December 31, 2025, 2024 and 2023, respectively.

² Receivables net of allowance and other reserves.

NOTE 18. TOWER TRANSACTION

In December 2013, we closed our transaction with Crown Castle International Corp. (Crown Castle) in which Crown Castle gained the exclusive rights to lease and operate 9,048 wireless towers and purchased 627 of our wireless towers for \$4,827 in cash. The leases have various terms with an average length of approximately 28 years. As the leases expire, Crown Castle will have fixed price purchase options for these towers totaling approximately \$4,200, based on their estimated fair market values at the end of the lease terms. We are subleasing space on the towers from Crown Castle over an estimated original term of 20 years, at current market rates, subject to further optional renewals in the future.

We determined that we did not transfer control of the tower assets, which prevented us from achieving sale-leaseback accounting for the transaction, and we accounted for the cash proceeds from Crown Castle as a financing obligation on our consolidated balance sheets. We record interest on the financing obligation using the effective interest method at a rate of approximately 3.9%. The financing obligation is increased by interest expense and estimated future net cash flows generated and retained by Crown Castle from operation of the tower sites, and reduced by our contractual payments. We continue to include the tower assets in "Property, Plant and Equipment – Net" on our consolidated balance sheets and depreciate them accordingly. At December 31, 2025 and 2024, the tower assets had a balance of \$569 and \$608, respectively. Our depreciation expense for these assets was \$39 for each of 2025, 2024 and 2023.

Payments made to Crown Castle under this arrangement were \$274 for 2025. At December 31, 2025, the future minimum payments under the sublease arrangement are \$280 for 2026, \$285 for 2027, \$291 for 2028, \$297 for 2029, \$303 for 2030 and \$1,086 thereafter.

NOTE 19. TRANSACTIONS WITH DIRECTV

Prior to its sale, we accounted for our investment in DIRECTV under the equity method and recorded our share of DIRECTV earnings as equity in net income of affiliates, with DIRECTV considered a related party. On July 2, 2025, we sold our interest in DIRECTV to TPG. (See Note 10)

The following table sets forth our share of DIRECTV's earnings included in "Equity in net income of affiliates" and cash distributions received from DIRECTV:

	2025	2024	2023
DIRECTV's earnings included in Equity in net income of affiliates	\$ 1,926	\$ 2,027	\$ 1,666
Distributions classified as operating activities	\$ 1,926	\$ 2,027	\$ 1,666
Distributions classified as investing activities	—	928	2,049
Cash distributions received from DIRECTV	\$ 1,926	\$ 2,955	\$ 3,715

For the years ended December 31, 2025, 2024 and 2023, we billed DIRECTV approximately \$240, \$536 and \$730 under commercial arrangements and transition service agreements, which were recorded as a reduction to the operations and support expenses incurred.

NOTE 20. FIRSTNET

In 2017, the First Responder Network Authority (FirstNet) selected AT&T to build and manage the first nationwide broadband network dedicated to America's first responders. Under the 25-year agreement, FirstNet provides 20 MHz of valuable telecommunications spectrum and success-based payments of \$6,500 to support network buildout, which has been substantially completed. We are required to construct a network that achieves coverage and nationwide interoperability requirements and have a contractual commitment to make sustainability payments of \$18,000 over the 25-year contract. These sustainability payments represent our commitment to fund FirstNet's operating expenses and future reinvestments in the network which we own and operate, which we estimate in the \$3,000 or less range over the life of the 25-year contract. After FirstNet's operating expenses are paid, we anticipate the remaining amount, expected to be in the \$15,000 range, will be reinvested into the network. On January 30, 2024, FirstNet agreed to reinvest up to \$6,300 in the network over 10 years, subject to authorization.

During 2025, we submitted \$420 in sustainability payments, with future payments under the agreement of \$896 for 2026, \$1,566 for 2027, \$1,658 for 2028, \$1,474 for 2029, \$1,115 for 2030, and \$9,320 thereafter. Amounts paid to FirstNet, which are not expected to be returned to AT&T to be reinvested into our network, will be expensed in the period paid. In the event FirstNet does not reinvest any funds to construct, operate, improve and maintain this network, our maximum exposure to loss is the total amount of the sustainability payments, which would be reflected in higher expense.

NOTE 21. CONTINGENT LIABILITIES

We are party to numerous lawsuits, regulatory proceedings and other matters arising in the ordinary course of business. In evaluating these matters on an ongoing basis, we take into account amounts already accrued on the balance sheet. In our opinion, although the outcomes of these proceedings are uncertain, they should not have a material adverse effect on our financial position, results of operations or cash flows. See Note 12 for a discussion of collateral and credit-risk contingencies.

We have contractual obligations to purchase certain goods or services from various other parties. Our purchase obligations are expected to be approximately \$8,545 in 2026, \$10,698 in total for 2027 and 2028, \$2,505 in total for 2029 and 2030 and \$2,890 in total for years thereafter.

NOTE 22. SUPPLIER AND VENDOR FINANCING PROGRAMS**Supplier Financing Program**

We actively manage the timing of our supplier payments for operating items to optimize the use of our cash and seek to make payments on 90-day or greater terms, while providing suppliers with access to bank facilities that permit earlier payment at their cost. Our supplier financing program does not result in changes to our normal, contracted payment cycles or cash from operations.

At the supplier's election, they can receive payment of AT&T obligations prior to the scheduled due dates, at a discounted price from the third-party financial institution. The discounted price paid to participating suppliers is based on a variable rate that is indexed to the overnight borrowing rate. We agree to pay the financial institution the stated amount generally within 90 days of receipt of the invoice. We do not have pledged assets or other guarantees under our supplier financing program.

Our outstanding payment obligations are included in "Accounts payable and accrued liabilities" on our consolidated balance sheets and are reported as operating or investing (when capitalizable) activities in our statements of cash flows when paid.

The following table presents the change in the supplier financing obligation for the years ended December 31:

	2025	2024
Confirmed obligations outstanding at the beginning of year	\$ 2,498	\$ 2,844
Invoices received	17,939	15,510
Invoices paid	(17,347)	(15,856)
Confirmed obligations outstanding at the end of year	\$ 3,090	\$ 2,498

Direct Supplier Financing

We also have arrangements with suppliers of handset inventory that allow us to extend the stated payment terms by generally 90 days at an additional cost to us (variable rate extension fee). Direct supplier financing outstanding is included in “Accounts payable and accrued liabilities” on our consolidated balance sheets and is reported as operating activities in our statements of cash flows when paid.

