TECHNOLOGY

INTRODUCTION

Public safety faces several challenges today with technology:

The introduction of IP-based broadband technology creates a game-changing opportunity for PSAPs to build in interoperability, security, economies of scale, a broad and competitive marketplace, and innovation from the start.

- Networks, services, and equipment may be costly, siloed, and proprietary
- The vendor community is specialized and small
- 9-1-1 authorities have little bargaining power and few options
- Interoperability is difficult and expensive to achieve, especially after-the-fact
- Innovation is limited and disconnected from advances in the consumer marketplace
- Upgrades are disruptive
- Consumer/user expectations are far removed from reality
- Cybersecurity must be part of the design and implementation from the outset

The introduction of IP-based broadband technology creates a game-changing opportunity for PSAPs to build in interoperability, security, economies of scale, a broad and competitive marketplace, and innovation from the start. The equipment and systems necessary to deliver and process IP-based communications from the point of entry into the PSAP and between public safety entities will change significantly. Evaluation of widely deployed commercial standards and existing consensus-based, accredited standards, best practices, and open system architecture will reveal opportunities for changes necessary to meet the needs of a broadband environment. It is important to note that the broadband implications to the PSAP encompass a full range of technologies including systems specific to public safety and those used by the general public.

Figure 4. **The Future Emergency Communications Technology Ecosystem**

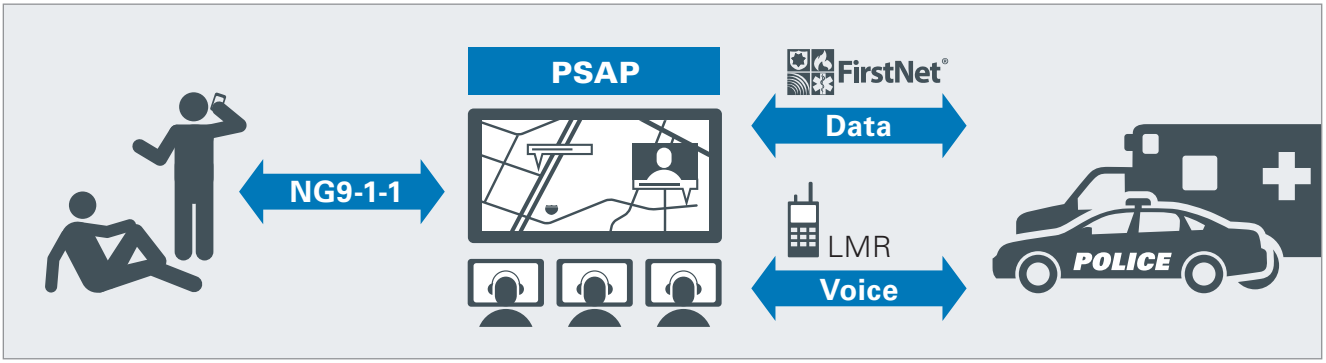
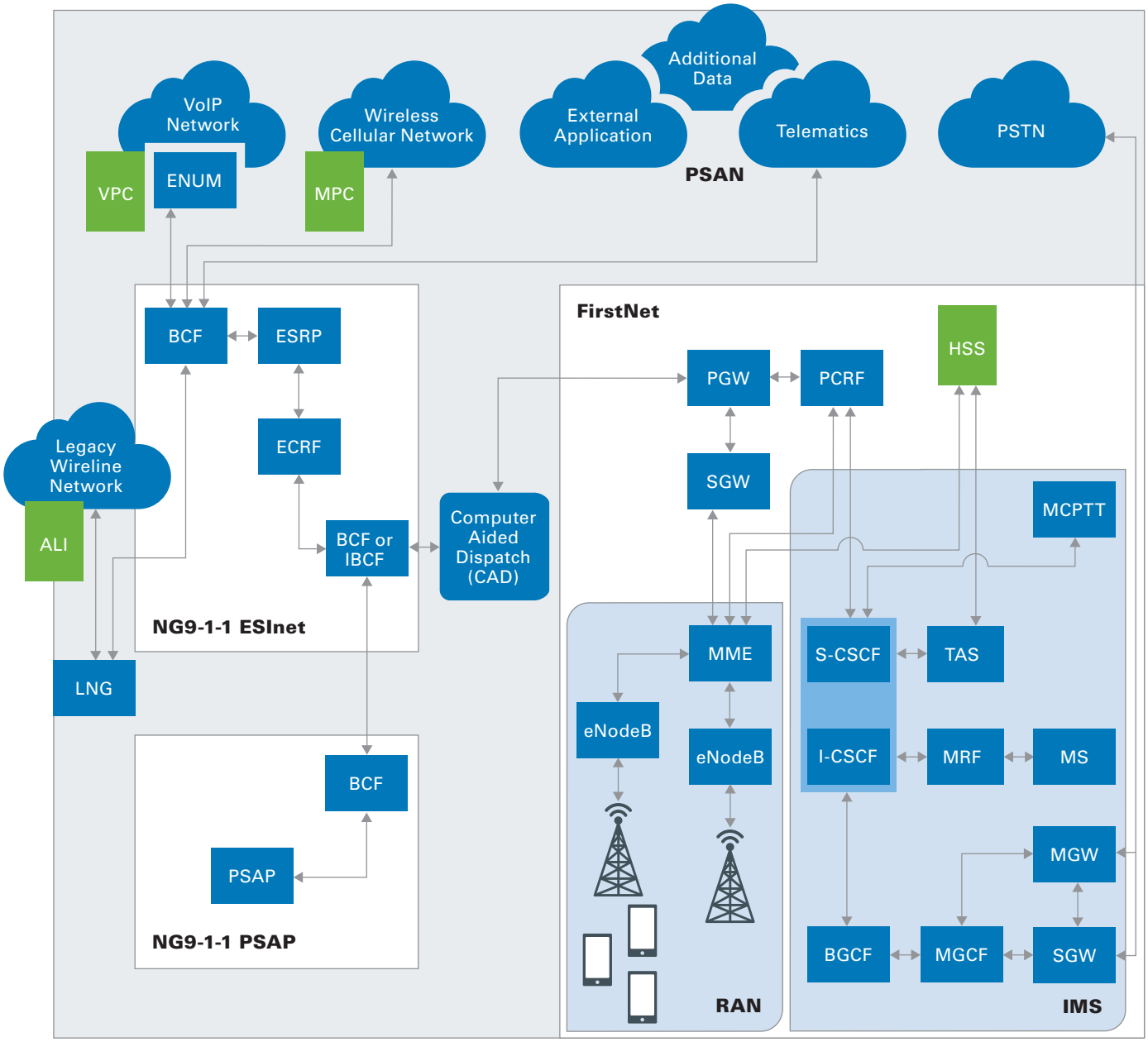


