FAQ Guide

Ohio NG 9-1-1

Department of Administrative Services

Version 2.0 April 2026

Ohio 9-1-1 Program Office • 614.728.2114 • ohio9-1-1@das.ohio.gov • Ohio 911

Table of Contents

Introduction

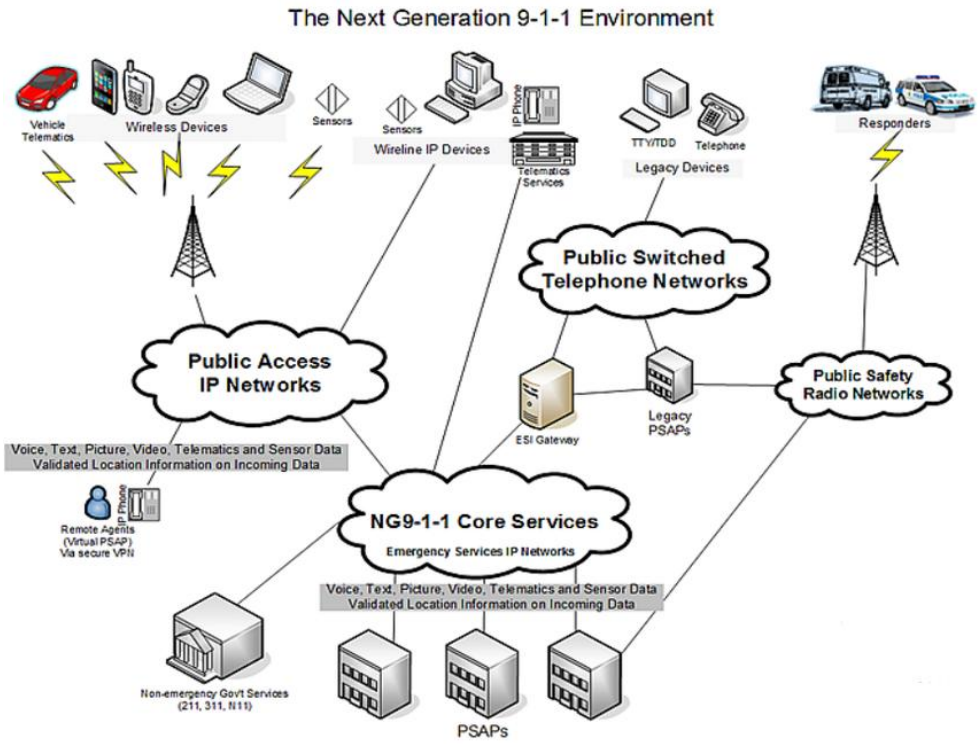
Welcome to the Ohio NG9-1-1 systems and services FAQ!

This guide is designed to provide clear, concise answers to the most frequently asked questions about navigating and using Ohio's Next-Generation 9-1-1 (NG9-1-1) system. Whether you're a new user just getting started or an experienced user seeking more in-depth information, you'll find valuable insights and guidance here.

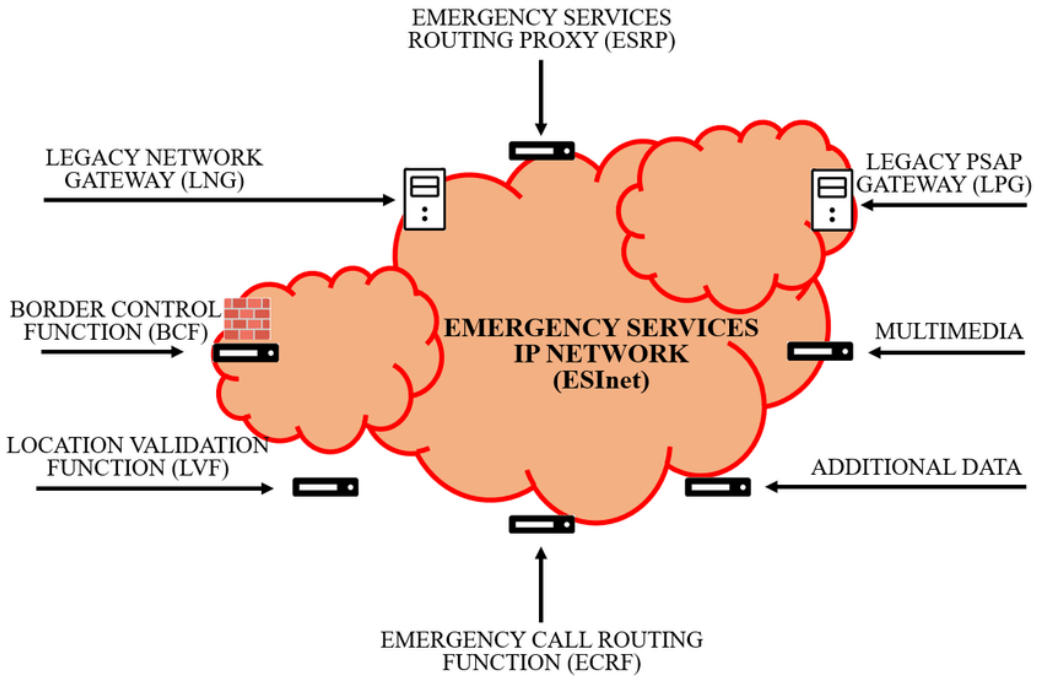
While this guide is not all-inclusive, it will continue to evolve as the NG9-1-1 project grows—serving as a living FAQ resource for users across Ohio.

If you don't find the information you need, please feel free to contact the Ohio 9-1-1 Program Office. We're here to help!

Understanding Next Generation 9-1-1

Q:	What is Next Generation 9-1-1?
A:	Next Generation 911 (NG911), is a new and improved way to receive and respond to 911 calls. Emergency callers traditionally dial 911 from a landline or a mobile device but with NG911, callers will have the ability to text, send pictures and videos from an incident and receive faster responses from accurate location data. NG911 is utilizing internet technologies to support these additional features but upgrading from legacy copper wire to fiber is a costly and time-extensive task. NG911 deployment in Ohio encompasses all NENA i3 standards version 2021 (NENA-ST-010) which includes voice and text delivery; as the standards evolve and are enabled for future media options will be implemented (*i.e. video, photo, ancillary devices*). APCO released the Definitive Guide to Next Generation 9-1-1 that provides great comprehensive approach to NG9-1-1 

Q:	How does NG9-1-1 work?
A:	When an emergency call is made from a cell phone, landline, or any internet-connected device, a network of internet services routes the call to the appropriate PSAP/ECC. This network is called an ESInet.

Q:	What is an ESInet?
A:	An ESInet manages delivery of location data, data security, and call and data routing to the appropriate PSAP/ECC and emergency services. When an ESInet efficiently communicates with local GIS data, it ensures that calls are reliably routed to the appropriate personnel. Once located and received, a computer aided dispatch (CAD) system prioritizes and records emergency calls, locates existing responders in the field, and dispatches the appropriate responders to an incident. The closest first responders are notified in near real-time with a variety of data to provide detailed situational awareness from the incident. This data may include images and/or video from the scene, building plans, or other critical data to support the event at hand. 

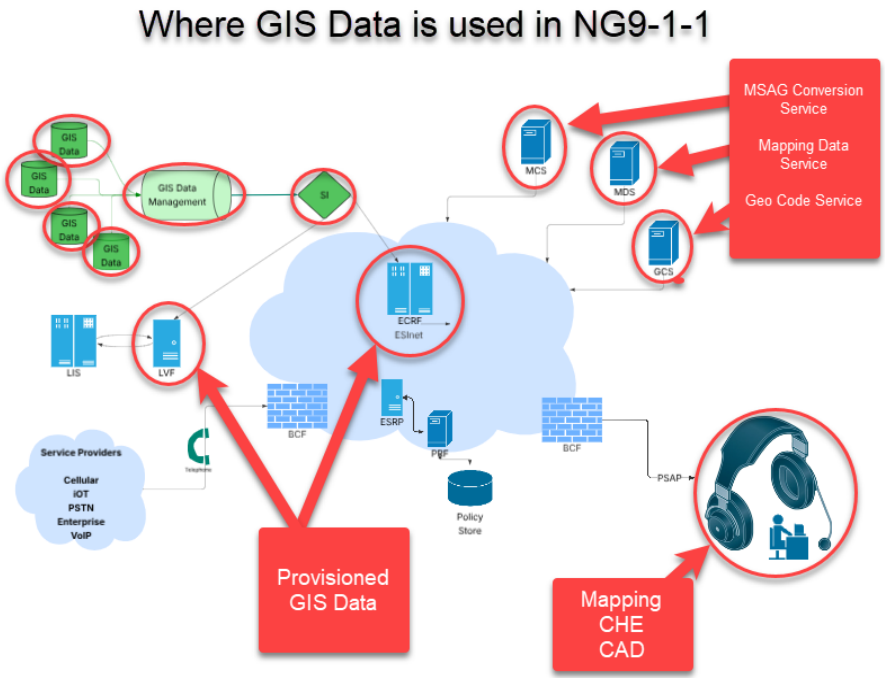
Q:	What are the benefits of NG9-1-1?
A:	NG9-1-1 fills the voids that legacy analog systems could never support. NG9-1-1 is about location accuracy and getting to an incident or a caller quicker than ever before. NG9-1-1 supports the following: • **Text, pictures, and video to 9-1-1**: NG9-1-1 provides standardized interfaces from call and message services to process all types of emergency calls including non-voice (multimedia) messages. This provides accurate location data even for callers who cannot speak. • **Acquires and integrates novel emergency call data**: acquire and integrate additional data useful to call routing and handling—deliver the calls/messages and data to the appropriate PSAPs and other appropriate emergency entities. • **Supports data and communications needs**: provide a secure environment for emergency communications for coordinated incident response and management.