The following table presents the change in the direct supplier financing obligation for the years ended December 31:

	2025	2024
Obligations outstanding at the beginning of year	\$ 6,272	\$ 5,442
Invoices extended	19,850	15,831
Invoices paid	(19,221)	(15,001)
Obligations outstanding at the end of year	\$ 6,901	\$ 6,272

Vendor Financing

We enter into multi-year software licensing arrangements, which, consistent with industry standards, are paid over the license terms of two to five years. Additionally, in connection with capital improvements and the acquisition of other productive assets, we negotiate favorable payment terms of 120 days or more (referred to as vendor financing), which are reported as financing activities in our statements of cash flows when paid.

The following table presents the change in the vendor financing obligation for the years ended December 31:

	2025	2024
Obligations outstanding at the beginning of year	\$ 1,424	\$ 2,516
Commitments	1,594	700
Payments	(1,181)	(1,792)
Obligations outstanding at the end of year ^{1,2}	\$ 1,837	\$ 1,424

¹ Total vendor financing payables at December 31, 2025 and 2024 were \$1,892 and \$1,448, respectively, of which \$956 and \$749 are included in “Accounts payable and accrued liabilities.”

² Includes software licensing arrangements of approximately \$1,200 and \$850 at December 31, 2025 and 2024, respectively.

NOTE 23. ADDITIONAL FINANCIAL INFORMATION

	December 31,	
	2025	2024
Consolidated Balance Sheets		
Accounts payable and accrued liabilities:		
Accounts payable	\$ 29,910	\$ 27,433
Accrued payroll and commissions	2,002	2,015
Current portion of employee benefit obligation	635	570
Accrued interest	2,361	2,020
Accrued taxes	585	1,301
Other	3,021	2,318
Total accounts payable and accrued liabilities	\$ 38,514	\$ 35,657

	2025	2024	2023
Consolidated Statements of Income			
Advertising expense	\$ 3,105	\$ 2,505	\$ 2,576
Interest income	\$ 403	\$ 212	\$ 303
Interest expense incurred	\$ 7,025	\$ 7,120	\$ 7,578
Capitalized interest – capital expenditures	(165)	(162)	(179)
Capitalized interest – spectrum ¹	(56)	(199)	(695)
Total interest expense	\$ 6,804	\$ 6,759	\$ 6,704

¹ Included in “Acquisitions, net of cash acquired” in our consolidated statements of cash flows.

Cash and Cash Flows We typically maintain our restricted cash balances for purchases and sales of certain investment securities and funding of certain deferred compensation benefit payments.

The following table summarizes cash and cash equivalents and restricted cash balances contained on our consolidated balance sheets:

Cash and Cash Equivalents and Restricted Cash	December 31,			
	2025	2024	2023	2022
Cash and cash equivalents	\$ 18,234	\$ 3,298	\$ 6,722	\$ 3,701
Restricted cash in Prepaid and other current assets	157	1	2	1
Restricted cash in Other Assets	136	107	109	91
Cash and cash equivalents and restricted cash	\$ 18,527	\$ 3,406	\$ 6,833	\$ 3,793

The following tables summarize certain cash flow activities during the periods:

Consolidated Statements of Cash Flows	2025	2024	2023
Cash paid (received) during the year for:			
Interest	\$ 6,625	\$ 7,132	\$ 7,370
Income taxes, net of refunds	1,353	2,456	1,599
Purchase of property and equipment	\$ 20,677	\$ 20,101	\$ 17,674
Interest during construction - capital expenditures ¹	165	162	179
Total Capital expenditures	\$ 20,842	\$ 20,263	\$ 17,853
Business acquisitions	\$ —	\$ —	\$ —
Spectrum acquisitions	323	181	2,247
Interest during construction - spectrum ¹	56	199	695
Total Acquisitions, net of cash acquired	\$ 379	\$ 380	\$ 2,942

¹ Total capitalized interest was \$221, \$361 and \$874 for 2025, 2024 and 2023, respectively.

Labor Contracts As of December 31, 2025, we employed approximately 133,030 persons. Approximately 43% of our employees are represented by the Communications Workers of America (CWA), the International Brotherhood of Electrical Workers (IBEW) or other unions. After expiration of collective bargaining agreements, work stoppages or labor disruptions may occur in the absence of new contracts or other agreements being reached. The main contracts set to expire in 2026 include the following:

- A contract covering approximately 9,000 employees across 36 states and the District of Columbia is set to expire in February.
- A contract covering approximately 4,300 employees across five states is set to expire in April.
- Two wireline contracts covering approximately 1,800 employees across all 50 states as well as the U.S. Virgin Islands and Puerto Rico are set to expire in April.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

During our two most recent fiscal years, there has been no change in the independent accountant engaged as the principal accountant to audit our financial statements, and the independent accountant has not expressed reliance on other independent accountants in its reports during such time period.

ITEM 9A. CONTROLS AND PROCEDURES

Disclosure Controls and Procedures

The registrant maintains disclosure controls and procedures that are designed to ensure that information required to be disclosed by the registrant is recorded, processed, summarized, accumulated and communicated to its management, including its principal executive and principal financial officers, to allow timely decisions regarding required disclosure, and reported within the time periods specified in the SEC's rules and forms. The Chief Executive Officer and Chief Financial Officer have performed an evaluation of the effectiveness of the design and operation of the registrant's disclosure controls and procedures as of December 31, 2025. Based on that evaluation, the Chief Executive Officer and Chief Financial Officer concluded that the registrant's disclosure controls and procedures were effective as of December 31, 2025.

There have not been any changes in our internal control over financial reporting during our most recent fiscal quarter that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Internal Control Over Financial Reporting

a. Management's Annual Report on Internal Control over Financial Reporting

The management of AT&T is responsible for establishing and maintaining adequate internal control over financial reporting. AT&T's internal control system was designed to provide reasonable assurance as to the integrity and reliability of the published financial statements. AT&T management assessed the effectiveness of the company's internal control over financial reporting as of December 31, 2025. In making this assessment, it used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in Internal Control – Integrated Framework (2013 framework). Based on its assessment, AT&T management believes that, as of December 31, 2025, the Company's internal control over financial reporting is effective based on those criteria.

b. Attestation Report of the Independent Registered Public Accounting Firm

The independent registered public accounting firm that audited the financial statements included in the Annual Report containing the disclosure required by this Item, Ernst & Young LLP, has issued an attestation report on the Company's internal control over financial reporting.

ITEM 9B. OTHER INFORMATION

- a. There is no information that was required to be disclosed in a report on Form 8-K during the fourth quarter of 2025 but was not reported.
- b. In the quarter ended December 31, 2025, none of our directors or officers (as defined in Rule 16a-1(f) of the Exchange Act) adopted or terminated a plan for the purchase or sale of our securities intended to satisfy the affirmative defense conditions of Rule 10b5-1(c) or a non-Rule 10b5-1 trading arrangement for the purchase or sale of our securities, within the meaning of Item 408 of Regulation S-K.

