WHITEPAPER

When the Call Has to Get Through

A field brief for county 911 directors, emergency communications leaders, and the county IT and executive teams who fund and approve their networks.

By Anthony Rasco, Managing Director, SLED, Lightpath

Every county 911 director I work with carries the same core promise, whether it's written down or not: When someone calls 911, the call gets through, and the people who answer it have what they need to send the right help fast. Next Generation 911 (NG911) exists to make that promise stronger. It changes what a 911 center can know the moment a call comes in.

Agencies across New York, New Jersey, Connecticut and Massachusetts are moving toward NG911 for the response it enables, not the technology itself. NG911 brings voice, data, text and video into one platform so that responders arrive with situational awareness instead of just a phone call and an address.

That can change what happens before anyone reaches the scene.

- A traffic accident can put live video in front of a dispatcher, and into a responding officer's vehicle
- A domestic-violence caller who cannot safely speak can text, send photos and share video, so that the officers walking up to the door already know what they are walking into
- A structure fire call can surface building floor plans and live exterior video, so the first engine on scene already knows the layout and where to stage

The point is speed and the quality of the response: fire, police and emergency medical services working from the same picture, sooner.

Legacy 911 equipment cannot carry that.

NG911 promises better information reaching more responders faster. But that promise depends on the network underneath it. And a promise that the center never goes dark is only as good as the path the call travels to get there.

What NG911 Actually Asks of Your Network

NG911 is built to a published standard. The architecture most agencies are building toward is NENA i3, the National Emergency Number Association's i3 Standard for Next Generation 9-1-1 (NENA-STA-010). It is a consensus, non-proprietary standard that defines the pieces of a complete NG911 system: an Emergency Services IP Network (ESInet) that carries the traffic, the NG911 Core Services that route and process the calls, and the use of standard internet protocol (IP) signaling so that calls, text and media move between agencies.

To do what NG911 promises, the network has to do two things well:

- Carry more information without slowing down. The system now has to move large files, such as video, images and mapping data, at the same time as voice, and it cannot lag when it matters most.
- Keep the whole response network connected. The public safety answering points (PSAPs) that take the calls, the backup centers that take over when a primary center fails, and the NG911 platform itself all have to stay in constant communication with one another.

That's where physical network path diversity comes in.