Q:	Are there industry standards associated with NG9-1-1 technology?
A:	The National Emergency Number Association (NENA) sets the standards that encompasses the entire framework for the NG9-1-1 umbrella. These standards not only include GIS and attribute data but the network and system components that make up NG9-1-1. All NENA standards are publicly available and regularly updated and enhanced. All current NENA standards for NG9-1-1 are listed below and publicly available: ***Network:*** • NENA-STA-010, NENA i3 Standard for Next Generation 9-1-1 • NENA-STA-019, NG9-1-1 Call Processing Metrics Standard • NENA-STA-021, Standard for Emergency Incident Data Objects (EIDO) • NENA-STA-024, Conveyance of Emergency Incident Data Objects (EIDO) between Next Generation (NG9-1-1) Systems and Applications • NENA-STA-034, NENA Legacy Selective Router Gateway (LSRG) Standard • NENA-INF-003, Demarcation Points in NG9-1-1 Information Document • NENA-INF-011, NENA NG9-1-1 Policy Routing Rule Operations Guide • NENA-INF-043, NENA Spoofing Mitigation Information Document ***Security:*** • NENA-STA-040, Security for Next Generation 9-1-1 Standard (NG-SEC) • 75-502, Next Generation 9-1-1 Security Audit Checklist Information Document ***Database:*** • NENA-STA-004, NENA Next Generation 9-1-1 United States Civic Location Data Exchange Format (CLDXF-US) Standard • NENA-STA-006, NENA Standard for NG9-1-1 GIS Data Model • NENA-STA-012, NG9-1-1 Additional Data Standard • NENA-STA-029, NENA Next Generation 9-1-1 (NG9-1-1) Canadian Civic Location Data Exchange Format (CLDXF-CA) Standard • NENA-REQ-002, NENA Next Generation 9-1-1 Data Management Requirements • NENA-REQ-003, NENA Requirements for 3D GIS for E9-1-1 and NG9-1-1 • NENA-INF-014, NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1 • NENA-INF-027, NENA Information Document for Location Validation Function Consistency • NENA-INF-028, NENA Information Document for GIS Data Stewardship for NG9-1-1 • NENA-INF-046, NENA GIS Data Transition Information Document ***Planning:*** • NENA-STA-017, NENA Changing Role of the Telecommunicator in NG9-1-1 • NENA-REQ-001, NG9-1-1 PSAP Requirements Document • NENA-INF-008, NG9-1-1 Transition Plan Considerations Information Document • NENA-INF-040, Managing & Monitoring NG9-1-1 Information Document • NENA-INF-041, NENA NG9-1-1 Operational Impacts on the PSAP Information Document

Q:	What are Next Generation Core Services (NGCS)?
A:	In essence, NGCS is the engine under the hood of NG9-1-1, driving a more sophisticated, responsive, and adaptable emergency service network. It brings about a transformative upgrade over the previous systems, making emergency services more reliable and effective, no matter the scale or nature of the crisis at hand. Next Generation Core Services (NGCS) are crucial components that power the functionality of NG9-1-1. They represent a major leap from the capabilities of legacy 9-1-1 systems, enabling a more dynamic, efficient, and adaptable emergency response framework. Here's a simplified breakdown: 1. **Geospatial Call Routing:** Unlike legacy systems which route calls based on fixed zones, NGCS uses real-time location data to route emergency calls to the nearest and most relevant response units. This geospatial routing is much quicker and more accurate, ensuring help arrives as fast as possible. 2. **Policy Routing Function:** This feature allows for the customization of call-routing based on specific local policies or priorities. For instance, during a tornado, policy routing could prioritize calls from affected areas to ensure swift response. 3. **Last Resort Routing:** In case the primary routing methods fail, the Last Resort Routing ensures that the call still reaches a dispatch center. It's a backup to ensure every call for help is answered, even under challenging circumstances. 4. **AI/ML (Artificial Intelligence/Machine Learning):** NGCS can leverage AI and ML technologies to analyze data and improve system performance over time. For instance, predicting call volumes to better allocate resources or identifying trends in emergency situations. 5. **Interstate/Intrastate Interconnectivity:** NGCS fosters better communication and coordination among emergency services across town, county, and state lines. This is crucial during large-scale emergencies that require a coordinated response across different regions. 6. **Enhanced Data Management:** NGCS allows for better management and sharing of critical data among emergency response entities. Unlike legacy systems, data can be shared seamlessly, ensuring all parties have the necessary information to respond effectively.

Q:	What is Call Handling as a Service (CHaaS)?
A:	Call Handling as a Service (CHaaS) is a model for providing 9-1-1 services that rely on cloud-based technology and infrastructure rather than on-premise hardware and software. In a CHaaS model, 9-1-1 calls are routed to a cloud-based call center, which is answered and processed by trained 9-1-1 operators. CHaaS is often seen as an alternative to traditional on-premise infrastructure, which can be more expensive and complex to maintain. One advantage of CHaaS is that it can be more scalable and flexible than on-premise infrastructure. Because the call center is cloud-based, it can be easily expanded or contracted to meet changing demand and can be accessed from anywhere with an internet connection. CHaaS can also be more reliable and secure than on-premise systems, as it is typically supported by multiple redundant servers and is managed by experienced professionals. CHaaS can often be implemented more quickly and with fewer upfront costs than on-premise systems, making it an attractive option for organizations looking to modernize their 9-1-1 services.

Q:	What is offered for CHaaS by Ohio?
A:	The State of Ohio offers Call Handling as a Service (CHaaS) for local jurisdictions that choose to utilize and contract with Allerium as their CHaaS provider. This option is designed to provide flexibility in implementation while ensuring alignment with the state's NG9-1-1 framework and technical standards. 1) Guardian: Guardian is a comprehensive 9-1-1 call handling and management solution for Public Safety Answering Points (PSAPs). It offers a flexible, user-centric platform for managing voice, data, and video emergency calls. Key features include integrated text-to-911, location mapping, and a robust Management Information System (MIS) for call logging, tracking, and reporting.

Q:	How is GIS used in NG9-1-1 and what happens to the ALI/MSAG?
A:	Geographic Information System (GIS) technology is essential in Next Generation 9-1-1 (NG9-1-1) because it helps to accurately locate and route emergency calls to the appropriate public safety answering point (PSAP). A traditional 9-1-1 system uses Automatic Location Information (ALI) and the Master Street Address Guide (MSAG). ALI is a database that contains information about the location of every telephone number (TN) in a given area. When a 9-1-1 call is made, the ALI database determines the caller's location so the call can be routed to the appropriate PSAP. The MSAG database contains information about a given area's street addresses and geographic boundaries. It is used to determine a particular PSAP's jurisdiction and ensure that 9-1-1 calls are routed to the correct PSAP. In NG9-1-1, GIS technology is used to supplement and enhance the capabilities of ALI and MSAG. GIS can provide more detailed and accurate location information, including the caller's precise latitude and longitude and information about the surrounding environment. GIS can also enhance the routing of 9-1-1 calls in NG9-1-1 systems. By integrating GIS data with routing protocols, NG9-1-1 systems can more accurately route calls to the appropriate PSAP based on the caller's location and the surrounding environment. Overall, the integration of GIS technology in NG9-1-1 systems helps to improve the accuracy and efficiency of the 9-1-1 system, ensuring that emergency calls are routed to the correct PSAP as quickly as possible. 

Q:	What are the three levels of redundancy for the project?
A:	NG9-1-1, Next Generation 9-1-1, refers to a modernized, internet-based version of the 9-1-1 system. It is designed to be more flexible, efficient, and reliable than traditional 9-1-1 systems. It can support a wide range of advanced features such as text, photo, and video messaging and location tracking. To ensure the reliability of the NG9-1-1 system, it is often designed with multiple levels of redundancy, which means that it has multiple backup systems in place in case one or more of the primary systems fail. The three main redundancy levels for NG9-1-1 are: • MPLS (Multiprotocol Label Switching): This networking technology is used to transmit data across a network of interconnected devices. MPLS is often used as a primary means of transmitting 9-1-1 calls in NG9-1-1 systems, as it is fast and reliable. MLPS Networks must have complete diversity and paths to be considered redundant. Broadband: This refers to high-speed internet connectivity that is provided through a variety of technologies such as cable, DSL, or fiber. (*Note: Cable and DSL are not acceptable methods in Ohio for NG9-1-1 connectivity*) • 5G LTE (Long-Term Evolution) through FirstNet: This wireless networking technology provides fast, high-capacity connectivity. FirstNet is a dedicated communications network for first responders and public safety agencies. It can be a tertiary means of transmitting 9-1-1 calls in NG9-1-1 systems if the primary MPLS and secondary broadband connections fail. • LEO (Low Earth Orbit) satellite solutions offer high-speed, low-latency internet connectivity, particularly beneficial for remote access area and application requiring real-time data exchanges. Satellite solutions like that of Starlink or OneWeb are often utilized for connectivity options depending on network, CHE requirements, and design. Using multiple redundancy levels, NG9-1-1 systems can ensure that 9-1-1 calls can always get through, even if one or more of the primary systems fail. This helps to ensure that the 9-1-1 system is always available and reliable, which is critical in emergencies.

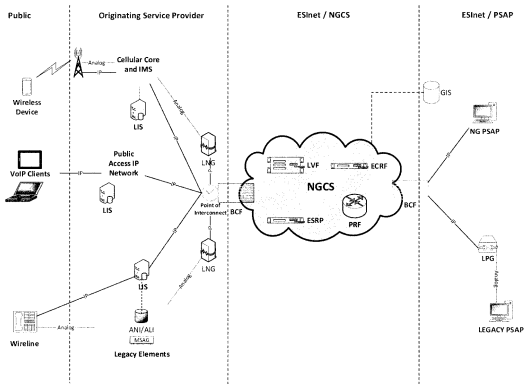
Expectations of Ohio NGCS

Q:	What are the benefits of connecting to the Ohio NGCS?
A:	Connecting to the Ohio Next Generation Core Services (NGCS) provides a wide range of operational and technical advantages for PSAPs and ECCs. Key benefits include: • **Accurate Call Routing** Ensures calls are directed to the correct PSAP based on geospatial data while enabling geographic-independent call access, transfer, and backup among PSAPs and between PSAPs and other authorized emergency organizations. • **Location-Based Call Routing** Enables precise routing based on caller location rather than legacy systems like cell tower triangulation. • **Integrated NGCS SMS Delivery** Supports the seamless handling and delivery of SMS (text-to-911) messages within the NGCS framework. • **i3 Compliance with NENA Standards** Aligns with NENA i3 architecture standards, ensuring interoperability and future-proofing systems. • **Evolution Toward Enhanced Data Integration (EDIO)** Supports the inclusion of rich, non-voice data (e.g., sensor alerts, video, telematics) as NG9-1-1 evolves. • **Interoperability** Facilitates collaboration and data sharing between agencies and across jurisdictions. • **Dynamic Emergency Call Rerouting** Enables the ability to reroute calls in real time based on capacity, call volume, outages, or special events. • **Advanced Location Services** Utilization of advanced location technologies to pinpoint a caller's exact location improving emergency response. • **Accessibility for All** The system is designed to support various communication methods for people with disabilities, including text, video, and sign language interpretation. • **Disaster Response Enhancement** Will aid in managing call overload during disasters, enabling faster call routing and data sharing. • **Expanded E9-1-1 Processing** Enable E9-1-1 calls from any networked communication device. • **Public Safety Partnerships** Foster increased coordination and partnerships within the public safety community.

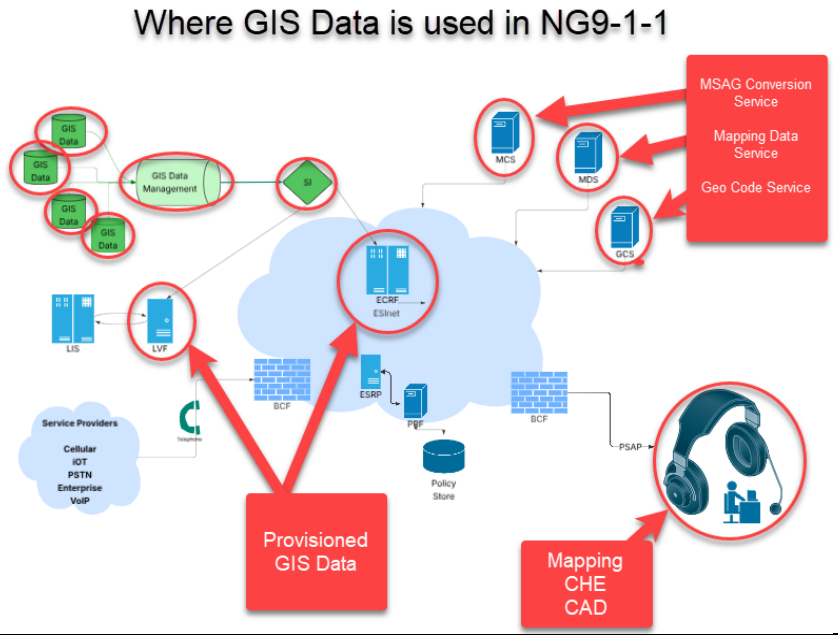
Q:	What is the potential cost saving incentives?
A:	Connecting to the Ohio Next Generation Core Services (NGCS) can offer significant cost savings to local PSAPs by reducing or eliminating the need for legacy infrastructure and services. Key areas of potential savings include: • **Decommissioning of CAMA Trunks** Legacy analog trunks can be phased out, eliminating associated recurring costs. • **MSAG Maintenance and Hosting** With the transition to GIS-based location routing, ongoing Master Street Address Guide (MSAG) maintenance and hosting costs are reduced or eliminated. • **Administrative and 9-1-1 Telephony** Simplified call routing and integrated systems reduce the need for redundant administrative telephony infrastructure. • **MARCS Connectivity** Ohio MARCS customers have the ability to connect their authorized radio consoles through the ESInet and depreciate other connectivity options. Contact Ohio MARCS for further information. By leveraging shared ESInet and NGCS infrastructure at the state level, local agencies can modernize their emergency communication systems while optimizing operational budgets.