Figure 5. **Conceptual Diagram for Integration of NG9-1-1 and the NPSBN**[73]



THE TECHNOLOGY ROLE

Broadband technology supports voice, data, text, photographic, telemetry, video, and multimedia communications. These technologies create opportunities to improve interoperability, resiliency, quality of service, analytics, information sharing across PSAPs and other entities, alignment with advances in the commercial sector, and customization. Broadband will significantly enhance PSAPs' ability to initiate the response to emergencies and serve as the nerve center for the emergency response. This will require managing inputs from the public via NG9-1-1, interfacing with first responders through LMR networks and the NPSBN, and addressing a variety of challenges introduced by broadband technologies. Figures 4 and 5 and the following sections are intended to help illustrate the implications of a variety of broadband-related issues for PSAPs. For a related list of functional elements associated with the integration of NG9-1-1 and the NPSBN, see Appendix 5.

NG9-1-1

NG9-1-1 lacks a universally-accepted definition, an issue introduced in the Executive Summary and that is explored further in the Findings and Recommendations sections. A general theme for discussions of NG9-1-1 is that modern technology will enable more effective communication between the public and PSAPs while allowing for dynamic communication among interconnected public safety agencies.

The legacy 9-1-1 network is based on analog, circuit-switched technology. Aside from limited data capabilities and add-ons to support wireless, VoIP, and SMS text, the system has not significantly changed in more than 40 years. Transitioning to IP-based networks for NG9-1-1 will entail significant changes for PSAP systems and equipment.

Most recently, elements of IP-based services are being added to the legacy system, such as ESInets and IP selective routers, as well as IP capabilities introduced into CAD, RMS, mapping systems, and some dispatch consoles. While not all of these IP features can be realized until a fully deployed NG9-1-1 system is implemented, they do already begin to introduce risks inherent to IP networks, including cybersecurity, connectivity, reliability, and redundancy. Thus, this transition must involve discussion of the processes needed to guide implementation in a secure manner that also meets public safety requirements.