ITEM 9C. DISCLOSURE REGARDING FOREIGN JURISDICTIONS THAT PREVENT INSPECTIONS

Not applicable.

PART III

ITEM 10. DIRECTORS, EXECUTIVE OFFICERS AND CORPORATE GOVERNANCE

Information regarding executive officers required by Item 401 of Regulation S-K is furnished in a separate disclosure at the end of Part I of this report entitled “Information about our Executive Officers.” Information regarding directors required by Item 401 of Regulation S-K is incorporated herein by reference pursuant to General Instruction G(3) from the registrant’s 2026 definitive proxy statement (Proxy Statement) under the heading “Management Proposal Item No. 1. Election of Directors.”

Information required by Item 405 of Regulation S-K is incorporated herein by reference pursuant to General Instruction G(3) from the registrant’s Proxy Statement under the heading “Delinquent Section 16(a) Reports.”

The registrant has a separately-designated standing audit committee established in accordance with Section 3(a)(58)(A) of the Securities Exchange Act of 1934. The members of the committee are Messrs. Luczo and McCallister, and Ms. Mayer and Taylor. The additional information required by Item 407(d)(5) of Regulation S-K is incorporated herein by reference pursuant to General Instruction G(3) from the registrant’s Proxy Statement under the heading “Audit Committee.”

The registrant has adopted a code of ethics entitled “Code of Ethics” that applies to the registrant’s principal executive officer, principal financial officer, principal accounting officer, or controller or persons performing similar functions. The additional information required by Item 406 of Regulation S-K is provided in this report under the heading “General” under Part I, Item 1. Business.

Information required by Item 408(b) of Regulation S-K is incorporated herein by reference pursuant to General Instruction G(3) from the registrant’s Proxy Statement under the heading “Insider Trading Policy.”

ITEM 11. EXECUTIVE COMPENSATION

Information required by this Item is incorporated herein by reference pursuant to General Instruction G(3) from the registrant’s Proxy Statement under the headings “Director Compensation,” “2025 Director Compensation Table,” “CEO Pay Ratio,” “Pay Versus Performance,” and the pages beginning with the heading “Compensation Discussion and Analysis” and ending with, and including, the pages under the heading “Potential Payments upon Change in Control.”

Information required by Item 407(e)(5) of Regulation S-K is included in the registrant’s Proxy Statement under the heading “Compensation Committee Report” and is incorporated herein by reference pursuant to General Instruction G(3) and shall be deemed furnished in this Annual Report on Form 10-K and will not be deemed incorporated by reference into any filing under the Securities Act of 1933 or the Securities Exchange Act of 1934.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED STOCKHOLDER MATTERS

Information required by Item 201(d) of Regulation S-K is included in the registrant’s Proxy Statement under the heading “Equity Compensation Plan Information,” which is incorporated herein by reference pursuant to General Instruction G(3). Information required by Item 403 of Regulation S-K is included in the registrant’s Proxy Statement under the heading “Common Stock Ownership,” which is incorporated herein by reference pursuant to General Instruction G(3).

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE

Information required by Item 404 of Regulation S-K is included in the registrant's Proxy Statement under the heading "Related Person Transactions," which is incorporated herein by reference pursuant to General Instruction G(3). Information required by Item 407(a) of Regulation S-K is included in the registrant's Proxy Statement under the heading "Director Independence," which is incorporated herein by reference pursuant to General Instruction G(3).

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

Information required by this Item is included in the registrant's Proxy Statement under the heading "Principal Accountant Fees and Services," which is incorporated herein by reference pursuant to General Instruction G(3).

PART IV

ITEM 15. EXHIBITS AND FINANCIAL STATEMENT SCHEDULES

(a) Documents filed as a part of the report:

	Page
(1) Report of Independent Registered Public Accounting Firm (PCAOB ID: 42)	39
Financial Statements covered by Report of Independent Registered Public Accounting Firm:	
Consolidated Statements of Income	42
Consolidated Statements of Comprehensive Income	43
Consolidated Balance Sheets	44
Consolidated Statements of Cash Flows	45
Consolidated Statements of Changes in Stockholders' Equity	46
Notes to Consolidated Financial Statements	48
(2) Financial Statement Schedules:	
II - Valuation and Qualifying Accounts	95

Financial statement schedules other than those listed above have been omitted because the required information is contained in the financial statements and notes thereto, or because such schedules are not required or applicable.

(3) Exhibits:

Exhibits identified in parentheses below, on file with the SEC, are incorporated herein by reference as exhibits hereto. Unless otherwise indicated, all exhibits so incorporated are from File No. 001-8610.

Exhibit Number	
2-a	Securities Purchase Agreement, dated September 29, 2024, by and among AT&T Services, Inc., AT&T Diversified MVPD Holdings LLC, AT&T MVPD Holdings LLC, Merlin Parent 2024, Inc., TPG Partners IX, L.P. and DIRECTV Entertainment Holdings LLC (Exhibit 2.1 to Form 10-Q for the period ending September 30, 2024)*
2-b	Purchase Agreement, dated as of May 21, 2025, by and among Lumen Technologies, Inc., the Sellers named therein, Forged Fiber 37, LLC, and, solely for purposes of Section 11.16 thereof, AT&T DW Holdings, Inc. (Exhibit 2.1 to Form 8-K filed on May 21, 2025)*
3-a	Restated Certificate of Incorporation, filed with the Secretary of State of Delaware on December 13, 2013 (Exhibit 3.1 to Form 8-K filed on December 16, 2013)
3-b	Bylaws (Exhibit 3.1 to Form 8-K filed on February 2, 2023)
3-c	Certificate of Designations with respect to Series A Preferred Stock (Exhibit 3.1 to Form 8-K filed on December 12, 2019)
3-d	Certificate of Designations with respect to Series B Preferred Stock (Exhibit 3.1 to Form 8-K filed on February 18, 2020)