Q:	What are the benefits of NG9-1-1 to public safety?
A:	Key benefits to the entire public safety spectrum include: • **Faster Response Times:** The ability to send multimedia information and improved location services will lead to quicker and more efficient emergency responses. • **Better Situational Awareness:** Receiving multimedia information like photos and videos will provide dispatchers and first responders with a clearer picture of the situation before arrival. • **Increased Resilience:** NG9-1-1 systems are designed to be more robust and resilient, capable of handling increased call volumes and potential disruptions. • **Improved Data Management:** NG9-1-1 will enable the sharing of more comprehensive data between different agencies, facilitating better incident management. • **9-1-1 Call Agnostic:** Decision-making within the Next Generation 9-1-1 (NG9-1-1) environment refers to the ability of the dispatch system to receive and process emergency calls regardless of their originating format (voice, text, photo, video, data from IoT devices) and then route them to the most appropriate public safety answering point (PSAP) and response resources, free from limitations imposed by outdated technology or jurisdictional boundaries.

Next Generation 9-1-1 Call Flow

Q:	How is a typical NG9-1-1 call delivered?
A:	1. **Initial Call Initiation:** • The caller initiates a call to 9-1-1, either by voice or through a non-voice communication method (e.g., text, video). • The call is routed through a digital IP-based network, rather than the traditional analog system. 2. **Location Data Extraction and Routing:** • NG9-1-1 systems use various methods to determine the caller's location, such as: ○ **Geolocation data:** This can be extracted from the caller's device (e.g., GPS coordinates from a smartphone). ○ **Civic address data:** This is information about the caller's address, which is also transmitted to the PSAP. • The location data is then used to route the call to the appropriate PSAP based on jurisdictional boundaries and other factors. 3. **Call and Data Delivery to PSAP**: • The call and any associated data (e.g., location data, text message, video) are delivered to the PSAP via the IP network. • The PSAP receives the call and data, allowing dispatchers to understand the nature of the emergency and the caller's location. 4. **Dispatch and Response**: • The PSAP dispatches the appropriate emergency services to the location based on the information received. • NG9-1-1 allows for real-time communication between the PSAP and emergency responders, including the ability to share multimedia. 5. **Interoperability and Enhanced Capabilities**: • NG9-1-1 enables seamless communication and data sharing between different PSAPs and other emergency entities, facilitating better coordination and response during large-scale events or emergencies. • It also offers enhanced capabilities such as call transfer, location-based routing, and the ability to handle non-voice communications. 

Q:	What are the Functional Elements of Next Generation 9-1-1 Core Services that Facilitate the NG9-1-1 Call Flow?
A:	The NENA i3 architecture also defines Functional Elements (FEs), which are interconnected and communicate via the ESInet. These FEs represent specific functions within the NG9-1-1 system. Some important functional elements mentioned in the search results include: • *Emergency Call Routing Function* (ECRF): Determines which PSAP should receive a call based on location and routing policies. • *Emergency Services Routing Proxy* (ESRP): Looks for emergency calls on the ESInet and routes them through the network based on location and routing policy. • *Location Validation Function* (LVF): Validates and provides detailed location information, including civic address and geodetic data. • *Legacy Network Gateway* (LNG) / Legacy Selective Router Gateway (LSRG): Provides interfaces between legacy 9-1-1 systems (non-IP based) and the NG9-1-1 system, supporting the transition process. In addition to these core components, NG9-1-1 systems also emphasize standardized interfaces, security measures, and operational policies and procedures to ensure interoperability, security, and effective emergency response.

Q:	How does GIS play a role in NG91-1?
A:	GIS plays a crucial role in NG9-1-1 by providing the foundational geospatial data and location services that enable accurate call routing, location validation, and enhanced situational awareness for emergency dispatchers. Essentially, GIS ensures that emergency calls are routed to the correct Public Safety Answering Point (PSAP) and that dispatchers can quickly and accurately identify the caller's location and the nature of the emergency. 

Q:	What are the key functions of GIS Data with respect to NG9-1-1?
A:	Data Model: • The NENA standard for the NG9-1-1 GIS data model defines the required attributes and formats for GIS data, ensuring interoperability across different systems. • NENA-STA-006 Data Layers: • GIS data is organized into layers, such as address points, road networks, and PSAP boundaries, allowing for efficient analysis and visualization. • NENA-STA-004 Data Sharing: • Local governments and PSAPs work together to maintain and share GIS data, ensuring that it is accurate and up-to-date. Data Quality: • NG9-1-1 relies on high-quality GIS data, and efforts are underway to ensure uniform standards and best practices for data sharing and maintenance • NENA-INF-028

Navigating the Last Mile Connectivity

Q:	Who provides the last mile connection?
A:	OARnet serves as the ESInet provider for Ohio's Next-Generation 9-1-1 system. The Ohio 9-1-1 Program Office will coordinate directly with OARnet to survey potential last mile providers and obtain service quotes. Once this information is gathered, the 9-1-1 Program Office will schedule a meeting with the local jurisdiction to review connectivity options and discuss ongoing costs associated with connecting the Public Safety Answering Point (PSAP) to the ESInet. **Important:** Local jurisdictions are strongly advised **not** to independently establish a last mile connection before consulting with the Ohio 9-1-1 Program Office. This ensures the connection meets NG9-1-1 requirements and aligns with the jurisdiction's assigned phase in the statewide deployment schedule. **DO NOT** *contact OARnet directly for ESInet connectivity, they cannot and will not assist or authorize connections to the ESInet for utilization*!

Q:	Can I just utilize my current network provider?
A:	Potentially, however, that needs to be evaluated. This is usually determined by your selected CHE and the connectivity requirements needed for ESInet.

Q:	Do all PSAPs require last mile connectivity?
A:	No! Agencies who utilize a hosted CHE solution usually do not require last mile connectivity.

Q:	Utilizing Spectrum Cable as a circuit for 9-1-1?
A:	Unfortunately, Spectrum has informed the State of Ohio that they do not wish to carry 9-1-1 traffic across their network. As a result, Spectrum cannot be used as part of any ESInet-connected solution. Agencies should plan accordingly and work with the Ohio 9-1-1 program office on obtaining approved providers that support the transport of 9-1-1 traffic in compliance with state and national standards, along with the ability to connect to OARnet.

Q:	What are the network circuit connectivity requirements?

A:	Pending system design and CHE selection, the following network requirements exist:
	• Dual geo-diverse last mile connections to different OARnet POPs.
	  ○ Point-to-Point Ethernet Circuit, Layer 2 interface
	  ○ Switched layer 2 circuit with VLAN and COS capabilities, layer 2 interfaces
	• 1MB per console with a minimum of 10MB diverse circuits; preferrable from different providers.
	• Quality of Service (QOS) requirements
	  ○ Packet loss: 1% maximum
	  ○ Jitter: 5ms maximum
	  ○ Latency: 50ms maximum
	The 9-1-1 program office will assist and advise on these connections to ensure consistency and that requirements are met as all circuits must land in specified locations and be free of third-party interconnects. The 9-1-1 program office will assist and source potential options to be selected by each jurisdiction.

GIS: Ohio LBRS Model

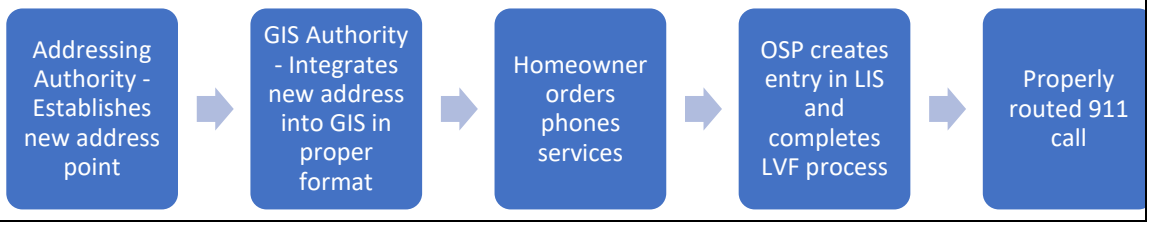
Q:	How does the LBRS data enter the NG9-1-1 system?
A:	Local GIS data is uploaded to the LBRS (Location-Based Response System) data repository, where it undergoes ingestion, transformation, and validation processes to meet NG9-1-1 system requirements. Once validated, the data is ingested into the Location Database (LDB), where it is stored and utilized to support accurate call routing through the Location Validation Function (LVF). This process ensures that location data is current, accurate, and compliant with standards necessary for effective emergency response.

Q:	How often should data be submitted?
A:	GIS data should be submitted on a regular basis, ideally daily if possible. At a minimum, it is currently recommended that GIS data be updated monthly to ensure accuracy and alignment with the NG9-1-1 system requirements. Local jurisdictions are encouraged to upload GIS data as frequently as they deem necessary based on the rate of changes within their area. Timely updates are critical, as this data is used to route 9-1-1 calls accurately and identify caller locations, directly impacting emergency response effectiveness.

Q:	What data elements and information are required for the LDB submission?
A:	All information and requirements with data specifications are located here: https://ohiolbrs-geohio.hub.arcgis.com/

Q:	What NAD should GIS data be projected in?
A:	All layers should be submitted in NAD_1983_StatePlane_Ohio_South_FIPS_3402_Feet

Q:	Where can I find the current Ohio LBRS specification and version?
A:	The current version of the LBRS in Ohio is 4.1. The specifications and related information can be downloaded from the following link: https://tinyurl.com/OHLBRSSPEC

Q:	Who is the addressing authority?
A:	Local jurisdictions remain the official addressing authority and should publish their address assignment processes and contact information on their respective websites. Per NENA standards, once a new address is assigned, it should be provisioned and entered into the NG9-1-1 database within 72 hours. Adhering to this standard ensures that any 9-1-1 call originating from that location is accurately routed and handled by the appropriate PSAP/ECC, supporting a timely and effective emergency response. Documenting and streamlining addressing and GIS workflows is critical to maintaining the integrity and functionality of NG9-1-1 call routing. 

