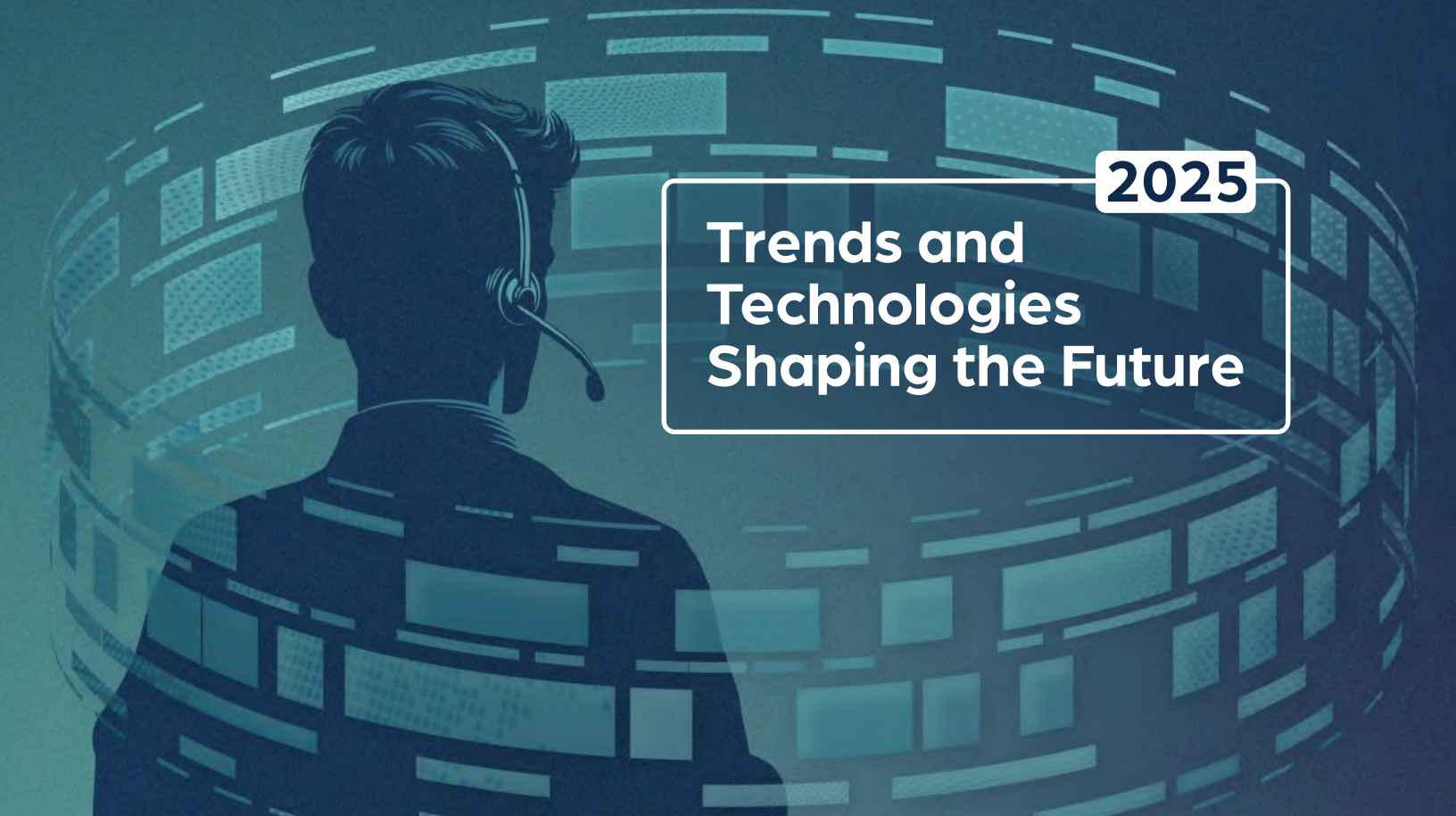
INTRADO

State of the 9-1-1 Industry



2025

Trends and Technologies Shaping the Future

INTRADO

State of the 9-1-1 Industry

John Snapp
VP Technology

Lauren Kravetz
VP Government Affairs

Introduction

These are exciting times to be in public safety. The functionality versus simplicity seesaw of NG9-1-1 continues to rock back and forth, with Emergency Services IP Networks, a wide range of state and local approaches to the i3 standard, and looming challenges with interoperability. Advancements in location technologies are greatly improving the data available to 9-1-1 telecommunicators, though challenges persist in attaching more comprehensive and precise location information — now in three dimensions, not just two — for emergency assistance requests. The rise of low earth orbit communication satellites has opened a tremendous opportunity to expand emergency communications coverage across the globe. Cloud migration for Public Safety Answering Points is a question of when, not if. Same with Artificial Intelligence, which is already helping 9-1-1 telecommunicators triage and translate calls.

Ensuring the cybersecurity of the 9-1-1 ecosystem is a hill we must climb faster. These advances bring new sources of requests for assistance and heightened public expectations. And, of course, it's all happening against the backdrop of government regulation and oversight intended to promote greater coverage, reliability, and security.

We address these developments head on at Intrado on a daily basis, and we are proud to present our industry insights in this **2025 State of the 9-1-1 Industry Report**. We hope this report will be read by a broad audience who care about 9-1-1. With this in mind, we have included a great deal of background information. If you are more advanced on these topics, thanks for bearing with us.

Our mission at Intrado since our founding nearly 50 years ago has always been to save lives and protect communities by helping them prepare for, respond to, and recover from critical events. We are in a unique position in the 9-1-1 ecosystem — standing at the intersection of emergency communications and serving both communications providers and public safety — which means we touch 90% of the 9-1-1 requests for assistance in the United States.

By maintaining trusted relationships with the providers that originate emergency calls, the PSAPs that handle them, and 9-1-1 telecommunicators who respond to those emergencies, we have developed a comprehensive understanding of the challenges and priorities across this space. We are leading the way in advocating for improvements that benefit the entire emergency response chain. This is #WorkWorthDoing.

Intrado Life & Safety

INTRADO
Always there in an emergency

9-1-1 INDUSTRY OVERVIEW

The 9-1-1 ecosystem involves multiple stakeholders with distinct roles and interests in ensuring effective 9-1-1 and emergency services. Get a cup of coffee, we're going to spend some time on this.

First and foremost, the public are the ultimate stakeholders — the users of 9-1-1 services who expect ready access to emergency assistance regardless of location or circumstances. They are why we do this.

9-1-1 is a larger and more complex ecosystem, with more players and parts than ever before. Changes — good changes — are coming.

Public Safety Stakeholders

9–1–1 Telecommunicators

PSAPs, Emergency Call Centers (ECC)

9-1-1 telecommunicators serve as the critical first point of contact in emergency response systems and the pivotal center of every 9-1-1 call. Their role has expanded tremendously since the early days of 9-1-1. These days, 9-1-1 telecommunicators answer and assess calls; gather essential details on callers and location; determine what resources to send; dispatch emergency services; manage highly emotional situations; and provide lifesaving instruction before help arrives on the scene.

As technology advances, 9-1-1 telecommunicators also manage an ever-increasing amount of data. They require specialized training, often certification, and, in many jurisdictions, continuing education.

It may surprise you, then, to learn that the occupation of 9-1-1 telecommunicator is still classified as a "clerical" position in the Standard Occupational Classification. Intrado is on record supporting reclassification as a "protective service" occupation. Some states and localities have already made this change, and federal legislation — the 9-1-1 SAVES Act — has been introduced (actually, reintroduced) that would require the Office of Management and Budget to make this adjustment at the earliest possible juncture.

PSAPs, Emergency Call Centers (ECC), or in FCC speak, "9-1-1 Special Facilities" are the locations that receive the requests for assistance and dispatch emergency response. According to NENA: The 9-1-1 Association (aka National Emergency Number Association), the collective association for PSAPs (and, to our mind, a trusted source for the number of PSAPs in the U.S.) as of 2021, there were 5,748 primary, secondary, or consolidated function PSAPs covering 3,135 jurisdictions.

No one type of agency or entity runs PSAPs. Rather, they are operated by a wide range of local and regional agencies, such as law enforcement; fire departments or districts; county, city, and parish governments; and large universities.

Depending on the state or jurisdiction, PSAPs operate at different levels of government: statewide, regional, or local. They play a centralizing role in emergency management and public safety infrastructure. As we'll discuss, PSAPs face many challenges — chief among them funding, but also staff recruitment and retention, management of increasing call volumes and types of calls (e.g. voice, text, or video), technology upgrades, and a growing number of data streams.

Emergency Responders

Emergency responders (law enforcement, fire, emergency medical services or EMS) focus on rapid response, accurate situational awareness, responder safety, and access to critical information before arriving on the scene of an emergency. They require reliable and interoperable communication systems that perform well in challenging environments.

The advent of the First Responder Network Authority (FirstNet) has greatly improved the ability of emergency services agencies to meet these needs. FirstNet is a dedicated communications platform specifically built for first responders and the public safety community. With respect to 9-1-1, FirstNet gives first responders priority access for critical communications. It provides expanded coverage and capacity, including special assets, such as Cell on Wheels, that can be deployed during disasters. It supports the transition to NG9-1-1 by enabling texts, images, videos, and advanced data. Perhaps most important, FirstNet provides interoperability between agencies and jurisdictions to create seamless communication during emergencies. More than 25,000 public safety agencies across the U.S. subscribe to FirstNet, comprising more than 7 million connections.

9-1-1 Authorities

9-1-1 Authorities can serve as the central administrative body responsible for 9-1-1 services across a state. The structure and powers of state 9-1-1 Authorities vary considerably: Some have broad authority and responsibilities to ensure an effective and cohesive 9-1-1 program, while others focus primarily on funding distribution and technical coordination.

Broadly speaking, states with a strong 9-1-1 Authority share several attributes: clear statutory authority, dedicated state funding mechanisms, and statewide coordination of technology implementations. These attributes position the authority to implement innovations uniformly, ensuring all residents benefit from advanced emergency communication capabilities regardless of local funding limitations. These states generally have an easier path to drive technological innovation, such as NG9-1-1 deployment, which also enables them to implement enhanced 9-1-1 location services, advanced multimedia communication capabilities, data integration, cloud migration, and cybersecurity. Looking down the road a bit, we expect that states with more centralized authority will more quickly develop applications to directly connect callers with features such as automatic crash detection. Indiana and North Carolina are examples of robust state 9-1-1 authorities that are on the leading edge of NG9-1-1 deployment.

Despite a more decentralized approach, Texas has implemented cutting-edge technology solutions — for example, through large regional Emergency Communications Districts such as the Greater Harris County 9-1-1 Emergency Network, which covers Houston and environs. Colorado is an example of a hybrid approach, where the state-level entity identifies and distributes funding to local jurisdictions, which then decide how to spend the money in their communities.

So-called "home rule" states — states where significant authority over emergency communications is delegated to counties, municipalities, or special districts — give local governments substantial autonomy in how they implement, fund, and operate their 9-1-1 systems. Funding in these environments varies greatly among jurisdictions, leading to differing technology implementation timelines and choice of vendors; more local control over staffing and operations; and greater challenges with interoperability between neighboring jurisdictions. Examples include Florida, Michigan, New York, Ohio, Pennsylvania, and West Virginia.

A word on funding.
Let's face it, technology upgrades cost money, and the ability of a state, 9-1-1 Authority, or regional district to innovate depends as much on the structure and remit of the 9-1-1 Authority as on available funding mechanisms. An uncomfortable truth is that many states and localities depend on inadequate and unstable funding mechanisms, including subscriber fees, state/local fiscal appropriations, and the occasional federal grant.

All 50 states plus the District of Columbia charge subscribers some form of 9-1-1 fee to support 9-1-1 services. Communications providers collect these fees and remit them to the state or locality. The average 9-1-1 fee is approximately $0.75 per month. Without going down the fee diversion rabbit hole, states and localities may not use 9-1-1 subscriber fees to fund anything other than 9-1-1. But some have, and a couple still do.

When traveling around the country to work with states and PSAPs, it quickly becomes apparent that 9-1-1 agencies lack sufficient funding for just about everything — salaries, technology upgrades, training, and basic equipment (think desks and chairs). This is not to say that states are not investing, but the fact is that we've observed unmet needs. We'll touch on funding again later.

This was the successful funding mechanism used to provide initial, non-taxpayer funding for FirstNet.

The FCC does not currently have authority to auction spectrum, though as of this writing, it appears likely that the Commission's spectrum auction authority is likely to be restored with enactment of the 2025 budget reconciliation legislation. NG9-1-1, however, is not among the initiatives to be funded from auction proceeds.

Existing MSS enables continuous communication in emergency situations, using networks such as Globalstar (Apple's partner for its SOS feature) and Iridium (using Garmin inReach® devices) to deliver satellite-based Sos messaging. Some satellite companies are working in partnership with terrestrial mobile wireless operators to provide D2D service over terrestrial wireless spectrum – this is called Supplemental Coverage from Space, and we'll talk a lot more about this in a minute.

Public Safety Membership and Advocacy Organizations

Three major organizations represent the interests of public safety stakeholders and exert influence over 9-1-1 policy, standards, and operations. All three belong in any national conversation about 9-1-1.

APCO International (APCO)

is the oldest and largest organization of public safety communications professionals. Its membership comprises 40,000+ public safety communications officials who "manage, operate, build and support public safety communications systems for law enforcement, fire, emergency medical and other public safety agencies." APCO's interests are broader than 9-1-1; it covers the entire emergency communications landscape, such as law enforcement, fire radio systems, and emergency alerts to the public.

National Association of State 911 Administrators (NASNA)

comprises state leadership of 9-1-1, representing 49 member-states and the District of Columbia on, in their words, "the public policy issues impacting the successful implementation of 9-1-1 systems." NASNA members design, implement, and manage 9-1-1 systems and NG9-1-1 across the country.

NENA: The 9-1-1 Association

is focused solely on 9-1-1 operations, technology, education, and policy issues. Its membership comprises PSAPs and the thousands of 9-1-1 telecommunicators and other 9-1-1 professionals. NENA is also recognized for its standards development; the NG9-1-1 i3 standard was developed under NENA's auspices.

A number of law enforcement and firefighter organizations are also very present in the 9-1-1 conversation, such as the International Association of Chiefs of Police, International Association of Fire Chiefs, Major County Sheriffs of America, and others.

Industry Players

Communications providers have always played a pivotal role in routing and processing 9-1-1 calls from wireline, mobile wireless, Voice over Internet Protocol (VoIP), and satellite providers that route traffic to 9-1-1 networks. Most calls to 9-1-1 still originate on the network of a communications provider and route to the dedicated 9-1-1 network (an ESInet in the NG9-1-1 environment, or the Selective Router [SR] in a legacy environment). We call this the "ingress" path. Much of the technological innovation in 9-1-1 emanates from the communications providers.

Communications providers are the focus of federal regulation of 9-1-1. They bear the responsibility of maintaining their networks to ensure that callers can be connected to PSAPs. The FCC 9-1-1 rules requiring the delivery of all 9-1-1 calls to the most geographically appropriate PSAP with accurate location data and notification to PSAPs in the event of an outage are obligations addressed to communications providers. The FCC often uses the blanket term "Originating Service Providers" (OSPs), which we find handy and will use when describing situations where the FCC also uses that term. New to the scene, some over-the-top providers, such as those offering Unified Communications as a Service (UCaaS), also have 9-1-1 regulatory obligations.

Communications providers also carry 9-1-1 calls as they exit the 9-1-1 network to a PSAP from an ESInet, SR, or old-timey legacy circuits (which we call the "egress" path).

9-1-1 technology and equipment providers and other vendors cover a broad landscape. Generally speaking, they provide services that allow PSAPs to receive, effectively process, and promptly respond to requests for assistance. Some, such as Intrado, cover most or all of the landscape; some are quite specialized, providing a particular piece of equipment or a particular data stream. Most PSAPs work with a range of vendors:

- **Next Generation Core Services** (NGCS) supply modern, IP-based systems that handle text, images, video, and data beyond traditional voice calls.
- **Call Handling Equipment** (CHE) allows 9-1-1 centers to receive calls and dispatch assistance. CHE probably needs to be upgraded for NG9-1-1 to expand beyond the ability to receive simple Internet Protocol (IP) traffic.
- **Computer-Aided Dispatch** (CAD) systems are a technology backbone that help PSAPs manage emergency response.
- **Data Enhancement Platforms** involve data links directly to PSAPs from connected devices, apps, and sensors.
- **Geographic Information Systems** (GIS) constitute advanced mapping and location technology that helps identify caller locations and nearby direct responders. This is a critical element in NG9-1-1.
- **Recording and logging systems**
- **Integration services** ensure all components work together seamlessly.

New Faces in the 9–1–1 Space

The traditional emergency response system is evolving and offering intermediary services that are transforming how PSAPs receive requests for assistance. These include:

Alarm monitoring companies with advanced technology, have been providing connections to 9-1-1 for many years. Over the last decade, these services have evolved significantly. ADT's SMART platform, for example, reduces false alarms and increases the speed and accuracy of alarm information delivery to PSAPs. In the past, when an alarm was triggered, the monitoring company would place a regular phone call to a 9-1-1 center. Now, alarm systems can automatically send a text message to text-enabled PSAPs or even insert the incident directly into the PSAPs CAD system for dispatch.

Incident management platforms, which campuses/buildings use to quickly assess a developing emergency situation and notify the PSAP, are gaining importance. Most prominent is the growing trend for K-12 schools to deploy silent panic alarms that connect to an incident management platform, which notifies the PSAPs (and can also notify parents).

Automotive telematics services support automatic collision notification by providing notification when detecting a collision. There are several on the market, including Toyota's Safety Connect and GM's OnStar. Some of these services include additional features such as roadside assistance and stolen vehicle location services. Behind the scenes, vendors, such as Bosch, build the sensors and automotive networks that help power these services.

Internet of Things (IoT) device manufacturers. Take smartwatches, for example. Most modern smartwatches can connect to emergency services either directly (if the watch has cellular capabilities) or via a nearby phone with a wireless network connection or Wi-Fi calling. Some newer watches can even connect to emergency services in areas without cellular coverage via satellite.

- **Apple Watches**, at least more recent models, will detect a hard fall while you're wearing them and ping your wrist, sound an alarm, and display an alert. If you do not dismiss the alert, and you remain immobile for at least one minute the watch will automatically call 9-1-1, share your location coordinates, and notify your pre-designated emergency contacts.
- **Samsung Galaxy Watches** will send alerts to your emergency contacts but does not directly call 9-1-1 at this time.
- **Google Pixel Watches** use motion sensors to detect falls. This initiates a check-in and countdown and sounds an alarm that bypasses Do Not Disturb and Bedtime modes. If you don't respond, the watch will automatically call 9-1-1, play an automated message informing the PSAP of a potential emergency, and share your location data. You can take over the call at any point, if you're able.

Specialized consumer apps have been on the scene for more than a decade. A classic example would be a web-based app that allows users to create profiles that travel with them and can be available to the PSAP. This can include key details about household members, access points like hidden driveways or gate codes, and information about vehicles and pets. These apps are usually free for consumers, but not for the PSAP. And, of course, we can't forget the medical alert system providers, such as Life Alert (of "Help! I've fallen and I can't get up®" fame) that provide monitoring and connection to 9-1-1 for seniors.

K-12 schools should now be considered stakeholders in the 9-1-1 space, as they are increasingly implementing security solutions like silent alarms and panic buttons that connect directly to 9-1-1 and emergency responders through dedicated hardware and smartphone apps.

Hospitality and large retail establishments must also be counted as stakeholders, with some forward-looking legislation enacted in New York and Washington, D.C. Large retailers will be required to provide silent panic buttons for employees starting in 2027. For example, New York's Safe Hotels Act mandates panic buttons that connect to 9-1-1 for employees who must enter occupied guest rooms. Hotel chains such as Marriott have also started to mandate panic buttons for employees across the 30 hotel chains it manages in North America, as part of the 5-Star Promise program of the American Hotel and Lodging Association to enhance safety and security. Ready access to 9-1-1 is becoming a workplace safety issue, and we expect to see more states enact this type of legislation for hospitality and other sectors going forward.

We'll talk more about all of the new faces later.

Consultants

We would be remiss if we failed to mention the role of consultants in the NG9-1-1 deployment process. NG9-1-1 implementation is complex and involves much more than just new hardware and software. It requires extensive planning and coordination with a wide range of state and local entities. In addition to a Next Generation Core Service Provider (NGCSP), it is not uncommon for a state 9-1-1 Authority or PSAP to hire an outside consultant to help plan, design, and implement NG9-1-1 systems, with the goal of optimizing NG9-1-1 call-delivery technologies, operations, and policies.

For example, the NG9-1-1 procurement process involves engaging one or more entities for ESInet services call-handling upgrades, and NGCS. you may find consultants analyzing current systems; bridging transition gaps; supporting data integration and analytics; and managing other vendors. For a real-world example, consider Arizona, where consultants used proprietary methodology to help the state's 9-1-1 program assess more than a dozen 9-1-1 systems serving 81 ECCs, with the goal of connecting all centers to improve data sharing and emergency response.

9-1-1 Call Volume

The 9-1-1 system handles an enormous volume of calls: approximately 240 million in the United States each year, or roughly 657,000 calls per day. Nowadays, more than 80% of 9-1-1 calls originate from mobile phones — a significant shift from the landline-dominated era of early 9-1-1 implementation. VoIP services and traditional landlines encompass the remaining calls, with landline calls decreasing year after year.

This platform shift has created both opportunities and challenges for the ecosystem. Wireless calls require more sophisticated location technology but also allow for enhanced data transmission capabilities, such as text-to-9-1-1 services, and the potential to send photos and videos to emergency services.

9-1-1 is one of the most important public services in our country. It's written into our collective consciousness and has saved countless lives. Now, our nation's 9-1-1 system is undergoing complete modernization of its 60-plus-year-old infrastructure, including enhancements to enable IP connectivity and other new capabilities. With this comes heightened public expectations from individuals that a 9-1-1 telecommunicator will receive their request for assistance, and emergency responders will be able to find and help them wherever they are.

Realizing the benefits of these advancements depends in part on the convergence of 9-1-1 with commercial technologies — for example, in the areas of text and VoIP. We discuss all this next and hope we do it justice.

INTRADO
State of the 9-1-1 Industry

PSAP SYSTEMS AND OPERATIONS

In the evolving landscape of emergency response, PSAPs play a pivotal role in ensuring efficient and effective crisis management. They are the technological and operational backbone of emergency communication systems, housing sophisticated telecommunications equipment that enables 9-1-1 telecommunicators to efficiently receive, process, and send appropriate emergency response.

Systems

The primary system in the PSAP is the CHE. There are also mapping systems including GIS, which help the PSAP connect incidents to locations. On the outbound side, CAD (computer aided dispatch) systems, together with radio systems, help the PSAP dispatch responders and manage incidents.

Beyond these fundamental systems, PSAPs employ a variety of specialized systems to enhance their emergency response capabilities. We'll call out just a few examples.

Most PSAPs have call recording systems that document all communications for quality assurance and legal purposes. In legacy architecture, Automatic Number Identification (ANI) and Automatic Location Identification (ALI) work in tandem to immediately display caller information, especially important when the caller is unable to speak. And, of course, the systems that enable NG9-1-1 are increasingly common, as are a multitude of data streams. Modernized PSAPs utilize advanced mapping systems and Automatic Vehicle Location (AVL) technology to track emergency vehicles and optimize response times.

Call handling systems are the backbone of emergency communications, serving as the critical link between the public and the emergency services they urgently need.

Less discussed but equally critical, PSAPs maintain backup power supplies and communication channels. When it comes to 9-1-1 systems, ensuring reliable and uninterrupted emergency communication is vital. Two key strategies that make this possible are redundancy and resiliency, and PSAPs generally have ways to achieve both. The NG9-1-1 environment greatly strengthens the ability of PSAPs to operate redundant and resilient systems.

Though they're often confused, redundancy and resiliency serve distinct roles. Redundancy means having backup components or systems in place. For example, if one circuit, data center, or server goes offline, another automatically steps in to keep everything running smoothly. This "spare" setup prevents any single failure from disrupting emergency services.

Resiliency, meanwhile, is about the system's ability to bounce back and keep functioning even when faced with unexpected challenges like cyberattacks, natural disasters, or surges in call volume. It's not just about having backups; it's about smart design features that detect problems, isolate issues, and quickly recover without losing service quality. While redundancy provides the safety net, resiliency ensures the system can adapt and maintain performance no matter what. Together, these approaches build a stronger, more dependable 9-1-1 network that keeps communities safe when every second matters.

"Network diversity" is a cornerstone of robust NG9-1-1 systems, achieved by integrating multiple connectivity methods to guarantee seamless communication during emergencies. While traditional, wired IP connections form the stable backbone for handling high volumes of emergency calls, NG9-1-1 networks are increasingly leveraging wireless technologies, notably FirstNet – the nationwide public safety broadband network established by Congress -- to ensure the availability of backup.

PSAPs are classified as Primary Users on FirstNet, meaning they receive priority and preemptive treatment. A number of states have implemented statewide FirstNet wireless backup for their PSAPs, such as Iowa and Tennessee. The backup connectivity can increase access and reliability for PSAPs, even during network congestion and natural or manmade disasters. Complementing wireless broadband are satellite links, which provide critical connectivity when both wired and terrestrial wireless networks are compromised. By combining wired IP, wireless, and satellite communication, PSAPs can increase their network diversity in the NG9-1-1 environment, bolstering resiliency and ensuring that first responders and ECCs stay connected.