-
- 3-e Certificate of Designations with respect to Series C Preferred Stock (Exhibit 3.2 to Form 8-K filed on February 18, 2020)
 - 4-a No instrument which defines the rights of holders of long-term debt of the registrant and all of its consolidated subsidiaries is filed herewith pursuant to Regulation S-K, Item 601(b)(4)(iii)(A), except for the instruments referred to in 4-b, 4-c, 4-d, 4-e, 4-f below. Pursuant to this regulation, the registrant hereby agrees to furnish a copy of any such instrument not filed herewith to the SEC upon request.
 - 4-b Guaranty of certain obligations of Pacific Bell Telephone Co. and Southwestern Bell Telephone Co. (Exhibit 4-c to Form 10-K for the period ending December 31, 2011)
 - 4-c Guaranty of certain obligations of Ameritech Capital Funding Corp., Indiana Bell Telephone Co. Inc., Michigan Bell Telephone Co., Pacific Bell Telephone Co., Southwestern Bell Telephone Company, Illinois Bell Telephone Company, The Ohio Bell Telephone Company, The Southern New England Telephone Company, Southern New England Telecommunications Corporation, and Wisconsin Bell, Inc. (Exhibit 4-d to Form 10-K for the period ending December 31, 2011)
 - 4-d Guarantee of certain obligations of AT&T Enterprises LLC (Exhibit 4-e to Form 10-K for the period ending December 31, 2011)
 - 4-e Indenture, dated as of May 15, 2013, between AT&T Inc. and The Bank of New York Mellon Trust Company, N.A., as Trustee (Exhibit 4.1 to Form 8-K filed on May 15, 2013)
 - 4-f Indenture dated as of November 1, 1994 between SBC Communications Inc. and The Bank of New York, as Trustee (Exhibit 4-h to Form 10-K for the period ending December 31, 2013)
 - 4-g Deposit Agreement, dated December 12, 2019, among AT&T Inc., Computershare Inc. and Computershare Trust Company, N.A., collectively, as depository, and the holders from time to time of the depository receipts described therein (Exhibit 4.3 to Form 8-K filed December 12, 2019)
 - 4-h Deposit Agreement, dated February 18, 2020, among the Company, Computershare Inc. and Computershare Trust Company, N.A., collectively, as depository, and the holders from time to time of the depository receipts described therein (Exhibit 4.3 to Form 8-K filed February 18, 2020)
 - 4-i Description of AT&T's Securities Registered Under Section 12 of the Exchange Act
 - 10-a 2018 Incentive Plan (Exhibit 10-a to Form 10-K for the period ending December 31, 2017)**
 - 10-b 2016 Incentive Plan (Exhibit 10-a to Form 10-Q for the period ending March 31, 2016)**
 - 10-c Resolution Regarding John Stankey (Exhibit 10-b to Form 10-Q for the period ending September 30, 2017)**
 - 10-d 2011 Incentive Plan (Exhibit 10-a to Form 10-Q for the period ending September 30, 2015)**
 - 10-e Short Term Incentive Plan (Exhibit 10-e to Form 10-K for the period ending December 31, 2024)**
 - 10-f Supplemental Life Insurance Plan (Exhibit 10-f to Form 10-K for the period ending December 31, 2024)**
 - 10-g Supplemental Retirement Income Plan (Exhibit 10-e to Form 10-K for the period ending December 31, 2013)**
 - 10-h 2005 Supplemental Employee Retirement Plan (Exhibit 10-g to Form 10-K for the period ending December 31, 2021)**
 - 10-i Salary and Incentive Award Deferral Plan (Exhibit 10-k to Form 10-K for the period ending December 31, 2011)**
 - 10-j Stock Savings Plan (Exhibit 10-l to Form 10-K for the period ending December 31, 2011)**
 - 10-k Stock Purchase and Deferral Plan as amended May 16, 2024 (Exhibit 10.2 to Form 10-Q for the period ending June 30, 2024)**
 - 10-l Cash Deferral Plan as amended May 16, 2024 (Exhibit 10.1 to Form 10-Q for the period ending June 30, 2024)**
 - 10-m Master Trust Agreement for AT&T Inc. Deferred Compensation Plans and Other Executive Benefit Plans and subsequent amendments dated August 1, 1995 and November 1, 1999 (Exhibit 10-dd to Form 10-K for the period ending December 31, 2009)**
 - 10-n Officer Disability Plan (Exhibit 10-n to Form 10-K for the period ending December 31, 2024)**
 - 10-o AT&T Inc. Health Plan (Exhibit 10.1 to Form 10-Q for the period ending June 30, 2025)**
 - 10-p Pension Benefit Makeup Plan No.1 (Exhibit 10-n to Form 10-K for the period ending December 31, 2016)**
 - 10-q AT&T Inc. Equity Retention and Hedging Policy as amended March 24, 2022 (Exhibit 10.2 to Form 10-Q for the period ending March 31, 2022)

10-r	Administrative Plan (Exhibit 10.1 to Form 10-Q for the period ending September 30, 2023)**
10-s	AT&T Inc. Non-Employee Director Stock and Deferral Plan**
10-t	AT&T Inc. Non-Employee Director Stock Purchase Plan (Exhibit 10-t to Form 10-K for the period ending December 31, 2013)**
10-u	AT&T Inc. Board of Directors Communications Concession Program (Exhibit 10-u to Form 10-K for the period ending December 31, 2022)**
10-v	Form of Indemnity Agreement between AT&T Inc. and its directors and officers (Exhibit 10-v to Form 10-K for the period ending December 31, 2023)**
10-w	AT&T Executive Physical Program (Exhibit 10.4 to Form 10-Q for the period ending June 30, 2023)**
10-x	Attorney Fee Payment Agreement for John Stankey (Exhibit 10.1 to Form 8-K filed on July 3, 2018)**
10-y	\$12,000,000,000 Second Amended and Restated Credit Agreement, dated as of November 3, 2025, among AT&T Inc., the lenders named therein and Citibank, N.A., as agent (Exhibit 10.1 to Form 8-K filed on November 3, 2025)
10-z	\$17,500,000,000 Delayed Draw Term Loan Credit Agreement, dated as of November 3, 2025, among AT&T Inc., the lenders named therein and Bank of America, N.A., as agent (Exhibit 10.2 to Form 8-K filed on November 3, 2025)
10-aa	Third Amended and Restated Limited Liability Company Agreement of NCWPCS MPL Holdings, LLC (Exhibit 10.1 to Form 10-Q for the period ending September 30, 2024)*
10-bb	AT&T Inc. Change in Control Severance Plan (Exhibit 10-aa to Form 10-K for the period ending December 31, 2024)**
10-cc	Relocation Program Plan (Exhibit 10.2 to Form 10-Q for the period ending September 30, 2021)**
10-dd	Fourth Amended and Restated Limited Liability Company Agreement of AT&T Fiber Investment, LLC (Exhibit 10-ii to Form 10-K for the period ending December 31, 2024)*
10-ee	License Purchase Agreement, dated August 25, 2025, by and among EchoStar Corporation, the other parties set forth therein, and AT&T Mobility II LLC (Exhibit 10.1 to Form 10-Q for the period ending September 30, 2025)*
19	Insider Trading Policy (Exhibit 19 to Form 10-K for the period ending December 31, 2024)
21	Subsidiaries of AT&T Inc.
23	Consent of Ernst & Young LLP
24	Powers of Attorney
31	Rule 13a-14(a)/15d-14(a) Certifications
31.1	Certification of Principal Executive Officer
31.2	Certification of Principal Financial Officer
32	Section 1350 Certification
97	AT&T Inc. Clawback Policy (Exhibit 97 to Form 10-K for the period ending December 31, 2023)
99	Supplemental Interim Financial Information
101	The consolidated financial statements from the Company's Form 10-K for the year ended December 31, 2025, as filed with the SEC on February 9, 2026, formatted in Inline XBRL: (i) Consolidated Statements of Cash Flows, (ii) Consolidated Statements of Operations, (iii) Consolidated Statements of Comprehensive Income, (iv) Consolidated Balance Sheets, and (v) Notes to Consolidated Financial Statements, tagged as blocks of text and including detailed tags.
104	Cover Page Interactive Data File (formatted as Inline XBRL and contained in Exhibit 101)

* Certain schedules (or similar attachments) have been omitted pursuant to Item 601(a)(5) or Item 601(b)(2) of Regulation S-K. The registrant agrees to furnish copies of such schedules (or similar attachments) to the U.S. Securities and Exchange Commission upon request.