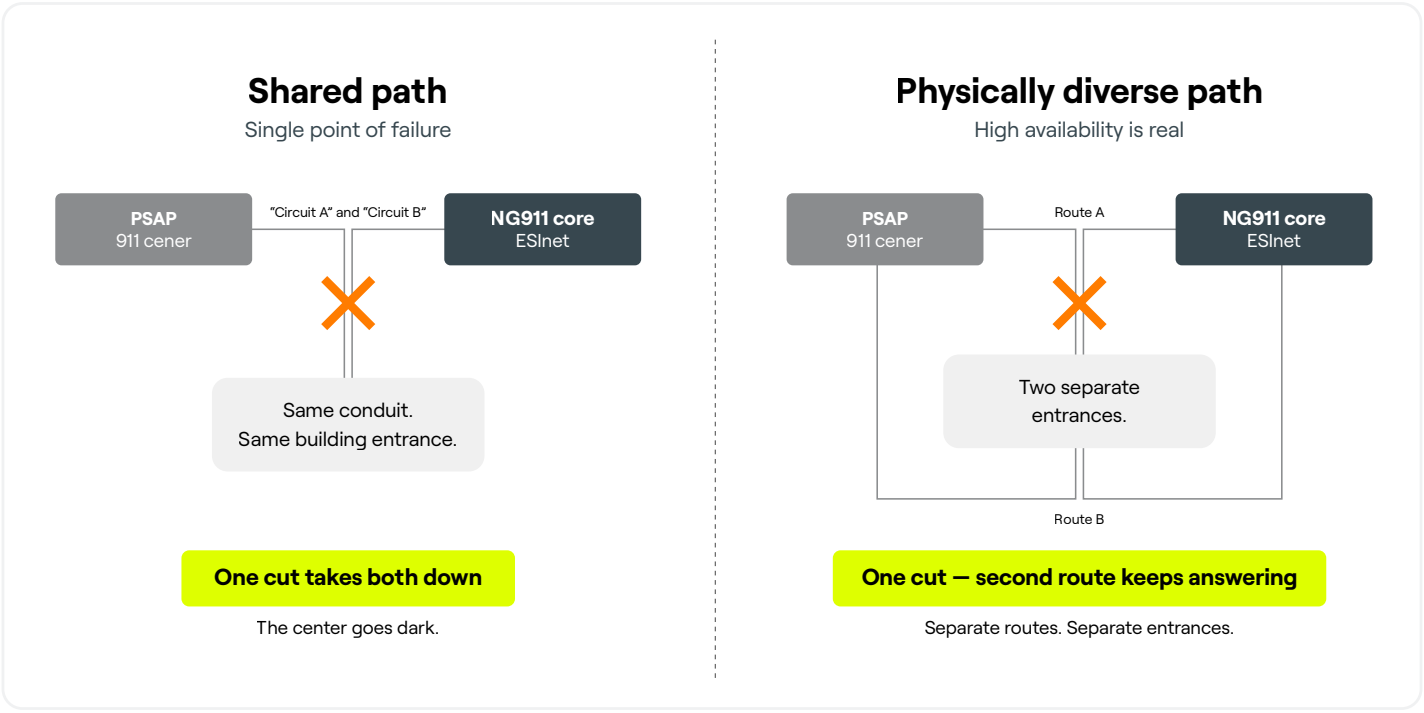
Let's be precise about why: diverse, redundant network paths are the foundation that makes high availability real.

High availability is the ability to keep operating when something breaks, and you cannot keep operating across a break if every path runs through the same conduit, the same building entrance or the same single carrier.

High availability keeps 911 running. Diversity is what makes that possible. It lets the system fail over to a second physically separate route, or a third, and keep answering.

Everything NG911 is supposed to deliver sits on top of that foundation. If the foundation is single path, the rest is a promise you cannot keep on the worst day.

Fig 1. Two Circuits Aren't Diverse if They Share One Path



When There Was No Second Path

Three recent disruptions in the Northeast make the risk concrete, and not one of them involved a cyberattack. Each came down to a single point of failure in the path.

Massachusetts: June 18, 2024

At about 1:15 p.m., the Massachusetts State 911 Department identified a statewide interruption to 911 service. It lasted roughly two hours, until service was fully restored at 3:15 p.m. The cause was a firewall, a protective element, that stopped calls from reaching dispatch centers; the state and its vendor confirmed it was not a cyberattack.

For those two hours, a single shared element sat between callers and every one of the commonwealth's 204 PSAPs, which together averaged about 8,800 calls a day the year before.

One shared component took down 911 across an entire state.[1]

[1] Massachusetts State 911 Department, "Massachusetts State 911 Department Determined Firewall Caused Statewide 911 Disruption," June 19, 2024.

Connecticut: October 22, 2024

Beginning around 11:50 a.m. and lasting until about 2:10 p.m., 911 service failed across Connecticut, including New Haven, Hartford and Danbury. Officials attributed it to an equipment failure within a single commercial carrier's transmission system, with no sign of a deliberate attack.

Landline calls and one major carrier's wireless calls did not complete; only about 130 calls reached New Haven's PSAP, from subscribers on two other wireless carriers whose traffic took a different route. Residents were directed to alternate emergency numbers while the system was down.

The lesson is hard to miss: when call delivery depends on one carrier's transport, that carrier's bad afternoon becomes a statewide 911 failure.[2]

AT&T, Nationwide: February 22, 2024

This one reached well beyond the Northeast, so I'm including it here because the federal government investigated it and published the findings.