Operations

PSAPs operate on a 24/7 basis, with trained 9-1-1 telecommunicators working in shifts to ensure continuous coverage for emergency calls. Typically, five staff members are required to fill one full-time telecommunicator position with 24/7 coverage. When a request for assistance comes in, the 9-1-1 telecommunicator gathers essential information from the caller. This information is usually entered into the CAD system, which helps prioritize the incident based on severity and urgency protocols. (Some smaller PSAPs that do not have CAD may still rely on pen and paper to record dispatch.)

The 9-1-1 telecommunicator then coordinates the appropriate emergency response, whether law enforcement, fire, medical, or mental health services. They maintain continuous communication with both the caller and the responding units throughout the incident. Many PSAPs employ quality assurance programs to review call handling and dispatch operations, ensuring adherence to protocols and identifying areas for improvement.

Recruitment and Retention

Eighty percent of U.S. PSAPs have five or fewer "seats," meaning 9-1-1 telecommunicator positions. Recruiting and retaining skilled personnel are among the greatest challenges facing our nation's 9-1-1 centers. The critical nature of emergency response demands highly trained professionals who can handle the pressures of the job with resilience and expertise. However, attracting and retaining such talent is difficult due to high stress, demanding hours, relatively low salaries, and the need for continuous specialization in a rapidly evolving technological landscape.

Efforts at the federal level, such as the 9-1-1 SAVES Act, seek to reclassify 9-1-1 professionals as "protective service" rather than "clerical" personnel. This change would recognize 9-1-1 telecommunicators as the first responders they are, rather than administrative personnel. It would highlight the crucial, lifesaving work they perform every day, from helping to deliver babies virtually, to suicide prevention, to command and control during mass casualty events. Several states and counties have already reclassified their 9-1-1 telecommunicators as protective service personnel.

Based on the work they perform, 9-1-1 telecommunicators should not be classified as "clerical" workers, but rather "protective service" workers. The 9-1-1 SAVES Act would ensure this nationwide.

For PSAPs, technology and change represent a double-edged sword that offers both opportunity and challenge. The best examples? NG9-1-1, migration to cloud-based services, and AI. Each has clear benefits, which we will discuss below. Each also requires — or will require — careful balancing of enhanced outcomes with stability and implementation risks.

PSAP Consolidation

PSAP consolidation is increasing, resulting in a smaller number of individual PSAPs covering larger geographic areas. NENA and Deltek have published data showing the number of PSAPs in the U.S. has decreased from 7,485 in 2013 to 5,748 in 2021, a 23% drop in eight years.

There are several reasons for this trend. One is economy of scale, which goes hand in hand with cost reduction, improved efficiency, and shared resources. It is cheaper to run a single 50-seat PSAP than 10 five-seat PSAPs. It is also easier to manage shift schedules at a larger facility.

There are, however, concerns about consolidation, including staff morale. Even if the new location has an upgraded facility, stress and disruption tend to follow change. Another consideration is the loss of local control when the newly consolidated PSAP is located in a different area or community.

9–1–1 Telecommunicator Health and Wellness

Emergency communications professionals grapple with unique and intense challenges that can significantly impact their mental health and wellness. They are often the first point of contact in emergencies, tasked with making swift decisions, providing critical information, and maintaining a calm demeanor amid chaos. The pressure to perform flawlessly in life-or-death situations can lead to high levels of post-traumatic stress, secondary stress, and vicarious trauma. The emotional burden of constantly dealing with traumatic events and distressed callers can build up over time, making it more difficult for 9-1-1 professionals to disengage and decompress when they are off the clock.

One of the most significant challenges 9-1-1 professionals face is the lack of adequate mental health support and resources. Despite the high-stress nature of the work, many emergency communication centers do not have comprehensive mental health programs in place for employees. This can result in telecommunicators and dispatchers feeling isolated, unsupported, and struggling to cope with the emotional toll of their job.

While many PSAPs/ECCs have adopted a more progressive and forward-thinking approach toward seeking professional assistance, there remains a stigma in emergency services that can deter individuals from reaching out for help for fear of being perceived as weak or unable to handle the demands of the job.

Another critical challenge is the unpredictable and relentless nature of the work. 9-1-1 professionals must be prepared to handle a wide range of emergencies without warning, from minor incidents to large-scale disasters. This unpredictability can lead to chronic stress and burnout, as telecommunicators and dispatchers never know what awaits them on their next call. Furthermore, the long hours, shift work, and mandatory overtime often required in emergency communications centers can disrupt personal lives and sleep patterns, contributing to physical and mental exhaustion. Balancing the demands of the job with personal well-being becomes a constant struggle, highlighting the need for more effective strategies and policies to support the mental health and wellness of 9-1-1 professionals.

Funding and Resourcing

One of the biggest challenges that PSAPs — and, more generally, state 9-1-1 programs — face is adequate funding. The two primary sources of funding for 9-1-1 have been state-appropriated funds and per-line subscriber surcharges — the 9-1-1 fee you probably see on your wireless or VoIP phone bill. Limited federal funding has been made available as grants and, sometimes, loans.

Most states allow local governments to decide how to spend some or all of the fees collected to provide 9-1-1. It sounds simple enough, but changing consumer usage patterns can make it challenging to collect the amount of funds necessary to cover the cost of 9-1-1.

We'll use Kentucky as an example, where 80% of 9-1-1 calls originate from wireless devices, yet the amount paid by wireless subscribers accounts for only 20-25% of the total cost to support 9-1-1. To overcome funding shortfalls, states may have to find additional funding to support 9-1-1 services, including the possibility of using general revenues. This holds true for many states.

Now is as good a time as any to mention that the surcharges states/localities collect to ensure that 9-1-1 is available to the public are distinct from "cost recovery" or "regulatory mandate" fees that communications providers charge to pay for the infrastructure they need to provide 9-1-1 to subscribers.

State and local governments are finding the traditional funding model for 9–1–1 insufficient to meet the requirements of the technology upgrades involved in the evolution to NG9–1–1.

State budget process constraints can pose additional challenges for PSAPs. In our interactions with PSAPs across the country, we see severe resourcing constraints. In a classic Catch-22, lack of funds to hire replacement staff lost to attrition can result in PSAPs spending more on overtime than it would cost to replace lost staff. This situation is not unique to public safety, but it does illustrate the challenges.

It will come as no surprise, then, that state and local governments are finding the traditional funding model for 9-1-1 insufficient to meet the requirements of the technology upgrades involved in the evolution to NG9-1-1.

NEXT GENERATION 9-1-1

How Did We Get Here?

(Hat Tip to Talking Heads)

1960s

The original 9-1-1 network was designed in the 1960s to provide a dedicated single number for people to dial to get help in an emergency. At that time, people could contact 9-1-1 only from a hardwired wireline telephone fixed to a specific location. Telephone numbers were assigned, and 9-1-1 calls were routed to the appropriate PSAP based on which local phone company office connected to the line.

1980s

In the 1980s, 9-1-1 evolved to Enhanced 9-1-1 (E9-1-1), in which the address of the wireline phone was provided to the PSAP. Phone companies and state/local agencies around the country created the Master Street Address Guide (MSAG) to standardize addresses and remove duplicates to ensure that every phone number within a community had a unique address provisioned in a standard format. This was particularly important in rural areas, where naming conventions were inconsistent, and many roads weren't named at all. The MSAG also associated an Emergency Service Number (ESN) to each address that defined the responsible law enforcement, fire, and EMS responders for that address. This information was stored in a database called the Automatic Location Information (ALI) database.

1990s

As wireless 9-1-1 calls were added to the 9-1-1 network in 1998, mechanisms had to be created to shoehorn mobile devices with no fixed location into a network designed for fixed wireline numbers and addresses. The concept of a geodetic location that precisely measures the Earth's shape, orientation, and gravity — often represented as a latitude and longitude — was added to a more dynamic version of the ALI database (which had previously been a static database of fixed addresses). Additional telephony changes, including local number portability and VoIP, resulted in awkward fixes to the 9-1-1 network that would allow these new technologies to work on a network originally designed for fixed wireline service.

2000s

In the 2000s, the main telephone networks began transitioning from analog technologies to VoIP technologies, and users rapidly replaced fixed wireline phones with wireless phones. The communications industry realized that the 9-1-1 network needed to evolve from an analog, voice-only, fixed phone-centric network to a mobile, digital-centric network that can also support technologies like text and video. Enter NG9-1-1.

NG9-1-1: A Once in a Lifetime Opportunity

NG9-1-1 is a modern emergency response system that incorporates digital and internet-based technologies over an IP-based network. It expands emergency communications services beyond the core functionality of legacy 9-1-1 and facilitates the use of enhanced capabilities of IP-based devices and networks. It replaces the old model of a wireline phone system that uses geographically fixed phone numbers and static physical addresses with IP technologies that support voice, video, and text, and can track dynamic and often changing locations. Ultimately, it will replace legacy 9-1-1 technology that has been in place since the 1960s.

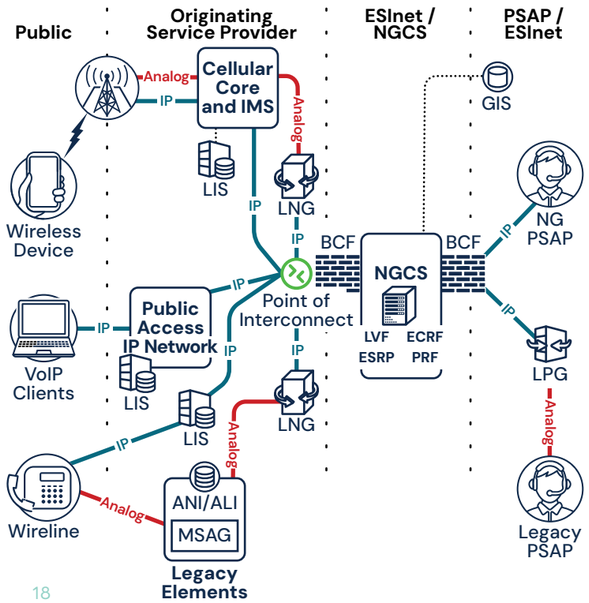
NG9-1-1 comprises two essential elements. First, the ESInet itself. This is an advanced, secure, redundant, and scalable IP-based network designed to support the routing and delivery of emergency communications (such as 9-1-1 calls and texts) to the PSAP. The ESInet is the transport between the OSP, the Next Generation Core Service (NGCS) elements, and the PSAP, as shown in the diagram below.

NGCS represent the second essential element, which facilitate the functions and services on the NG9-1-1 network, such as call routing (voice, text, and video), location delivery, transfers, and logging.

One way to visualize this is to think of the ESInet as your home WiFi network and NGCS as the computers and applications connected to that WiFi network.

There is ample reason for the country to push for end-to-end adoption of NG9-1-1 beyond simply the impulse to migrate to a new technology.

While base functionality is similar to the original 9-1-1 network that still exists today, NG9-1-1 creates a foundation for new functionality that was impossible on the legacy network. This new foundation enables dynamic efficiency and mobility on both the caller side and the PSAP side.



From a public safety agency perspective, NG9-1-1 enables interoperability between state/local agencies in the same jurisdiction, as well as between agencies in different jurisdictions. This allows emergency services to work together as never before, regardless of geographic or organizational boundaries.

For example, during large-scale emergencies, NG9-1-1 enables rapid coordination and resource allocation between neighboring counties and states. Last fall, NG9-1-1 significantly improved public safety capabilities during the response to Hurricane Helene by facilitating the automatic transfer of 9-1-1 calls to other PSAPs when the hurricane disrupted service at the primary PSAP.

From a call perspective, mature NG9-1-1 deployments will enhance the information available to 9-1-1 telecommunicators by improving its content, delivery, and shareability in myriad ways:

Multiple routing paths:
NG9-1-1 uses IP networking, which the U.S. Advanced Research Projects Agency Network (ARPANET, the internet's ancestor) originally designed to route around damage. The diversity and capability of the reroutes far surpass the limited reroute capability of analog and Time Division Multiplexing (TDM) circuits.

Geographic redundancy:
If one PSAP becomes unreachable, end-to-end NG9-1-1 can easily route 9-1-1 calls to backup PSAPs virtually anywhere.

Fewer single points of failure:
With the distributed nature of IP networks, proper network design can reduce or eliminate single points of failure that are common in analog (copper) networks.

Policy-based routing:
Instead of the Boolean routing logic of legacy selective routers, NG9-1-1 offers more robust routing based on policies defined by the PSAP on how they want to route calls. This allows PSAPs to streamline their voice routing and manage outages, high loads, localized traffic spikes, geographic routing, and Telephone Denial of Service (TDoS) attacks.

Geographic-based routing:
NG9-1-1 networks can utilize a mobile device's precise location to more accurately route a call to the appropriate PSAP, substantially reducing transfer rates for 9-1-1 calls.

Integrated data:
9-1-1 over IP networks creates the opportunity to make richer data available to the 9-1-1 telecommunicator — multiple locations, location "breadcrumbing," altitude and floor information, location floor plans, associated address of the caller, crash data from telematics devices, and alarm data from residential fire and burglar alarm systems. A key feature is the ability to handle and transfer multimedia communications (text, images, voice, and video). And NG9-1-1 systems can integrate data simultaneously from several sources — smartphones, GPS, and social media — to provide comprehensive situational awareness for 9-1-1 telecommunicators and other emergency responders. These capabilities allow 9-1-1 callers to send real-time information to emergency services and improve the accuracy of incident reporting.

Security:
ESInets support robust encryption, enabling better security than prior approaches. Keep in mind that security must constantly evolve to mitigate new threats. We'll talk more about this when we discuss cybersecurity.

Accessibility:
There is also the potential to improve emergency response for the deaf and hard-of-hearing by leveraging advanced text-to-9-1-1, Rich Communications Service (RCS), video, and Real-Time Text (RTT) technologies.

Transitioning to NG9-1-1 can be a heavy lift on both sides of the call (the OSP and the PSAP). OSPs are the, well, originating service providers, that provide the means for the public to initiate 9-1-1 calls. For OSPs, the transition requires the ability to send traffic in Session Initiation Protocol (SIP), a significant technical and logistical overhaul. To implement this requires a new approach to data transmission — managing PSAP requests to deploy, monitoring NG9-1-1 readiness status for each PSAP the OSP serves, and meeting FCC compliance deadlines.

The bottom line is that NG9-1-1 equals faster and more efficient emergency response, ultimately enhancing public safety and saving lives.

On the other hand, in order to deploy NG9-1-1, PSAPs must identify funding for these upgrades (more on that later), choose a NGCS provider, establish an ESInet, and ensure they have the requisite infrastructure and equipment to make a valid request to OSPs that serve the jurisdiction.

Successful NG9-1-1 deployment requires a new level of collaboration between OSPs, NGCSPs, and PSAPs.

Where Is NG9-1-1 Deployed?

The transition from legacy to NG9-1-1 is well underway in the United States, but implementation has been gradual, and only a portion of the country is covered by at least some features of NG9-1-1 service. Understanding the state of NG9-1-1 deployment in the United States is not straightforward, however, because there is currently no entity focused on collecting and updating with detailed information. The reason for this requires a longer conversation involving Congress.

A key data point in understanding the overall status of NG9-1-1 deployment in the U.S. is the number of states and localities that have established — or have begun to establish — an ESInet. As we look through the data available as of the end of 2024, we come to the conclusion that approximately 35 states have initiated this process, either statewide or in one or more specific localities, and/or are operating at least one ESInet. (Our apologies to any state we left out of this calculation.) This translates to approximately 70% of the U.S. population living in a state that has at least begun to implement NG9-1-1. No state has implemented end-to-end NG9-1-1 with all the PSAPs and OSPs in the state.

This is a good time to mention that the approach to ESInet deployment varies significantly across states. Some (such as Delaware, North Carolina, and Indiana) have opted for statewide implementation, while others (such as Texas, New York, and West Virginia) are adopting a more regional or local strategy.

Even with the large amount of data available to the NGCSPs that are responding to state and local requests for proposals (RFP) and deploying NG9-1-1 systems, using it to estimate how much of the population has access to some form of NG9-1-1 services is...complicated. State and local procurement approaches vary significantly, with some states taking a statewide approach, some regions using a regional approach, and some individual PSAPs issuing their own RFPs — possibly resulting in multiple in-state RFPs for different stages of NG9-1-1. Given the limited updated public information we were able to obtain — and we tried — it is extremely challenging to estimate the number of people, or a precise percentage of the population, that is covered by at least some features of NG9-1-1. The difficulty of making this calculation factors into the funding discussion below.

Full nationwide coverage of NG9-1-1 is an ongoing process. States and counties have been issuing RFPs on an ongoing basis for almost a decade. The Pennsylvania Emergency Management Agency and the Commonwealth's Department of General Services, for example, have an open RFP seeking vendors. They have chosen an ESInet provider and are now reviewing proposals for a statewide NG9-1-1 call-handling system. The due date for solicitations expired on April 18, 2025, so Pennsylvania will soon determine which vendor will provide this element of NG9-1-1 services. Other states and localities are following a similar process, which will continue until NG9-1-1 has full nationwide coverage.

The Retirement of Legacy 9-1-1 Networks Will Not be a Flash Cutover

One of most challenging and least discussed aspects of the transition to NG9-1-1 is the complexity of retiring legacy 9-1-1 networks, which can be likened to switching aircraft engines in the middle of a flight.

As of the end of 2021, the National 911 Program Office at the National Highway Transportation Safety Administration reported that approximately 2,300 PSAPs (which is to say less than half) are in the process of transitioning (or have transitioned) their interfaces from analog trunking and ALI databases to IP voice and data. The transition is both technologically and operationally complicated, exacerbated by the need to support both technologies (and both phases of NG9-1-1) until NG9-1-1 is fully operational.

Many of the legacy 9-1-1 systems currently in place are more than 30 years old. Manufacturers no longer make components for the core telephony systems of 9-1-1, and many parts can be sourced only from the used parts market. The legacy TDM circuits that connect OSPs to SRs and SRs to PSAPs are also at the end of life and are being decommissioned by the Incumbent Local Exchange Carriers (ILECs). In fact, 9-1-1 systems are often the last users of these devices.

As irreplaceable hardware reaches and surpasses its natural lifespan and becomes increasingly difficult to support, the commercial cost of sustaining these systems increases exponentially. Because 9-1-1 is possibly the only current use for some of this equipment, public safety stakeholders that are not prepared to start transitioning to NG9-1-1 might end up assuming the total cost of ownership of that equipment — an unreasonable burden and poor use of scarce budgetary resources. To put it another way, while the cost of moving to NG9-1-1 may seem expensive now, the cost of delaying a move or not moving at all may be even greater.

While the cost of moving to NG9-1-1 may seem expensive now, the cost of delaying a move or not moving at all may be even greater.

At this time, states/regions/localities may be able to begin decommissioning some TDM circuits that support the legacy SRs, but they will not be able to decommission the SRs and ALI systems until all the OSPs and PSAPs that connect to those elements transition to NG9-1-1 networks. Today, some NG9-1-1 deployments also support the concept of IP selective routing, but this is a costly option that is typically not fully covered by the contracts between these legacy PSAPs and the 9-1-1 service provider. While retirement of analog 9-1-1 systems is starting in pockets of the country — and despite the FCC's acceleration framework — we are years away from end-to-end NG9-1-1 in the United States.

One of most challenging and least discussed aspects of the transition to NG9-1-1 is the complexity of retiring legacy 9-1-1 networks, which can be likened to switching aircraft engines in the middle of a flight.

As the country continues the transition to NG9-1-1, initial and partial deployments do not on the surface visually showcase many new capabilities. The initial deployments may look to PSAPs like a one-to-one functional replacement of analog with IP, but at a higher cost. Although many PSAPs will initially use limited functionality that resembles legacy infrastructure, this migration lays a solid foundation for deploying a wide range of more advanced features and capabilities later on. If you want to build a house, you start with the foundation.

PSAPs that are not prepared to transition may face other negative impacts. Those that are less advanced technologically or do not have reliable IP options available from the OSPs that serve the area (the same OSPs that may lack resources to transition to IP-based technology) may face a more challenging transition to NG9-1-1. PSAPs that delay too long may find themselves moved over to ESInet connection via conversion boxes to support their legacy technology. This will likely introduce service issues, including reduced audio quality and echo, while also increasing the overall cost of PSAP operation of an analog system.

The transition to NG9-1-1 is not just a matter of taking down the old systems. Something must remain in place during the transition to handle both TDM and IP-based 9-1-1 traffic seamlessly, 24/7, with "five nines" availability (available 99.999% of the time), even in an overly complicated and underfunded hybrid environment.

Before legacy systems can be retired and migration to end-to-end IP networks completed, public safety agencies must build an ESInet for OSPs and PSAPs to connect with, and OSPs and PSAPs must migrate from analog connectivity to IP connectivity. This takes time and is easier for PSAPs and OSPs that have more modern systems and greater resources.

For Now: Patchwork Solutions

For some time, then, the country will remain betwixt and between, with PSAPs — even neighboring PSAPs — at various stages of deployment, where some are using NG9-1-1, some legacy ALI, and some OSPs using both. Imagine a situation where an OSP using NG9-1-1 routes a call to a PSAP that also uses NG9-1-1 — but the PSAP must then transfer that call to a legacy PSAP. This scenario, which is common in the current transitional environment, makes it exponentially more complex to achieve timely network management and effective emergency response. With increased complexity comes increased cost and, with it, risk to public safety.

Transition costs will continue to ride on the back of public safety until the transition is complete or until additional funding is available to cover both public safety and enable smaller, mostly Rural Local Exchange Carriers (RLEC) to route traffic in IP. The cost of supporting these systems increases constantly, and public safety agencies are in no position to assume the total cost of ownership to maintain aging and obsolete infrastructure and equipment.

Additionally, the substantial transitional costs of migrating to IP and delivering 9-1-1 traffic to the designated NG9-1-1 point(s) of interconnection (POI) could pose a material financial threat to some of these RLECs that lack new funding sources. Meanwhile, these wireline stragglers delay the total migration to NG9-1-1 and the retirement of the analog legacy 9-1-1 networks. The rapid decommissioning of TDM circuits in areas where basic IP is not yet available threatens 9-1-1 reliability — or even 9-1-1 availability — in those communities.

Where Will the Money Come From?

Funding discussions regarding NG9-1-1 generally focus on mechanisms available to states and localities to undertake the move. States have no federal funding source on which to rely, though not for lack of trying. The states and localities that have moved forward with NG9-1-1 have identified one or more state sources of funding.

With respect to the possibility of federal funding, at least one bill in each of the last several Congresses has included a federal grant program, administered by NTIA (National Telecommunications and Information Administration), for states, tribes, and territories to transition to NG9-1-1 using proceeds from FCC spectrum auctions, as opposed to a federal appropriation. This was the successful funding mechanism used to provide initial, non-taxpayer funding for FirstNet.

Intrado's discussions with lawmakers and regulators focus on the close link between NG9-1-1, reliability, cybersecurity, and national security.

The FCC does not currently have authority to auction spectrum, though as of this writing, it appears likely that the Commission's spectrum auction authority is likely to be restored with enactment of the 2025 budget reconciliation legislation. NG9-1-1, however, is not among the initiatives to be funded from auction proceeds.

One might assume that NG9-1-1 is no longer a top priority for most federal lawmakers, but we don't think that's the case. 9-1-1 has several champions in Congress, and public safety advocates, including Intrado, continue to keep the issue in the news. Meanwhile, we expect to see new constituencies start taking an interest in advancing the NG9-1-1 transition to ensure that the benefits of NG9-1-1 are available to everyone in the country. Intrado's discussions with lawmakers and regulators focus on the close link between NG9-1-1, reliability, cybersecurity, and national security. More on that later.

There is something missing, though, from the discussion about legislating federal funds for NG9-1-1. Estimates of funds needed to complete the transition across the country have become stale. Earlier we discussed the fact that there is no comprehensive, ongoing data collection regarding the status of NG9-1-1 deployment across the country. Without a data-driven estimate of actual need, any legislative effort for NG9-1-1 funding is likely to fail.

Who's Collecting the Data?

Data collection for NG9-1-1 was for many years the responsibility of the National 9-1-1 Program Office at the National Highway Transportation Safety Administration (NHTSA), under the U.S. Department of Transportation. NHTSA's authority to collect this information lapsed several years ago, and no other agency has been authorized to undertake a similar collection. While public safety associations such as NENA, NASNA, and APCO, and 9-1-1 providers like Intrado can assemble large parts of the picture, there is currently no comprehensive, updated resource on the status or cost of attaining end-to-end NG9-1-1 nationwide.

Our view is that advocacy efforts this Congress should focus on enacting a data collection bill that authorizes a federal agency — whether NHTSA, NTIA, or FCC — to assess the status of NG9-1-1 deployment in the U.S. and provide Congress with an estimate of the funding requirements. We think this information could be collected in time to support authorization of federal funding for NG9-1-1 in the next Congress. What would follow is a period of several years to establish the grant program; for states/localities/tribe/territories to apply; and for consideration of applications and, ultimately, awards. The timing of awards directly affects how much longer the current 9-1-1 network must depend on aging and obsolete analog systems.

Interconnectivity Is More Than Connecting Two Plugs

ESInet interconnectivity deserves a great deal more attention, because a central promise of NG9-1-1 — seamless transfer of information between PSAPs — depends on it. State and local ESInet owners should engage now with neighboring jurisdictions, rather than treating this like a "second stage" implementation issue.