The Flexibility of IP-Based Solutions

In a legacy environment, there is limited ability to reroute a call when circumstances might necessitate doing so, and no guarantee that a rerouted call will arrive with basic caller and location information, let alone CAD records. An IP environment provides significant flexibility in the ways that calls can be routed, distributed, and delivered within an individual PSAP, as well as between interconnected IP-based PSAPs. Additionally, IP technology affords new abilities to analyze call characteristics that in turn could help optimize many aspects of operations including the transfer of calls.

In the case of a major disaster, an IP environment offers even greater advantages in terms of redundancy and resiliency. In the legacy Centralized Automatic Message Accounting (CAMA) world, call rerouting options are limited. If a large PSAP without a backup center becomes inoperable, the rerouted call volume can overwhelm a neighboring, smaller operation. In an IP environment, however, calls can be rerouted quickly and easily based upon established call handling system capabilities in conjunction with policies that are designed to distribute call loads efficiently and effectively across numerous PSAPs as desired by the 9-1-1 authority.

One of the greatest advantages of implementing IP-enabled call handling is the opportunity for hosting or sharing technology that can serve multiple PSAPs. Because next generation call handling is scalable and based upon IP connectivity, it is possible for PSAPs within a region to share core system equipment and related costs if preferred by local jurisdictions. This becomes especially valuable as equipment becomes more sophisticated and feature-rich while offering greater configurability to meet specific requirements. By centralizing shared system elements, jurisdictions are able to implement fewer systems that are more robust and have greater capabilities than could be implemented as isolated stand-alone solutions. Shared use of core systems can also facilitate information sharing in real time, improved situational awareness, and above all else, interoperability.

One of the greatest advantages of implementing IP-enabled call handling is the opportunity for hosting or sharing technology that can serve multiple PSAPs.

Emergency Services IP Networks (ESInets)

An ESInet is a flexible communications infrastructure that replaces legacy telecommunications transport technology. An ESInet should be a network of networks that connects and supports multiple PSAPs across jurisdictions and that provides new advanced services.

ESInets being deployed today are offering PSAPs IP connectivity as a starting point, along with (in some cases) substituting the legacy selective router with an IP selective router. ESInets are designed to be interoperable and when properly designed and implemented should provide interoperability between PSAPs and ESInets, even when on separate ESInet systems. In fact, the basic premise of the ESInet, and of NG9-1-1, is to be an open ecosystem of IP interconnected, secure, trusted networks. The ESInet, a network of networks, is the basic building block of that interoperability.

ESInets are designed to be interoperable and when properly designed and implemented should provide interoperability between PSAPs and ESInets, even when on separate ESInet systems.

It is important to note that until originating service providers deliver 9-1-1 traffic to the ESInet as IP-based traffic, the multimedia, fully interoperable, scalable world of NG9-1-1 will not be a reality. When originating service providers deliver incoming 9-1-1 traffic as IP to ESInets, NG9-1-1 elements will be able to achieve end-to-end IP connectivity from NG9-1-1 callers through PSAPs. This, along with needed upgrades to PSAP equipment, will eventually enable enhanced features and significant efficiencies.

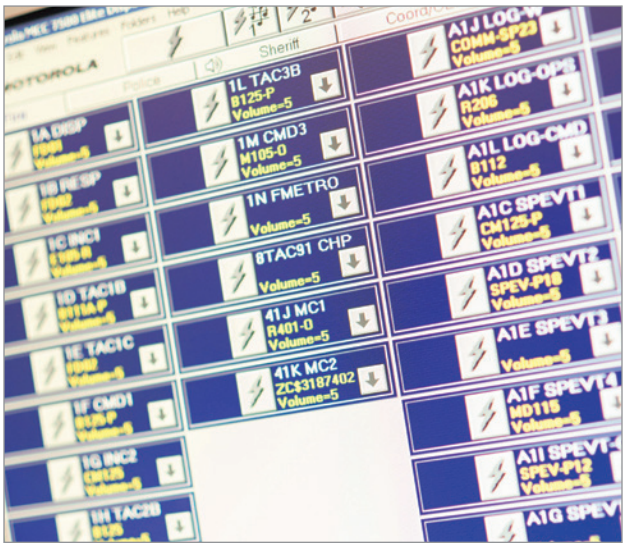
Customer Premise Equipment (CPE)

CPE is what enables the delivery of a voice-generated request for assistance from a 9-1-1 caller to a PST. Legacy CPE evolved out of early operator services technology that was modified to meet the unique needs of emergency communications. The majority of these systems were purpose-built hardware and software that utilize analog CAMA trunks to deliver 9-1-1 calls from telecommunications service providers to a legacy 9-1-1 call handling system. These legacy systems were designed such that the majority of the equipment resides in the PSAP's premises. To the extent that there is interoperability, meaning seamless transfer of the call with ALI and ANI, it is often limited to transfer between primary and secondary PSAPs. PSAPs have started to replace legacy CPE with IP-based equipment, but many of these systems are deployed using legacy PSAP and/or legacy network gateways to accept the incoming 9-1-1 call.