A misconfigured network element, installed at 2:42 a.m. without adequate review, drove AT&T's mobility network into a protective shutdown three minutes later. More than 125 million devices were affected and over 25,000 calls to 911 were blocked; full restoration took at least 12 hours.

It also hit public safety directly: FirstNet was unavailable from 2:45 a.m. to 5:00 a.m. Although AT&T restored FirstNet ahead of commercial service, it did not notify FirstNet customers until about three hours in, nearly an hour after service was already back.

A single misconfigured element blocked 25,000 calls to 911 and took 125 million devices offline.[3]

The Massachusetts, Connecticut and AT&T outages were all continuity failures. The path went down, and there was no physically separate path to carry the load. Every minute a 911 system is dark is a minute someone cannot reach help. That is what's at stake, stated plainly, and it is why these events stay in the record long after service is restored.

---

[2] New Haven Independent, "What Went Down When 911 Went Down," Oct. 23, 2024

[3] Federal Communications Commission, Report on the February 22, 2024 AT&T Mobility Network Outage (DOC-404150A1), July 2024

The Transport Question Behind the Transition

The federal transition to NG911 is no longer theoretical. In Report and Order FCC 24-78, adopted in July 2024, the Federal Communications Commission (FCC) put a mechanism in place that lets a 911 Authority require originating service providers to deliver 911 traffic in modern IP format to the state's designated delivery points, once the authority certifies it can receive and route that traffic.[4] The Commission has since moved to look harder at the reliability of the transport that carries this traffic, including dedicated high-capacity facilities that aggregate 911 traffic from multiple carriers.[5]

Here's the part that gets missed in the rush to "go IP." Modern IP signaling makes 911 traffic faster and more capable. But it does nothing about the path that traffic rides.

The same single-path exposure that took down Massachusetts and Connecticut survives the conversion intact. Only now, it's single-path IP.

The Order assumes resilient transport is already underneath it. The Commission's closer look at transport makes the point clear: resilience doesn't arrive with the protocol. Someone still has to fund and build it.

What Real Separation Looks Like in Practice

Network diversity is a Layer 0 question, about the fiber in the ground and the conduits and buildings it passes through. Two circuits that ride the same physical route, enter the same building through the same vault or hand off through the same single carrier are not diverse.

Real diversity means physically separate routes and separate building entrance facilities, with the ability to fail over to an alternate path, and where it matters, to an adjacent county's PSAP, without depending on the link that just failed.