Before we examine the work ahead, let's quickly review the benefits of ESInet interconnection:

- **Reduced response times** compared to the legacy practice of the receiving PSAP calling a second PSAP to convey information.
- **Improved situational awareness** through real-time data-sharing that allows caller information, GIS data, and other data points to follow the call.
- **The ability of multiple PSAPs to work together** in emergency situations to reduce delay.
- **The ability of PSAPs in a disaster area to seamlessly enlist backup assistance** from one or more PSAPs outside the disaster area.

To realize these benefits, the public safety community must address several threshold issues regarding how ESInets will talk to each other:

- **Varying interpretations and applications of the i3 standard:**
  The great majority of deployments have relied on NENA's i3 standard, which includes guidelines for ESInet interoperability. There is, however, room for interpretation, as well as differing PSAP preferences and differing NGCSP approaches to implementation. This deserves attention, because it can cause technical inconsistencies that can make interconnection more complex.
- **Intergovernmental agreements:**
  State and federal agencies must establish intergovernmental agreements to define data disclosure, assign oversight responsibilities between agencies, and adopt dispute resolution measures.
- **Funding for ongoing operations:**
  Many state 9-1-1 Authorities plan to invest resources to implement NG9-1-1, but not necessarily for second-stage implementation of interconnectivity. Establishing interconnectivity requires funding for both infrastructure and ongoing maintenance. Additionally, it could be challenging to determine who among multiple state 9-1-1 Authorities bears responsibility for the costs.
- **The need for IT support:**
  Most PSAPs operate with limited IT staff, making it difficult to manage and troubleshoot interconnectivity issues without external support. Those that rely on external IT support — for example, from another part of the state or local agency — must educate these external IT staff on the infrastructure and applicable standard and compete for the resource with other agency functions.

APCO recently published a comprehensive guide to NG9-1-1. If you can't read all 170 pages in one sitting, flip to page 153 for the Handouts directed to PSAP directors, law enforcement, 9-1-1 telecommunicators, elected officials, and the public.

NG Also Stands for "New Gremlins"

Every 9-1-1 call should be completed to the appropriate PSAP. Yet, even with comprehensive, well-planned testing with major NG9-1-1 providers, the complexity of production 9-1-1 networks is such that issues will arise and lead to periodic outages. Early implementations will inevitably unearth new "gremlins" to fix, a process that will yield even more robust, reliable, and capable emergency service communications over NG9-1-1 networks that are far more reliable than analog networks. It will take time to discover and vanquish these gremlins but addressing them will make NG9-1-1 networks better.

Legacy 9-1-1 networks have matured over time, and overcoming challenges has strengthened their defenses and expertise. This stability will remain until the secondary market for parts for critical legacy routers or ALI systems is exhausted. When parts are no longer available, these networks will feel the impact and become less stable. It's difficult to predict when this scale will tip. In the meantime, keep checking eBay for parts.

We're struggling with something. Other industries that impact safety (for example, aviation and automotive) are regulated in a manner that permits rapid industrywide improvements when safety-related issues are discovered. In the aviation context, the discovery of safety-related issues results in airworthiness directives. In the automotive industry, such discoveries result in recalls. The telecommunications industry is different. Safety-related issues lead to enforcement against individual companies followed by rulemaking to achieve industrywide improvements. This leaves us with questions. Is there a better approach for telecommunications that would result in industrywide improvements sooner? Would a model that more closely resembles that of the aviation and automotive industries do more to serve the public interest and encourage innovation in public safety technology?

Let's Get this Party Started: **The "Valid Request" Dance**

In July 2024, the FCC adopted a framework to accelerate NG9-1-1 rollout. Both OSPs and "9-1-1 Authorities" (which could be a state or local public safety agency or a single PSAP) have obligations under these new rules. A 9-1-1 Authority initiates this process by submitting a valid request for service (RFS) to receive OSP traffic in basic SIP (a Phase 1 request) or in full NG format using a commonly accepted standard — usually NENA i3 (a Phase 2 request). To be valid, an RFS must be based on actual (not projected) operational readiness.

Advice for OSPs

Until quite recently, OSPs had the option to choose whether to cooperate with a state or PSAP that indicated readiness to move to NG9-1-1. No longer. As of March 25, 2025, wireline, commercial wireless, interconnected VoIP, and covered text providers must take steps to start delivering 9-1-1 traffic in an IP-based format following a valid request from a 9-1-1 Authority. Nationwide OSPs must comply within six months; non-nationwide within 12 months. If a provider has multiple traffic types, the longest applicable deadline applies to all of that provider's traffic.

OSPs must be prepared to support three scenarios in the near term as NG9-1-1 evolves, because OSPs may need to interface with PSAPs in legacy, SIP (Phase 1), and i3 (Phase 2) states. This requires a new approach to managing PSAP requests to deploy; monitoring NG9-1-1 readiness status for each PSAP the OSP serves; and meeting compliance deadlines in the FCC's rules. PSAPs must identify funding for these upgrades (more on that later), choose an NGCSP, establish an ESInet, and ensure they have the requisite infrastructure and equipment operational to make a valid request to deploy NG9-1-1 to OSPs that serve the jurisdiction. Successful deployment requires a new level of collaboration between OSPs, NGCSPs, and PSAPs.

As we said earlier, transitioning to NG9-1-1 can be a heavy lift on both sides of the call — ingress from the OSP to the ESInet and egress from the ESInet to the PSAP. For OSPs, the transition requires multiple steps:

- **The first phase** requires the OSPs to transition from analog voice circuits to VoIP circuits. While OSPs will still utilize the legacy ALI database, taking this step will allow for decommissioning TDM in the 9-1-1 network and moving away from these legacy circuits.

- **In the second phase**, OSPs will move away from legacy ALI databases to NG9-1-1 location databases and modern addressing schemes.

This is a good time to mention that OSPs need to determine how to fulfill their obligation to support SIP signaling for Phase 1 and full i3 signaling for Phase 2.

OSPs should not expect direct contact from PSAPs regarding readiness. The FCC's rules do not require 9-1-1 Authorities to send individual requests for service to each OSP that serves the jurisdiction, though some may opt to notify individual OSPs. We think that most 9-1-1 Authorities will choose to submit requests in the FCC's public registry, which is docket number 25-143, created for this purpose. OSPs are responsible for monitoring submissions and should regularly check for filings, because the clock starts when the RFS is filed. Depending on the circumstance, the clock may restart if the RFS is amended and refiled. All of us in the 9-1-1 industry expected a rash of requests for service in the first few weeks, possibly causing a bottleneck. So far, the pace of requests has been slow.

The first thing we want OSPs to do is determine validity of the RFS. Determining validity quickly may rest on which form the 9-1-1 Authority chooses to use for the RFS, because they differ in the degree of detail provided. Ideally, OSPs will receive as much detail as possible as early as possible. The ability to determine validity quickly will depend on how much information the the 9-1-1 Authority includes in the request. If the filing sticks to the four corners of the FCC-provided form, that may not be enough information to determine readiness. In that case, reach out to the filer for more information.

Establishing a working relationship with the 9-1-1 Authority from the beginning is critical, especially if there are questions about readiness. While there is a process for OSPs to file with the FCC to challenge readiness within 60 days of the submission of an RFS (those get filed in docket 25-144), a challenge does not stop the clock. More important, the FCC has signaled several times that they expect everyone to work cooperatively, and that the rules are the default parameters. A more expedient path than filing a challenge would be to spend those cycles working with the 9-1-1 Authority to alter the default parameters, whether that's the deployment timeline and/or other deployment issues. It is the responsibility of the OSP to file these mutual agreements in FCC docket number 25-145.

PRO TIP: OSPs should be prepared for RFSs to vary in how the requesting entity wishes to implement, especially with respect to Phase 2 i3.

Advice for 9-1-1 Authorities

The readiness requirements in the FCC's rules are simple.

- **For a Phase 1 request**, the 9-1-1 Authority must have infrastructure in place and ready to receive IP-enabled SIP 9-1-1 traffic, and secured agreements with ESInet, NGCSP, and call-handling equipment providers.

- **For a Phase 2 request**, you should plan on supplying the same information as in Phase 1 and confirm that the infrastructure in place complies with NG9-1-1 industry standards (i3 for most deployments). Then confirm that the ESInet connects to a fully functional NGCS network that can provide access to a Location Validation Function (LVF) and interface with a Location Information Server (LIS) or equivalent. Finally, make sure testing partners are on board with meeting compliance timelines.

9-1-1 Authorities have the option of submitting RFSs into the FCC's public docket 25-143 or contacting OSPs directly to convey an RFS. If you submit by filing with the FCC, you should use the FCC's form, which includes the required certifications and avoids asking for sensitive information that should probably not be in a public docket. Based on our work with OSPs, the FCC's form does not include all of the information that OSPs will need to move forward with deployment. You can – and should -- facilitate the process by ensuring the OSP(s) receive information such as contact information for your ESInet, NGCSP, NG9-1-1 delivery points, CHE providers, and any other vendors you have selected that should be involved in deployment and testing. Network diagrams, too.

All of this information will streamline the deployment process and coordination of required testing. ATIS/ESIF and NENA have very helpful resources to help you put together information that would be valuable to OSPs. The more detail OSPs receive, the greater the likelihood of a smooth deployment and less chance an OSP will ask to change default parameters in the FCC's rules or file a challenge at the FCC regarding your readiness. Don't expect the FCC to read every RFS and act as a check — but know that in these early days, they are reading them and have already notified a few PSAPs of the need to correct information.

Your NGCSP should be able to help you through the process.

PRO TIP:

Take advantage of the thorough readiness checklists from ATIS/ESIF and NENA. Ensure your NGCSP has a firm grasp on the FCC's framework and, more importantly, is completely fluent in i3 with a track record of successful previous deployments.

Future Direction of NG9-1-1

As we review the initial deployments of NG9-1-1, we are already seeing the rollout of additional benefits and functionality. These include:

Advanced Automobile Collision Notification (AACN) transmits additional crash data with the call to the PSAP, including severity, airbag status, number of occupants, seatbelt status, and car orientation. AACN enables PSAPs to send the most appropriate response to an accident. So far, these solutions are over-the-top applications and not integrated with ESInets.

Emergency Incident Data Object (EIDO) is the data exchange protocol that contains incident and related information that passes between functional elements in 9-1-1 CHEs. It facilitates the transfer of incident data to allow the legacy CAD "spill" from CHE to CAD initially, then replace with a rich data exchange of all of the information the CHE knows about a call. This data can also be transferred to other agencies, and beyond, to follow the incident.

Video calls/imagery will be added to the stream to provide better situational awareness to PSAPs, 9-1-1 telecommunicators, and first responders. Video calls may be in the form of PSAP-initiated requests for video feeds during a voice or text call, or even as a video-initiated call, similar in user experience to a FaceTime call.

Pictures with text and RCS messaging.

Additional data to the PSAP, such as medical data, enhanced location, associated and additional addresses, and alarm data will allow the 9-1-1 telecommunicator to quickly identify the nature and location of the emergency.

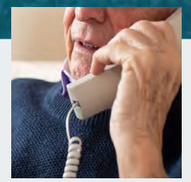
Advanced applications of artificial intelligence are possible now with the deployment of NG9-1-1, including:

- Answering and assisting with calls to PSAP administrative lines and transmitting these calls back to emergency trunks
- Dealing with non-emergency calls transferred from 9-1-1 trunks
- Summarizing 9-1-1 calls
- Automatic language translation and language detection of 9-1-1 calls
- Triage of 9-1-1 calls during periods of extremely high call volume
- Detection of TDoS attacks
- Threat assessment of swatting calls that could result in erroneous dispatch of Special Weapons and Tactics (SWAT) units

The multiplicity of NG9-1-1 features and applications adds tremendous value to emergency response. They also, in our opinion, pose the greatest risk to the future of NG9-1-1: complexity. Greater complexity, combined with the many options available in the evolution of the i3 standards, is becoming a liability. Instead of focusing on critical interfaces linking OSP to ESInet, ESInet to ESInet, and ESInet to PSAP, the i3 standards delve deeply into details of systems that would typically be internal to the ESInet and — again, in our opinion — add unnecessary complexity to the NG9-1-1 environment that does not need to be incorporated into standards, let alone the multiple methods defined in i3 to transmit similar data. Two examples: i3 defined AACN as a new, unique mechanism to set up the call and transmit data, but existing mechanisms could have fulfilled the same role. Second, EIDO treatment in the i3 standard duplicates functionality with the Additional Data Repository (ADR).

As i3 evolves, the public safety community should consider removing duplicate, unused, and unnecessary functionality to reduce complexity. As states and regions develop their requirements for NG9-1-1, they should focus on interoperability between OSPs, ESInets, and PSAPs, as well as on the security, reliability, redundancy, and actual functionality they need and will use. Any additional requirements will increase costs and complexity for functionality that may never be needed.

Location Technologies



Not Your Grandpa's Location Data

Let's rev up the wayback machine. The 9-1-1 system was designed in the 1960s and 1970s for wireline phones, which routed calls through physical, copper wires to a PSAP. Identifying the caller's location was fairly simple. It was based on the address where the phone company installed the telephone and tied to the phone number assigned to that address. When someone called 9-1-1 from a wireline phone, their address would be displayed on a little screen at the PSAP, with an indication of which law enforcement, fire, and EMS agencies were responsible for that address.

Enter Wireless Enhanced 9–1–1

In 1998, when wireless was first connected into the 9-1-1 network, a new mode had to be developed to transmit the location of the wireless 9-1-1 caller to the PSAP. Wireless Enhanced 9-1-1 Phase 1, which provides a callback number to the PSAP, was designed to integrate with existing 9-1-1 networks without requiring many changes to PSAP systems. When a wireless caller dialed 9-1-1 in an area that had implemented Wireless Enhanced 9-1-1 Phase 1, the wireless carrier would pass the physical address of the cell tower to which the wireless phone attached. While this address could be displayed on existing equipment at the PSAP, in most cases it was not accurate enough to actually locate the caller. It did, however, allow PSAPs to call back in the event of disconnection.

In 2001, deployment of Wireless Enhanced 9-1-1 Phase 2 technologies began. With this advance, wireless providers — specifically, Commercial Mobile Radio Service providers (CMRS) — started to deliver more accurate latitude and longitude data for the caller. Latitude and longitude were accompanied by an "uncertainty radius" — a circular area centered on those coordinates that the PSAPs could use as a search area with 90% confidence that the caller was there. The search area is extremely important, because the latitude and longitude do not indicate the exact point where the caller is located but rather the center of the search area where emergency responders should search — whether it's as small as a gas station parking lot or as vast as Central Park.

This new Phase 2 location required changes at the PSAP: specifically, new mapping systems that could receive and plot latitude, longitude, and uncertainty radius. It may seem counterintuitive, but trying to pinpoint latitude and longitude coordinates to precisely identify a caller's location is not actually the fastest method for finding the caller. More education is required to reinforce this for PSAPs, because many still do not understand the value of uncertainty and its relationship to the search area, and thus may not display it on the screen. Not knowing where to search for a caller beyond the point defined by the latitude and longitude puts PSAPs at a disadvantage.

GPS Hits the Scene

Early on, CMRS providers utilized several different location technologies. GPS proved the most accurate and became the primary location technology. Other less accurate network-based technologies — such as cell ID, enhanced cell ID, and angle of arrival — were used if a GPS location could not be determined.

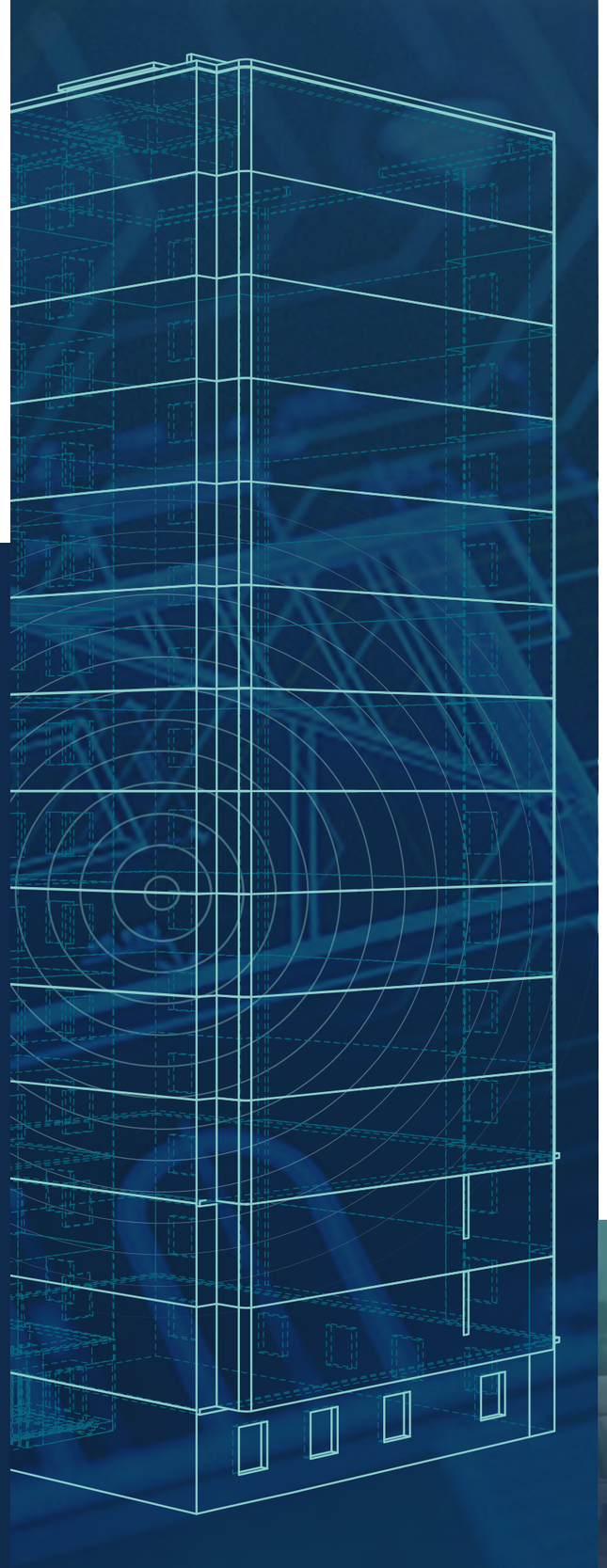
Original implementations of GPS by the CMRS providers for 9-1-1 used a GPS technology called Assisted GPS (AGPS), where the network assisted the handset in computing the GPS location. This helped reduce startup time (TTFF, or time to first fix). This was a valuable location technology when phones' processors and batteries were limited because it required fewer mobile resources than a pure mobile station-based GPS.

Phone, Locate Thyself

In 2007, after the initial release of the iPhone, location technology advanced to the point where the phone had the ability to accurately locate itself without assistance from the network. Handset operating system (OS) providers also started to use other sensors, such as Wi-Fi, Bluetooth, altimeters, and accelerometers, to augment GPS and provide more accurate indoor positioning. All this was done to support commercial applications on the phone, but was not available for 9-1-1. People started to ask, "Why can Uber locate me but 9-1-1 cannot?" Eventually, handset OS providers, along with the CMRS providers, began to integrate this location data into the 9-1-1 call flow.

In 2018, handset OS providers started providing commercial location data to 9-1-1, an approach called "hybrid location," which combines GPS, Wi-Fi, cell ID, and other device sensors. Based on hybrid location, Google created Fused Location Provider (FLP), and Apple created Hybridized Emergency Location (HELO). These approaches together are called Device-Based Hybrid location (DBH). Remember this.

The location data provided by DBH (FLP and HELO) is conveyed to PSAPs from the CMRS provider via two mechanisms: legacy Automatic Location Information (ALI) or NG9-1-1 protocols, both of which are considered primary location data. While CMRS providers deployed this new location data, over-the-top providers delivered the same location data outside the CMRS and 9-1-1 networks via IP. This over-the-top location data is considered supplemental location data. The only difference between the primary and secondary locations is when the data is sent and what path it takes. Carrier-based location works even if the phone is NSI or service is disconnected. An over-the-top path requires the user to have active service with data enabled.

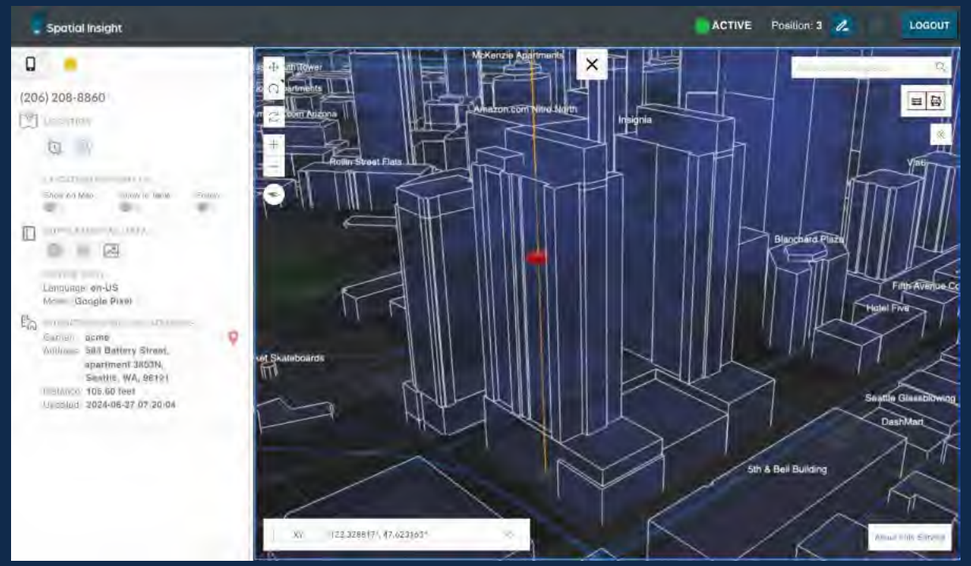


Indoors: The Final Frontier

In 2021, wireless OSPs began to deliver altitude (z-axis) information to PSAPs along with horizontal coordinates, rendering location data in 3D. Because DBH is a fusion of multiple technologies, it currently provides the most precise and accurate altitude information, particularly for indoor locations, where GPS struggles.

Vertical uncertainty is critically important to delivering altitude location, in the same way that horizontal uncertainty is important to delivering 2D location. A vertical uncertainty of 3 meters could indicate a range of two floors in a building, while an uncertainty of 30 meters could be 18 floors. Without the uncertainty, the altitude value is almost unusable. If systems are in place at the PSAP to properly display and map the data, altitude location can be accurate enough to provide a meaningful enhancement to locate a 9-1-1 caller. Several challenges, however, prevent us from fully utilizing altitude data.

We want to be clear about something. Uncertainty is a measure of location quality, not location accuracy. It provides a search area within which there is a 90% probability that the caller is located. The caller is just as likely to be in the exact center in the search area as at the edge. PSAPs should utilize search area both horizontally and vertically to locate 9-1-1 callers, instead of dispatching based on the dot that is defined by the latitude, longitude, and altitude points.



3D wireframe of building

An Ellipsoid Walks into a Bar ...

Here's how altitude data works. We're going to go full-on geek here, so bear with us.

First, in NG9-1-1, the OSP transmits the 3D location data to the PSAP as a shape called an "ellipsoid point," which can convey latitude, longitude, horizontal uncertainty, altitude, and vertical uncertainty. All five pieces of data are necessary to utilize 3D location data to find the caller. With latitude, longitude, and horizontal uncertainty, there is a 90% probability that the person is calling from an area that is up to a specific number of meters away from the point, as defined by the latitude and longitude. This point is the search area, and the distance from the point is defined by the horizontal uncertainty.

The altitude displayed to the PSAP is a bit more complicated. It displays as "height above ellipsoid," which is how the FCC requires wireless carriers to report vertical location. Computers understand this concept well, but humans do not. GIS can convert the height above ellipsoid to "height above ground," if high-resolution elevation map data is available for the area. In a multi-story building, this would identify the caller's floor level, assuming a high-accuracy indoor map is available. A cylinder in space can also visually represent this 3D search area. Providing the vertical uncertainty is just as important for locating a caller as providing the vertical search area.

To make 3D location data actionable, the PSAP needs:

- All five location components must pass from the carrier through the ESInet and CHE and into the CAD. Sometimes one or more of these elements is stripped or changed by the ESInet, CHE, or CAD/mapping.
- The mapping system must be able to convert this location to a human-readable format. This could be a 3D map with a cylinder representing the search area, or it could be a detailed floor plan showing the possible floors based on vertical uncertainty.

The ability to use altitude information to improve emergency response depends not only on the PSAP receiving the data, but also on having proper maps or systems to display the data in a usable format. A former 9-1-1 director in Houston put it succinctly: "First responders can't respond to X/Y." He meant that X/Y/Z coordinates alone are not useful for a first responder; PSAPs must be able to convert these coordinates into a map or a dispatchable location, such as an address, floor, or even a room. A PSAP can do this only by means of a map that can plot 3D location. The industry has mostly solved this for X and Y coordinates, with fairly universal maps available to PSAPs across the U.S. However, relatively few PSAP mapping systems that incorporate 3D indoor maps are able to utilize the provided z-axis information.

The issue with 3D maps, then, is not one of technology, but rather implementation. Technology is available to create extremely accurate 3D maps but these maps are expensive to develop and, therefore, few have been developed that are usable and available to PSAPs. An alternate way that PSAPs can make some use of vertical location data would be for the PSAP to use simple GIS systems, leveraging National Oceanic and Atmospheric Administration and United States Geological Survey data, to convert height above ellipsoid (in meters) to height above ground (in feet), so that a 9-1-1 telecommunicator can give responders some sense of where a caller is in a building. This is not as accurate as precise 3D indoor maps but does provide usable vertical location information to the first responder.