** Management contracts and compensatory plans and arrangements required to be filed as exhibits pursuant to Item 15(b) of this report.

We will furnish to stockholders upon request, and without charge, a copy of the Annual Report to Stockholders and the Proxy Statement, portions of which are incorporated by reference in the Form 10-K. We will furnish any other exhibit at cost.

ITEM 16. FORM 10-K SUMMARY

None.

SCHEDULE II – VALUATION AND QUALIFYING ACCOUNTS

Allowance for Credit Losses

COL. A	COL. B	COL. C			COL. D	COL. E
		Additions				
		(1)	(2)	(3)		
	Balance at Beginning of Period	Charged to Costs and Expenses (a)	Charged to Other Accounts	Acquisitions	Deductions (b)	Balance at End of Period (c)
Year 2025	\$ 553	2,271	—	—	2,174	\$ 650
Year 2024	\$ 756	1,969	—	—	2,172	\$ 553
Year 2023	\$ 1,011	1,969	—	—	2,224	\$ 756

(a) Includes amounts previously written off which were credited directly to this account when recovered.

Excludes direct charges and credits to expense for nontrade receivables in the consolidated statements of income.

(b) Amounts written off as uncollectible.

(c) Includes balances applicable to trade receivables, loans, contract assets and other assets subject to credit loss measurement (see Note 1).

Allowance for Deferred Tax Assets

COL. A	COL. B	COL. C			COL. D	COL. E
		Additions				
		(1)	(2)	(3)		
	Balance at Beginning of Period	Charged to Costs and Expenses	Charged to Other Accounts	Acquisitions	Deductions	Balance at End of Period
Year 2025	\$ 4,338	(360)	—	—	—	\$ 3,978
Year 2024	\$ 4,656	(318)	—	—	—	\$ 4,338
Year 2023	\$ 4,175	481	—	—	—	\$ 4,656

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized, on the 9th day of February, 2026.

AT&T INC.

/s/ Pascal Desroches

Pascal Desroches

Senior Executive Vice President
and Chief Financial Officer

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the date indicated.

Principal Executive Officer:

John T. Stankey*
Chairman of the Board,
Chief Executive Officer and President

Principal Financial Officer:

Pascal Desroches
Senior Executive Vice President
and Chief Financial Officer

/s/ Pascal Desroches

Pascal Desroches, as attorney-in-fact
and on his own behalf as Principal
Financial Officer

Principal Accounting Officer:

Sabrina Sanders
Senior Vice President, Chief
Accounting Officer and Controller

/s/ Sabrina Sanders

February 9, 2026

Directors:

John T. Stankey*
William E. Kennard*
Kelly J. Grier*
Marissa A. Mayer*
Michael B. McCallister*

Beth E. Mooney*
Matthew K. Rose*
Cynthia B. Taylor*
Luis A. Ubiñas*

* by power of attorney

References

¹Reached locations with fiber include consumer and business locations (i) passed with fiber, and (ii) served with fiber through commercial open-access providers.

²EBITDA is net income plus income tax, interest, and depreciation and amortization expenses minus equity in net income of affiliates and other income (expense) — net. Adjusted EBITDA is calculated by excluding from EBITDA certain significant items that are non-operational or non-recurring in nature, including dispositions and merger integration and transaction costs, significant abandonments and impairments, benefit-related gains and losses, employee separation, and other material gains and losses. For 2025, adjusted EBITDA of \$46.4 billion is calculated as net income of \$23.4 billion, plus income tax expense of \$3.6 billion, plus interest expense of \$6.8 billion, minus equity in net income of affiliates of \$1.9 billion, minus other income (expense) — net of \$7.8 billion, plus depreciation and amortization of \$20.9 billion, plus adjustments of \$1.3 billion, which include transaction, legal and other operating costs. Transaction, legal and other costs include certain legal reserves and settlements that cover extended historical periods and/or are unpredictable in both magnitude and timing, and therefore are distinct and separate from normal, recurring legal matters. Such costs are presented net of expected insurance recoveries and are primarily associated with legacy legal matters and the expected resolution of certain litigation associated with cyberattacks disclosed in 2024. The year ended December 31, 2025, also includes approximately \$440 million of apportioned property and casualty settlements. For 2024, adjusted EBITDA of \$44.8 billion is calculated as net income of \$12.3 billion, plus income tax expense of \$4.4 billion, plus interest expense of \$6.8 billion, minus equity in net income of affiliates of \$2.0 billion, minus other income (expense) — net of \$2.4 billion, plus depreciation and amortization of \$20.6 billion, plus adjustments of \$5.1 billion. Adjusted EBITDA margin for 2025 of 36.9% is calculated as adjusted EBITDA of \$46.4 billion divided by total operating revenues of \$125.6 billion.

Adjusted EBITDA margin for 2024 of 36.6% is calculated as adjusted EBITDA of \$44.8 billion divided by total operating revenues of \$122.3 billion. Adjustments for all periods are detailed in the Discussion and Reconciliation of Non-GAAP Measures included in our Form 8-K dated January 28, 2026.

³Capital investment includes capital expenditures and cash paid for vendor financing. For 2025, capital expenditures were \$20.8 billion and cash paid for vendor financing was \$1.2 billion.

⁴Net debt-to-adjusted EBITDA is calculated by dividing net debt by the sum of the most recent four quarters of adjusted EBITDA. Net debt is calculated by subtracting cash and cash equivalents and time deposits (deposits at financial institutions that are greater than 90 days, e.g., certificates of deposit and time deposits), from total debt. Net debt-to-adjusted EBITDA of 2.63x at March 31, 2025, is calculated as net debt of \$119.1 billion (total debt of \$126.2 billion less cash and cash equivalents of \$6.9 billion and time deposits of \$0.2 billion) divided by the sum of adjusted EBITDA beginning with the second quarter of 2024 through the first quarter of 2025 of \$45.2 billion. Reconciliations between GAAP and non-GAAP measures are available on AT&T's Investor Relations website.