Q:	What is the best resource for a GIS checklist?
A:	The National 9-1-1 Program has published a white paper focused on the critical role of Geographic Information Systems (GIS) in Next-Generation 9-1-1 (NG9-1-1). This publicly available document is an important resource for understanding the evolving scope and growing importance of GIS data and personnel within the public safety ecosystem. As NG9-1-1 continues to advance, accurate GIS data becomes foundational to call routing, location validation, and emergency response. All stakeholders—including public safety agencies, GIS professionals, and PSAP administrators—are encouraged to review the white paper to stay informed and prepared. NG9-1-1 Checklist

Q:	Should I ask for GIS data from neighbors?
A:	PSAPs and ECCs should, at a minimum, maintain regional NG9-1-1 GIS data within their respective mapping systems. This is essential for accurately locating callers in rollover or backup scenarios involving neighboring PSAPs/ECCs, where local call handling may be temporarily shifted. To support this capability, GIS data sharing agreements should be established with regional partners. These agreements help ensure that PSAP/ECC staff have the necessary tools and location data to effectively assist during service disruptions or high call volumes. Proactive collaboration enhances situational awareness and improves the overall effectiveness of emergency response.

Q:	Can NG9-1-1 funding be utilized for GIS data remediation project?
A:	Yes, funding has been increased and allocated to support NG9-1-1 readiness and related projects, ensuring the capability for full implementation of NG9-1-1 across the state.

Q:	Where can GIS professionals turn for help and information?
A:	The Ohio GIS user groups and regional organizations are a great place to start and continue conversations on how neighbors and friends within the GIS andNG9-1-1 communities can work together to achieve the common goals. Visit the OHIO GIS Community at the link below: https://ohio-gis-community-geohio.hub.arcgis.com/

Q:	What are the requirements for GIS data to be considered NG9-1-1 Ready?
A:	GIS layers must not contain any critical errors and the Automatic Location Identification (ALI) to Road Centerline match rate must reach or exceed 98% accuracy.

GIS: Emergency Service Boundaries

Q:	What is an Emergency Service Boundary (ESB) and how does it get used in NG9-1-1?

A:	An Emergency Service Boundary is a defined geographic area that outlines the jurisdictional responsibility of a specific emergency service provider—such as PSAP, law enforcement, fire, or emergency medical services (EMS).
	
	In Next-Generation 9-1-1 (NG9-1-1) systems, emergency service boundaries are critical GIS data layers used to determine which Public Safety Answering Point (PSAP) or emergency agency should receive and respond to a 9-1-1 call, based on the caller's location.
	• Types of Boundaries:
	  ○ PSAP Boundary
	  ○ Law Enforcement Boundary
	  ○ Fire Service Boundary
	  ○ EMS Boundary
	• These boundaries are used by the Emergency Call Routing Function (ECRF) and the Location Validation Function (LVF) in NG9-1-1 systems to route calls accurately.
	• Maintaining accurate and up-to-date emergency service boundaries is essential for:
	  ○ Ensuring calls are routed to the correct PSAP.
	  ○ Avoiding delays in response due to misrouted calls.
	  ○ Supporting mutual aid and backup scenarios.
	Emergency service boundaries ensure the right call goes to the right place, every time.

Q:	How granular can ESBs be created?
A:	Emergency Service Boundary (ESB) layers should include as much detail as possible. These boundaries are used by any jurisdiction that may be answering a 9-1-1 call, particularly in situations where calls are rerouted to backup or neighboring PSAPs. It's important to remember that the NG9-1-1 system is designed to function on a broader scale—even across state lines—making it essential that GIS data is highly detailed. Whenever possible, ESB layers should define response areas down to the station, zone, or beat level. This ensures precise call routing and supports accurate dispatching, regardless of where the call is answered. Example: ZXC Fire operates four stations—ZXC40, ZXC45, ZXC44, and ZXC47—each with its own defined response area represented by separate polygons. These polygons are essential for clearly identifying jurisdictional boundaries and support accurate call processing. In an NG9-1-1 environment, even if the CAD system is down, the Call Handling Equipment (CHE) would display the correct response agency (e.g., "ZXC45") based on

	the caller's location. This functionality is especially valuable during system outages, when calls are being handled by a backup PSAP, or even when calls are routed across the state—or across state lines. This level of GIS-based detail ensures continuity of service and accurate emergency response under any circumstances.

Q:	Are there any gaps allowed within the ESB topology?
A:	No gaps are permitted within the topology. All layer delineations must be precisely snapped together, and all county boundaries must align exactly with those of neighboring counties. All Emergency Service Boundaries must match the county boundaries also with no gaps or overlaps between any polygons. To ensure topological consistency, each county must coordinate with its adjacent counties to verify that all shared boundaries are properly aligned and free of gaps or overlaps.

Q:	What data schema needs to be followed for ESBs?
A:	The following fields are needed inside each layer for all four disciplines.

Field Name	Data Type	Description
ServiceURI	Text 100	**Uniform Resource Identifier (URI)** of the agency (e.g., urn:agency:police:OH:ColumbusPD). *These are specific to each County/PSAP and are assigned by Comtech.* **Required**.
ServiceType	Text	Type of emergency service (PSAP,Law, Fire, EMS). **Required**.
AgencyName	Text 100	Name of the emergency service agency (e.g., "Columbus Division of Fire"). **Required**.
AgencyID	Text 50	Unique ID or code for the agency (may be assigned by the state or region – Consider utilizing response corresponding station numbers/names). **Required**.
ContactPhone	Text	Administrative or emergency contact number for the agency. *Alternatively, the number that can be contacted to obtain dispatchable deployment.*
Email	Text	(*Optional*) Contact email address for the agency.
EffectiveDate	Date	(*Optional*) Date when this boundary became effective.
ExpirationDate	Date	(*Optional*) Date when this boundary is no longer valid.
UpdateDate	Date	(*Optional*) Most recent date of boundary update.
Geometry	Polygon	Geospatial polygon representing the emergency service boundary. **Required**.

Q:	What does the complete NGUID look like?
A:	**NGUID** Text 100 Example **urn:emergency:uid:gis:Pol:100:psapoh.com** Black is a constant Purple identifies the layer (Pol, Fire, Ems, Psap) Red can be any unique local ID that you choose Blue is your agency ID/county domain.

Q:	How do we resolve county boundary issues?
A:	While OGRIP can assist with mitigation efforts, it's important to note that GIS data is locally controlled. Therefore, any discrepancies or alignment issues must be addressed in coordination with surrounding counties, agencies, and jurisdictions. Each county is individually responsible for the accuracy and completeness of GIS data within its boundaries. If adjacent boundaries do not align, it is the responsibility of those counties to work together to develop agreements or implement solutions to ensure seamless edge matching. There must be **NO** gaps between county boundaries—all boundaries must be snapped together and edge-matched in accordance with NG9-1-1 standards.

GIS: Data Accuracy and Maintenance

Q:	What is provided to maintain NG9-1-1 GIS data?
A:	As part of Ohio's NG9-1-1 implementation plan, the Datamark Technologies *Data Maintenance Tool* is provided at no cost to agencies that wish to utilize it. This online tool allows for direct editing and maintenance of GIS data that has been submitted and uploaded through the LBRS (Location-Based Response System) portal. Once the submitted data has been transitioned and formatted to meet NG9-1-1 standards, the Datamark Data Maintenance Tool can be used to manage and maintain the data online in a centralized environment. This ensures consistency, accuracy, and readiness of GIS data for NG9-1-1 systems across the state in real-time. Agencies are encouraged to leverage this resource to support ongoing GIS data quality and compliance.

Q:	What is the LDB (Location Database)?
A:	The Location Database is: • It's a crucial component of NG911, an IP-based system designed to enhance emergency number services and improve the speed, flexibility, resiliency, and scalability of 911. • The LDB replaces the Automatic Location Information (ALI) database used in legacy 911 systems. • It stores customer address records and other location-related data, such as civic addresses and geocoordinates. • The information in the LDB is validated against the Location Validation Function (LVF), which ensures its accuracy and helps in routing emergency calls to the correct Public Safety Answering Point (PSAP). • It functions as a server retaining all current ALI information and interfaces, while also accommodating the new protocols of NG9-1-1 deployments.

Q:	How do I manage the NG9-1-1 Location Database?
A:	During your NG9-1-1 implementation and go-live, training will be provided along with access to the Location Database (LDB). This access will allow authorized personnel to identify and resolve addressing discrepancies that may arise during data validation. Discrepancies can either be corrected directly within the system or escalated to the appropriate party for resolution. This process ensures that the location data used for call routing is accurate, up-to-date, and compliant with NG9-1-1 standards. Authorized personnel will also be configured to receive regular LDB discrepancy reports; to ensure data integrity and compliance with standards.

Q:	How can I determine the status of my county's NG9-1-1 GIS data readiness?
A:	GIS data is actively tracked and monitored within the NG9-1-1 Dashboard to ensure it meets established standards and guidelines. This continuous oversight is essential to maintaining data accuracy and integrity, helping to ensure that 9-1-1 calls are routed correctly and no calls are misrouted due to GIS data issues. The dashboard provides visibility into data quality, completeness, and alignment with NG9-1-1 requirements, supporting proactive data maintenance and issue resolution. The GIS Dashboard is located here: https://tinyurl.com/OHNG911GISDASH

Q: What errors are validated and compiled in the GIS Dashboard?

A: The following errors are compiled and tracked as part of the NG9-1-1 GIS Dashboard. These errors are important indicators of data quality and are used to assess compliance with NG9-1-1 standards.

It is important to note that these same issues are also documented in the GIS Data Discrepancy Reports, which are provided to authorized users for review and resolution. These reports support ongoing data maintenance efforts and help ensure that all GIS datasets are accurate and suitable for use in emergency call routing.

ID	Severity	ErrorDescription
200	Critical	Road has invalid or non-Line string geometry.
201	Critical	Road must have a street name.
404	Critical	Duplicate address name set in different PSAPs.
405	Critical	Address State must not be empty.
406	Critical	Address Country must not be empty.
407	Critical	Address House Number and Landmark should not be empty simultaneously.
409	Critical	Address ClientID must not be empty.
410	Critical	Address Muni has an invalid value.
503	Critical	Road Left State must not be empty.
504	Critical	Road Right State must not be empty.
507	Critical	Road Left Country must not be empty.
508	Critical	Road Right Country must not be empty.
509	Critical	Road ClientID must not be empty.
510	Critical	Road Left Muni has an invalid value.
511	Critical	Road Right Muni has an invalid value.
605	Critical	Service boundary override service URN must not be empty.
609	Critical	Service boundary ClientID must not be empty.
619	Critical	Service boundary has one or more invalid URIs.
620	Critical	Service boundary SIP URI must start with sip: or sips:.
621	Critical	Service boundary SIP URI is not a known URI.
622	Critical	Service boundary SIP URI is missing.
630	Critical	Service boundary overlaps another.
640	Critical	Service boundary extends beyond Provisioning Boundary.
650	Critical	Gap in service boundary layer.
680	Critical	SQL geography is not valid.
681	Critical	Service boundary Effective date must be before Expires date
800	Critical	Change count above threshold.
801	Critical	Change count above threshold.
238	High	Road Left parity does not match address range.
239	High	Road Right parity does not match address range.
240	High	Road Left address range is invalid.

	241	High	Road Right address range is invalid.
	403	High	Address is outside of the Provisioning Boundary.
	541	High	Geocode area of Road outside of Provisioning Boundary
	591	High	Address Range conflict.
	715	High	Not a registered value for Address PLC.

Q: How do I resolve and update the errors and issues presented in the GIS Dashboard?

A: The quality control errors are reported back to County GIS for resolution in two ways:

1. Directly within Accuglobe Data Maintenance for those customers. The errors can be resolved here in real-time (i.e. fix the data and the QC error disappears). *(Accuglobe Data Maintenance solution is provided to the local GIS authority at no cost.)*
2. Sent to the county GIS in shapefile format. The errors can be loaded into whatever GIS application the county is using to maintain the data. Fixing the data would not resolve the QC errors in real-time. The corrected data would then need to be submitted for update through the OGRIP portal.