Wireless geodetic location will continue to improve, but these advancements won't make it easier to find 9-1-1 callers in multi-story buildings until accurate 3D building maps are developed, deployed, and integrated into public safety mapping systems.

2D map

3D map with floorplan

Location-Based Routing

Location-based routing (LBR) has received a lot of attention in the last year because the FCC began requiring it for wireless 9-1-1 voice calls in 2024. The deadline for the three major wireless providers to deploy LBR has passed; non-nationwide providers must implement LBR by May 2026.

LBR technology uses location information from the handset to route the call, rather than relying on cell site location. Before LBR, the system routed 9-1-1 calls to the appropriate PSAP based solely on the cell site to which the call attached. This resulted in nearly 20% of all 9-1-1 calls requiring a transfer to a neighboring PSAP, because the technology was sufficient to tell that the call was placed from a location near a PSAP boundary but not precise enough to determine the correct PSAP to route the call to.

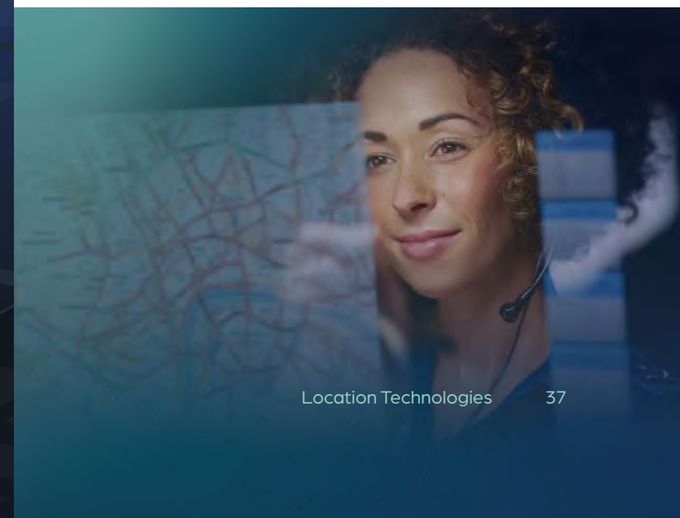
Traditionally, a wireless call to 9-1-1 would not begin to identify the location until the call was received by the cellular network. Without LBR, good location data was not available in time to avoid misrouting. The alternative was to delay the call to give the network a chance to catch up. Now, with DBH location, which uses the handset to determine the location, the handset knows before the network that a user wants to dial 9-1-1 and can start the location determination process earlier. This means location is available by the time the network is ready to route the call to 9-1-1.

The Future of Location Data

The capabilities of location data will continue to improve. Specifically, we expect that altitude location information will improve as phone sensors improve and as location data providers fine-tune their methods. As handset OS providers continue to improve DBH location for commercial purposes, 9-1-1 will instantly benefit.

With 5G wireless, new network location technologies promise dramatic improvements over GPS for indoor locations and will continue to enhance the accuracy of X/Y/Z locations. The challenge is that, without accurate 3D maps — including floorplans — better location accuracy will not necessarily make it easier for first responders to locate the caller.

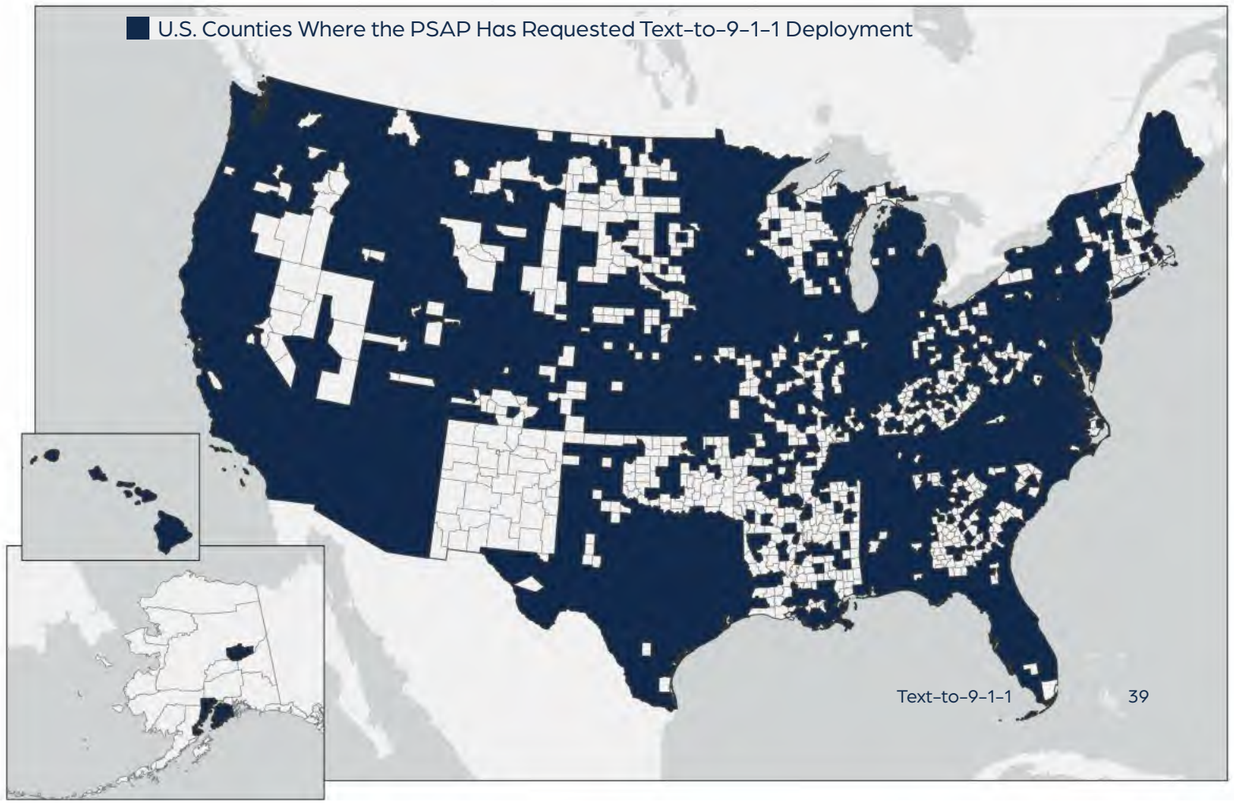
We'll conclude this discussion by making sure you know that there are companies working to create better maps. As you read this, aircraft are flying over cities, using survey-grade GPS and Light Detection and Ranging to create centimeter-level, hyper-accurate maps of building exteriors and the actual ground level point. This data will lead to more precise location information and get help to people who need it — faster.



TEXT-TO-9-1-1

Text-to-9-1-1 was first deployed over a decade ago. Since then, approximately 85% of the U.S. population has gained coverage from PSAPs that have implemented text-to-9-1-1. Under the FCC's rules, "covered text providers" must deploy text-to-9-1-1 following a PSAP request to make text available. If text is not available at the PSAP, the caller will receive a bounce-back message that says "Make a voice call to 9-1-1 for help; text-to-9-1-1 is not available."

Some say that text-to-9-1-1 is not very accurate. Let's bust that myth right now. Providers can deliver highly accurate location with text-to-9-1-1. The challenge is ensuring PSAPs have systems in place to use that information. When text-to-9-1-1 was initially deployed, only coarse cell-based location was available. Over time, text-to-9-1-1 location accuracy has dramatically improved and is today almost on par with voice 9-1-1 location accuracy — including having the ability to transmit altitude information. Unfortunately, many PSAPs are not aware of these improvements, because they are not displaying or mapping the improved uncertainty (search area) and altitude information.



Current Challenges with Text-to-9-1-1

Despite all these positive developments, several challenges remain:

Longer call durations:
Text-to-9-1-1 conversations inherently take longer than voice calls, because 9-1-1 telecommunicators must identify the nature of the emergency and verify the location of the emergency through a series of text exchanges, which causes delays.

Unanswered text messages from PSAPs that have deployed text-to-9-1-1:
Based on records from the Intrado Text Control Center (TCC), we observe that, nationwide, accounting only for PSAPs with text-to-9-1-1 enabled, approximately 10% of text-to-9-1-1 requests go unanswered (instead sending a bounce back message indicating the service is unavailable). The percentage of unanswered text messages could be much higher for certain PSAPs. In fact, according to our assessment, some text-enabled PSAPs fail to answer nearly 100% of texts-to-9-1-1. We'll discuss why 9-1-1 text messages may go unanswered at text-enabled PSAPs in more detail below.

Incomplete PSAP deployment:
So why are some PSAPs still not deploying text? It could be because of the cost; lack of staffing; lack of understanding of the value of text-to-9-1-1; a misconception that deployment would result in staff being overwhelmed by texts or that text locations are not accurate; or possibly even a concern that people will abuse text-to-9-1-1. One solution could be to establish a nationwide text-to-9-1-1 relay center that will answer text messages from areas outside of deployed PSAPs, or that will send unanswered messages to deployed PSAPs. Similar solutions have been adopted for satellite SCS and MSS text services and text-to-988. It might also be possible to utilize AI for text-to-speech conversion of 9-1-1 text messages sent to a voice-only PSAP.

Limited use of improved location data:
On the whole, PSAPs do not utilize improved location data available with 9-1-1 text messages. Instead, they plot points representing the x and y coordinates on a map, without clearly displaying the uncertainty radius (aka search area). If this sounds familiar, that's because we just finished discussing this with respect to Location Technologies. This is important — more below.

Achieving full text-to-9-1-1 coverage could be as simple as establishing a nationwide text-to-9-1-1 relay call center that will answer text messages from areas outside of deployed PSAPs or send unanswered messages to deployed PSAPs.

Non-emergency text messages:
As with voice calls, text-to-9-1-1 sometimes transmits pocket dials, misdials, or automated texts without a human sender. Protocol requires that 9-1-1 telecommunicators respond and wait for a reply to determine if a real emergency exists, consuming valuable time. AI will be able to alleviate this problem by detecting non-human texters.

Language support limitations:
A significant number of 9-1-1 texts received by PSAPs are in languages the telecommunicator does not speak (or, perhaps more important, read). While language lines assist voice calls effectively, it's been challenging to implement similar solutions to translate texts. The advent of AI translation capabilities integrated with PSAP CHE is helping to address this in Columbus, Ohio, for example.

Newer entrants' failure to recognize that they are a "covered text provider":
Non-traditional communications providers allow users to purchase customized packages that can include both regulated and unregulated services; one example of this is Unified Communications as a Service (UCaaS). We have observed that these new entrants are often unaware they qualify as a covered text provider under current FCC rules, and therefore should incorporate text-to-9-1-1 interconnection into the native 9-1-1 network.

PRO TIP:

Providers – if your service allows subscribers to text their mother's cell phone, you're probably a covered text provider under the FCC's 9-1-1 rules.

Lack of public awareness leading to underuse:
There is uneven public awareness that text-to-9-1-1 is available where people live, and even less understanding that it's available beyond the home area. In our opinion, this results in underuse of texting to seek emergency help from 9-1-1, especially juxtaposed against significant growth of other text use in similar situations, such as texting to 988. We would like to see both the FCC and state 9-1-1 Authorities more proactively engage the public to increase awareness about where text-to-9-1-1 is available and what to expect when initiating a request for emergency assistance via text.

More on unanswered texts. Text-to-9-1-1 is an extremely high-value use of text messaging. Many of the most critical text calls we have seen have been from deaf and hard-of-hearing individuals; people who do not feel safe making a voice call; or people whose anxiety makes it difficult for them to make a voice call to 9-1-1. Without text-to-9-1-1, these calls for help could go unanswered. There are several possible reasons for this:

- The PSAP has not requested or deployed text-to-9-1-1.
- A single workstation is assigned to take text-to-9-1-1 calls, and no one is monitoring that workstation.
- The text system is monitored but times out. The 9-1-1 telecommunicator is subsequently logged out, unbeknownst to them, and won't be notified of text messages unless they log into that system again — which may not be part of their CHE.
- In situations where all telecommunicators are occupied with 9-1-1 voice calls, 9-1-1 text messages might go unanswered because of longer handling times. This issue significantly impacts response capabilities during major emergencies or disasters, when texting might be the only viable communication method.

The problem of unanswered texts-to-9-1-1 is not theoretical. Below is a text message relayed through our TCC that the PSAP never answered, despite having publicly advertised that they support text-to-9-1-1. It is not a unique case.

I need help.
Caller

Make a voice call to 9-1-1 for help; text-to-9-1-1 is not available.
Automated message from PSAP

I cant talk on the phone.
Caller

Help me please.
Caller

My husband is hurting me.
Caller

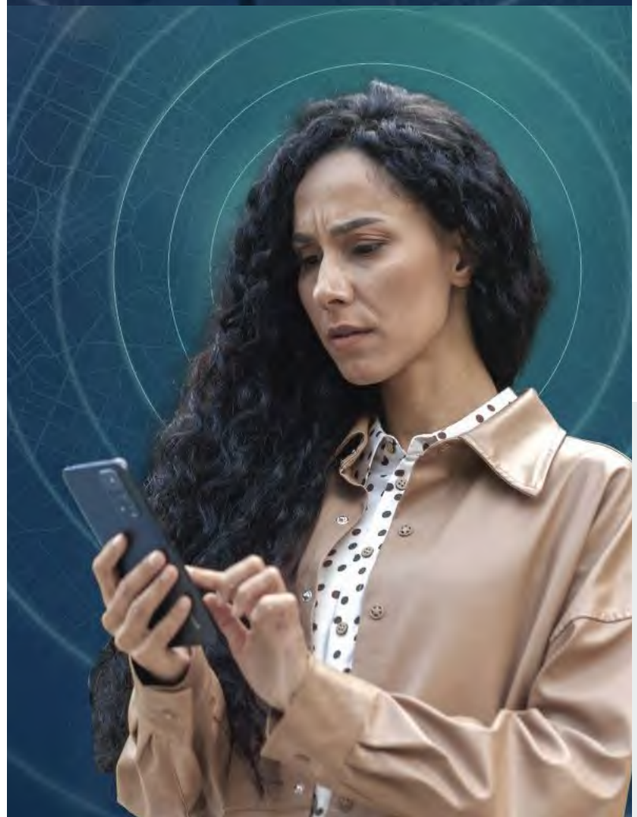
I need help but he is sitting right in front of me.
Caller

Location Data for Text-to-9-1-1 and Location Data for Voice Are Equally Accurate

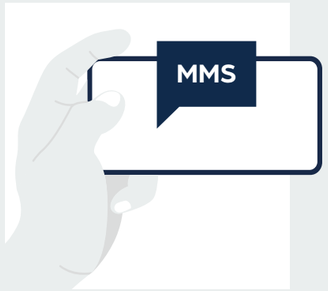
Currently, the median horizontal location uncertainty for text-to-9-1-1 is approximately 31 meters (102 feet). This is similar to voice call accuracy — which is to say pretty darn accurate. Apple smartphones generally have a higher percentage of accurate locations than Android smart phones, based on how and when they send location data. Some carriers, such as AT&T Mobility, also provide altitude information with nearly all their text-to-9-1-1 calls.

As with voice calls, to use text location, PSAPs must have a mapping system within the CHE that displays text location data. Because most CHE was initially setup to support cell-based location (as this is all that was available when text-to-9-1-1 was launched), the PSAP call-handling equipment generally has not kept up with location accuracy improvements. Most of the CHE out there for text-to-9-1-1 does not readily distinguish between specific and inexact locations, as they do for voice calls (phase 1 vs. phase 2 class of service in voice calls). Many systems show only a point on a map to define a search area, without graphically representing the uncertainty as a circle on the map or as a numerical uncertainty radius.

The point is: without a clear display of the uncertainty, it is impossible for 9-1-1 telecommunicators to convey the size of the geographic area where first responders should search for a caller. And, as you just read, current PSAP systems typically do not display altitude (z-axis) location, hindering response to emergencies in multi-story buildings.



Future Developments in Text-to-9-1-1



Multimedia Messaging Service (MMS) is an extension to Short Message Service (SMS) that supports the inclusion of images, videos, and audio with a text, which traditional SMS does not. It has been widely deployed in the U.S. since 2003. While MMS is not an official part of the text-to-9-1-1 standards, one might argue that, under the FCC's rules, the text portion must be delivered. At least one major U.S. wireless carrier has integrated MMS into text-to-9-1-1, allowing their 9-1-1 texters to send photos, videos, or other media with the text message. Currently, media content that is part of a 9-1-1 text is stored and delivered to the PSAP via separate mechanisms because of limitations of the current ATIS/TIA joint standard (J-STD-110) on text-to-9-1-1. This makes it difficult for the PSAP to easily make use of the included photos, videos, or audio clips.

Rich Communications Services (RCS): The wireless industry has renewed efforts to integrate RCS since its original launch in 2007 as a messaging service designed to eventually replace SMS. RCS is widely used by Android users and, starting in late 2024, by Apple devices. It's possible that we'll see integration of RCS deployments into the existing text-to-9-1-1 infrastructure as early as the end of 2025. Examples of the benefits of RCS include high-resolution photos and videos, links, delivery/read receipts, and typing indicators. From an architectural standpoint, RCS has some advantages over SMS because text-to-9-1-1 call flows use similar protocols as RCS, allowing RCS to eventually flow directly from the handset to the PSAP as a NG9-1-1 native call (and not require protocol conversion). RCS also has significant advantages over SMS and MMS in that photos and videos arrive faster, are a much higher resolution, and are not limited to 150 characters per individual message.

Satellite Text-to-9-1-1: Apple's SOS service essentially results in a text-to-9-1-1. Providers such as T-Mobile have launched satellite-based texting for 9-1-1 calls in areas lacking voice connectivity; others, including AT&T and Verizon, are trialing this service, which activates only when terrestrial mobile networks are unavailable. Several issues must be addressed, chief among them latency. More on this in the upcoming section about 9-1-1 over satellite.

INTERLUDE ON DISRUPTIVE AND EMERGING TECHNOLOGIES

The future of 9-1-1 is shaped by disruptive and emerging technologies that promise to transform emergency response. Advanced AI and machine learning are being integrated into emergency systems to enhance decision-making and automate routine tasks. For instance, AI-powered chatbots can handle non-emergency calls, allowing human operators to focus on urgent situations. In Los Angeles, an AI-driven system has been introduced to triage emergency calls, improving efficiency and response times.

The integration of IoT devices and wearable technology is also paving the way for smarter and more responsive 9-1-1 systems. IoT sensors can provide real-time data on environmental conditions, such as air quality and weather, which can be critical during emergencies. Wearable devices such as smartwatches can monitor vital signs and automatically alert emergency services in case of abnormalities. In New York City, IoT sensors have been deployed to enhance urban safety and emergency response. The data these sensors collect help first responders make informed decisions and respond more effectively.

Emerging technologies such as augmented reality (AR), virtual reality (VR), and mixed reality (MR) are being explored for various purposes, including personnel recruitment and retention. These technologies can streamline the candidate vetting and onboarding process and improve training for new and veteran 9-1-1 professionals. For instance, AR can provide real-time information overlays for first responders, enhancing situational awareness and making training sessions more interactive and engaging. VR offers immersive training experiences that prepare emergency personnel for various scenarios, allowing them to practice responding to emergencies in a safe and controlled environment. MR combines elements of both AR and VR to create a hybrid experience that can be tailored to specific training needs.

By leveraging these innovative approaches, the industry can attract and retain skilled professionals who are better equipped to handle the demands of emergency situations, contributing to a more effective and responsive 9-1-1 system.

Next, we focus on 9-1-1 over satellite; PSAP transition to cloud call handling; the expanding 9-1-1 ecosystem; artificial intelligence in 9-1-1 operations; and strategies for addressing growing cybersecurity threats.

INTRADO
State of the 9-1-1 Industry

9-1-1 OVER SATELLITE

These are exciting times for satellite communications in the public safety space. Where once satellite connectivity was the domain of the military, the wealthy, or large-scale commercial interests, we are seeing an unparalleled democratization of the technology, resulting in the ability to reach un/underserved, remote, or disaster-stricken areas.

Satellite Has a Long History of Supporting Public Safety

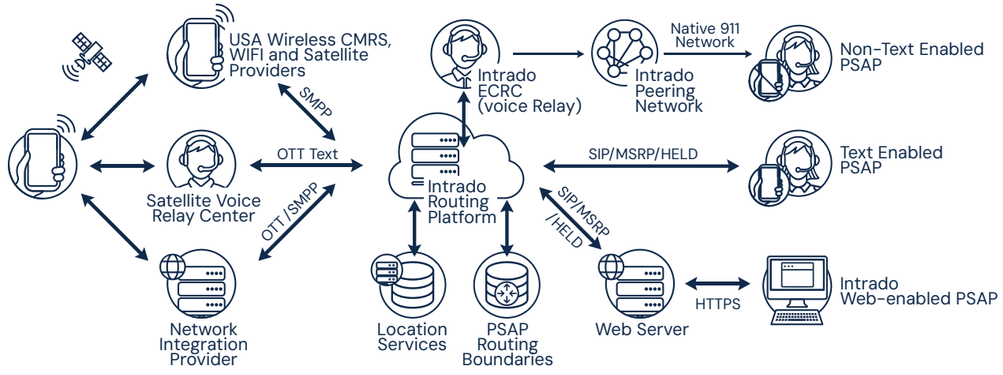
We don't want to leave the impression that public safety is a new use of satellite technology, when in fact commercial satellite technology has supported real-time monitoring and assessment of emergency situations for a long time. Mobile Satellite Service (MSS), where a satellite mobile phone acts as a mobile earth station, has enabled satellite service to handheld devices for a couple decades, including to relay emergencies to 9-1-1. Earth observation satellites can capture high-resolution images and provide valuable data for authorities to make informed decisions and allocate resources. For instance, satellite imagery was used during the 2019 California wildfires to track the spread and identify the most affected areas, facilitating a more targeted and efficient response. For many years, integrated satellite technology has enhanced location-based services and improved the accuracy, effectiveness, and reliability of 9-1-1 emergency response.

Satellite-Based 9-1-1 Services: The Next Evolution

As discussed above, satellite technology is proving to be a critical tool for emergency response. Historically, people outside terrestrial coverage relied on dedicated satellite devices. Today there is much broader availability for satellite to supplement terrestrial wireless coverage and extend emergency response capabilities. Modern smartphones provide Direct-to-Device (D2D) service, assisted by the increasing number of low earth orbit (LEO) satellites that make connections cheaper and with lower latency.

Some satellite companies provide D2D service using terrestrial spectrum, in partnership with terrestrial mobile wireless operations. Others use MSS spectrum. Existing MSS enables continuous communication in emergency situations, using networks such as Globalstar (Apple's partner for its SOS feature) and Iridium (using Garmin inReach® devices) to deliver satellite-based Sos messaging. Some satellite companies are working in partnership with terrestrial mobile wireless operators to provide D2D service over terrestrial wireless spectrum – this is called Supplemental Coverage from Space, and we'll talk a lot more about this in a minute.

Satellite Text-to-9-1-1



But First, a Short Tutorial

Before we go any further, it might be helpful to take a deeper dive into how satellites are used to support requests for assistance to 9-1-1, as well as explain some of the terminology.

Satellite communications to handsets can be delivered several different ways. It's like a 3D chessboard. To understand what is behind each service, we must consider three issues: What spectrum is the service using? What device is the service using? And what type of satellite orbit is the service using? For example, some applications require a phone capable of using satellite spectrum and protocols, while others use a regular smartphone. Still others relay a signal from a purpose-built IoT device to a satellite.

So what's the frequency, Kenneth?

Which Spectrum?

MSS (Mobile Satellite Service) spectrum, also known as L-band, is used by Iridium, Inmarsat, Globalstar, Thuraya, and others on frequencies ranging from 1.5-2.5 GHz. Connecting to satellites using MSS spectrum requires special handsets tuned to those frequencies. MSS is also used in the IoT context for SOS features. For example, Apple devices starting with the iPhone 14 connect to MSS operator Globalstar. On the Android side of the house, the Snapdragon MSS chipset enables similar functionality for devices such as the Samsung Galaxy 25.

MNO (Mobile Network Operator) spectrum (terrestrial wireless spectrum) frequencies in the U.S. refer to the portion of the radio spectrum used by conventional terrestrial mobile network operators, such as AT&T, T-Mobile, and Verizon, for their networks. In the SCS context, the terrestrial mobile network operator partners with a satellite operator to extend coverage for the terrestrial network. The call is placed using a regular smartphone and remains on the MNO spectrum for the duration of the call.

What Type of Device?

D2D/D2C (Direct-to-Device and Direct-to-Cellular) refer to communications between a mobile handset or IoT device and a satellite network.

MSS-based satellite phones are proprietary phones satellite operators use to provide service directly to end users that use MSS spectrum and protocols.

What Type of Orbit?