⁵Adjusted EBITDA, adjusted EPS and free cash flow estimates depend on future levels of revenues, expenses, cash from operating activities, capital expenditures and vendor financing payments, which are not reasonably estimable at this time. Accordingly, we cannot provide reconciliations between these projected non-GAAP metrics and the most comparable GAAP metrics without unreasonable effort.

AT&T Inc. Board of Directors



John Stankey, 63 ⁽³⁾

Chairman of the Board,
Chief Executive Officer and President
AT&T Inc.
Director since 2020
Background: Telecommunications, technology



Beth E. Mooney, 71 ^(3,4,5)

Retired Chairman and Chief Executive Officer
KeyCorp
Director since 2013
Background: Banking



William E. Kennard, 69 ⁽⁴⁾

Independent Lead Director
Former U.S. Ambassador to the European Union
Former Chairman of the Federal
Communications Commission
Director since 2014
Background: Law, telecommunications,
public policy



Matthew K. Rose, 66 ^(2,3,4)

Retired Chairman and Chief Executive Officer
Burlington Northern Santa Fe, LLC
Director since 2010
Background: Freight transport



Kelly J. Grier, 56 ^(2,5)

Retired U.S. Chair and Managing Partner (CEO)
Ernst & Young, LLP
Director since 2025
Background: Public accounting, financial
reporting, audit quality, regulatory matters



Cynthia B. Taylor, 64 ^(1,3)

President and Chief Executive Officer
Oil States International, Inc.
Director since 2013
Background: Public accounting, oil and gas



Stephen J. Luczo, 68 ^(1,2,3)

Senior Partner
Crosspoint Capital Partners, L.P.
Director since 2019
Background: Technology, finance,
operations management



Luis A. Ubiñas, 63 ^(4,5)

Chairman
The Statue of Liberty – Ellis Island Foundation
Director since 2021
Background: Telecommunications,
government, nonprofits



Marissa A. Mayer, 50 ^(1,2)

Founder and Chief Executive Officer
Dazzle AI Inc.
Director since 2024
Background: Technology, consumer



Michael B. McCallister, 73 ^(1,5)

Retired Chairman of the Board
and Chief Executive Officer
Humana Inc.
Director since 2013
Background: Healthcare

Committees of the Board:

- (1) Audit
- (2) Corporate Development and Finance
- (3) Executive
- (4) Governance and Policy
- (5) Human Resources

Information is provided as of February 9, 2026.

Executive Officers of AT&T Inc. and Its Affiliates



John Stankey, 63

Chairman of the Board,
Chief Executive Officer and President



Lori Lee, 60

Global Marketing Officer and
Senior Executive Vice President
– International



Pascal Desroches, 61

Senior Executive Vice President
and Chief Financial Officer



Jeremy Legg, 56

Chief Technology Officer
AT&T Services, Inc.



Ed Gillespie, 64

Senior Executive Vice President
– External and Legislative Affairs
AT&T Services, Inc.



David R. McAtee II, 57

Senior Executive Vice President
and General Counsel



Darcie Henry, 54

Senior Executive Vice President and
Chief Human Resources Officer



Jeff McElfresh, 55

Chief Operating Officer



Kellyn Smith Kenny, 48

Chief Marketing and Growth Officer

[THIS PAGE INTENTIONALLY LEFT BLANK]

[THIS PAGE INTENTIONALLY LEFT BLANK]

Stockholder Information

Toll-Free Stockholder Hotline

Call us at **1-800-351-7221** between 8 a.m. and 8 p.m. Eastern time, Monday through Friday (**TDD 1-888-403-9700**) for help with:

- Common stock account inquiries.
- Requests for assistance with your common stock account, including stock transfers.
- Information on The DirectSERVICE™ Investment Program for Stockholders of AT&T Inc. (sponsored and administered by Computershare Trust Company, N.A.).

Written Stockholder Requests

Please mail all account inquiries and other requests for assistance regarding your stock ownership to:

AT&T Inc.
c/o Computershare Trust Company, N.A.
P.O. Box 43078
Providence, RI 02940-3078

You may also reach the transfer agent for AT&T Inc. at att@computershare.com or visit the website at **computershare.com/att**

DirectSERVICE Investment Program

The DirectSERVICE Investment Program for Stockholders of AT&T Inc. is sponsored and administered by Computershare Trust Company, N.A. The program allows current stockholders to reinvest dividends or purchase additional AT&T Inc. stock. For more information, call **1-800-351-7221**.

Stock Trading Information

AT&T Inc. is listed on the New York Stock Exchange with a dual listing of its common stock on NYSE Texas. Ticker symbol: T

Information on the Internet

Information about AT&T Inc. is available on the internet at **about.att.com**

Annual Meeting

The 2026 Annual Meeting of Stockholders of AT&T Inc. will be conducted virtually on the internet at 3:30 p.m. Central time, Thursday, May 14, 2026. There will be no in-person meeting. The meeting will be accessible at **meetnow.global/ATT2026**

SEC Filings

AT&T Inc.'s U.S. Securities and Exchange Commission filings, including the latest 10-K and proxy statement, are available on our website at **investors.att.com**

Investor Relations

Securities analysts and other members of the professional financial community may contact the Investor Relations staff as listed on our website at **investors.att.com**

Independent Auditor

Ernst & Young LLP
2323 Victory Ave., Suite 2000
Dallas, TX 75219

Corporate Offices and Non-Stockholder Inquiries

AT&T Inc.
208 S. Akard St.
Dallas, TX 75202
210-821-4105





Appendix M - PSAP Implementation Project Plan Nebraska AT&T

[illegible]