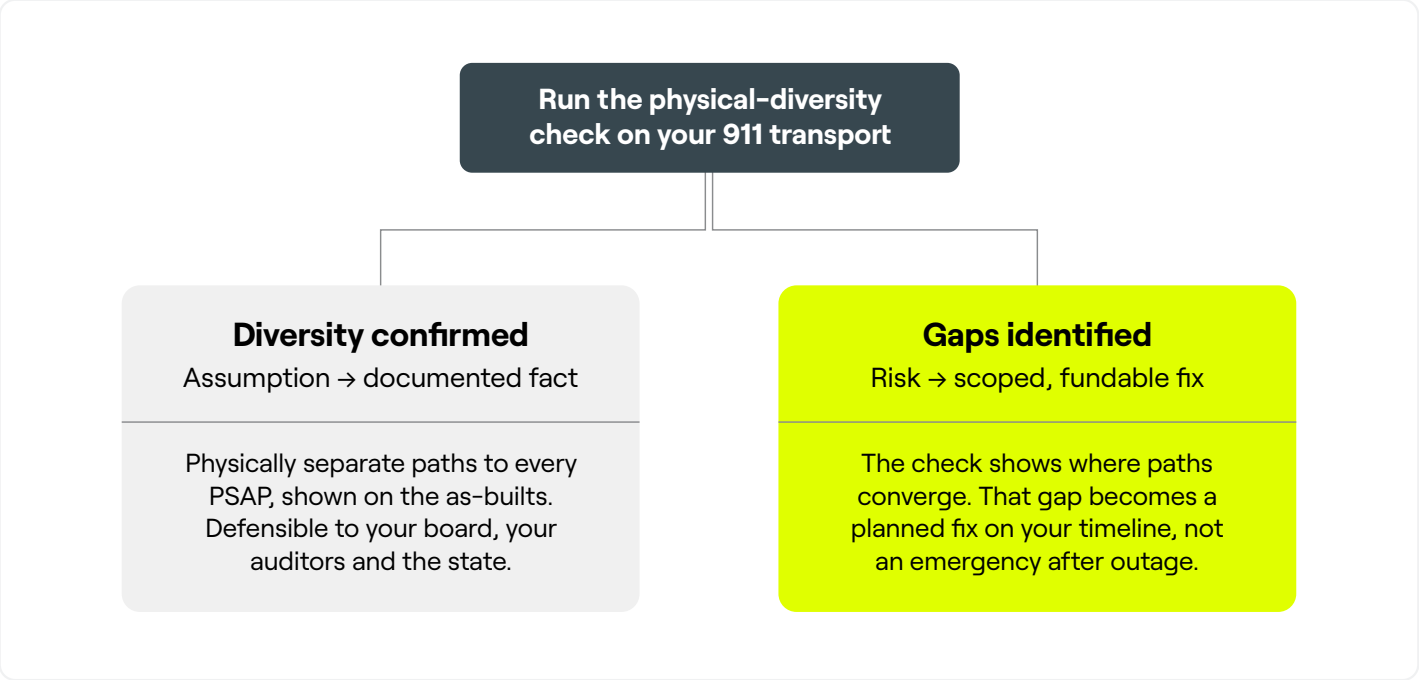
The way to know what you actually have is to look at the records of where your fiber was physically installed. In practice that means a network assessment done together: you bring your location and route data, including your mapping (KMZ) files and site list, and we overlay where Lightpath fiber actually runs, so the diverse paths and the gaps are visible on a map.

The design that comes out of that is collaborative, and it is built to fully support the NG911 platform you're standing up.

---

[4] Federal Communications Commission, Report and Order FCC 24-78, "Facilitating Implementation of Next Generation 911 Services," July 18, 2024.
[5] Federal Register, "Facilitating Implementation of Next Generation 911 Services (NG911); Improving 911 Reliability," June 4, 2025.

Fig 2. Run the Check: Either Finding is Worth Having



There's a second kind of separation underneath all of this: not just diverse routes, but a 911 network that doesn't share infrastructure with anything else.

A 911 network should be treated as a mission-critical workload on its own deterministic, private network, kept as physically separate as possible even from the county, municipal or state network it sits beside. The 911 path is not where you want shared dependencies. The goal is a path as physically separate as the local geography allows.

Lightpath approaches this from a position of owned infrastructure.

Owning the route is what makes it possible to document real separation rather than just promise it. And where local geography constrains how separate two paths can be, that conversation belongs in a design review, not a post-mortem. It surfaces the points where two paths quietly share a bridge, a pole line or a building entrance, and forces a decision on what compensating controls — microwave, LTE failover, secondary entrance — close the gap, and who carries the residual risk.

Funding and Scoping the Second Path

The money question comes up early, so let me be direct about it. There is funding for this. Emergency-communications and 911 programs generally can draw on their own dedicated funds, outside the county's general budget, and they typically run their own networks, which is exactly as it should be for a mission-critical service. A well-designed engagement should help an agency make the most of the Next Generation 911 grant funding available to it, alongside those dedicated 911 funds and the agency's own capital.