Non-terrestrial networks can be sliced into four segments:

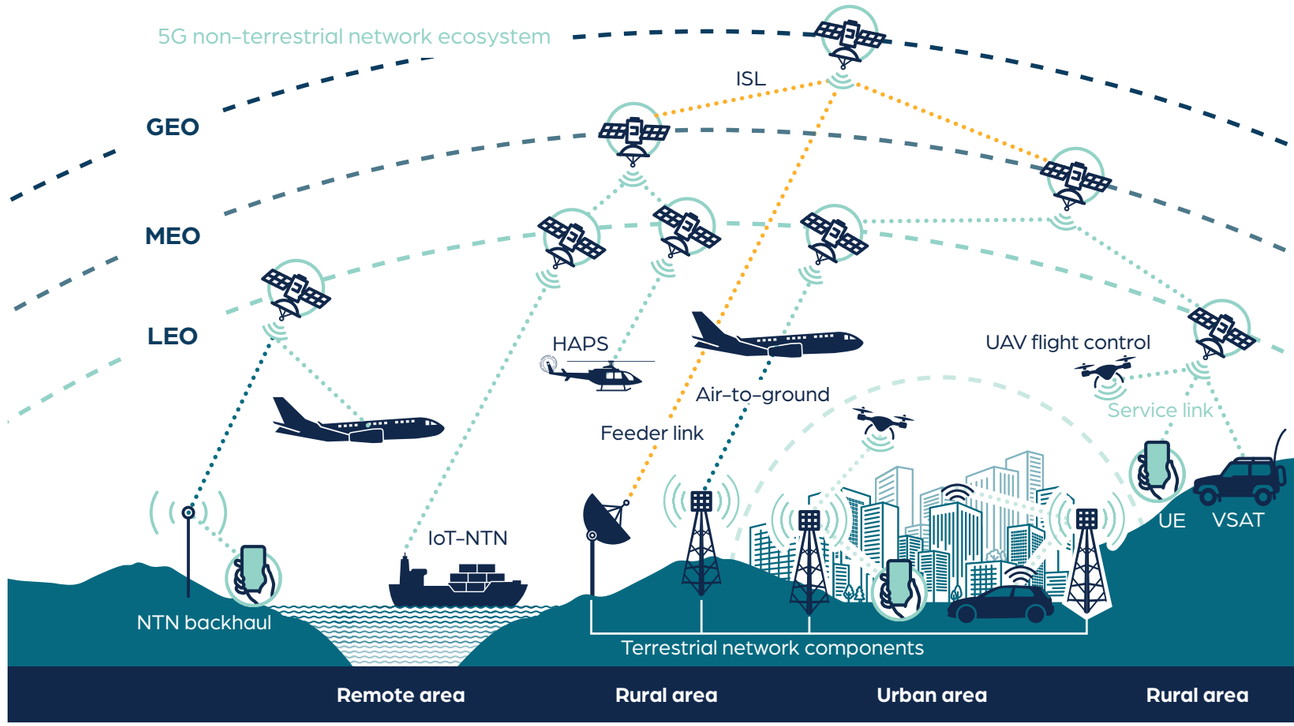
Geosynchronous earth orbit (GEO) satellites are in orbits that exactly match the length of the day, meaning that a GEO satellite will always appear to be over the same part of the earth, making line-of-site communications relatively easy. A challenge is latency. The altitude of geosynchronous or geostationary orbits is 22,236 miles (35,786km). Established players such as Inmarsat, Hughes, and Intelsat have long provided voice and broadband satellite communication, maintaining a strong presence in global telecommunications.

Low earth orbit (LEO) satellites orbit at a relatively low altitude, typically between 124 to 1,243 miles (200 to 2,000 km) above the Earth's surface. They are used for communications as well as Earth observation and scientific research. The advent of small, lower latency, cost-effective satellites, combined with advances in networking that allow for more effective coverage handoffs, is resulting in an explosion of new D2C and D2D applications. Companies such as SpaceX/Starlink, Amazon's Kuiper Project, AST SpaceMobile, and Lynk Global dominate this segment. As of March 2025, Starlink leads in deployed infrastructure, with 7,105 working satellites.

Medium earth orbit (MEO) satellites orbit between LEO and GEO, usually 1,243 to 22,236 miles (2,000 to 35,785 km) above the Earth's surface. Organizations like O3b that specialize in enterprise, maritime, and government communications use MEO satellites to offer high-throughput connectivity with lower latency compared to traditional GEO satellites.

High-Altitude Platform Stations (HAPS) are long-endurance, high-altitude, often unmanned aircraft that operate in the atmosphere at altitudes of 12.5 to 31 miles (20 to 50 km). They're not technically satellites, but they're super cool and provide communication and observation similar to satellites. They can be solar-powered, remain aloft through atmospheric lift, and be either aerodynamic (like airplanes) or aerostatic (like airships or balloons). HAPS enable the use of existing handsets with low latency and also provide coverage in areas lacking traditional wireless coverage or where wireless infrastructure has been damaged or destroyed. Companies including SoftBank occupy this segment.

To summarize, GEO, MEO, and LEO involve satellites in particular orbits, while HAPS remain in the atmosphere at high altitudes. Historically, GEOs have dominated voice communication. MEOs are integral to global navigation systems. LEOs are rapidly evolving and increasingly viable for both text and voice applications, as satellite capability is integrated into smartphones and purpose-built IoT devices such as wearables, vehicle tracking systems, and smart sensors. Here's a visual.



Now, back to our regularly scheduled 9-1-1 programming.

Single Network Frontier: Supplemental Coverage from Space

SCS is provided through a partnership between a satellite operator and a terrestrial mobile wireless provider (specifically, a CMRS provider). This service enables texts (and, eventually, voice) connectivity in areas where the terrestrial network lacks coverage. The value of SCS was recently showcased when SpaceX and T-Mobile SCS service assisted in the response to Hurricane Helene last fall. In addition to enabling text-to-9-1-1, the SpaceX/T-Mobile SCS service allowed local jurisdictions in the disaster area to reach the public with Wireless Emergency Alerts when terrestrial coverage was unavailable.

In early 2024, the FCC adopted a regulatory framework for SCS to streamline the types of approvals that are required to effectuate the service contemplated by these partnerships. This framework is intended to "incentivize creative partnerships between terrestrial network and satellite operators" as these companies work to meet growing demand for seamless connectivity in remote locations.

When the FCC adopted the SCS framework, it put in place interim rules for 9-1-1 calls over SCS networks. For the time being, providers must route calls to a geographically appropriate PSAP via a nationwide call center or by means of LBR. Because the call originates on the mobile network over commercial mobile spectrum, the bulk of the SCS rules address the obligations of the CMRS provider.

Current deployment of 9-1-1 over SCS relies primarily on text-based relay deployment models. Under this model, a call center — such as Intrado's Emergency Call Relay Center (ECRC) — receives the request for assistance, currently as a text message; obtains information from the person seeking help; and makes a voice call to the PSAP to relay information regarding the emergency.

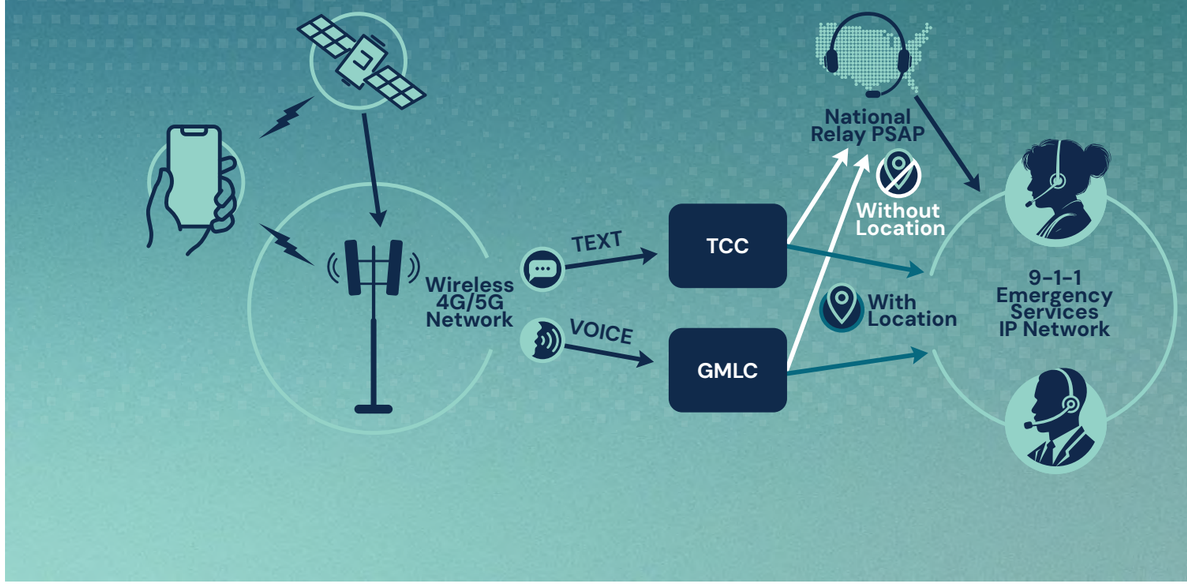
To compare, other satellite-supported 9-1-1 connections utilize text-based or voice-based relay models using MSS rather than terrestrial wireless spectrum. In the MSS model, a caller's message either directly routes to the PSAP over native text-to-9-1-1 connectivity using mobile-station-based GPS location or, when direct text routing is not feasible, to a backup emergency call center for "warm transfer" over native trunks to the PSAP. The telecommunicator at the PSAP stays involved in the transfer to ensure it is completed.

Over the next few years, consumers will see SCS begin to supplement text and, eventually, voice calls that originate on a satellite network. Similar to the routing mechanism for text-relayed 9-1-1 via MSS, routing for SCS 9-1-1 will occur in one of two ways (presuming the FCC's rules do not change and new technology is not introduced):

When location is available via LBR in time to route, device-based GPS will provide direct routing to the geographically appropriate PSAP

When LBR is not available at the time of routing, calls will continue to route to a nationwide backup emergency call center, where the telecommunicator will attempt to retrieve location from the handset to route to the appropriate PSAP. If the location is unavailable through that means, call center staff will ask for the location and the nature of emergency, relay the call to the appropriate PSAP over native trunks, and transmit any available location information natively to the PSAP.

The FCC's interim requirement for SCS 9-1-1 aligns with the current routing model depicted in the high-level diagram below:



These emerging text-based relay deployments of SCS to 9-1-1 generally incorporate handheld devices with mobile-station-based GPS location — which means they should be able to support the routing/location requirements for CMRS in the FCC's rules. In fact, because SCS support is utilized only with outdoor 9-1-1 calls/messages when there is a clear view of the sky, a handset connecting to SCS for 9-1-1 will almost always be able to see multiple GPS satellites. This allows for a GPS fix that tends to be more reliable and accurate for dispatch than the typical 9-1-1 call from terrestrial cell sites, which are commonly complicated by indoor location technologies.

Because cell-sector routing is not possible with satellites, and GPS information for SCS is sometimes unavailable at call setup, certain SCS 9-1-1 calls/texts will need to be routed to a nationwide 9-1-1 relay call center. This center must be able to retrieve location from the handset or verbally ask the user for the location and nature of emergency; relay the call to the appropriate PSAP over native trunks; and transmit any available location information natively to the PSAP.

We foresee no imminent material deviation from the 9-1-1 routing model described above in any of the emerging SCS deployments. To reach its full potential, the underlying technology and integration with terrestrial service needs time to develop.

All the Cool Kids Are Doing It

The number of satellite offerings currently available or on the horizon (we do love a pun) that use an off-the-shelf mobile device to connect to 9-1-1 is growing. They include:

SpaceX/T-Mobile:
Testing is underway to enable SCS text services to existing phones, with voice and data services expected in 2025.

AT&T/AST SpaceMobile (AST):
AST launched its first five commercial satellites in September 2024 leveraging an SCS arrangement. They recently obtained special temporary authority from the FCC to test its solution with AT&T and FirstNet.

Verizon/AST:
In May 2024, Verizon announced a $100 million strategic partnership with AST to provide D2C service leveraging an SCS arrangement, with plans to launch satellite-enabled emergency text and location services for compatible Android smartphones. Google Pixel Pro devices and the Samsung Galaxy S25 device are expected to be among the first to access to this service. AST has obtained special temporary authority to test its system also with Verizon.

Apple/Globalstar Emergency SOS:
iPhone models 14 and above (running on iOS 18+) allow users to connect with emergency services by text message via Globalstar satellites leveraging MSS arrangements.

Skylo is teaming up with device manufacturers and communications providers to launch commercial D2D service leveraging MSS arrangements.

Iridium: Using Iridium satellite phones, Iridium provides access to 9-1-1 leveraging MSS.

So What Does All This Mean for PSAPs?

9-1-1 over satellite reaches the PSAP much the same as ordinary terrestrial wireless calls; however, there are slight operational differences for PSAPs depending on whether the 9-1-1 request for assistance is routing via SCS or via MSS.

New players: PSAPs should be prepared to receive calls from a wider range of third-party call centers than in the past, and to recognize that the emergency has been triaged and likely confirmed to be real. Further, PSAPs should be prepared to coordinate any post-dispatch or pre-arrival instructions with the third-party call center, since the person seeking help cannot make or receive voice calls.

Long call times and latency: PSAPs must be prepared for longer call durations and greater latency with 9-1-1 requests for assistance over satellite. This includes maintaining communication with the caller while possibly coordinating search and rescue operations with multiple agencies. Further, the user could appear inactive for periods of time due to the satellite coverage gaps as the satellite continues to orbit.

Uncharted territory: Given the robustness of satellite coverage, PSAPs are receiving requests for assistance from geographic areas from which end user could not previously send requests. To prepare for this, PSAPs should routinely review their jurisdictional boundaries to ensure they are up to date, especially in rural/remote areas. Additional training for telecommunicators and dispatchers specific to remote locations may be helpful.

Increased coordination: Satellite-based calls may require heightened coordination efforts, especially for maritime search and rescue missions or those in remote locations. PSAPs must work closely with emergency response teams (which could include specialized rescue teams, such as mountain or water rescue) and local authorities (which could include the park or forest service) to ensure effective and timely assistance.

Satellite-Capable Devices and Equipment:
A Rapidly Expanding Market

Satellite-capable devices represent the fastest-growing sector within the satellite industry. These devices dramatically reduce coverage gaps between terrestrial and satellite networks. Key advancements include:

Consumer mobile devices: Smartphones from Apple (iPhone 14 and later running on iOS 18+), Samsung (Galaxy S25+), and Google Pixel 9 now support direct satellite connectivity on MSS spectrum, enabling voice and text communication in previously unreachable locations. This is in addition to the satellite connectivity enabled by SCS on existing handsets that use MNO spectrum.

Dedicated satellite devices: Purpose-built satellite communication tools such as Iridium satellite phones and Inmarsat's IsatPhone remain the gold standard for professional and emergency use.

Chipset and modem manufacturers: Companies such as Skylo, Qualcomm, and MediaTek are pioneering the hardware integration necessary to seamlessly bridge satellite and terrestrial networks, allowing ubiquitous connectivity.

A Note on 9-1-1 Calls Made from Offshore

Historically, 9-1-1 calls could be made only close to shore, and the 9-1-1 system was set up to handle calls within 3 miles of the shore. Now, smartphones can make 9-1-1 calls from farther offshore — and even from the middle of the ocean.

So many questions! Where will these new calls be routed? Who is going to answer them? The Coast Guard or a PSAP — or maybe a new Coast Guard PSAP(s)? If the Coast Guard is answering the call, should they be connected to other ESInets to facilitate call transfer with location information? Should they follow the NG9-1-1 standard? As a nation, we have arrived at the point where these questions are ripe for resolution.

Future Direction of 9-1-1 Over Satellite

If you had any doubt before, it should be crystal clear that satellites are crucial tools for public safety, and that the importance of satellite to 9-1-1 will continue to grow as coverage extends to devices and users who previously had no access to this powerful technology.

Of course, challenges remain; for example, text latency, defining PSAP/emergency response jurisdiction in remote areas, and determining who or what should become a PSAP (as we just mentioned with respect to calls originating offshore). The satellite industry will need to work closely with regulatory bodies and public safety agencies at all levels of government to help this promising technology reach its full potential.

Before we wrap up this discussion, we want to call your attention to the next step in the evolution of 5G, because it relates to satellite. 5G over non-terrestrial networks (5G NTN), as its name suggests, is intended to allow 5G communications over satellite. 5G NTN has two components:

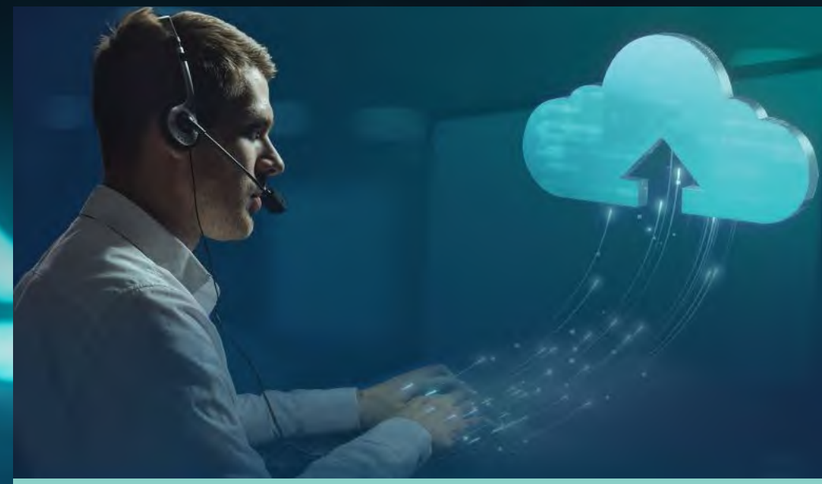
Non-terrestrial networks-internet of things (NTN-IoT) extend and enhance current wireless IoT use cases. NTN-IoT has relatively slow data speeds and low power consumption. It operates at GEO and LEO altitudes, with most current services at GEO.

Non-terrestrial networks-new radio (NTN-NR) will bring connectivity to smart phones, laptops, fixed wireless access hot spots, and other devices that require additional bandwidth.

Testing has begun for 5G NTN, which is expected to provide more options for connectivity in areas where terrestrial networks are unavailable to reach or difficult to deploy — offering a more global and ubiquitous 5G experience and could further expand the reach of 9-1-1.

The satellite industry will need to work closely with regulatory bodies and public safety agencies at all levels of government to help this promising technology reach its full potential.

PSAP MIGRATION TO CLOUD



The shift to cloud computing is one of the most significant changes in the public safety industry in the last 10 years.

Let's get straight what we mean by "cloud," why it matters, the requirements for transitioning to the cloud, and its advantages and disadvantages.

What Is "Cloud" for a PSAP and Why Does It Matter?

For a PSAP, moving to the cloud means relocating your 9-1-1 systems from local infrastructure to external data centers. These data centers may belong to a public cloud provider (such as AWS, Microsoft Azure, Google Cloud, or Oracle Cloud), where the 9-1-1 software or services run on infrastructure managed by the provider.

Alternatively, a PSAP might utilize a private cloud solution, where the provider operates software on their own privately hosted infrastructure. Applications hosted in these cloud environments can range from traditional virtualized systems (previously run on physical hardware) to modern, "containerized" applications or "serverless" architectures.

Moving to the cloud enables individual PSAPs, regardless of size, to achieve greater scalability, economies of scale, geographic redundancy, and enhanced security, as well as access to advanced toolsets typically available only to larger organizations.

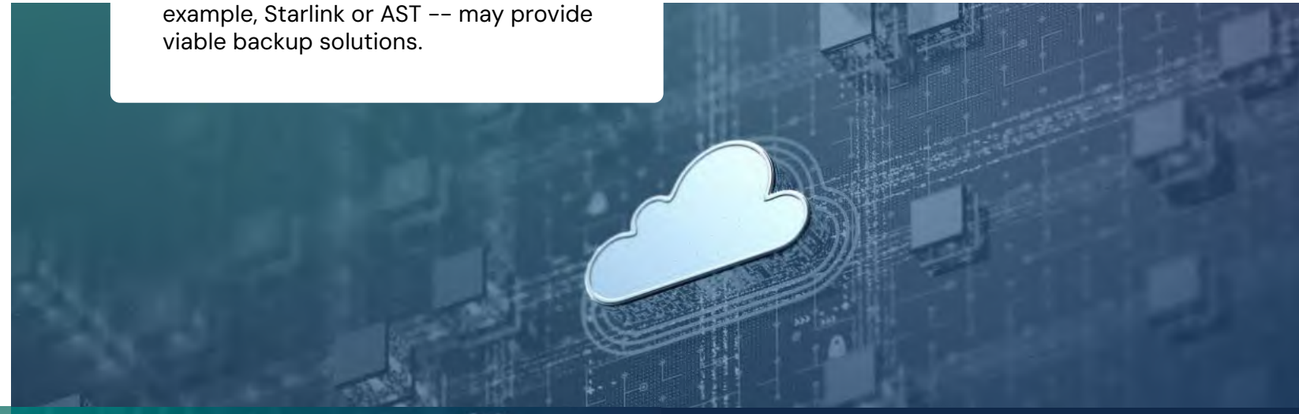
Cloud Options and Considerations

Each cloud deployment type — serverless, containerized, or virtualized — offers different benefits in terms of scalability, cost, reliability, and portability. Different cloud providers also vary significantly in their capabilities and costs. For example, while public cloud providers may offer lower initial costs for serverless architectures, this can lead to vendor lock-in, limiting portability if business terms or service requirements change.

Unique PSAP Requirements

Public safety environments have unique demands. Unlike services like Netflix, scalability isn't the primary challenge for 9-1-1; reliability, consistent availability, and geographic redundancy are far more critical. Traffic for emergency services remains relatively steady, and systems must be ready instantly, eliminating the option of waiting for infrastructure to scale dynamically. Because of these unique requirements, there is no universally optimal choice among public, private, or hybrid cloud providers or technologies (serverless, containerized, or virtualized).

A critical requirement for cloud adoption is reliable, redundant internet connectivity. While obtaining such connectivity is increasingly common, many regions still face challenges with limited network redundancy. In such scenarios, secondary paths like FirstNet, commercial 4G/5G networks, or LEO satellite services — for example, Starlink or AST -- may provide viable backup solutions.



Advantages of Cloud for PSAPs

- **Enhanced reliability:** PSAPs no longer depend on single point-of-failure local systems. Cloud infrastructures provide geographic redundancy by distributing systems across multiple locations or states.
- **Geographic flexibility/local survivability:** PSAPs can easily relocate or activate backup sites. Cloud-based applications require only an internet connection, allowing PSAPs to be supported by geographically distant locations during times of high call volume or local disruption.

Challenges of Moving to the Cloud

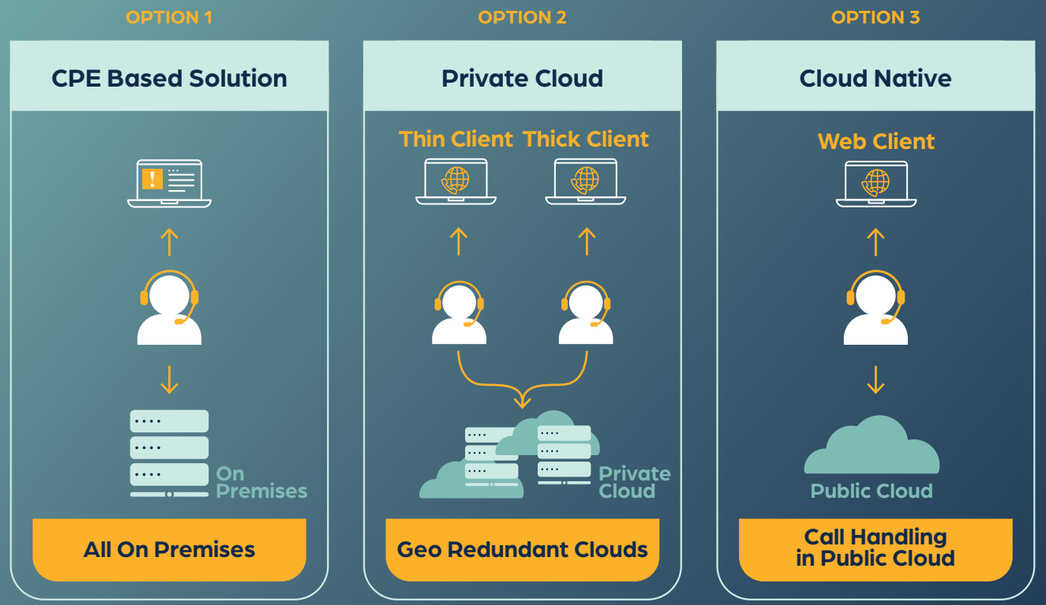
Transitioning to the cloud introduces new security challenges. Traditional, on-premises equipment often used air-gap firewalls to physically isolate critical systems — for example, CAD and CHE — from the internet, providing inherent protection from external cyber threats. Physical data security was maintained by restricting physical access.

Cloud migration and IP-based voice transport remove the protection offered by air-gap isolation, requiring PSAPs to implement comprehensive cybersecurity strategies, firewalls, managed detection and response systems (MDR), and strict operational practices to ensure data integrity and security.

As we said in the introduction, it really is a question of *when*, not *if*.

Cloud-Based Call Handling Strategy

Meeting PSAPs Where They Are in Their Cloud Journey



Artificial Intelligence in 9-1-1 Operations

Open the Pod Bay Doors, Hal

You may already know the story of AI, so please bear with us while we review some history and provide some context. Then we'll discuss how AI will transform 9-1-1.

AI is the field of computer science that builds systems that can simulate human intelligence to perform tasks such as learning, reasoning, problem-solving, perceiving, decision-making, and understanding language. It allows computers to do things that in the past could be done only by humans.

While the idea of intelligent machines dates back to ancient myths and philosophical speculation, modern AI began taking shape in the mid-20th Century. Mathematician Alan Turing posed the question, "Can machines think?" at the University of Manchester in 1950. The 1956 Dartmouth Conference, a summer workshop led by John McCarthy, Marvin Minsky, Allen Newell, and Herbert Simon, is widely considered to be the event that launched the field. These pioneering scientists believed that machines could replicate human intelligence using logic and symbols.

> The Turing Test, also known as the Imitation Game, is a thought experiment created by cryptologist and computer scientist Alan Turing in 1949, in which a human judge in one room interrogates a human and a computer in another room. If the judge cannot distinguish the computer's responses from the human's, the computer, by proving its intelligence, has passed the Turing Test. Modern large language models (LLMs), including ChatGPT, have passed the Turing Test.