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Resource Names
20	Process and Send Service Order Requests, along with all pre-sale work products	1 day	Mon 12/1/25	Mon 12/1/25		21	AT&T
21	Service Order Request Received	0 days	Mon 12/1/25	Mon 12/1/25	20	23	Intrado, AT&T
22	Service Order Acceptance	0 days	Mon 12/1/25	Mon 12/1/25			
23	Review Service Order and Send Acceptance	0 days	Mon 12/1/25	Mon 12/1/25	21	24, 39, 26, 41	Intrado
24	Send Intrado PSAP IDs with Service Order Acceptance	0 days	Mon 12/1/25	Mon 12/1/25	23		Intrado
25	Project Planning	13 days	Tue 12/2/25	Thu 12/18/25			
26	ESInet Project Kickoff	1 day	Tue 12/2/25	Tue 12/2/25	23	28, 27, 164	Intrado, AT&T
27	Escalation and Contact Info sharing	1 day	Wed 12/3/25	Wed 12/3/25	26	28	Intrado, AT&T
28	Introductory call with customer	1 day	Thu 12/4/25	Thu 12/4/25	27, 26	31, 29	Intrado, AT&T
29	Collaborate on overall project schedule and individual PSAP IPPs	10 days	Fri 12/5/25	Thu 12/18/25	28		Intrado, AT&T
30	Customer Kick-Off Meeting	25 days	Fri 12/5/25	Thu 1/22/26			
31	Presentation, materials, and discussion - Project team and customer	10 days	Fri 12/5/25	Thu 12/18/25	28	32	AT&T
32	Conduct PSAP Customer Kickoffs	15 days	Fri 12/19/25	Thu 1/22/26	31	34, 43FF+2 wks	AT&T
33	PSAP Site Survey	30 days	Fri 1/23/26	Thu 3/5/26		50	
34	Conduct PSAP site visits	20 days	Fri 1/23/26	Thu 2/19/26	32	35	AT&T
35	Complete site assessments	10 days	Fri 2/20/26	Thu 3/5/26	34	36	AT&T
36	Deliver PSAP Site Assessments to customers	0 days	Thu 3/5/26	Thu 3/5/26	35	54	AT&T
37	Infrastructure Data Collection	5 days	Tue 12/2/25	Mon 12/8/25		50	
38	Aggregation Site Evaluation	5 days	Tue 12/2/25	Mon 12/8/25			
39	Aggregation Site Location identification. If any new locations are needed, follow Aggregation Site creation project plan	5 days	Tue 12/2/25	Mon 12/8/25	23		Intrado, AT&T
40	ESInet Network Requirements	5 days	Tue 12/2/25	Mon 12/8/25			

S

N

J

M

M

J

S

N

J

M

M

J

S

PSAP Implementation Project Plan Nebraska AT&T

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Resource Names	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
								S	N	J	M	M	J	S	N	J	M	M	J	S			
41	Identify Specific PSAP Requirements (carrier circuits, last mile,circuit sizing etc)	5 days	Tue 12/2/25	Mon 12/8/25	23	66	Intrado,AT&T																
42	GIS Data Readiness	21 days	Thu 2/5/26	Thu 3/5/26																			
43	Training session #1	1 day	Thu 2/5/26	Thu 2/5/26	32FF+2 wks	44FF+3 wks,45FF+2 wks																	
44	Training session #2	1 day	Thu 2/26/26	Thu 2/26/26	43FF+3 wks																		
45	Customer submits GIS Data	1 day	Thu 2/19/26	Thu 2/19/26	43FF+2 wks	46	AT&T																
46	Initial error report provided	0 days	Thu 2/19/26	Thu 2/19/26	45	47	Intrado																
47	Work to correct errors and map fields	10 days	Fri 2/20/26	Thu 3/5/26	46	48FF	Intrado																
48	Resubmit GIS Data	1 day	Thu 3/5/26	Thu 3/5/26	47FF	49	Intrado,AT&T																
49	GIS Data Preparation Complete	0 days	Thu 3/5/26	Thu 3/5/26	48	121,50	Intrado,AT&T																
50	Data Collection Complete	0 days	Thu 3/5/26	Thu 3/5/26	49,5,37,33	51																	
51	Definition Phase Complete	0 days	Thu 3/5/26	Thu 3/5/26	50																		
52	Architecture Phase	69 days	Mon 12/1/25	Thu 3/19/26																			
53	PSAP Site Remediation	10 days	Fri 3/6/26	Thu 3/19/26																			
54	Review Customer PSAP Site Requirements	5 days	Fri 3/6/26	Thu 3/12/26	36	55	Intrado,AT&T																
55	Identify Customer PSAP Site Remediation	5 days	Fri 3/13/26	Thu 3/19/26	54	112	Intrado,AT&T																
56	Network Design	40 days	Mon 12/1/25	Fri 2/6/26		71																	
57	Regional Ingress Network Design	40 days	Mon 12/1/25	Fri 2/6/26																			
58	ILEC and other existing service provider interconnection requirements	5 days	Mon 1/19/26	Fri 1/23/26	10	63,80	AT&T																
59	Facilitate inter-local agreements	10 days	Mon 1/19/26	Fri 1/30/26	10	63	AT&T																
60	Legacy SR and other existing service providerinterconnection paths	10 days	Mon 1/19/26	Fri 1/30/26	10	63	AT&T																
61	Split rate center design	10 days	Mon 1/19/26	Fri 1/30/26	10	63	AT&T																
62	OSP interconnection design	20 days	Mon 12/1/25	Fri 1/9/26		63	AT&T																
63	Ingress Network Design review	5 days	Mon 2/2/26	Fri 2/6/26	58,59,60,61,62	64	Intrado,AT&T																

Page 3

PSAP Implementation Project Plan Nebraska AT&T

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Resource Names	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	
64	Ingress Network design finalized	0 days	Fri 2/6/26	Fri 2/6/26	63		Intrado,AT&T	S	N	J	M	M	J	S	N	J	M	M	J	S
65	Egress Network Design (to PSAPs)	25 days	Tue 12/9/25	Mon 1/26/26																
66	Customer PSAP MPLS circuit connection design	10 days	Tue 12/9/25	Mon 1/5/26	41	67,68	Intrado,AT&T													
67	Customer PSAP LAN design	10 days	Tue 1/6/26	Mon 1/19/26	66	69	Intrado													
68	ESInet interconnection design	5 days	Tue 1/6/26	Mon 1/12/26	66	69	Intrado													
69	ESInet Design Review	5 days	Tue 1/20/26	Mon 1/26/26	67,68	70	Intrado,AT&T													
70	Finalize PSAP Customer Architecture	0 days	Mon 1/26/26	Mon 1/26/26	69	122,123,124	Intrado,AT&T													
71	Architecture Review	2 days	Mon 2/9/26	Tue 2/10/26	56	72	Intrado,AT&T													
72	Architecture Phase Complete	0 days	Tue 2/10/26	Tue 2/10/26	71	114,76,77														
73	Integration Phase	87 days	Tue 1/6/26	Wed 5/6/26																
74	POI to Agg Site Network for Region	45 days	Wed 2/11/26	Tue 4/14/26		128														
75	Create POI Facility	45 days	Wed 2/11/26	Tue 4/14/26																
76	Physical Work	30 days	Wed 2/11/26	Tue 3/24/26	72		AT&T													
77	POI to Agg Site Circuit Orders	30 days	Wed 2/11/26	Tue 3/24/26	72	78	AT&T													
78	POI to Agg Site Trunk Orders	15 days	Wed 3/25/26	Tue 4/14/26	77		AT&T													
79	FSR Interconnection Process for Region	73 days	Mon 1/26/26	Wed 5/6/26		128														
80	Confirm FSR 9-1-1 contacts	1 day	Mon 1/26/26	Mon 1/26/26	58,12	81	AT&T													
81	Circuit orders to FSRs	45 days	Tue 1/27/26	Mon 3/30/26	80	84,85	AT&T													
82	Connections to FSR & Transit Solution for Region	27 days	Tue 3/31/26	Wed 5/6/26																
83	Trunk orders	23 days	Tue 3/31/26	Thu 4/30/26																
84	Create Trunk Model Diagram	1 day	Tue 3/31/26	Tue 3/31/26	81	86	Intrado,AT&T													
85	FOC ILEC Trunk Orders	15 days	Tue 3/31/26	Mon 4/20/26	81	88	Intrado													
86	Submit Originating and Transfer Trunk Orders	15 days	Wed 4/1/26	Tue 4/21/26	84	87	Intrado													
87	Transfer Trunk Test and Turn Up	2 days	Wed 4/22/26	Thu 4/23/26	86	88	Intrado,AT&T													
88	Provision Trunks in ESInet	3 days	Fri 4/24/26	Tue 4/28/26	87,85	89,91	Intrado													