In both cases, when updated GIS data is imported into DataManager (prior to publishing to the ECRF) the quality control checks are re-run. The error counts shown on the dashboard would be resolved upon the next dashboard update (twice weekly).

Q: How important is the local addressing authority?

A: Local jurisdictions remain the official addressing authority and should publish their address assignment processes and contact information on their respective websites.

The local addressing authority plays a critical role in the successful implementation of Next Generation 9-1-1 (NG9-1-1). In accordance with NG9-1-1 standards, once a new address is issued, it must be provisioned into the NG9-1-1 GIS database and uploaded to the system within **72 hours** of issuance. Meeting this standard ensures that any 9-1-1 call originating from that location is accurately routed and handled by the appropriate PSAP or ECC, supporting a timely and effective emergency response.

Accurate and timely address provisioning ensures that caller location information is correctly routed, and that all relevant local data is available to the PSAP/ECC—enabling a precise, dispatchable location for responders.

Additionally, local addressing authorities should provide education or informational materials to address recipients, emphasizing the importance of correctly updating their address with service providers. Some VoIP and static cellular devices require users to manually enter their service address. Likewise, large Multi-Line Telephone Systems (MLTS) must comply with current FCC requirements for address provisioning to ensure spatial call routing is available and properly implemented.

Q:	How do I gain access to the LDB?
A:	During agency training and after go-live, authorized personnel will be granted access to the Location Database (LDB).

Q:	How do I access training for LDB management and issue mitigation?
A:	Once you have received your credentials for the Location Data Gateway (LDG), access to training will be scheduled and provided. Additionally, the training materials remain available for ongoing reference in the Comtech Insights Training Library, where DDTI/Datamark Technologies has posted and maintains all relevant training resources.

Q:	What standard is followed for 9-1-1 addressing?
A:	The current standard by NENA is the *Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDFX-US) Standard*. NENA-STA-004.2-2024

Policy Based Call Routing

Q:	What is the best method to plan for emergencies within the 9-1-1 / Emergency Communications Ecosystem?
A:	Maintaining operability, interoperability, and continuity of emergency communications is critical for emergency response regardless of the operating conditions. Primary, Alternate, Contingency, Emergency (PACE) communications plans are a tool for helping organizations prepare for backup communications capabilities in out-of-the-ordinary situations. PACE planning helps organizations establish options for redundant communications capabilities if primary capabilities are disrupted or degraded.

Q:	What is the best reference and information available for PACE planning?
A:	CISA and SWIC developed documentation on PACE planning in 2024 that can be referenced: https://tinyurl.com/CISA-SWIC-PACE

Q:	What is PACE methodology?
A:	**Primary Plan:** This is your ideal plan. The one you'd like to execute if everything goes according to your expectations. It involves the use of the main communications system and could include technologies such as landline phones, cellular networks, or internet-based tools like email, messaging, and Voice over IP (VoIP) services. This is what you use day-to-day. **Alternate Plan:** This is your backup plan. The one implemented when your primary form of communication is unavailable. These methods may be less convenient for everyday use but effectively ensure around-the-clock readiness. Examples include having a backup two-way radio solution, satellite phones, or substitute internet connections such as mobile hotspots. **Contingency Plan:** This is your plan for dealing with unexpected events when the alternate solution isn't successful. It focuses on implementing additional backup technologies that are more robust and resilient. From backup power generators to dedicated backup radio networks, these solutions are implemented to ensure the continuous operation of connected systems. For organizations, it's typically difficult to invest in this stage (and subsequently, the latter stage). This is often due to the cost, perceived unlikelihood of severe events, and limited resources. However, to ensure there is comprehensive investment and understanding in all stages, conducting risk assessments is key. This would help evaluate potential risks, and consequences, and allocate resources accordingly.

Emergency: This is your plan for dealing with catastrophic events when all the above fails. Examples include the utilization and consideration for satellite voice and data were the only means of stable communications for days and weeks following the disaster.

Example PACE Chart:

Communications	Voice	Data
PRIMARY		
ALTERNATE		
CONTINGENCY		
EMERGENCY		

Q: How does PACE planning take into consideration NG9-1-1 and policy routing?

A: PACE planning provides a structured framework to support resilient and adaptable communication strategies during emergency situations.

Next Generation 9-1-1 (NG9-1-1) enhances an agency's ability to implement and operationalize their PACE plans in advance. Through NG9-1-1 capabilities, agencies can program call routing and backup procedures to ensure that 9-1-1 calls are answered and routed appropriately—even in disrupted or degraded conditions.

While many agencies have developed PACE plans for routine operations, it is critical to plan beyond day-to-day scenarios. True resilience comes from preparing for the unexpected. Ensuring that all calls are properly routed and answered—regardless of the emergency—helps maintain continuity of service, uphold public safety standards, and ensure no call for help goes unanswered during times of crisis.

Q:	What are call-routing considerations and examples of policy?
A:	NG9-1-1 call routing is dynamic and can be programmed in advance through the Emergency Call Routing Function (ECRF) to accommodate a wide range of operational scenarios. This functionality replaces the legacy "switch on the wall," which manually rerouted calls by physically busying out trunks within the PSAP/ECC. The ECRF uses a sophisticated Policy Store that applies both real-time ("applied") and pre-configured ("pre-staged") rules to ensure that 911 calls are routed correctly based on pre-established policies. Examples of Call Routing Policies: • All call takers are busy — after 24 seconds, route the call to a neighboring PSAP/ECC. • All call takers are busy and the neighboring PSAP/ECC is offline — route the call to the next nearest county. • PSAP/ECC is offline, neighboring PSAP/ECC is busy, and neighboring county is also offline — route the call to an opposite-region PSAP/ECC for processing. These scenarios highlight the importance of proactive planning and coordination—not just with local and neighboring PSAPs/ECCs, but also with regional, opposite-region, and even out-of-state partners. It is critical to build strong relationships with PSAPs/ECCs of similar size and capability who are willing and prepared to assist in times of need. Remember, **9-1-1 calls are processed in milliseconds**. If your PSAP is out of service, it may take time to restore local operations—but call delivery cannot wait. Calls must continue to be routed and answered without delay to ensure uninterrupted emergency services across the state. The ECRF is a powerful, dynamic tool. When supported by well-considered and clearly written policies, it enables **seamless call delivery and exceptional service continuity**, especially within the State of Ohio.

Preventative Maintenance

Q:	Who is responsible for NG9-1-1 hardware maintenance?
A:	Allerium is responsible for the hardware maintenance of all NGCS (Next Generation Core Services) and PSAP (Public Safety Answering Point) equipment. As part of their ongoing responsibilities, a Allerium technician will schedule and conduct maintenance visits to each connected PSAP. These visits will be scheduled in advance by Allerium to ensure coordination with PSAP staff.

Q:	What is entailed with hardware maintenance?
A:	Biannual maintenance includes: During each visit, the technician will perform the following tasks: • Inspect equipment labels for accuracy and visibility • Clean hardware components as needed • Verify and update asset tags • Complete the alarm clearance maintenance • Completion of the Allerium preventative maintenance checklist

Q:	Who pays for BCF (Cisco Edge Router) maintenance?
A:	Cisco Edge Routers may be maintained locally by the agency's IT staff, provided they have the appropriate expertise and support structure in place. If the routers are already covered under an existing Cisco maintenance agreement, they can be included in the agency's regular Cisco maintenance program. Allerium can provide configuration information for those who have infrastructure already in place to meet the requirements also. For agencies that do not have internal support or an active Cisco maintenance plan, maintenance services must be contracted through Allerium to ensure proper support and device management.

Q:	Should the PSAP/ECC Policy Routing Function (PRF) be tested?
A:	It is recommended that each PSAP conduct PRF (Policy Routing Function) functional testing at least quarterly. Regular testing ensures that all programmed functions within the PRF are fully operational and performing as expected. This proactive approach helps maintain system integrity, supports rapid issue identification, and ensures continued compliance with operational and routing requirements. Each PSAP is responsible for testing their network connections. While generally preferred that OARnet be notified of testing, it is not required in simulation testing of PSAP/ESInet outages.

Q:	Who maintains the NG9-1-1 Forest Guide (*aka: phonebook*)?
A:	The Forest Guide is maintained by NG9-1-1 Interoperability Oversight Commission (NIOC). NIOC serves as the independent oversight governance body for the NG9-1-1 Public Key Infrastructure (PKI), Forest Guide, and other technical-interoperability services necessary for the security and smooth functioning of NG9-1-1 systems. Updates are maintained and coordinated via the Ohio 9-1-1 program office.

Q:	Who maintains the master PSAP/ECC directory and listing?
A:	The statewide PSAP/ECC directory and listing is maintained by the Ohio 9-1-1 Program Office. The office maintains and updates the directory regularly to ensure statewide interoperability and compliance with all NG9-1-1 initiatives. A PSAP FCC ID is required for all NG9-1-1 PSAPS/ECC to ensure interoperability and Forest Guide inclusion.

Q:	Should 9-1-1 data maintenance and retention policies be updated?
A:	Absolutely! It is important for agencies to review and update their records retention policies to reflect the expanded data environment associated with Next Generation 9-1-1 (NG9-1-1). Agencies should also conduct periodic reassessments of their systems and policies as technology continues to evolve and mature. When developing an NG9-1-1 retention policy, agencies must account for significantly more data types than were present in legacy 9-1-1 systems. NG9-1-1 environments generate voice, text, multimedia, GIS data, system logs, and operational metadata, each of which may have different legal, operational, and technical retention requirements. Key items to consider and include in a retention policy: • Voice recordings (9-1-1 calls and administrative lines) • Text-to-911 and RTT messaging sessions • Multimedia data (images, video, or sensor data when supported) • Call Detail Records (CDR) and session logs • GIS data and location information (PIDF-LO) • CAD incident records • Radio recordings and communications • ALI/LDB queries and responses NG9-1-1 retention policies should balance legal compliance, operational needs, cybersecurity considerations, and storage management, while ensuring that critical emergency communications data remains available for investigations, audits, public records requests, and overall accountability.

Security and Privacy

Q:	How does the Border Control Function (BCRF) work?
A:	The BCRF in an NG9-1-1 system acts like a firewall. Its primary role is to provide a secure entry point into the Emergency Services IP Network (ESInet) for emergency calls presented to the network. Think of it as a security guard at the entrance to the NG9-1-1 network. It helps control and manage the flow of incoming emergency calls, ensuring only authorized and legitimate traffic enters the system.

Q:	Who maintains the BCRF?
A:	BCRF maintenance is maintained by Allerium, who ensures upgrades, compliance, and connectivity to the Ohio NGCS.

Q:	What role does the PSAP play in security?
A:	PSAPs act as the first line of defense for NG9-1-1 security at the local level. Their efforts to secure their infrastructure, protect data, collaborate with providers, and train their personnel are critical to maintaining the trustworthiness and reliability of the entire system.