Early AI research in the 1950s and 1960s produced programs that could solve algebra problems, play games like checkers and chess, and prove logical theorems. In the 1970s, however, the limitations of computing power and overly optimistic expectations led to setbacks known as "AI winters," during which funding and interest declined.

The development of expert systems in the 1980s revived AI, allowing computers to emulate decision-making in fields like medicine and engineering. In the 1990s and 2000s, machine learning became more prominent, emphasizing data-driven algorithms over hand-coded rules.

A breakthrough occurred in the 2010s with deep learning and neural networks. Using vast datasets and powerful graphics processing units (GPUs), AI systems began to surpass human performance in complex tasks. You might say that machine learning grew up to be AI. Notable milestones include IBM's Watson Deep QA computer defeating Jeopardy! champions Ken Jennings and Brad Rutter in 2011 and DeepMind's AlphaGo defeating the world champion in the game of Go in 2016.

In the 2020s, large language models (LLM) such as GPT-3 and GPT-4, part of a wave of generative AI, supported a leap forward. These models can generate human-like text, write code, compose music, and even create art. Generative AI has transformed how we interact with machines by enabling natural language interfaces and powerful creative tools. As this technology advances, society faces new opportunities and ethical challenges around authorship, misinformation, and the future of human-machine collaboration.

A Five-Level Framework of AI Capability

Some experts have categorized AI development into a five-level framework to help understand its increasing complexity and potential. We think it's a helpful reference and useful model to assess where current AI stands and where it could go next. Only the first two levels have manifested; both are relevant for 9-1-1 today:

Level 1: Reactive machines involve basic functionality with no memory or learning. These systems respond to specific inputs with programmed responses. A good example is IBM's Deep Blue, which could play chess but had no ability to learn or improve after a match.

Level 2: Limited memory is AI that learns from historical data and makes decisions based on it. Most modern AI systems fall into this category, including chatbots, image recognition systems, and autonomous vehicles.

Ongoing research into machine learning, neuroscience, and cognitive modeling will allow AI to evolve to three higher levels:

Level 3: Theory of mind is AI that understands emotions, beliefs, and social cues. This would allow machines to interact better with humans in personal and dynamic ways. It's still in the research phase, particularly with respect to human-AI empathy and cognitive modeling.

Level 4: Self-aware/sentient AI refers to machines that have "consciousness" and a sense of self. These machines would be able to understand their own internal states. At this point, self-aware AI is entirely theoretical and a major focus of philosophical, ethical, and scientific debate.

Level 5: Artificial Superintelligence (ASI) is AI that surpasses human intelligence across all fields. ASI would be capable of independent innovation, strategic thinking, and creativity beyond any human. It represents the pinnacle of AI and a potential existential risk if not carefully controlled. Think Cylons on Battlestar Galactica.

How Can AI Enhance 9-1-1?

AI has the potential to help PSAPs and 9-1-1 telecommunicators manage a complex operational environment and make the emergency response system even more efficient. AI can handle tasks in the background, manage data overload, and improve the speed of incident assessment — allowing 9-1-1 telecommunicators to focus on decision-making and reducing the financial burden of unnecessary dispatches.

As 9-1-1 systems evolve, think of AI as a force multiplier — informing human judgment, managing data overload, and improving service resilience, all while maintaining the speed, accuracy, and public trust on which emergency response depends. We aren't there yet, but we should all be in awe of how AI can and will improve public safety. Here are some examples.

Call Taking and Incident Entry

- **Real-time transcription:** AI instantly converts spoken words into text, allowing telecommunicators to focus on the conversation while AI creates a searchable log.
- **Speech-to-intent detection:** AI analyzes the caller's language and tone to identify key emergency details — for example, location, type of incident, and urgency.
- **Multilingual translation:** AI-powered translators can convert languages or dialects into English in real time, eliminating the delay of bringing translation services into the call; improving accessibility for non-English-speaking callers; and accelerating response times.
- **Triage initiation:** AI chatbots for text-to-9-1-1 can initiate triage during text conversations by asking structured questions and flagging high-risk situations for immediate attention.
- **Sentiment analysis:** AI can detect stress, panic, or aggression in a caller's voice, alerting telecommunicators to volatile situations or possible mental health crises.
- **Gesture recognition:** AI can analyze gestures in incident-related video to better evaluate the situation and potentially flag people who are intoxicated, injured, or in emotional distress.
- **Location analysis:** AI can look at multiple geodetic and civic locations for the caller — along with mapping and additional information, such as personally associated addresses — and provide additional insight to help the telecommunicator locate the caller.
- **TDoS detection:** AI can easily detect patterns of repeat, spoofed numbers or IP addresses, automated calls, and unusual spikes from individual carriers that may annoy or swamp 9-1-1 centers or ESInets.
- **Image detection and summarization:** AI can summarize images or video and notify the 9-1-1 telecommunicator of anything inappropriate or disturbing before it's displayed.

Dispatch and Resource Allocation

- **Automated call classification:** AI can categorize calls — burglary, fire, overdose — and recommend appropriate response protocols based on historical patterns and current context.
- **Predictive dispatching:** Using real-time and historical data, AI can forecast demand and recommend proactive unit placement to reduce response times.
- **Responder recommendation:** AI can suggest the best available units based on location, traffic, and equipment.
- **Dynamic routing optimization:** AI-based navigation systems factor in traffic, weather, and road closures to suggest the fastest and safest route for responders.

Field Response and Situational Awareness

- **Real-time video and image analysis:** AI can analyze live video from bodycams, drones, or bystanders to detect weapons, crowd size, or hazardous materials.
- **Voice assistant for responders:** Hands-free AI interfaces allow field personnel to access critical information — for example, building layouts and medical records — via voice queries.
- **Smart incident summarization:** Using structured and unstructured data, AI can auto-generate incident summaries to aid with post-incident reporting and analysis.

Detecting Swatting

AI can help detect swatting calls to 9-1-1 through a combination of pattern recognition, voice analysis, caller behavior modeling, and data correlation across systems. While no system can guarantee 100% accuracy, AI can significantly improve the odds of identifying and flagging potentially fraudulent or malicious calls in real time. Here's how:

Pattern recognition

AI systems trained on historical swatting incidents can learn the common features — for example, claims of extreme violence, hostage situations, or requests for large police responses — that later proved to be false.

Anomaly detection

Machine learning algorithms can detect outliers by comparing current call patterns to confirmed legitimate calls and swatting calls.

Voice and Language Analysis

- **Natural Language Processing (NLP)** can analyze the caller's speech for inconsistent or overly scripted language; lack of emotion or unusual stress patterns; and use of technical or third-person descriptions, e.g. "I heard gunshots" vs. "I'm being shot at."
- **Voice biometrics** can flag repeat offenders by comparing voice prints to previous swatting attempts.

Geolocation and Context Validation

AI can cross-reference the reported location with telegeospatial data from DBH, ALI, or NG9-1-1 location systems; known addresses tied to prior false reports; and unusual distance between the caller's number origin and the reported incident.

Call History and Device Fingerprinting

Using metadata analysis, AI can link spoofed numbers or VoIP endpoints to prior malicious calls, or automatically flag repeated use of anonymized or masked caller IDs across multiple jurisdictions.

Real-Time Alerting and Operator Support

Flagging of suspicious calls can occur in real time, giving supervisors a chance to assess and potentially verify before dispatch. AI-generated confidence scores guide telecommunicators about how urgently to treat a call without delaying legitimate response.

So What Are the Current Applications of AI in 9–1–1 Emergency Response?

The use of AI in 9-1-1 response is still new, but several applications that don't require the PSAP to have transitioned to NG9-1-1 are currently in use.

Transcription and summarization — real-time language and dialect translation

Triaging to redirect non-emergency calls

Identifying multiple calls about the same incident

In March 2026, the FCC's flagship advisory committee on security and reliability -- the Communications Security, Reliability, and Interoperability Council -- will consider a report and recommendations on the use of AI in public safety networks, including 9-1-1. We're participating in the development of the report and look forward to sharing more about it with you next year.

Public safety agencies should have clear, transparent guidelines governing AI usage, emphasizing both operational benefits and responsible deployment to maintain public trust and confidence.

Principles of Responsible AI

Before we move on, we should talk for a moment about principles of responsible AI, because it is still very new. Based on the work we have done at Intrado to develop AI for use at PSAPs, we speak from experience when we say that public safety agencies should have clear, transparent guidelines governing AI usage, emphasizing both operational benefits and responsible deployment to maintain public trust and confidence. Frankly, all organizations that are considering or already using AI should adopt such guidelines.

Here are some areas that deserve careful consideration as you consider deploying AI systems.

Data privacy:

Careful handling of sensitive data is paramount. Deploying self-hosted or private AI solutions via secure platforms (AWS, Azure, Google Cloud Platform) will ensure that data remains within controlled environments. Data encryption, both in transit and at rest, is essential. Public cloud application programming interfaces (API) should never handle sensitive or non-anonymized data.

Vendor compliance:

Agencies should regularly audit vendors to verify their compliance with data protection regulations such as HIPAA (Health Insurance Portability and Accountability Act) and CJIS (Criminal Justice Information Services).

Public perception:

Public safety agencies should proactively manage the internal perception of AI applications to avoid misconceptions around surveillance, predictive policing, or automated handling of emergency calls.

We'd also like to share some common principles we use when working with our developer teams on AI-powered products. As AI takes on more critical roles, especially in 9-1-1, we believe the public safety community will need assurance that AI has been trained using ethical and moral reasoning. This includes weighing competing values, assessing fairness, and considering societal impact when making decisions.

Below are the attributes we believe the public safety sector should look for when choosing AI providers.

Fairness: Avoid bias and discrimination in AI systems; ensure that outcomes are equitable; regularly test for and mitigate algorithmic bias.

Transparency: Make AI systems understandable and explainable; clearly communicate when users are interacting with AI; provide documentation on how AI models are trained and how decisions are made.

Privacy and security: Protect user data and ensure compliance with data protection regulations; implement strong cybersecurity practices regarding data and models; use data minimization and de-identification when possible.

Accountability: Assign clear responsibility for AI decisions and outcomes; maintain auditability logs and records that can track AI decisions; establish governance frameworks to monitor AI use.

Reliability and safety: Ensure AI systems function as intended across use cases; perform robust testing in realistic and edge-case scenarios; institute fail-safes or human override mechanisms in critical applications.

Inclusiveness/beneficial use: Engage a broad set of stakeholders, especially those impacted by AI; design AI to benefit society and avoid harmful or exploitative use.

You Can't Lick a Badger Twice and Other Hallucinations

As this is being written, there is a meme circulating the interwebs in which users feed nonsense idioms to an AI engine and ask what the idiom means. Instead of the expected "I'm sorry, Dave. I'm afraid I can't do that," some AI engines are instead making up reasonable sounding — but completely wrong — explanations and serving them to unsuspecting users with a straight face and no indication that it is wild guesswork.

For example: Someone tweaked Google Gemini to explain that "you can't lick a badger twice." Gemini explained that it means you can't fool someone twice after they've fallen for a trick once. Which makes sense — it sounds like a folksy, old-timey saying your great-grandmother might have used.

It is not. AI made it up.

Whether this is a feature or a hallucination, it highlights both the potential and risks of AI. We can't know what the future will bring, but we can confidently predict that, over time, more memes, scandals, problems, and gremlins will arise — and, we hope, be addressed.

What About Agentic AI?

Agentic AI refers to systems that can autonomously achieve goals without constant human guidance, using machine learning, natural language processing, and automation. Agentic AI differs from other flavors largely through a focus on making decisions; taking autonomous action; and having the ability to execute complex series of actions and interactions to achieve goals and complete activities.

Some areas you can expect to see agentic AI used to good effect in the PSAP include cybersecurity, call triage, and call-handling co-pilots. The promise of this technology is great.

A Word to All You PSAPs Out There

The script for AI in 9-1-1 is still being written. With that in mind — and without sounding too...well...preachy — we have some suggestions for how to help your team and community get the most out of AI as more applications are rolled out.

First and foremost, don't think of AI as a replacement for people — it isn't, and it shouldn't be. Think instead of how your team can use AI as a force multiplier to bring their experience and human judgement into play more quickly and effectively, and on more calls.

Consider all the myriad ways AI can shorten calls and accelerate time to dispatch. Language translation for both text and voice is a prime example. During a call surge, AI-powered geofencing and triage could help you more effectively deal with situations by confirming basic information, e.g. "Thank you for calling about the [vehicle fire] on [I-680 South] near [the Berryessa exit]. We are aware of [the vehicle fire] and have dispatched [a fire crew]. Thanks again for your help and support!"

What are some other possibilities? Can AI help you optimize staffing and shift schedules? What about quality assurance and training? Can call analysis, including full-text indexing, provide better examples of what "best in class" effort looks like? Can you use voice and pattern analysis to not only better handle a caller's emotional state, but also identify and head off burnout and wellness issues before they impact your team?

Most PSAPs have access to increasing amounts of data, but insights are harder to come by. Can AI help with some of the drudgework of sifting through gigabytes and gigabytes of call records, transcripts, and other data to identify insights and patterns that will help you more effectively lead your team or support your 9-1-1 telecommunicators and your community?

Training, education, and efforts to inform stakeholders are vital to the overall success of a technology upgrade or deployment. These considerations should be baked into your thinking around AI and your plans for implementation.

We thought for a long time about how to end this section of the report and decided to bring it full circle by reiterating something we said at the beginning: AI has the potential to help PSAPs and 9-1-1 telecommunicators manage a complex operational environment and infuse additional efficiency into the emergency response system.

It falls to us humans to unlock that potential in responsible, meaningful, and lifesaving ways.

PRO TIP:

Training, education, and efforts to inform stakeholders are vital to the overall success of a technology upgrade or deployment. These considerations should be baked into your thinking around AI and your plans for implementation.

(NOT) THE SAME AS IT EVER WAS:

THE EXPANDING 9–1–1 ECOSYSTEM

Now, let's discuss some of the emerging technologies that underlie new types of requests for assistance or ways of delivering those requests, which are bringing a wide range of new stakeholders into the 9-1-1 ecosystem. The proliferation of connected devices capable of initiating emergency calls represents significant technological evolution in public safety technology, with vehicle systems, smartwatches, and other Internet of Things (IoT) devices now able to automatically detect emergencies and contact 9-1-1 on behalf of users/wearers who may be incapacitated or unable to call for help themselves.

These technology advancements, however, have occurred largely without coordination with PSAPs, and this has created a disconnect between, on the one hand, the sophisticated capabilities of these devices and, on the other hand, the infrastructure designed to receive and process emergency communications and PSAP protocols to absorb fully the additional information. These devices have sophisticated capabilities that allow transmission of valuable data such as precise location information, health metrics, and crash detection alerts, but many PSAPs lack the technical infrastructure and standardized protocols necessary to effectively capture, interpret, and act upon this information, which potentially limits the lifesaving benefits these innovations were designed to provide. The gap highlights the critical need for better collaboration between device manufacturers and emergency services early in the development process to ensure that technological advances in emergency communication translate into improved response capabilities and outcomes for those in crisis.

This discussion of the larger 9-1-1 ecosystem also includes reimagining what a PSAP is or could be, along with identifying new ways to bring situational awareness to public safety. We will also touch on the relationship of 9-1-1 to private wireless networks and how to reach 9-1-1 as an international roamer in the U.S.

This is not intended to be a deep dive into these issues. We hope you take away from this discussion an understanding that the 9-1-1 ecosystem includes more players and more platforms interacting with each other in more ways than ever before — and how the industry/providers will manage some of the unanticipated consequences. If you're left with a lot of questions, you're in good company.

Requests for Assistance from IoT Devices

We'll illustrate this by focusing on three examples of new devices connecting to 9-1-1: vehicles, alarm systems, and panic buttons.

Vehicles

Connected Vehicle and Vehicle-to-Everything (V2X) initiatives are revolutionizing the automotive industry by enabling seamless communication between vehicles and public safety infrastructure, which has tremendous potential to further enhance safety. Automotive Original Equipment Manufacturers (OEMs) and Telematic Service Providers are integrating systems that collect crucial data from vehicles involved in crashes, including location, severity, and specifics of the incident, which can be swiftly transmitted to PSAPs and emergency responders. This evolution not only promises faster dispatch and better post-crash care, but also underscores the importance of improving public safety outcomes through technological advancements.

We focus here on Advanced Automatic Collision Notification (AACN), a telematics system that activates reactively after a vehicle crash to facilitate emergency response. As we noted earlier in this report, when car sensors detect a crash event, AACN automatically captures detailed data to transmit to a PSAP, including location, information about the vehicle make and model, crash severity, airbag deployment, impact direction, and particulars of the incident (whether it involves a crash, rollover, fire, or something else). OnStar introduced this technology nearly 30 years ago. Its use in the U.S. is growing, but not universal.

When a collision is detected, the AACN system sends an alert to a dedicated call center, where a call handler triages the event, calls the vehicle, and transmits the information to a PSAP electronically (if they support electronic delivery of AACN data) or verbally (if they do not).

Current AACN deployments are "over the top," meaning that they use proprietary PSAP displays and internet rather than dedicated emergency service networks and NG9-1-1 systems. Eventually, the goal is for AACN data to be delivered directly to the PSAP over NG9-1-1 networks.

NG9-1-1 will enable the delivery of the AACN data along with voice. The most common NG9-1-1 industry standard, NENA i3 (specifically, i3v3), incorporates Vehicle Emergency Data Sets (VEDS), which defines an XML framework for formatting and delivering data related to a collision. With NG9-1-1, VEDS arrives with the call setup, simplifying call handing and potentially accelerating dispatch of medical assistance, resulting in better outcomes.

We're not sure we need to say it, but the public safety benefits of AACN are clear. Annually, law enforcement reports over 6 million vehicle crashes, which underscores the utility of enhancing emergency response for vehicle collisions. Analysis from the National Highway Traffic Safety Administration (NHTSA) indicates that full implementation of AACN would likely reduce fatalities from vehicle incidents from 3.3% a year to approximately 1.6% (combining the benefits of trauma center care for severely injured patients with faster crash notification via AACN).

Currently, there are limitations to the use and effectiveness of AACN, including the lack of AACN capability in some vehicles; additional charges for AACN by some automakers; and the inability of some PSAPs to receive the data. AACN technology continues to advance and will likely become more widely available in the U.S. over the next year, in light of recent moves by major automakers to offer it at no extra cost. We still have a long way to go, though, to achieve full implementation in the U.S.

Things are different in Europe, where all new vehicles have been required since 2018 to include minimal crash notification data sets and service at no additional cost. Such a requirement has not yet been adopted in the U.S.

However, the European system (dubbed eCall) presents challenges to PSAPs. Under eCall, cars call 112 (Europe's 9-1-1) directly, when a passenger presses an SOS button inside the vehicle, or automatically, through vehicle sensors. This means calls are not routed through an intermediary call center that can triage and filter out false alarms. Approximately 40% of button presses and 5% of automatic calls are false alarms — which in turn dramatically raises false alarm traffic to PSAPs. This is an average; in some countries, it's even worse. In Greece, 78% of all eCall calls are false alarms. The European implementation presents a useful case study on potential pitfalls of implementing a similar system in the U.S.

Integration of AACN systems into Connected Vehicle and broader V2X and CV2X frameworks is a significant milestone in road safety and emergency response efficacy. As the automotive industry continues to innovate, the ability to collect and transmit detailed crash data to 9-1-1 will play a crucial role in saving lives and reducing fatalities. The anticipated widespread adoption of AACN technology in the United States, coupled with ongoing advancements in NG9-1-1 systems, will usher in a new era in public safety.

Don't be surprised if you see announcements later this year about car manufacturers and ESInets starting to support and deploy i3-compliant solutions for AACN. Just sayin'.

TRAFFIC COLLISIONS OVER TIME

Traffic Crash Victims, Fatalities

2010 to 2023

Traffic Safety Facts DOT/NHTSA
https://cdan.dot.gov/tsftables/tsfar.htm

Alarm Systems

Safehome.org estimates that 94 million households have some type of security system, with 66% using professional monitoring. Professionally monitored systems involve 24/7 oversight by trained personnel who can quickly respond to and evaluate alarms and relay the system/subscriber to a PSAP for emergency support, when necessary. Yet, out of approximately 14 million households that are considering installing an alarm system, only 7% would consider including professionally monitored services.

Why, you might ask? Because of smartphones and DIY security systems, such as those that are integrated with doorbells and other smart home applications. Increased smartphone access to security systems and a growing market for DIY alarm systems have significantly influenced market direction. According to Safehome.org, subscribers will likely opt for self-monitored or lower-cost solutions to avoid the expense of professional monitoring.

This is not without its challenges. When self-monitored systems trigger, it's harder to clearly convey the required level of response to a 9-1-1 telecommunicator or first responder.

One possible solution to this challenge is Alarm Validation Scoring (AVS-01), an alarm industry standard that helps determine: the severity of an alarm event; who should respond; what response is required; and how quickly the response should be executed. A consideration with AVS-01 is that, when a homeowner receives an alert from their smart security system, they are responsible for triaging; whereas professional monitoring centers obviously have more experience triaging emergency situations based on sensor activity and can do so before alerting the subscriber.

Currently, somewhere between 94% and 97% of automated burglar alarms are false, a disappointingly high number. The introduction of IoT networks and devices to 9-1-1 raises the question of whether to require human verification before responding to burglar and other types of alarms. Currently, some PSAPs require verification for certain types of alerts before responding, such as a phone call from someone on the premises or a neighbor. As the intelligence, self-verification, and real-world accuracy of these technologies improve, they may evolve to a point where an intermediate human verification step won't be necessary.

Some additional thoughts regarding self-monitoring alarm systems. If the subscriber is traveling or commuting when an alarm triggers, will they even know how to contact their home PSAP? Without the ability of these systems to natively express the AVS-01 score to the PSAP in the security system vertical, the subscriber will need to provide this information to the PSAP. How will they make that assessment? And wouldn't it be advantageous if the PSAP had access to or a summary of the sensor data? Hey, we're in the 9-1-1 business.

AVS-01 Alarm Level Definitions:

Alarm Level 0 No Call for Service

Alarm Level 1 Call for Service with limited to no additional information

Alarm Level 2 Call for Service with confirmed or 'highly probable' human presence with unknown intent

Alarm Level 3 Call for Service with confirmed threat to property

Alarm Level 4 Call for Service with confirmed threat to life

ANSI/TMA-AVS-01 2024 Alarm Validation Scoring Standard

Personal Emergency Response Systems (PERS) and Silent Panic Buttons/Alarms

Sometimes referred to as panic buttons, PERS have evolved quite a bit from the days of "I've Fallen, and I Can't Get Up®." Earlier versions of PERS connected to landlines and had limited mobility within short-range radio perimeters. Advances in cellular connectivity and battery technology have increased user mobility and freedom.

The design of PERS has also changed significantly. Previously, PERS were predominantly pendants worn around the neck. Now there are many more options, including mobile apps and watches that connect to 9-1-1. For example, Apple Watches have fall detection that can trigger a 9-1-1 call.

One issue remains with respect to integrating PERS with 9-1-1 and minimizing false alarms. Identifying key data, making it available, and integrating it into existing 9-1-1 workflows will be crucial for effective emergency response.

Let's talk for a moment about school safety. One of the fastest-growing uses of panic buttons is K-12 incident management solutions. The ALYSSA's Law movement promotes legislation to address emergency response times in schools through the installation of silent panic alarms that are directly linked to PSAPs. Typically, this solution includes panic buttons and/or a mobile phone app that allows school faculty to initiate security or lockdown procedures when they push the button. Strategically placed beacons attach location information to the panic button alert message. When the school administration's central software platform receives the message, it processes the information and sends it to the local PSAP, along with pre-loaded information regarding school safety procedures; the number of people on the campus that day; and anything else pertaining to emergency response.

These solutions are connecting schools to the 9-1-1 space in a new way. The ALYSSA's Law movement has resulted in new state laws (with similar legislation pending in some states and in Congress) requiring that K-12 schools provide silent panic buttons and/or a mobile app for teachers and faculty that connect directly to 9-1-1.

We are also seeing silent panic alarms/buttons required more broadly as a workplace safety measure. A growing number of states and localities require retail establishments, healthcare facilities, social work offices, and/or hospitality venues to give employees the ability to summon help quickly and silently. We talk more about this in the Regulation and Legislation section at the end of this Report.

Private Wireless Networks

Private wireless networks are expanding rapidly as an enterprise communication solution, particularly in industrial settings. These are dedicated telecommunications networks intended to serve a limited, defined area. They give enterprises greater control over their wireless infrastructure at their facilities, including better security, customized coverage, guaranteed bandwidth, and specific quality of service levels that might not be possible with public carrier networks or traditional Wi-Fi.

Many private 5G networks, however, may not fully support 9-1-1 service requirements, if owners and operators believe that the "private" label exempts them from complying with 9-1-1 rules. Depending on the network, this may be true. Some of these networks, however, operate both within and outside the enterprise and may allow users to call 9-1-1. This makes sense as these environments are often massive and involve operations and technologies with a high risk of physical injury, such as manufacturing or oil fields.

This leaves us wondering whether and under what circumstances the owners and operators of private networks would be obligated to comply with the FCC's 9-1-1 rules.

Non-Traditional PSAPs

Facilities such as universities, the Coast Guard, and other branches of the military have long managed their own public safety operations while relying on the local jurisdiction to answer 9-1-1 calls. These non-traditional settings are increasingly establishing their own PSAPs — receiving calls directly, dispatching emergency response, and maintaining a sanctioned security team to respond. As we discussed earlier, satellite services are changing the landscape of where 9-1-1 calls are being placed and, therefore, also where they might be answered.