PSAP Implementation Project Plan Nebraska AT&T

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Resource Names	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	
								S	N	J	M	M	J	S	N	J	M	M	J	S
89	Perform Unit Testing	2 days	Wed 4/29/26	Thu 4/30/26	88		Intrado,AT&T													
90	End to End Circuit testing with FSR	2 days	Wed 4/29/26	Thu 4/30/26																
91	FSR Circuit Testing	1 day	Wed 4/29/26	Wed 4/29/26	88	92,93	Intrado,AT&T													
92	Confirm gain settings	1 day	Thu 4/30/26	Thu 4/30/26	91		Intrado													
93	FSR Circuit Testing Complete	0 days	Wed 4/29/26	Wed 4/29/26	91	95														
94	FSR Transit Routing Solution	5 days	Thu 4/30/26	Wed 5/6/26																
95	Submit Formal Transition request notification to FSR ILEC	1 day	Thu 4/30/26	Thu 4/30/26	93	96,98	AT&T													
96	Determine routing ESN from FSR to Intrado	2 days	Fri 5/1/26	Mon 5/4/26	95		Intrado													
97	Test Transit Routing Solution with FSR ILEC	4 days	Fri 5/1/26	Wed 5/6/26																
98	Create Transit Test Plan	1 day	Fri 5/1/26	Fri 5/1/26	95	99	Intrado													
99	Confirm Transit Test Plan w/ ILEC	1 day	Mon 5/4/26	Mon 5/4/26	98	100	Intrado,AT&T													
100	Schedule Transit testing with ILEC	1 day	Tue 5/5/26	Tue 5/5/26	99	101	AT&T													
101	Conduct Routing Solution testing	1 day	Wed 5/6/26	Wed 5/6/26	100	103FF,102	Intrado,AT&T													
102	ESINet Implementation/Testing Complete	0 days	Wed 5/6/26	Wed 5/6/26	101															
103	FSR Transit routing solution confirmed	1 day	Wed 5/6/26	Wed 5/6/26	101FF		AT&T													
104	Equipment Installation - PSAP #1	36 days	Wed 3/4/26	Wed 4/22/26		128														
105	Order edge routers and PDUs	20 days	Wed 3/4/26	Tue 3/31/26	114FS-30 days	106	Intrado													
106	Schedule equipment Installation with PSAP	3 days	Fri 4/17/26	Tue 4/21/26	105,112		AT&T													
107	Ship PSAP Equipment to PSAP	5 days	Wed 4/1/26	Tue 4/7/26	114FS-10 days	108,123	Intrado													
108	Installation of edge routers and PDUs	2 days	Wed 4/15/26	Thu 4/16/26	107,114	116	AT&T													
109	Equipment and Network Test and Turn-up	2 days	Tue 4/21/26	Wed 4/22/26	117	110	Intrado,AT&T													
110	Equipment Installation Complete	0 days	Wed 4/22/26	Wed 4/22/26	109	119														
111	Egress Network Ordering and Turn Up for PSAP #1	52 days	Wed 2/11/26	Thu 4/23/26		128														
112	Confirm PSAP #1 site remediation is complete	20 days	Fri 3/20/26	Thu 4/16/26	55	106	AT&T													

Page 5

[illegible]

[illegible]

PSAP Implementation Project Plan Nebraska AT&T

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Resource Names	1st Quarter S	2nd Quarter N	3rd Quarter J	4th Quarter M	1st Quarter M	2nd Quarter J	3rd Quarter S	4th Quarter N	1st Quarter J	2nd Quarter M	3rd Quarter M	4th Quarter J	1st Quarter S
158	Go / No Go for Cutover	1 day	Tue 5/19/26	Tue 5/19/26	143,144,156	159,135FS-1	Intrado,AT&T													
159	Systems Cutover Event	1 day	Wed 5/20/26	Wed 5/20/26	158	160	Intrado,AT&T													
160	Cutover Complete	0 days	Wed 5/20/26	Wed 5/20/26	159	161														
161	PSAP Voice Live	0 days	Wed 5/20/26	Wed 5/20/26	160	171,172,168,														
162	Begin billing	0 days	Wed 5/20/26	Wed 5/20/26	161		Intrado,AT&T													
163	PSAP Deployment - Balance Of PSAPs	371 days	Wed 12/3/25	Wed 5/19/27																
164	Execute PSAP deployment prep steps for balance of 126 PSAPs - prep can be run concurrently	18 mons	Wed 12/3/25	Tue 5/4/27	26															
165	Schedule and execute cutovers for balance of PSAPs	13 mons	Thu 5/21/26	Wed 5/19/27	161															
166	Maintenance Phase - Begins with PSAP #1 Live and continues as other PSAPs go live	320 days	Wed 5/20/26	Wed 8/11/27																
167	Manage Regional OSP direct connections	320 days	Thu 5/21/26	Wed 8/11/27			Intrado,AT&T													
168	Create target migration plan for OSP direct connections	10 days	Thu 5/21/26	Wed 6/3/26	161	169,170SS+1 mon														
169	Facilitate OSP circuit orders, ongoing until completed	13 mons	Thu 6/4/26	Wed 6/2/27	168		AT&T													
170	Provision, test, and turn up OSP trunks as orders are received	15 mons	Thu 6/18/26	Wed 8/11/27	168SS+1 mon		Intrado													
171	Handoffs for ongoing System Maintenance and Support	0 days	Wed 5/20/26	Wed 5/20/26	161		Intrado,AT&T													
172	NOC monitoring and support begins	0 days	Wed 5/20/26	Wed 5/20/26	161															

Page 8