Here's what this looks like state by state:

New York

In New York, the state's current county NG911 grant program is built first around call-handling equipment, and it explicitly allows certain ESInet costs, including fiber-optic infrastructure that directly supports 911 call delivery, construction of redundant network entrance facilities and connectivity between PSAPs, including between counties, as eligible expenditures once the call-handling work is addressed and with the state's prior approval.[6]

In other words, the grant can help fund a diverse path, but only as a deliberate, approved part of the plan. It's not a pot of money sitting idle for fiber. The right move is to scope the diverse path early, while the rest of the NG911 build is being planned, so that it can be funded the right way rather than bolted on after an outage forces the question.

New York is mid-transition and, by the State Comptroller's own June 2025 audit, behind the schedule the state set for itself,[7] even as the state has put real money in front of all 57 counties outside New York City to prepare for NG911.[8]

For a county building toward i3 now, the diverse path and the redundant entrance facility are not next year's problem; they are part of this year's scope, and they are the kind of cost the state's program contemplates with prior approval. The most useful first step is a joint assessment that shows, on a map, where a county's 911 traffic has a second physical path today and where it does not.

New York's NG911 grant program can help fund a diverse network path, provided it's a deliberate, approved part of your plan.

---

[6] NYS Division of Homeland Security and Emergency Services, SFY2025 Next Generation 911 (NG911) Grant Program — Grant Guidelines and Application Kit (rev. May 28, 2025), Sec. V, Authorized Program Expenditures.

[7] Office of the New York State Comptroller, "Action Needed on New York's Long-Delayed Adoption of Crucial Next Generation 911," June 4, 2025 (Audit SGA-2025-23S40).

[8] Office of Governor Kathy Hochul, "Governor Hochul Announces $85 Million to Enhance Next Generation 911," Sept. 25, 2025.

New Jersey

New Jersey already has a statewide ESInet,[9] so for most counties the open question is how each PSAP connects to it, and whether that connection has a second, physically separate entrance. The moment a PSAP cuts over is the right moment to answer that question, because it's far cheaper to design in a diverse entrance than to add one after the fact.

Connecticut and Massachusetts

Both states run mature, centrally operated NG911 systems, and both lived through a statewide outage in 2024 that came down to a single point in the path. In states like these, the useful work is resilience layered onto the existing core: reviewing, honestly, how many physically separate paths reach each center today, and closing the gaps the outages exposed.

The scoping conversation belongs with the state authority that owns the system, and the first step is the same one it always is: pulling the as-builts and tracing where the two paths actually run.

[9] State of New Jersey, Office of Emergency Telecommunication Services (OETS), FY2026 Next Generation 9-1-1 (NG9-1-1) PSAP Grant Program (grant period July 1, 2025–June 30, 2026), Program Objectives

A Diligence Checklist for Your Own Network

Before your next vendor conversation, or your next outage, these are the questions to answer about your own 911 transport. The answers will show you where your network is resilient, and where it's only assumed to be.

Seven Questions to Answer Before the Next Outage

1	How many physically separate paths reach each PSAP and backup center today, meaning physical routes, not logical ones?
2	Do any of your "diverse" circuits share a conduit, building entrance or single carrier anywhere along the route?
3	If your primary path failed right now, where does traffic go, and have you tested that failover end to end this year?
4	Can you fail over to an adjacent county's PSAP without relying on the link that just failed?
5	Is your 911 network physically separate from the county, municipal and state networks, or does it share infrastructure?
6	Do you have current as-builts showing where your 911 fiber actually runs, or only a logical diagram?
7	As you scope your NG911 build and grant spend, is the diverse path in the plan now, or assumed "already handled?"

If you can answer all seven with confidence, your foundation is sound. If a few of them give you pause, that's the gap to close now — the kind of gap a route mapping assessment is built to find.

Either way, the next step is useful. You may run the checklist and decide you need help, or you may decide you'd rather bring in a partner to run it with you. Both paths lead to the same place: knowing, and mapping, whether the promise behind your 911 system can survive one bad afternoon.

Lightpath