International Roaming

This discussion is not technically about 9-1-1 calls from non-traditional devices, but rather about calls to 9-1-1 from devices that are roaming in the U.S. from other countries. Over the next several years, the U.S. will host several international sporting events that will draw visitors from around the globe. At the request of CISA, the Communications Sector Information Sharing and Analysis Center recently analyzed the ability of mobile devices from other countries to reach a PSAP in the U.S. Intrado was a key participant in these discussions, which we'd like to share with you now.

The first thing to know is that 3G/4G/5G mobile wireless devices that are properly provisioned in their home country and configured to operate in accordance with 3GPP (3rd Generation Partnership Project) specifications should be able to initiate an emergency call in the U.S. by dialing either a home-country emergency number, 9-1-1 or 112 (the primary emergency number in the European Union).

The mobile device itself identifies wireless calls made to emergency numbers, even those from other countries, as emergency calls. These calls are routed the same as 9-1-1 calls from a U.S. domestic device. The device does not pass the actual dialed digits; instead, it identifies the call as an emergency call to the servicing network as follows:

- **5G/4G networks:** Emergency calls flagged via SIP R-URI (Session Initiation Protocol Request-Uniform Resource Identifier).
- **2G/3G networks:** Emergency calls flagged via TS.12.

The specific numbers a device will identify and route as an emergency call (via the flags noted above) include:

- **9-1-1 and 112** — under 3GPP standards, both U.S. and European 3-digit codes are hard-coded as emergency numbers in all devices (i.e. U.S., European, and other devices).
- **Home network, country-unique emergency numbers** should be provisioned by the home country network carrier and loaded to the device/SIM card. For example, a device originally provisioned in a Brazilian network should identify all Brazilian emergency numbers (190 for police, 192 for EMS, and 193 for fire) as emergency numbers, in addition to the "hard-coded" 9-1-1 and 112. Therefore, a device originally provisioned in Brazil that is roaming in the U.S. would route any of those dialed digits as an emergency call on the servicing network.

This is all good news. However, challenges remain with callback, location data, and unregistered devices. These issues should be resolved as the industry continues to address international roamers calling 9-1-1.

Challenges with Callback

ANI may not display the entire international number, which affects callback ability. This is because, in the U.S., ANI allows only 10 digits. Longer numbers — for example, a telephone number with an international country code — may transmit incompletely, with only the first 10 digits displayed. The NG9-1-1 architecture should consider supporting the E.164 numbering scheme (a globally recognized standard for formatting international telephone numbers), in addition to the North American Numbering Plan to which it is currently limited. Typically, 9-1-1 calls in the U.S. that originate from numbers outside the U.S. don't display as "international" — therefore, the PSAP will not know that the call is from a non-U.S. device and that the callback number is an international number. This is true even if the callback number contains the entire country code and phone number of the caller.

Challenges with Location Data

ALI will likely function normally, but with caveats. Some non-U.S. devices may have licensing or privacy settings that preclude developing and/or sharing dispatchable location data. At a minimum, they would share cell tower location to support correct routing to a local PSAP. And even though some modern devices have multiple means of acquiring accurate location (e.g. GPS and Google's Emergency Location Service), we should not expect phones from non-U.S. carriers that are roaming in the U.S. to provide accurate location as often as calls from subscribers to U.S. carriers.

We should not expect phones from non-U.S. carriers that are roaming in the U.S. to provide accurate location as often as calls from subscribers to U.S. carriers.

Challenges with Unregistered Devices

Wireless networks will most likely treat devices that are in the U.S. but lack valid roaming agreements as Non-Service Initialized (NSI) devices. If these phones pick up a base station and are using a supported protocol — such as 4G — they should be able to make 9-1-1 calls just like a U.S. device would. Non-U.S.-provisioned devices may, however, have different radio frequency (RF) bands enabled or disabled, limiting access to the complete available U.S. spectrum and, therefore, having more limited RF connectivity to the servicing base.

Supporting international roamers is not a trivial task. The entire 9-1-1 network was originally designed to support only 10 digits. Supporting full international phone numbers could require changing the NGCS elements in the ESInet, in CHE and CAD equipment, and in downstream systems. This is important in light of the fact that the U.S. will host the FIFA World Cup in June 2026.

Additional Potential Failure Cases

While the majority of international visitors using a non-U.S. wireless phone should be able to reach a PSAP, there are some "edge" cases that could potentially fail.

- **Wi-Fi calling** — if Wi-Fi calling is selected on the device and an emergency call is initiated outside of wireless network coverage, all calls — including emergency calls — will route back to the home nation network for handling. Devices prefer cellular for emergency calls, even if normal voice service is over the Wi-Fi connection.

- **Texting** — to the extent that the home nation network supports texting at all, texts to emergency services would be routed to the home nation carrier. Satellite "SOS" texts should function normally (i.e. route to a U.S. PSAP); however, this is an option only if no terrestrial network is available.

- **U.S. SIM cards** — an international visitor who buys a U.S. SIM card for their non-U.S. phone, or who buys a U.S. device for use in the U.S., might not have their home country-unique emergency numbers stored on the device. Calls to the hard-coded 9-1-1 or 112 would still work, but calls dialed to any other home nation emergency number (e.g. 190, the emergency number to reach law enforcement in Brazil) might not.

- **Wireline calls** — U.S. wireline networks do not register non-U.S. emergency numbers as emergency calls. International visitors would need to know to dial 9-1-1 to get help if the only available phone is a landline.

CYBERSECURITY:

SECURING THE 9–1–1 ECOSYSTEM

The increasing digitization of emergency response systems has transformed the way 9–1–1 centers operate. Traditional analog systems, once considered relatively secure, are being phased out in favor of NG9–1–1 technology, which integrates VoIP, SMS, video, and real-time text communication.

These advancements come with significant security and efficiency benefits, but also new risks and vulnerabilities that drive the need for new, and better, approaches to cybersecurity. Growing security threats require more advanced cybersecurity protections.

Ensuring the cybersecurity of the 9–1–1 ecosystem is a hill we must climb faster.

We know we don't have to say it, but we will: Cyberattacks on emergency services can have devastating consequences — disrupting communication, hindering response efforts, and putting lives at risk. For instance, in March 2018, a ransomware attack rendered the CAD system of a major U.S. city inoperable for 17 hours, forcing telecommunicators to relay caller information manually. The next year, another ransomware attack targeted most of the same city's computer systems, causing significant disruptions and delays in service. Recovery took months and cost more than $18 million.

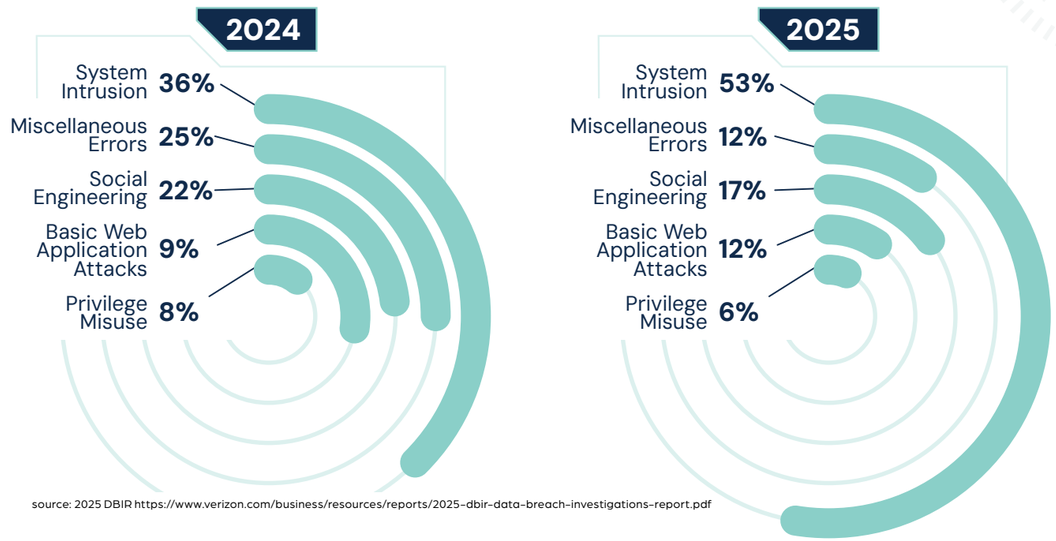
Eighty percent of PSAPs are small operations without the specialized staffing and resources of a major city. What does this mean for them, especially as the limited federal grants that were available may soon disappear?

We're in for Nasty Weather:

A Quick Look at Common Threats

Before we discuss what an effective PSAP cybersecurity strategy looks like, let's take a quick look at top exploits and current trends.

Cybersecurity Breach Types – 2024 vs 2025



source: 2025 DBIR https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Distributed Denial-of-Service (DDoS) and Telephony Denial-of-Service (TDoS) Attacks

Cybercriminals launch Distributed Denial-of-Service (DDoS) and TDoS attacks to overwhelm emergency call systems with excessive traffic, which prevents legitimate calls from getting through. These attacks can disrupt entire regions, as happened with a TDoS attack that impacted seven large counties and 21 public safety agencies in one state in August 2024.

It is an unfortunate fact that "DDoS-as-a-Service" is readily available on underground markets, allowing even relatively unskilled hackers to launch effective large-scale attacks. The barrier to entry is incredibly low. It took only minutes for us to find an actual menu of prices online to purchase a suite of DDoS attacks.

Attackers may use one or more of the following approaches to launch these attacks:

Botnets are networks of compromised devices, either created by the attacker or rented, used to generate large volumes of traffic.

NSI phones are mobile phones that have no carrier subscription or service plan; all NSIs, even those with no SIM card or disable SIMS, are required to be able to dial 9-1-1.

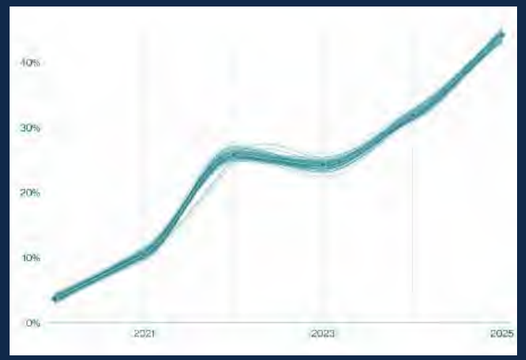
Compromised Private Branch Exchanges (PBX) — A business phone system, once compromised, can be used for telephony attacks.

VoIP systems, similar to PBXs, can be used for attacks.

Ransomware and Data Theft

As we just discussed, ransomware attacks have become a major threat to public safety agencies. Hackers infiltrate 9-1-1 networks, encrypt files, and demand payment to restore access. These attacks can cripple emergency call centers and leave dispatchers unable to coordinate response. Beyond operational disruptions, cybercriminals also target caller data — including medical information, home addresses, and personal details — that can be sold on the dark web or used for identity theft.

RANSOMWARE ACTION OVER TIME IN BREACHES



Verizon, 2025 Data Breach Investigations Report
www.verizon.com/business/resources/T4a8/reports/2025-dbir-data-breach-investigations-report.pdf

According to data published in Verizon's 2025 Data Breach Investigation Report, while the number of ransomware attacks is increasing, the median ransom payout is trending downward: $115,000 in 2024, down from $150,000 in 2023. Of particular concern for PSAPs: the average size of targeted organizations is getting smaller.

Victims always ask if they should pay the ransom. The FBI advises against it, for a couple of reasons. First, payment does not guarantee the safe return of your data; and second, payment does guarantee that you are incentivizing criminals and their bad actions. In case you're wondering, organizations are increasingly refusing to pay the ransom. None of these risks are unique to public safety, but the potential impact to public safety could threaten lives.

Social Engineering and Insider Risks

Even when organizations institute strong cybersecurity measures, they are still vulnerable to breach as a result of human error. Attackers frequently use phishing emails, fraudulent IT requests, or impersonation tactics to trick employees into granting access to critical systems. Weak passwords, shared credentials, and a lack of cybersecurity awareness further increase the risk of insider-related breaches.

Unsecured Data and Privacy Risks

With NG9-1-1 systems transmitting sensitive voice, text, and video data over the internet, encryption is essential. Without proper security measures, cybercriminals and unauthorized third parties can intercept communications and expose private information. As more states enact and enforce data protection laws, emergency response agencies risk legal and financial consequences when caller information is compromised.

Shields Up! How PSAPs Can Strengthen Their Cyber Defenses

To counteract these very real threats, PSAPs need to adopt a comprehensive cybersecurity framework or policy. Whatever you call it, you need a plan that covers physical security; program leadership; risk mitigation and incident management; network defenses; data encryption; security audits; employee training; and more. These will help you build a robust and adaptive cybersecurity program and create a culture of security.

That said, the PSAP community does not yet have a widely adopted certification program for cybersecurity excellence — but there are many resources and case studies that coalesce around critical actions. We're drawing from our own knowledge and incorporating common themes from CISA, the National Institute for Standards and Technology (NIST), the National 911 Program at the National Highway Transportation Safety Administration (NHTSA), NENA, APCO, and the FCC's Task Force on Optimal PSAP Architecture.

Within each of these themes, PSAPs have deployment decisions to make, potentially resulting in a nationwide patchwork of cyber defenses for 9-1-1. This is a concern because non-standard deployments across the PSAP community will result in the need for a wider range of controls and introduce more types of attack surfaces. While every PSAP is unique, driving toward greater standardization of cyber defenses across the 9-1-1 ecosystem will benefit everyone.

Key elements of an effective cybersecurity strategy include:

Physical Security

We know what you're thinking, but there is plenty that you can do now at little to no cost, regardless of the size of your agency.

Of course, physical security involves procedures and technologies to protect a facility from unauthorized access, intrusion, or damage. When it comes to cybersecurity, this extends to eliminating opportunities for unauthorized access to systems, especially computer ports. It means establishing internet usage policies. Look for vendors and consultants whom you trust and with whom you anticipate building a long-lasting relationship. This will serve you better than hiring ad hoc for transactional projects.

PRO TIP: Federal agencies such as CISA, NIST, and NHTSA have a wealth of resources available about securing emergency response systems, which are designed to help public safety agencies protect their networks and data from cyber threats. CISA also provides cyber risk assessment technical assistance.

Use MFA and Access Controls

Implementing basic cyber hygiene measures like multi-factor authentication (MFA) has a significant positive impact on security. Requiring employees to verify their identity with multiple authentication methods — such as passwords combined with biometrics or security tokens — adds an extra layer of defense. Role-based access controls further reduce risk by ensuring staff members have access only to the data and systems necessary for their specific job functions.

Have a Disaster Recovery Plan, Train on It, and Conduct Preparedness Exercises

Even the most advanced security systems can't compensate for a workforce that lacks cybersecurity awareness. Routine training sessions help employees recognize phishing scams, suspicious links, and other social engineering tactics. In the same way that incident management drills test employee preparedness, simulated cyberattack exercises can test readiness and improve response strategies.

Perform Regular Security Audits and Compliance Checks

Frequent audits help identify vulnerabilities before they are exploited. Adhering to cybersecurity guidance and best practices set by organizations like NIST and CISA ensure that 9-1-1 centers are adopting best practices for protecting their networks. We don't have any inside information on this, but suffice it to say that cybersecurity audits are being built into some regulatory models. The best example is the Cybersecurity Maturity Model Certification, which is required to do business with the U.S. Department of Defense.

Adopt a Zero Trust Security Model

Traditional IT network security can be described as a hard, crunchy shell with a soft, chewy inside. Once upon a time, firewalls and other equipment were sufficient to protect the internal network. But firewalls can be breached, letting bad actors run wild in an environment where everyone is trusted everywhere.

Instead of assuming that users and devices within the network are trustworthy, Zero Trust requires continuous verification for everything and everyone trying to access network resources. By restricting permissions and monitoring real-time activity, this approach minimizes the risk of unauthorized entry and mitigates damage in the event of a breach.

What is Zero Trust?
Zero Trust is a cybersecurity approach that requires constant verification for every access request, instead of trusting users and devices simply because they are inside a network. It operates on the principle of "never trust, always verify." This means every user, device, and application must be authenticated and authorized before accessing any resource, regardless of their location or previous trust level.

Use AI-Powered Threat Detection

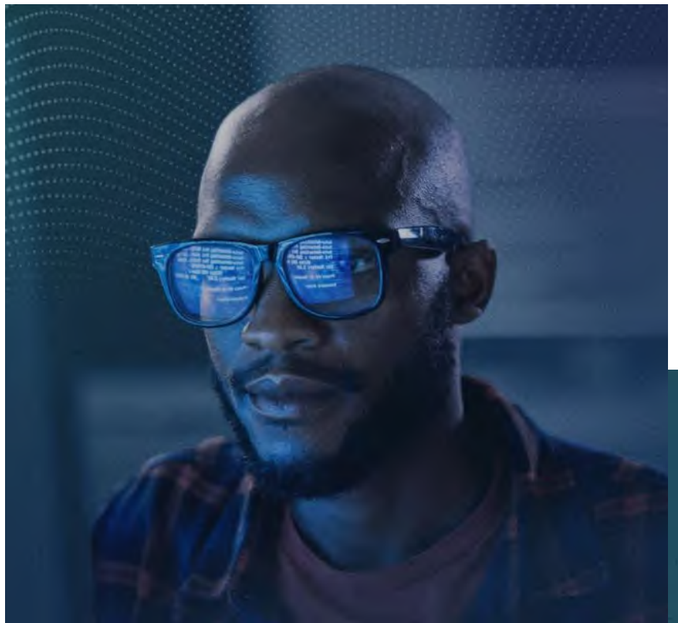
AI and machine learning (AI/ML) can analyze network activity to identify unusual traffic patterns and potential threats before they cause damage. AI-driven security systems can detect early signs of ransomware infections, unauthorized access attempts, and even insider threats, allowing agencies to respond proactively.

Deploy End-to-End Encryption

Encrypting all voice, text, and video transmissions ensures that, if a breach occurs, the data remains unreadable to unauthorized parties. Strong encryption protocols protect against data theft and help agencies comply with evolving privacy regulations.

Segment Critical Networks and Eliminate Single Points of Failure

Segmenting networks, which is to say separating emergency call systems from other government or administrative networks, prevents cyberattacks from spreading across critical infrastructure. Having redundant systems in place also eliminates single points of failure and ensures continuity of operations. Eliminating single points of failure where you can is one of the best things you can do to help ensure uptime in your PSAP. Is your call-handling system georedundant? Do your cloud systems support local survivability? You have an uninterruptable power supply, right? When did you last test it? How about backups? Everyone runs backups, but when was the last time you tried a restore?



What PSAPs Need to Know About the Future of Cybersecurity

Here are some key trends shaping the future of public safety cybersecurity.

Threat Intelligence Sharing

PSAPs can't operate as islands anymore. Public safety agencies are starting to collaborate with state and federal cybersecurity organizations to share real-time threat data and improve response strategies. Federal agencies like CISA and DHS are advocating for more coordinated threat-sharing across local, state, and national levels. Real-time intelligence on attack patterns and emerging threats will become a cornerstone of defense, but it requires active participation.

How to prepare:

- **Join a threat-sharing network** such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), run under the auspices of CISA. If available consider joining an Emergency Communications Cybersecurity Center (EC3), which is a regional cybersecurity collaboration for threat detection across multiple PSAPs. Participate in CISA's Cyber Resilient 9-1-1 program.
- **Appoint a cybersecurity lead** to stay in sync with federal and regional partners.
- **Set up systems that can quickly process** external threat feeds and alerts.

Regulatory Oversight

We've mentioned that an increasing number of states are enacting state-specific privacy and data protection laws. Application of these laws regarding public safety and PSAPs varies from state to state, as does enforcement. This report does not include a nationwide, 56-jurisdiction survey; we encourage you to familiarize yourself with which laws impact you and how.

At the federal level, frameworks like the NIST Cybersecurity Framework 2.0 and CISA guidelines are instructive but not mandatory. There are no fines or penalties for non-compliance, unlike other sectors — for example, PCI DSS (Payment Card Industry Data Security Standard) or HIPAA. Cyber incident reporting is on the horizon, perhaps as early as 2026, that may impact public safety agencies.

A notable exception of current security obligations: PSAPs that access the FBI's Criminal Justice Information Services (CJIS) must comply with the CJIS Security Policy to ensure the integrity and security of FBI databases, motor vehicle records, and other proprietary government data essential to the effective operation and trustworthiness of public safety operations. This includes elements like mandatory training for personnel, background checks, rigorous authentication protocols, and periodic FBI audits.

In the best of all possible worlds, regulatory obligations would focus on network protection and risk mitigation rather than post hoc reporting of incidents, which doesn't impact 9-1-1 system uptime or the overall safety of the community. And one more thing: Even if cybersecurity risk mitigation practices were mandatory, don't confuse compliance with security.

How to prepare:

- Conduct regular compliance reviews and identify weak spots.
- Assign a team or officer to track policy changes and ensure adherence.
- Align day-to-day practices with evolving standards now, not later.

Cloud Security Enhancements

As more 9-1-1 centers transition to cloud-based NG9-1-1 platforms, new approaches to security are critical for preventing unauthorized access. Old approaches like air-gapping systems may no longer be effective. While cloud solutions offer scalability and uptime, they also introduce new security challenges, especially around access control and data protection.

How to prepare:

- Vet all cloud vendors for compliance with public safety and Zero Trust requirements.
- Use advanced access controls, encryption, and monitoring tools.
- Tailor your incident response plan for cloud-based systems.

Vendors Can Be the Attack Vector

Threat actors are targeting supply chains, especially third-party vendors with access to PSAP systems and data. Your cybersecurity posture is only as strong as your weakest partner.

How to prepare:

- Regularly assess all vendors for cyber risk.
- Require third parties to provide security audits like SOC 2 or the equivalent.
- Include cybersecurity requirements in contracts.

Quantum Computing and Data Encryption

We want to leave you thinking about the impact of quantum computing. Encryption plays a critical role in protecting data at rest and data in motion. By converting sensitive information into unreadable code, encryption ensures that even if data is intercepted, it cannot be deciphered without the appropriate decryption key. Emergency communications commonly use Advanced Encryption Standards (AES) and Public Key Infrastructure (PKI) to secure data. However, advances in quantum computing are on the horizon that will effectively nullify current encryption standards.

NIST has been developing quantum-resistant cryptographic algorithms through the Post-Quantum Cryptography (PQC) standardization process, something they kicked off in 2016. This may sound space age-y, but we need to start thinking now about moving the entire 9-1-1 ecosystem to PQC in preparation for the inevitable use of quantum computing.

How to prepare:

- Take inventory of encryption methods currently used in your NG9-1-1 infrastructure.
- Follow NIST's ongoing recommendations for post-quantum cryptography.
- Work with capable IT/cybersecurity vendors and consultants to phase in quantum-safe solutions.

Charles Gifford,
Intrado CISO

"As the 9-1-1 ecosystem continues to grow and become increasingly interconnected, we must all share the responsibility of securing it."

A consistent theme throughout this Report has been how the modernization and evolution of 9-1-1 systems brings advanced capabilities, while also changing how those systems are managed and used, and how they interact with each other. Cybersecurity is no exception. New systems and approaches come with new, and different, cybersecurity risks.

As attackers become more sophisticated, a proactive, multi-layered defense strategy will be essential to ensuring that 9-1-1 systems remain reliable, resilient, and secure. We should view cybersecurity as an ecosystem, with interconnected layers of protection and proactive measures that allow for a comprehensive approach to safeguarding sensitive information and delivering service without interruption. This is a journey, not a destination.

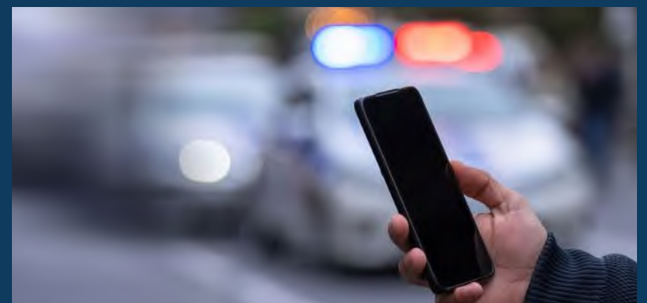
IMPACT OF REGULATION AND LEGISLATION

Federal regulation — specifically, FCC regulation — plays a central role in advancing 9-1-1, and the FCC has been active on 9-1-1 issues over the last several years to an unprecedented level. Public safety initiatives are generally less controversial than, say, the Universal Service Fund, or robocalls, or broadband mapping. There is often bipartisan agreement among the FCC commissioners on the broad outlines of regulating 9-1-1 services and reliability. Public safety policy, especially regarding 9-1-1, moves forward even during contentious political times.

A word about the states. Clearly, states and localities have the authority to regulate public safety and 9-1-1 services in their jurisdiction. States and localities also have primary responsibility for 9-1-1 systems and operations, and most operational funding and governance happens at the state and/or local level. This gives states significant influence over how emergency communications systems operate within their borders.

On the other hand, Congress has given the FCC broad authority to adopt 9-1-1 policies to establish baseline availability and reliability requirements, and that's what we're focusing on here. This bifurcated approach to 9-1-1 regulation allows states to tailor systems to their specific needs, but it also creates challenges for nationwide standardization and technological advancement. This is becoming more of an issue with the transition to NG9-1-1 and the subsequent emergence of new capabilities.

For the most part, recent FCC actions will dramatically improve 9-1-1 availability and performance. We discussed several policy actions taken over the last couple of years in detail earlier in this report; here we direct your attention to the regulatory posture.