Q:	Where are the best cybersecurity resources and training for the NG9-1-1 PSAP/ECC?
A:	The Cybersecurity & Infrastructure Security Agency (CISA) maintains a **9-1-1 Cybersecurity Resource Hub**, which offers information, training, and best practices for Public Safety Answering Points (PSAPs) and Emergency Communications Centers (ECCs). This resource is available at the following link: https://www.cisa.gov/911-cybersecurity-resource-hub

Q:	Are there cybersecurity considerations and recommendations?
A:	A comprehensive cybersecurity policy and recommendations guide is available through the Ohio 9-1-1 Program Office to assist PSAPs and ECCs in implementing appropriate safeguards. While this guide provides valuable best practices, it is ultimately the responsibility of each local PSAP/ECC to ensure these practices are properly implemented and enforced within their environment. All Call Handling Equipment (CHE) vendors must adhere to the strict cybersecurity standards defined by NENA NG-SEC (STA-040.2-2024). These standards outline essential protections for NG9-1-1 systems to maintain operational integrity and secure emergency communications. In addition, all PSAP/ECC personnel should receive annual cybersecurity training to reinforce best practices and ensure a consistent, statewide approach to cybersecurity. This is critical to protecting call delivery, safeguarding sensitive data, and preventing disruptions to emergency services across Ohio.

Q:	Does your PSAPs and CHE meet security standards for connection?
A:	CHE contracted agencies should request and maintain on file the current **NENA-REF-012.1-2025 Security Audit Checklist** from their vendor to ensure that their chosen Call Handling Equipment (CHE) meets the required security provisions. Additionally, every PSAP should ensure compliance with the requirements outlined in **NENA-STA-040.2-2024**, which establishes the applicable security standards for NG9-1-1 systems and associated operational environments. Regular review of these standards and vendor documentation helps ensure that systems remain aligned with current security expectations and industry best practices.

System Maintenance

Q:	How do I know if Maintenance Notifications pertain to Ohio?
A:	All Allerium maintenance notifications that are distributed pertain to the Ohio NGCS. While some of these notifications may reference locations such as Dallas or Arizona, they still impact on the Ohio NGCS. This includes services such as Text-to-911 and other ancillary features supported through the Ohio NGCS. Each notification provides detailed information about the scheduled maintenance or upgrade, including the potential impact to customer services. Please keep in mind: If any issues arise during a maintenance window, contact the Allerium NOC immediately, using the contact details provided in the notification.

Q:	Does Ohio NGCS have a set maintenance schedule?
A:	Yes, the Ohio 9-1-1 Office reviews and approves all NG9-1-1 maintenance windows. Each maintenance window undergoes a rigorous review process prior to being scheduled, including thorough evaluation of all documentation, rollback procedures, and potential service impacts. Currently, there is a set schedule for maintenance to occur on Tuesdays and Thursdays, with all work completed by 16:00 hours. • Fridays are excluded from regularly scheduled maintenance. • Wednesdays are also avoided, as other maintenance activities and windows are already scheduled on those days. This approach helps ensure minimal disruption while maintaining the integrity and reliability of the Ohio NG9-1-1 system.

Q:	What is the current NGCS maintenance schedule?
A:	**Ohio ESInet and NGCS Maintenance and Upgrade Windows**

Monthly	Monday	Tuesday	Wednesday	Thursday	Friday
Week 1	SOI			SOI	EmergMaint Only
Week 2	SOI	Guardian 0700-1600	EmergMaint Only	SOI	EmergMaint Only
Week 3	SOI	NGCS CLE 0700-1600	EmergMaint Only	SOI	EmergMaint Only
Week 4	SOI	NGCS COL 0700-1600	EmergMaint Only	SOI	EmergMaint Only

Telecommunications Service Priority

Q:	How does an agency ensure priority service?
A:	Once your agency has successfully connected and established connectivity through the Ohio ESInet and Emergency Communications Network to Next Generation 9-1-1 Core Services (NGCS), you must register and obtain Telecommunications Service Priority (TSP) codes for your connections. These codes can then be provided to your last-mile service provider so the circuits can be properly tagged and designated for priority restoration in the event of an outage, fiber cut, or other service disruption. Registering for Telecommunications Service Priority (TSP) codes through the Cybersecurity and Infrastructure Security Agency (CISA) requires submitting a request to the Department of Homeland Security (DHS) to prioritize the installation or restoration of critical voice and data circuits. This program is intended for organizations supporting national security, emergency preparedness, healthcare, and public safety operations. Obtaining TSP codes ensures that the circuits supporting NG9-1-1 and emergency communications infrastructure receive the highest available priority for repair and restoration during service disruptions. Once issued, these codes should be provided to the circuit provider so they can be associated with the appropriate connections supporting the ESInet. Here is how to register for TSP codes: **1. Identify Your Point of Contact (POC)** • **Establish a POC:** If your organization is new to the program, you must first establish a point of contact to manage the enrollment. • **Contact CISA:** Call the Priority Telecommunications Service Center at **866-627-2255** or email **support@gwids.cisa.gov** to start the process. **2. Submit the Application (Form SF315 – OMB No 1670-005)** • **Fill out Form SF315:** Complete the "Telecommunications Service Priority Request for Service Users" form, also known as SF315. • **Specify Services:** Identify each specific circuit, telephone line, or data service that require priority coverage. • **Submit to DHS:** Send the completed form to the DHS Priority Telecommunications Service Center via email at tsp@cisa.dhs.gov. **3. Verification and Authorization** • **Review Period:** The Service Center reviews applications within 5 business days. • **Approval:** Once approved, the TSP Program Office will issue a unique **TSP Authorization Code** for each circuit, usually within 30 days.

	4. Provide Codes to Service Vendors • **Submit to Vendor:** Take the TSP Authorization Codes and submit them to your telecommunications service provider (e.g., AT&T, Verizon, Comcast). • **Finalization:** The vendor will update their systems to prioritize your lines for restoration or installation. **Important Considerations** • **Eligibility:** You must certify that your service supports national security/emergency preparedness (NS/EP) functions. • **Non-Federal Entities:** If you are not a federal agency, you may require a federal sponsor to enroll. • **Validity:** TSP codes are valid for 3 years, after which they must be revalidated. • **Cost:** While enrollment is managed by CISA, service providers may charge fees (*approximately $100 for enrollment, ~$3 monthly per line*). Once registered, develop an internal process to track and reaffirm your TSP codes, as all Telecommunications Service Priority (TSP) codes expire and must be reaffirmed every three years. This reaffirmation can be completed through the CISA reaffirmation process and associated filings. TSP codes should be stored securely and maintained as part of your organization's Continuity of Operations Plan (COOP). They should also be reviewed periodically to ensure the information remains accurate and up to date. Additionally, verify that the designated primary Point of Contact (POC) remains current and on file. Maintaining accurate contact information is critical in the event that priority restoration or coordination is required during a service disruption. Further information available within the TSP Code FAQ.

Call Handling Equipment (CHE)

Q:	Looking at new CHE, what options area available?
A:	All Allerium maintenance notifications that are distributed pertain to the Ohio NGCS. While some of these notifications may reference locations such as Dallas or Arizona, they still impact on the Ohio NGCS. This includes services such as Text-to-911 and other ancillary features supported through the Ohio NGCS. Each notification provides detailed information about the scheduled maintenance or upgrade, including the potential impact to customer services. Please keep in mind: If any issues arise during a maintenance window, contact the Allerium NOC immediately, using the contact details provided in the notification.

Q:	What standard function must NG9-1-1 CHE have?
A:	Currently, CHE needs to be able to meet the NENA i3 2021 standards version f. Basical functionality requirements are as follows: • Full Session Imitation Protocol (SIP) support for call delivery and adherence to the NENA-STA-010.3f-2021. • Capability to process rich data, including location information, text, video, and automatic crash notification. • Capabilities for GIS-based routing (location mapping) and integration with Computer-Aided Dispatch (CAD) via Emergency Incident Data Object (EIDO) • Strict adherence to security standards to prevent unauthorized access and industry-standard cybersecurity. • Mandatory lab certification from iCERT and passage within the Ohio CHE Lab environment for the version software version procured. • Full compliance with NENA-STA-040.2-2024 and Type II SOC 2 for NG9-1-1 and all vendors should provide yearly compliance documentation to have on file.

Q:	What options are available in CHE solutions?
A:	There are four primary models for call handling software currently available in the market: 1. **On-premise servers and software** – The call handling equipment (CHE) is hosted locally within the PSAP using on-site servers and infrastructure maintained by the agency or its vendor. 2. **Hosted software (off-premise solution)** – The call handling software is hosted by a provider in a remote data center environment. Examples include state-hosted solutions such as Guardian or vendor-hosted platforms provided by companies such as Frontier, AT&T, or InDigital.

	3. **Cloud-based software** – The software is deployed within commercial cloud infrastructure such as Amazon Web Services (AWS) or Microsoft Azure. In this model, the application is typically hosted within the cloud environment but may still follow traditional software architecture. 4. **Cloud-native software** – The application is specifically designed and built for cloud environments using cloud-native architecture and microservices. These platforms are developed to fully leverage cloud scalability, resilience, and distributed services.

Q:	What should be considered when purchasing new CHE?
A:	1. Do you have the internal IT support and resources necessary to manage and maintain the solution in-house? 2. Do you prefer a capital expenditure (CapEx) model with upfront infrastructure investment, or a software-as-a-service (SaaS) model with ongoing subscription costs? 3. What are the "must-have" capabilities and operational requirements for your county and 9-1-1 center? 4. What type of backup or redundancy solution will be required to ensure continuity of operations? 5. What are the ongoing costs, licensing structures, and maintenance agreements associated with each option? 6. What will the CHE require to connect to the Ohio ESInet and NGCS?

Q:	Are there any special considerations regarding CHE and the NGCS?
A:	Yes. Once you have selected the vendor and solution your agency wishes to procure, the following steps should be considered: • Check Ohio Buys to determine whether the CHE solution is available through a cooperative purchasing contract. • Consult with the Ohio 9-1-1 Office regarding vendor connectivity requirements and overall system design. • Discuss the purchase with the Ohio NG9-1-1 Manager to ensure connectivity, functionality, and compliance with applicable NENA standards. • Review the current list of CHE solutions and supported software versions to confirm compatibility with the Ohio NGCS. • Obtain documentation from the CHE vendor confirming full compliance with NENA-STA-040.2-2024 and Type II SOC 2 requirements for NG9-1-1 environments and require updated documentation on an annual basis. • Require the prospective vendor adherence to NENA-REF-012.1 Security Audit Checklist and provide a updated copy yearly.

Q:	What should be considered when changing CHE after being connected to the Ohio ESInet and NGCS?
A:	There are several factors that must be considered if a CHE change is made after a PSAP is already connected and operational on the Ohio ESInet and NGCS: • Consult with the Ohio 9-1-1 Office and the NG9-1-1 Program Manager to review the proposed change and understand any potential impacts to NGCS connectivity and operations. • Submit a request for a quote and complete a Service Enhancement Request Form (SERF) with Allerium to initiate the formal process and determine what will be required to support the change. • Evaluate potential network impacts, including any necessary changes to circuits, routing, connectivity, or security configurations. • Review the current network topology, security posture, and contractual agreements to ensure alignment with NG9-1-1 standards and operational requirements. • Assess impacts to integrated systems, including CAD, voice recording platforms, logging systems, and any other equipment that interfaces with the CHE. These considerations help ensure that any transition to a new CHE platform is coordinated properly and does not disrupt existing NG9-1-1 services or ESInet connectivity.