9–1–1 HAS EVOLVED WITH TECHNOLOGY, DRIVEN BY LAW AND REGULATION

1996
ENHANCED 9–1–1 FOR EMERGENCY CALLING SYSTEMS

First FCC order adopting rules for Enhanced 9–1–1.

1999
WIRELESS COMMUNICATIONS AND PUBLIC SAFETY ACT (9-1-1 ACT)

Established 9-1-1 as the universal emergency number and mandated wireless enhanced 9-1-1 service with ANI and ALI. FCC implementing rules followed in 2000 and imposed accuracy standards for wireless 9-1-1 calls.

2004
USDOT NEXT-GEN INITIATIVE

Established first NG9-1-1 model based on IP-based infrastructure.

2008
NET 9-1-1 IMPROVEMENT ACT

Enacted to facilitate IP-enabled 9-1-1 and E9-1-1 services, improve 9-1-1 and E9-1-1 access to those with disabilities, required VoIP services to offer 9-1-1 service to their subscribers. FCC implementing rules followed in 2008.

2012
WIRELESS E9-1-1 LOCATION ACCURACY

Standards strengthened.

2012
NEXT GENERATION 9-1-1 ADVANCEMENT ACT

Committed U.S. to an interconnected public safety broadband network interconnected with NG9-1-1, and initiated reporting on state use of 9-1-1 fees.

2013
9-1-1 RELIABILITY

9-1-1 Reliability rules require providers to maintain 9-1-1 circuit diversity, backup, and network monitoring.

2014
TEXT-TO-9-1-1

Text-to-9-1-1 support required of CMRS and interconnected text messaging providers.

2018
KARI'S LAW & RAY BAUM'S ACT

Kari's Law requires direct dial access to 9-1-1 and RAY BAUM's Act requires all owners and operators of MLTS to ensure that 9–1–1 calls convey dispatchable location. FCC implementing rules followed in 2019.

2020
Z-AXIS (VERTICAL) LOCATION REQUIREMENTS

Required CMRS providers to add z-axis coordinates or dispatchable technology in major markets.

2022
9-1-1 RELIABILITY/ PSAP OUTAGE NOTIFICATION

Outage notification rules extended to more providers and tightened.

2024 (January)
LOCATION BASED ROUTING

Rules reduce misrouted wireless 9-1-1 calls.

2024 (March)
SUPPLEMENTAL COVERAGE FROM SPACE

Adopted with interim rule for 9-1-1.

2024 (July)
NG9-1-1 TRANSITION ORDER

NG9-1-1 Transition Order creates nationwide framework to advance NG9-1-1.

NG9–1–1 Transition Order

This FCC action, which is accelerating NG9–1–1 deployment, is in our view the most significant 9–1–1 regulatory action in over a decade. To give you some perspective, Intrado wrote our first business case for NG9–1–1 25 years ago and started working on NG9–1–1 in the mid–2000s.

Progress in public safety can move slowly for several reasons: the need to identify funding and develop standards; the slow pace of policy adoption; and the need to exercise due caution when public safety is at stake.

NG9–1–1 has been no exception. There clearly had been a significant amount of NG9–1–1 deployment before the FCC issued a framework, but reaching end–to–end NG9–1–1 in the U.S. — including fulfilling the industry's vision of replacing antiquated legacy infrastructure — was not going to happen without the FCC establishing some ground rules.

The FCC adopted the framework in July 2024, and OSP compliance with a "9–1–1 Authority" request for NG9–1–1 service is now required. OSPs are responsible for the cost of bringing traffic in IP to an in–state "NG9–1–1 delivery point," which is what we call the point of interconnection. PSAPs bear the cost of bringing traffic from the point of interconnection to the PSAP. (We discussed the framework in more detail in the NG9–1–1 section.) The FCC did not address funding for state/local deployments, as it does not have funding to dole out. That remains, for the time being, the states' responsibility.

While the overall framework addressed most issues, some are beginning to emerge that require resolution. Much of this can be addressed by speaking directly with the very able FCC staff who prepared the framework. As the process gathers steam, it's possible that, at some point, one or more issues will arise that require more formal clarification. Some could be addressed in the new rulemaking on NG9–1–1 Reliability that the FCC recently initiated.

Supplemental Coverage from Space

SCS is a technological development equivalent to NG9-1-1. Correction: it's bigger. In fact, SCS is a Holy Grail moment. Providers and technologists have long searched for ways to bring ubiquitous coverage to un/underserved locations across the globe using every day, off-the-shelf smartphones. SCS will help achieve that goal.

To refresh your memory, the impact of SCS on emergency response is twofold: PSAPs will be able to receive calls from new, possibly remote, locations, and emergency responders will be able to receive information from 9-1-1 callers in remote areas more quickly and with better location data, which could significantly improve search and rescue abilities.

Without going too far down the rabbit hole, enabling SCS had a lot of moving parts from a regulatory standpoint. Doing so required the FCC to create connective tissue between satellite and mobile wireless regulatory schemes.

The FCC's March 2024 order adopting rules for SCS laid out three key actions. First, the satellite operator must apply to modify its space station license(s) to allow operation on terrestrial frequencies. Then the satellite and the CMRS provider must file a lease application whereby the satellite provider leases spectrum from the terrestrial wireless provider. Finally, the wireless provider must apply for a blanket earth station license covering all its terrestrial devices that will be transmitting or receiving from the Earth station. The whole process is subject to public comment before the FCC will grant authority for the providers to offer the service.

The most significant issue with these application/lease packages is not 9-1-1, but rather the potential for satellite operations over terrestrial license frequencies to interfere with other satellite operations. As we see it, this is the primary reason it took as long as it did for the FCC to approve the first package of SCS authorizations, which was for the SpaceX/T-Mobile venture. Interference potential continues to be debated at the FCC because at least one satellite operator claims the interference would harm their operations.

With respect to 9-1-1 over SCS, the March 2024 FCC order adopting an SCS scheme included an interim rule for 9-1-1 over SCS requiring requests for assistance from 9-1-1 to be routed to a text-enabled PSAP (based on location available from the handset) or to a nationwide call center, such as Intrado's ECRC. The decision to adopt a permanent rule for 9-1-1 over SCS is pending. Satellite and CMRS providers agree that it's too early to make any changes because the service is in its infancy, and many deployment decisions that could affect how 9-1-1 is delivered have not yet been made. So far, this view is winning the day. We are comfortable saying, with a healthy dose of caution, that the FCC does not appear to be in a rush to make final decisions on this matter any time soon.

Location-Based Routing

This is a case where commercial usage truly drove the regulation, as opposed to the regulation driving commercial usage. By the time the FCC issued its January 2024 order requiring wireless providers to deploy LBR, the three major wireless providers had already initiated — or had plans to initiate — LBR. The deadline for them to deploy LBR has passed; non-nationwide providers are obligated to implement LBR by May 2026.

By using device location to route calls, as opposed to cell tower location, LBR reduces response times and incidents of misrouted 9-1-1 calls. This idea is not new; in fact, Intrado started building LBR into our systems 15 years ago. The evolution of the smartphone made this possible. The public safety sector voiced its support to the FCC; nationwide wireless providers were already headed down that path.

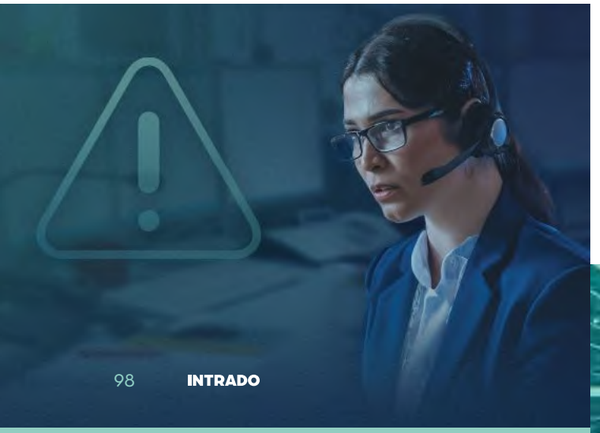
PSAP Outage Notification

This is the yin and yang of recent 9-1-1-related regulation. Public safety entities told the FCC that the outage notification regime was not serving them well, prompting the FCC to re-examine those rules. Public safety's concerns were that they were not receiving timely notifications, and the notifications they did receive did not provide actionable information. OSPs argued vociferously against three specific proposed changes:

- Changing the "as soon as possible" standard to a specific time clock;
- Turning every service outage into a 9-1-1 outage that required notifying PSAPs;
- And requiring every provider to maintain a PSAP contact list, as opposed to requiring the FCC to create one.

What emerged is a rubric that nobody likes.

In November 2022, the FCC updated its rules regarding how and when PSAPs are notified of outages. The new rule tightens the time frame for notifying PSAPs of outages that "potentially affect them" and applies to both "covered 9-1-1 service providers" (C9-1-1SP) and OSPs, including MSS operators.



C9-1-1SPs and OSPs must notify OSPs "as soon as possible, but no later than 30 minutes" after an outage becomes reportable, along with the "best known cause." Any additional material information must be relayed as it become available, but no later than two hours after the initial notification. OSPs may make "alternative arrangements" with PSAPs, which might ease the burden for either OSPs or PSAPs — but with 5,700+ PSAPs nationwide, such arrangements might be unwieldy to execute.

In addition, C9-1-1SPs and OSPs are required to use "special diligence" to "obtain and maintain up-to-date contact information for the 9-1-1 special facilities [PSAPs] in their service area to ensure that every potentially affected 9-1-1 special facility can receive notice about outages that potentially affect them." The FCC declined to articulate what "special diligence" means (beyond citing a law dictionary), but did say that PSAPs must verify contacts at least annually and "actively seek" to confirm the information, including escalating within the PSAP or to the state 9-1-1 Authority, if necessary.

It is not an understatement to say that the OSPs spent millions of dollars to comply with these rules, which they have included on a list of rules they would like to see the FCC delete, delete, delete (or, at least, revise, revise, revise). Meanwhile, PSAPs began complaining about the significant increase in outage notifications and the low level of detail included in the initial notifications, even before OSP compliance was required on April 15, 2025. Early in 2025, NENA, NASNA, and APCO jointly filed a concept paper with the FCC suggesting that there should be a dashboard for all of this; that PSAP participation should be voluntary; and that providers should pay for it. Yin and yang.

9–1–1 for Enterprises with Multi-Line Telephone Systems (MLTS)

Actually, this deserves attention because of inaction —on the part of entities that are not complying with the rules and, in our humble opinion, inaction from the FCC.

Kari's Law and RAY BAUM'S Act are statutes that create obligations for entities to ensure that any multi-line telephone system permits direct dialing of 9-1-1 without a prefix or area code; conveys "dispatchable" location information, including where to locate the caller within the building; and ensures that someone associated with the entity is aware that a 9-1-1 call has been placed.

These obligations apply to just about every type of entity — business, government, school, nonprofits — that owns or leases an MLTS. Both laws are forward-looking, but there are circumstances where older systems or equipment are obligated to comply and not "grandfathered."

The FCC adopted rules in 2019 to implement these two laws. The rules are complicated, especially for entities that are not used to parsing FCC rules, and the compliance timeline has several milestones. Suffice it to say that full compliance has been required since January 2022.

It's notably unusual for the FCC to be in a position of adopting and enforcing rules that apply to such a broad swath of both the private and public sectors. The FCC is monitoring compliance through its complaint processes. Kari's Law provides for fines of up to $10,000 per day for non-compliance; RAY BAUM'S Act includes fines of up to $10,000, with $500 for each additional day of non-compliance. Beyond monetary forfeiture, enforcement actions from the FCC often involve measures to ensure that 9-1-1 is available and reliable to anyone using the entity's MLTS system.

Based on what we see out in the wild, compliance levels are low. Our research covering several sectors shows that just over 60% of entities that should be complying with Kari's Law and RAY BAUM's Act believe — or at least kind of think — that they are already doing so. A surprising number do not plan to comply until forced. To date, however, the FCC has not announced any actions to enforce compliance with these rules.

Hence our statement about inaction — which won't be news to anyone at the FCC who might read this. In fact, we've suggested that providing an advisory statement or clarification of these (confusing) rules might go a long way toward improving 9-1-1.

The possibility of low compliance levels has the attention of Congress, at least insofar as several House and Senate bills over the last few years have included a call for an FCC Inspector General report on compliance with Kari's Law and RAY BAUM'S Act. It's hard to predict whether those bills might become law at this particular moment in our nation's history.

It may come as a surprise, or maybe not, that even in a highly deregulatory environment, there are new regulatory proposals on the table at the FCC that will impact 9-1-1. Remember what we said earlier about public safety being a high priority where bipartisan consensus is achievable.

NG9-1-1 Reliability

Hot on the heels of the NG9-1-1 Transition Order, the FCC has proposed rules on NG9-1-1 reliability, saying "NG9-1-1 networks must safeguard the reliability of critical components and support the interoperability needed to seamlessly transfer 9-1-1 calls and data from one network to another." The FCC considers this the next step toward fulfilling its commitment to facilitate the NG9-1-1 transition and avoid inadvertent vulnerabilities in critical public safety networks.

To account for the transition from legacy 9-1-1 to NG9-1-1, the FCC proposes to modify the definition of "covered 9-1-1 service provider" to specify certain NG9-1-1 capabilities as "functional equivalents" of NG9-1-1 elements; modify what "direct service" to a PSAP or other answering point means; and add five new NG9-1-1 CSP categories to "cover both the expanding network gap between OSPs and state and local governments and the increasingly interstate and interlinked nature of NG9-1-1 facilities."

If these proposals become rules, the scope of 9-1-1 regulation would expand to include many entities that have not been regulated in the 9-1-1 space before.

An additional highlight of these proposals would modify the decade-old 9-1-1 reliability certification process in an attempt to improve reliability and interoperability and to minimize burdens on service providers. This is juxtaposed with a proposal to permit 9-1-1 Authorities to obtain reliability and interoperability certifications directly from NGCSPs, so they can more easily access information to assess reliability and interoperability.

Public record development on these proposals will begin after the FCC publishes the document in the Federal Register, which could happen any day (and may well have happened by the time you're reading this). In our opinion, the most likely scenario is that the bulk of the record will be submitted by Labor Day 2025. It's tricky to forecast when the FCC might act. We're hoping they give the NG9-1-1 process adopted in the 2024 Transition Order a little time to percolate before taking action to adopt reliability and interoperability rules.

Location Accuracy

It is no surprise that FCC Chairman Brendan Carr has started a review of the location accuracy rules. He signaled his desire to revisit these rules in several speeches before he became chairman. The underlying goal of these proposals is to make location information more valuable and actionable for PSAPs and emergency responders. Their focus of the proposals is to strengthen the vertical location/z-axis accuracy requirements by requiring CMRS providers to deliver vertical location information to PSAPs in more actionable formats and to increase the number of wireless 9-1-1 calls that include dispatchable location information (as opposed to coordinate-based information).

Remember the ellipsoid we mentioned in the section on location technologies? The FCC's proposals would change location accuracy rules to rely on "height above ground level" rather than "height above ellipsoid." There are some challenges with this, and we think it's a step backward. We'll say more about this in the public record of the rulemaking.

The FCC is also reviewing how to improve horizontal location information and location accuracy for text-to-9-1-1, along with tweaking reporting requirements and cleaning up the location accuracy rules to eliminate those that are obsolete. Again, hard to predict the timing of the FCC's consideration of final rules. Our Spidey Sense is that the FCC is unlikely to act by the end of 2025, but perhaps not long after that.

Cyber Incident Reporting

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 instructs CISA to adopt rules for cyber incident reporting (both network-affecting incidents and paid ransoms) from entities in 16 critical sectors, including the communications sector, by September 2025. The proposals that emerged from CISA mid-2024 were largely panned by the industry as overly burdensome, not focusing on the right things, and not in harmony with cyber reporting obligations already in place from other agencies. We mention this here because the final rules, whenever they are adopted, may affect a number of entities in the 9-1-1 space, including state entities and perhaps even PSAPs. We can't predict what the final rules will look like and when they might be issued, except to say that if they are issued by late 2025, reporting obligations could start in 2026.

Legislation

Both federal and state legislation factor prominently in enhancing 9-1-1 availability. We wish we could point to federal legislation to fund the rest of the NG9-1-1 transition, but again, our sense is that legislators need updated cost estimates for the transition before a funding path can be identified.

This is not to say that there is nothing on the table with respect to 9-1-1. Here are some of the bills we're watching closely:

9-1-1 SAVES Act
(H.R. 637) (Federal)

It makes sense to start with the 9-1-1 Supporting Accurate Views of Emergency Services Act of 2025, which we referenced in the Industry Overview. This bipartisan legislation was introduced in January 2025 by Rep. Norma Torres (D-CA) — the only former 9-1-1 telecommunicator in Congress — and Rep. Brian Fitzpatrick (R-PA). It's intended to improve the life of 9-1-1 telecommunicators by requiring the Office of Management and Budget to reclassify them as "Protective Services Occupations," as opposed to the current "Office and Administrative Support Occupations." This would more accurately reflect the direct response and lifesaving role that 9-1-1 telecommunicators play in emergency services and, among other things, lead to increased salaries, access to more advanced training, and additional health services, including mental health. There is tremendous support for this change from key public safety organizations. The bill is under consideration in the House Education & the Workforce Committee.

Enhancing First Response Act
(S. 725) (Federal)

Also bipartisan, the Enhancing First Response Act was introduced in February 2025 by Senators Amy Klobuchar (D-MN) and Marsha Blackburn (R-TN) and includes the Senate counterpart for the House 9-1-1 SAVES Act. It addresses three issues not covered in the House version at this time, including:

- Requiring the FCC to hold public field hearings and issue additional reports after major disasters to assess the performance of the communications infrastructure;
- Requiring the FCC to study unreported 9-1-1 outages and develop recommendations to improve outage reporting; and
- Requiring the FCC's Inspector General to report on compliance with Kari's Law. and RAY BAUM'S Act.

The Enhancing First Response Act was recently approved by the Senate Commerce, Science & Transportation Committee and awaits consideration by the full Senate.

Cybersecurity Information Sharing Extension Act
(S. 1337) (Federal)

This is a short bill with a big impact. The Act would reauthorize through 2035 the current threat information-sharing environment between industry and government that, for the past 10 years, has helped address rapidly evolving cybersecurity threats. Current law has been instrumental in creating a collaborative environment for voluntary sharing of cybersecurity threat indicators — such as software vulnerabilities, malware, or malicious IP addresses — to prevent attacks from cybercriminals and nation-state actors.

Major industry groups such as USTelecom, the U.S. Chamber of Commerce, and the Bank Policy Institute strongly support reauthorizing the information-sharing regime — and so do we. Allowing this legislation to lapse would significantly weaken our nation's cybersecurity ecosystem across all critical infrastructure sectors. We have discussed our view with key congressional offices, and we encourage others who recognize the value of these public-private partnerships to do the same.

ALYSSA Act *(H.R. 1524) (Federal)* and ALYSSA's Law *(State)*

This is about school safety. Alyssa Alhadeff was one of the students murdered at Marjory Stoneman Douglas High School in Parkland, Florida, on February 14, 2018. Soon after, her parents launched a nationwide movement to require schools to implement silent panic alarms to reduce emergency response times in life-threatening situations. As Lori Alhadeff, Alyssa's mother, says, "Time=Life."

At the federal level, Reps. Josh Gottheimer (D-NJ), Jared Moskowitz (D-FL), Tony Gonzales (R-TX), and Don Davis (D-NC) are the primary sponsors of the bipartisan Alyssa's Legacy Youth in Schools Safety Alert (ALYSSA) Act. The bill does not identify specific funding for these upgrades, but rather incentivizes K-12 schools to adopt silent panic alarm technology to improve school safety by making it a condition to receive funds under the Elementary and Secondary Education Act. The ALYSSA Act is under consideration in the House Education & the Workforce Committee.

A number of states have enacted ALYSSA's Law, which includes the same requirement for silent panic alarms. In fact, the real momentum for these laws is in the states. Eleven have adopted a version of Alyssa's Law (Connecticut, Florida, Georgia, New Jersey, New York, Oklahoma, Oregon, Texas, Tennessee, Utah, and Washington), while nearly a dozen more are considering similar legislation.

What Policymakers Can Do to Promote Public Safety and 9-1-1

In our opinion, the highest priority actions policymakers could take in the near term to promote more effective 9-1-1 and improve public safety include:

Congress

9-1-1 Telecommunicators

Enact the 9-1-1 SAVES Act.

NG9-1-1

Authorize either NHTSA, NTIA, or the FCC to collect data on the status of NG9-1-1 deployment and produce an estimate of the cost to complete end-to-end nationwide deployment as a precursor to support funding the remainder of the NG9-1-1 transition.

Cybersecurity

- Enact the Cybersecurity Information Sharing Extension Act.
- Clarify authority for the FCC (or another federal agency with oversight of and expertise in telecommunications) to require communications service providers to maintain cyber risk mitigation plans and meet minimum security requirements.

School Safety

Enact a federal ALYSSA Act to require security upgrades, specifically silent panic alarms, in K-12.

FCC

NG9-1-1

Ensure that TDM circuits remain available during the transition in the areas of the country where RLECs claim they are not yet capable of sending 9-1-1 traffic in SIP.

Enterprise 9-1-1

Clarify the application of Kari's Law and RAY BAUM's Act.

Text-to-9-1-1

Promote consumer awareness of the availability of text-to-9-1-1.

State and Local Governments

Enact more ALYSSA's Laws to ensure that schools are making hard security improvements, such as silent panic alarms connected to 9-1-1, to reduce emergency response times and consider extending this to other contexts as a workplace safety measure.

INTRADO

State of the 9-1-1 Industry

Conclusion

This wraps up the 2025 Intrado State of the 9-1-1 Industry Report. Thanks for sticking with us. If you have any questions about anything we've said here, please reach out. We could talk about this stuff all day.

- NG9-1-1 adoption is moving forward, though slowly. The FCC's NG9-1-1 Transition Order is providing needed structure, though some additional clarity regarding the FCC's intent might be necessary with respect to a few issues. Federal funding will likely be necessary to achieve end-to-end NG9-1-1 in the U.S.
- PSAPs are starting to address cybersecurity, but adequate cybersecurity defenses remain a challenge, and more PSAPs need to take action to protect their systems. The advent of quantum computing poses a threat to the entire 9-1-1 ecosystem.
- Supplemental Coverage from Space is transforming the availability of 9-1-1 over satellite.
- AI tools are increasingly available to PSAPs and could address a number of current challenges.
- More PSAPs are making the move to cloud call-handling and away from traditional, on-premises solutions.
- 9-1-1 requests for assistance are originating from a wider range of devices and contexts, such as smartwatches, automobile crash scenes, and other IoT devices.
- The federal 9-1-1 SAVES Act will recognize the true nature of 9-1-1 work and workers.
- The ALYSSA's Law movement is resulting in more K-12 schools implementing solutions such as silent panic alarms to get help faster, and states and localities are beginning to apply this type of solution also as a more general workplace safety measure.

Conclusion (continued)

Looking ahead, we hope in the 2026 Intrado State of the 9-1-1 Industry Report to report progress on NG9-1-1 deployments; federal funding and legislation, including passage of the 9-1-1 SAVES Act and the federal ALYSSA Act; increased availability of 9-1-1 over satellite; greater PSAP deployment and use of text-to-9-1-1; advances in cybersecurity protection for PSAPs; and better staff recruitment and retention at PSAPs.

For additional insights throughout the year, we encourage you to attend our Share.Solve.Evolve. webinars led by Jeremy DeMar; read our blogs and white papers; and seek us out at the dozens of industry conferences we attend.

Let's keep in touch.

Acknowledgements

Creating this Report required the collaboration and expertise of many at Intrado. Sincere thanks to Tifini Aguilar, Marcus Andronici, Sam Bauder, Brian Boezeman, Josh Burch, Lonna Cain, Hope Collins, Tom Collins, Liam Cruz, Brian Davenport, D. Jeremy DeMar, Monica Ellis, Karen Freitag, Charles Gifford, Rich Johnston, Jason Lackey, Joe Lagattuta, Ravish Malhotra, Mike Matheson, Justin McLeod, Yan Roberts, Marie Thiele-Miranova, Sean Ward, Jerry Willke, and Matthew Alexander.

We extend our appreciation also to those outside Intrado, from both public safety and industry, who were kind enough to share their insights with us.

INTRADO

State of the
9-1-1
Industry

CEO Message

I have built my career on driving innovation at leading tech companies, and one thing I have learned over the years is that people are our most important resource — and at Intrado, we have the best, brightest, and most experienced team in the industry. These are people who hold among them over 100 key patents in public safety communications. These are people who create the standards others use to build their products and their networks. I've worked in telecommunications companies before, but public safety communications are different, and Intrado is special.

Intradoans are motivated by the mission to ensure that, when you dial or text 9-1-1 . . . or your smartwatch detects a bad fall . . . or your home alarm system goes off in the middle of the night . . . that your need for help reaches the right person in the right place to get to you quickly.

I want to thank these innovators and trail blazers — especially our primary authors, John Snapp and Lauren Kravetz — along with everyone at Intrado who contributed to this report. You can see from the Acknowledgements at left that this has been a team effort.

I also want to recognize and thank our nation's everyday heroes, our 9-1-1 telecommunicators. Over the last year, I have had the opportunity to meet, shake hands with, and convey my personal thanks to them. I hope you will, too.

Thank you again for reading our State of the 9-1-1 Industry Report.

INTRADO
Always there in an emergency

Matt Carter, CEO