Troubleshooting

Q:	Who should I contact if there is a 9-1-1 issue?
A:	The Allerium NSOC (Network Security Operations Center) is available 24/7/365 for any services related issues. It serves as the single point of contact for all customer inquiries—including reporting, escalating, and receiving status updates on incidents as well as other communications—and provides rapid access to a live technician. The NSOC serves more broadly as the customer service center for the life of the contract: • The center of all support requests and communications • The center of program operations • The liaison between the State/PSAPs, technical staff, partners, vendors, and other personnel tasked with supporting this project. Agencies are required to develop standard operating procedures (SOPs) and internal guidelines for PSAP personnel that clearly define when and under what circumstances the NSOC (Network Security Operations Center) should be contacted. Training is provided to ensure PSAP staff are familiar with NSOC procedures, as well as the change management policies and interaction guidelines related to Allerium. This training supports consistent communication, proper escalation, and adherence to operational protocols during service or network events. The NSOC can be contacted at 866.264.0911 or nsoc@comtech.com

Q:	Who do I contact if CAD is not receiving 9-1-1 data?
A:	Contact your CAD vendor to make sure the service is running to receive 911 data. At the same time contact the NSOC to advise them and update them with your CAD vendor contact information and ticket # so they can interact on your behalf should the need arise.

Q:	Who do I contact if we need to abandon our PSAP/ECC?
A:	Contact the NSOC and they can immediately reroute calls based upon your pre-programmed policy routing functions: Allerium NSOC: 866.264.0911 Contact the Ohio 9-1-1 Program Office also, so we can assist in your successful transition and ensure 9-1-1 continuity of service.

FAQs

Q: How has the NG9-1-1 Class of Service (COS) changed?

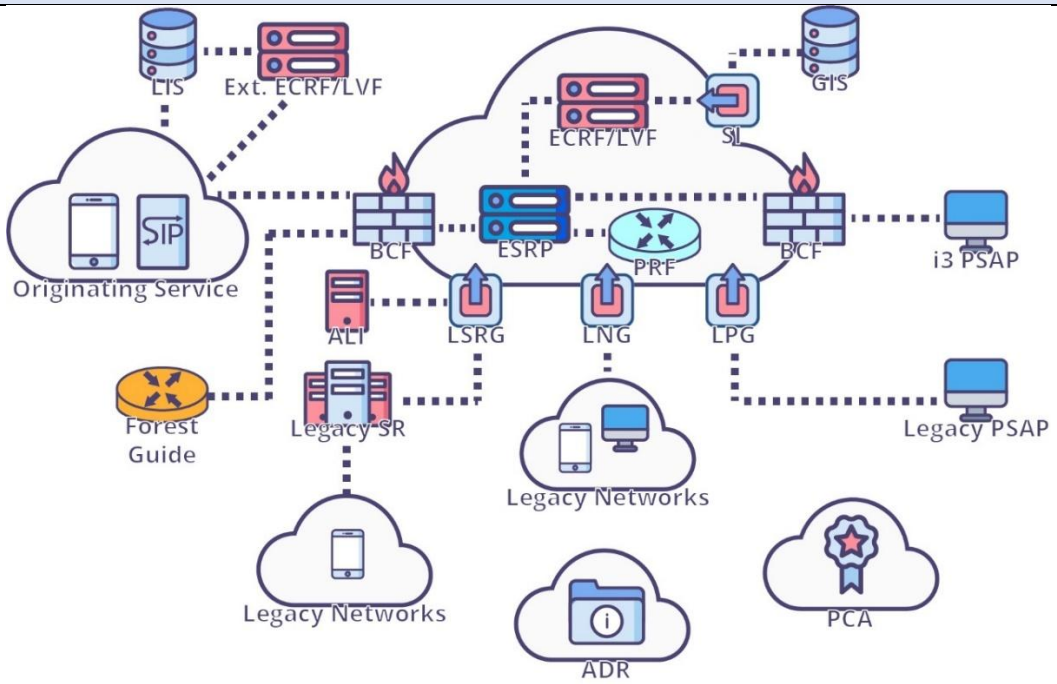
A: The implementation of Next Generation 9-1-1 (NG9-1-1) changes how Class of Service (CoS) is designated and reported by carriers to the NG9-1-1 Core Services (NGCS). The chart below outlines the current Class of Service designations and their translations as recognized within the 9-1-1 industry.

Description	Carrier Code	NENA COS Code	NG9-1-1 Service Type
Residence	1	RESD	POTS
Business	2	BUSN	POTS
Residence PBX	3	PBXR	MLTS-Local
Business PBX	4	PBXB	MLTS-Local
Centrex	5	CNTX	MLTS-Hosted
Coin 1 Way	6	PAY$	Coin; One way
Coin 2 way	7	COIN	Coin
Mobile, Wireless Phase 0	8	MOBL	Wireless
Residence OPX	9	RESX	POTS; OPX
Business OPX	0	BSNX	POTS; OPX
Customer owned coin telephone	A	COCT	COIN
VoIP Residential	C	VRES	Digital
VoIP Business	D	VBUS	Digital
VoIP coin/pay phone	E	VPAY	Digital; COIN
VoIP wireless	F	OBML	Digital; Wireless
Wireless Phase 1	G	WRLS	Wireless
Wireless Phase 2	H	WPH2	Wireless
Wireless Phase 2 with Phase 1 info	I	WHP1	Wireless
VoIP Nomadic	J	VNOM	Digital
VoIP enterprise solution	K	VENT	Digital
Wireless E9-1-1 Civic address	O	WCVC	Digital
Wireless E9-1-1 Dispatchable location 1	P	WDL1	Digital
Wireless E9-1-1 Dispatchable location 2	Q	WDL2	Digital
Supplemental Geodetic Location from Third-Party	R	SDXY	OTT
Telematics	T	TLMA	OTT
VoIP default COS	V	VOIP	Digital
Mobile	W	WRLS	Wireless

*Note: This table is likely to be updated as ATIS, IETF, and NENA continues to update the NG9-1-1 Method of Service Type.

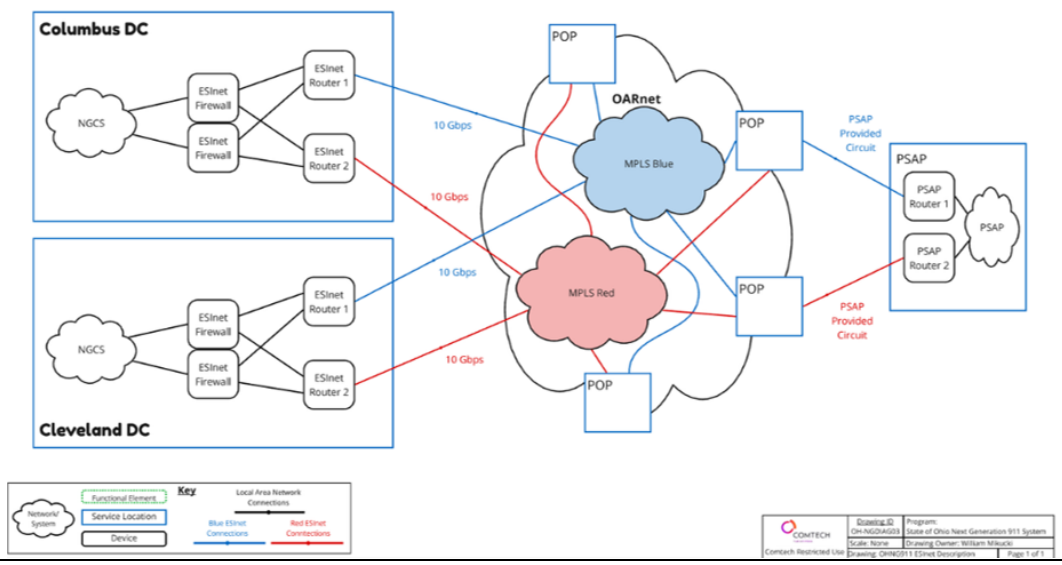
Q: What does the complete ESInet topology look like with respect to NG9-1-1?

A:



Q: What does the Ohio ESInet topology look like?

A:



Q:	What are important elements in the CHE call screen and the changes that will be displayed for call takers with NG9-1-1?
A:	Call Handling Equipment (CHE) utilizing Next Generation 9-1-1 (NG9-1-1) should display full CLDXF (Civic Location Data Exchange Format) information to the call-taker. NG9-1-1 is built around the CLDXF standard, which requires no abbreviations in address data—including street address, city, state, ZIP code, and emergency service providers for the location. This approach reduces the risk of errors and enhances interoperability, ensuring that fully NG9-1-1–enabled locations and i3-compliant PSAPs can deliver seamless and consistent service across regions, states, and the entire United States.

Q:	What happens to Emergency Service Numbers (ESN) in NG9-1-1?
A:	With NG9-1-1, the process of routing emergency calls is shifting from static legacy systems to dynamic, location-based services. Traditional Enhanced 9-1-1 (E9-1-1) systems rely on Emergency Service Numbers (ESNs) and Master Street Address Guide (MSAG) databases to route calls to the appropriate Public Safety Answering Point (PSAP). These systems require extensive maintenance and are tied to fixed address data. NG9-1-1 eliminates the need for ESNs and MSAG maintenance by leveraging Geographic Information System (GIS) data for geospatial call routing. This allows the Emergency Call Routing Function (ECRF) within the NG9-1-1 Core Services (NGCS) to determine the caller's precise location in real time and route the call to the correct PSAP or Emergency Communications Center (ECC) based on actual geographic boundaries. As a result, the legacy ESN-based routing framework is being deprecated in favor of more accurate, flexible, and future-proof geospatial solutions. ESN and MSAG maintenance will be depreciated following full NG9-1-1 implementation and compliance.

Q:	How often should the LDB be checked for discrepancies?
A:	The Location Database (LDB) discrepancy report should be reviewed daily, especially during the initial implementation phase. During this period, a high volume of issues may arise—particularly if the Master Street Address Guide (MSAG) has not been maintained locally in accordance with NENA standards. After this initial phase, the LDB discrepancy report may be reviewed weekly, once the volume of issues stabilizes. Eventually, as full NG9-1-1 implementation is completed statewide and the transition away from the LDB is finalized, ongoing processes should be established to ensure data accuracy and compliance with statewide update requirements.

Q:	Who should have access to the Location Database (LDB)?
A:	Access to the Location Database (LDB) should be highly restricted. When assigning access, it should be limited to personnel directly involved with 9-1-1 address management, GIS, and 9-1-1 operations. Best practice is to ensure that designated personnel are properly trained and understand the importance of the LDB, including how to monitor, maintain, and update the critical data and functions contained within the system. Careful management of access and responsibilities helps ensure the integrity and accuracy of location data that supports NG9-1-1 call routing and emergency response. Recommended personnel with LDB access: • 9-1-1 Coordinator • County GIS Administrator • GIS Analyst / Technician • PSAP Administrator It will be imperative regular maintenance of the LDB will need to be completed as many meet weekly to update and address issues after migration to generate a regular cadence.

Q:	How does Windows 10 End of Life impact 9-1-1?
A:	Microsoft has announced that **Windows 10 will reach end of support on October 14, 2025**. After this date, Microsoft will no longer provide free security updates, technical assistance, or feature updates for Windows 10. As a result, any computers still running Windows 10 will become increasingly vulnerable to security threats. This poses a significant risk to systems connected to the 911 network. Public Safety Answering Points (PSAPs) and Emergency Communications Centers (ECCs) must prepare and plan for the replacement or upgrade of all Windows 10 operating systems on 9-1-1 network-connected devices. Due to the increased exposure and vulnerability after October 14, 2025, NGCS (Next Generation Core Services) connectivity will be heavily monitored. To minimize operational and cybersecurity risks, it is strongly recommended that all Windows 10 devices be upgraded as soon as possible, with a final compliance deadline of **December 31, 2025**. Please begin assessment and planning efforts immediately to ensure uninterrupted service and continued compliance.

Q:	How do I ensure my county is ready for NG9-1-1?
A:	*The Are You Ready?* document is posted on the Ohio 9-1-1 Program website. PSAPs/ECCs should reference the checklist (*page one*) and ensure the county is ready and has all the information completed and documented for items 1-4. Consider any current contractual agreements in place along with other timelines or projects pending.

Q:	What are the phases of implementation for NG9-1-1?
A:	Since the FCC Report and Order, as each PSAP/ECC is connected to the NGCS, the migration process for carriers begins on a county-by-county basis following successful deployment. The 9-1-1 Program Office will file all Phase One Certification Letter with the FCC and notify the carriers that the county has transitioned and is ready to begin Phase One implementation. Phase One ensures that all 9-1-1 calls are delivered via SIP. Once this is complete, a Phase Two Certification Letter will be submitted, initiating the processes required to include location data within the SIP PIDF-LO.

Q:	Does the PSAP have to have an FCC ID?
A:	Yes, all Public Safety Answering Points (PSAPs) and Emergency Communications Centers (ECCs) operating on the Next Generation Core Services (NGCS) must have an FCC Registration ID. Obtaining an FCC ID is free of charge and involves a few key steps, outlined below: Steps to Obtain an FCC Registration ID 1. **Register with CORES (Commission Registration System):** PSAPs must first register with the FCC's CORES system to obtain a FCC Registration Number (FRN). This FRN serves as a unique identifier for all FCC-related transactions. CORES Registration Portal 2. **Register in the FCC Text-to-911 Registry:** PSAPs must then register in the FCC's Text-to-911 Registry, which enables them to receive emergency text messages. This registration also informs wireless carriers that the PSAP is ready to support text-to-911 communications. Text-to-911 Registry Information *(Comtech will assist in this process for those already implemented with Text-to-911 service and further assist with those implementing the service for the first time through the Ohio NGCS.)* 3. **Update the Master PSAP Registry:** PSAPs can also update their information in the FCC Master PSAP Registry, which supports the implementation of Enhanced 9-1-1 services. To update registry details, PSAPs can email: fccpsapregistryupdate@fcc.gov If you have questions or need assistance during this process, please contact the appropriate FCC support resources or your NG9-1-1 project lead.

Q:	Can our agency continue to get automated alarms on the NGCS?
A:	Yes! The Ohio NGCS and SMS Text-to-911 service does support alarm messages that are submitted by alarm companies to the Allerium Text Control Center (TCC). This capability is included as part of the Ohio NGCS solution. During migration planning meetings, agencies should confirm whether alarm center processing through the TCC is already enabled for their PSAP. Ensuring the project team is aware of this configuration will help avoid any disruption to existing alarm messaging workflows. Once a PSAP migrates from legacy services to the Ohio NGCS and TCC platform, alarm messaging will transition along with the rest of the services as part of the migration process. This ensures continuity of alarm notifications and messaging once the agency is operating within the NG9-1-1 environment.

Q:	How can my agency enable alarm center processing through the Ohio NGCS?
A:	Contact the alarm company (ie. ADT) directly and advise them that your agency wishes to have integrated alarm communications enabled through their Text-to-911 gateway. Request confirmation that their platform meets or supports NG9-1-1 messaging standards. Once this request has been made, be sure to complete an Allerium Service Enhancement Request Form (SERF) through the UpSkill Portal so the service can be properly routed, reviewed, and coordinated for implementation.

Q:	What is IoT testing?
A:	IoT testing (Internet of Things testing) is the process of verifying that connected devices, sensors, applications, and networks work correctly, securely, and reliably when they communicate with each other and backend systems. IoT systems typically include physical devices, connectivity networks, cloud platforms, and software applications, so testing ensures all components interact properly under real-world conditions. All software, hardware, and applications connected to the Ohio ESInet and NGCs must complete and pass IoT testing prior to implementation and deployment. There is then a second testing requirement for any new solution to pass acceptance testing by the State of Ohio and that of the customer prior to implementation.

Appendix

Sample MOU PSAP Mutual Boundary Agreement

Public-Safety Answering Point Mutual Boundary Agreement

THIS AGREEMENT is made and entered into this __(Day)__ day of ___(Month)_____, _(Year), by and between ***County A*** or its delegate and ***County B*** or its delegate (hereinafter "PARTIES") situated in the State of Ohio.

WHEREAS, the above PARTIES share a mutual PSAP boundary line; and,

WHEREAS, the PARTIES desire to resolve any conflicts that may arise by adjusting the mutual boundary line.

NOW, THEREFORE, the PARTIES agree as follows:

1. The boundary line between PARTIES is defined as such (either a physical GIS boundary or a statement of the GIS layer name, source, and creation date of the agreed upon layer [for example OH County Boundaries, DNR, 7/16/2018]).

2. County A or its delegate does hereby agree to not alter or change their mutual boundary with County B or its delegate without a new Mutual Boundary Agreement.

3. County B or its delegate does hereby agree to not alter or change their mutual boundary with County A or its delegate without a new Mutual Boundary Agreement.

4. The PARTIES will notify the Ohio Office of First Responder Communications, 9-1-1 Program of the change in their common boundary,

5. This agreement represents the entire agreement between the PARTIES.

Sample PSAP Key Emergency Contacts

PSAP KEY EMERGENCY CONTACTS

Agency:

Updated:

Category	Vendor/Service	Contact Name	24/7 Phone (Office)	After-Hours	Email	Account/ Contract #	SLA Response
State 911 Administrator	Ohio 911 Office	Patrick Brandt	(614) 728-0342	(614) 728-0342	Patrick.Brandt@das.ohio.gov		
State NG911 Program Manager	Ohio 911 Office	Ken Stewart	(614) 728-8589	(614) 728-8589	Kenneth.Stewart@das.ohio.gov		
9-1-1 System	NGCS Service Provider	Allerium NOC	(800) 959-3749	(800) 959-3749	nsoc@comtech.com		
9-1-1 CHE	Call Handling Equipment / Software						
9-1-1 System	CAD (Computer Aided Dispatch)						
9-1-1 System	Logging Recorder						
9-1-1 EC Network	Emergency Communications Network (ESInet)	OARnet NOC	(800) 627-6420	(800) 627-6420	oarnetnoc@service-now.com		
9-1-1 Last Mile Service (1)	Fiber Network Provider						
9-1-1 Last Mile Service (2)	Fiber Network Provider						
9-1-1 Last Mile Service (3)	Fiber Network Provider						
Radio	Radio System/Console						
Network	Internet Service Provider (ISP)						
IT/Security	Network Security/Firewall						
Facilities	Electrical/Power Utility						
Facilities	UPS Maintenance						
Facilities	Generator Maintenance						
Facilities	HVAC (Heating/AC)						
Security	Alarm/Physical Security						
LEADS	NLETS/LEADS/NCIC	LEADS NOC	(800) 589-2077	(800) 589-2077			

Glossary

NENA (National Emergency Number Association) glossary of terms is a comprehensive list of definitions and acronyms specific to the 9-1-1 emergency services community. It's a resource for understanding the terminology used in NENA standards, documents, and other publications related to 9-1-1.

The NENA glossary can be found here: https://kb.nena.org/wiki/Category:Glossary

Contact Support

Name	Email	Phone
Allerium NSOC	NSOC@comtech.com	866-264-0911
Ohio 9-1-1 Program Office	Ohio9-1-1@DAS.Ohio.gov	614.728.2114
OGRIP	gis.support@das.ohio.gov	614.466.4747
OARnet		800.627.6420

NG9-1-1 Project Support

Name	Email	Phone
Ken Stewart, OH NG9-1-1 Program Manager	Stewart.Kenneth@das.ohio.gov	614.728.8589
Stacey Ferguson, Allerium Program Manager Ohio	Stacey.Ferguson@comtech.com	517.302.3913
TBA, Allerium Project Manager	TBA@comtech.com	
Patrick Brandt, OH 9-1-1 Administrator	Brandt.Patrick@das.ohio.gov	614.728.0342

Release Notes

- **v1.0**: Initial release of Ohio NGCS information FAQ regarding Ohio deployment, connectivity, and general NG9-1-1 information.
- **v1.1**: System Maintenance section added.
- **v2.0:** Telecommunication Service Priority section added
- **v2.0:** Updated NG9-1-1 Project Support Contacts
- **v2.0:** Added CHE Guidance
- **v2.0:** Updated Security and Privacy
    - **Added:** Does your PSAP and CHE meet the security requirements for connection?
- **v2.0**: Updated: FAQs
    - **Updated:** Who should have access to the LDB?
    - **Added:** Can our agency continue to get automated alarms on the NGCS?
    - **Added:** How can my agency enable alarm center processing through the Ohio NGCS?
    - **Added:** What is IoT testing?
- **v2.0**: Added: Appendix
    - **Added**: Generic Sample GIS Boundary MOU
    - **Added**: Sample PSAP Key Emergency Contact List
- **v2.0**: Updated: Preventative Maintenance
    - **Added**: Should 9-1-1 data maintenance and retention policies be updated?
- **V2.0** System Maintenance
    - **Added**: What is the current NGCS maintenance schedule?
- **V2.0**: Updated: NG9-1-1 Project Support
    - Updated: Allerium Program Manager
    - Removed: Allerium Project Manager

Acknowledgments

Ohio Geographically Referenced Information Program (OGRIP)

National Emergency Number Association (NENA)

Association of Public-Safety Communications Officials (APCO)

National Association of State 9-1-1 Administrators (NASNA)

NHTSA National 9-1-1 Program (911.gov)

Comtech

Allerium

Datamark Technologies

Conclusion

We hope this guide has been helpful in answering your questions about the Ohio NG9-1-1 System Throughout this guide, we have provided an overview of key features, usage instructions, and best practices to help you get the most out of the platform—particularly in relation to the implementation and functionality of Next Generation 9-1-1 (NG9-1-1).

To summarize:

- NG9-1-1 is a comprehensive system made up of Emergency Services IP Networks (ESInets), IP-based software services and applications, databases, and data management processes, all interconnected with Public Safety Answering Point (PSAP) premise equipment.
- The system enables location-based call routing to the appropriate emergency service entity, utilizing available data elements and business policies to improve routing accuracy.
- It supports the seamless transfer of emergency calls and associated data to other NG9-1-1–capable PSAPs or authorized entities.
- NG9-1-1 offers standardized interfaces for voice and multimedia message services and is capable of handling all types of emergency communications.
- It retains full support for traditional E9-1-1 features, while also meeting the evolving needs of modern emergency communication systems.

If you have any further questions or encounter any issues while using our platform, please don't hesitate to contact our office using the information provided in the Contact Support section of this guide.

Thank you for connecting to the Ohio NGCS. We are committed to supporting your transition to NG9-1-1 and ensuring you are equipped to deliver reliable, accurate, and interoperable emergency services.

Disclaimer

This FAQ is intended to provide general information and should not be considered professional advice. While every effort is made to ensure the information is accurate and up to date, we make no guarantees regarding its completeness or accuracy.

Users should not rely solely on the content of this FAQ and are encouraged to consult with a qualified professional for specific guidance related to their individual circumstances.

We assume no responsibility for any errors, omissions, or actions taken based on the information provided herein.