Next generation call handling solutions (if properly configured and accompanied by appropriate service level agreements) are more efficient, effective, and capable of evolving with changing technology and industry standards, reversing the need for multi-year replacement cycles characteristic of existing technology. In a next generation environment, PSAPs can transition premises-based call handling to distributed systems using ESInet connectivity to establish a robust and unified system among numerous PSAPs. This configuration enables a higher level of reliability by placing core systems at redundant hosted locations to protect operational continuity from local outages to large-scale disasters.

Computer-Aided Dispatch (CAD)

CAD systems create requests for service based on information received from the CPE and PSTs, and then may allow for tracking and prioritizing of the incident. CAD systems may also make recommendations based on PSAP-established rules about the type of response and dispatch requirements, and display available responders to the PST. Today, CAD systems in some cases are connected to mobile data terminals (MDTs,



sometimes called mobile digital computers or MDCs) via commercial networks or LMR data technology. These systems generally have limited data rates, security, and functionality. To enhance efficiency, first responder next generation applications, covered later in this section, that are integrated into future devices may replace many of the components or features in current MDT configurations. In a next generation environment, CAD systems will be capable of linking vast amounts of data in order to enable the PST to deliver additional enhanced incident information to the field in the most effective way possible. CAD functionality will become increasingly valuable in a broadband environment, heightening the importance of seamless interoperability and data sharing among CAD and RMS systems and between PSAPs.

CAD functionality will become increasingly valuable in a broadband environment, heightening the importance of seamless interoperability and data sharing among CAD and RMS systems and between PSAPs.

Records Management Systems (RMS)

Presently, RMS provides a platform to enter, store, and retrieve incident reports and information for police, fire, and EMS including accidents, fires, citations, arrests, investigations, evidence, and other data. These systems provide a mechanism to analyze trends by producing a report based on incident types, locations, and other incident data. This information is often captured through a direct interface to CAD. RMS integration with next generation applications will likely be utilized to enter and retrieve data that includes multimedia. For example, a police officer running a premise history query might have access to video taken during previous incidents at the same location, and to maps or schematics of the location involved. All of this increases the officer's situational awareness prior to arrival. As broadband expands the data elements available and additional data streams become available, seamless integration through RMS will be increasingly valuable for PSAP operations.

Hosted Solutions

Hosted solutions, sometimes referred to interchangeably as cloud-based solutions, use network connectivity to enable physically remote users to leverage assets such as equipment or software held in a separate location, and enable real-time information sharing and enhanced cybersecurity. In next generation terms, a public safety hosted or cloud-based environment means that 9-1-1 calls or emergency requests in a particular jurisdiction are processed by equipment and infrastructure that may or may not be in the local PSAP facility. A hosted or cloud-based system distributes common services to multiple PSAPs, reduces the need for redundant equipment, shares costs, and offers improved operational continuity when an emergency event threatens the physical structure of a PSAP. On-premise systems, such as a PST workstation or CAD terminal, can all be supported by hosted, remote services. This allows for scalability, economies of scale, and flexibility for each PSAP participating in the cloud-based system. Cloud-based solutions are independent of location because the connectivity to the cloud system is IP-based and utilizes broadband distributed networks. As long as a PSAP maintains an IP connection to the cloud (which should have a redundant and resilient path), whether it is based on terrestrial access, wireless broadband or other access mechanisms, calls can be processed and solutions can be accessed from anywhere, whether it is a neighboring PSAP, a consolidated center, a tactical PST in the field, or a mobile communications vehicle. This provides a virtual replica of PSAP operations without costly static backup locations that are often geographically vulnerable to the same crisis that compromised the primary facility.

Enhanced Data from IoT, Smart Cities, Intelligent Highways, Telematics, etc.

With broadband connectivity, PSAPs have the opportunity to connect with other broadband-driven technologies such as IoT, smart cities, intelligent highways, vehicle telematics, and automated alarms. As illustrated in the emergency response scenario in the Executive Summary, the PSAP of the future could benefit from information such as biometric devices on 9-1-1 callers, collision data, and information from non-public safety systems – resulting in a more effective emergency response.

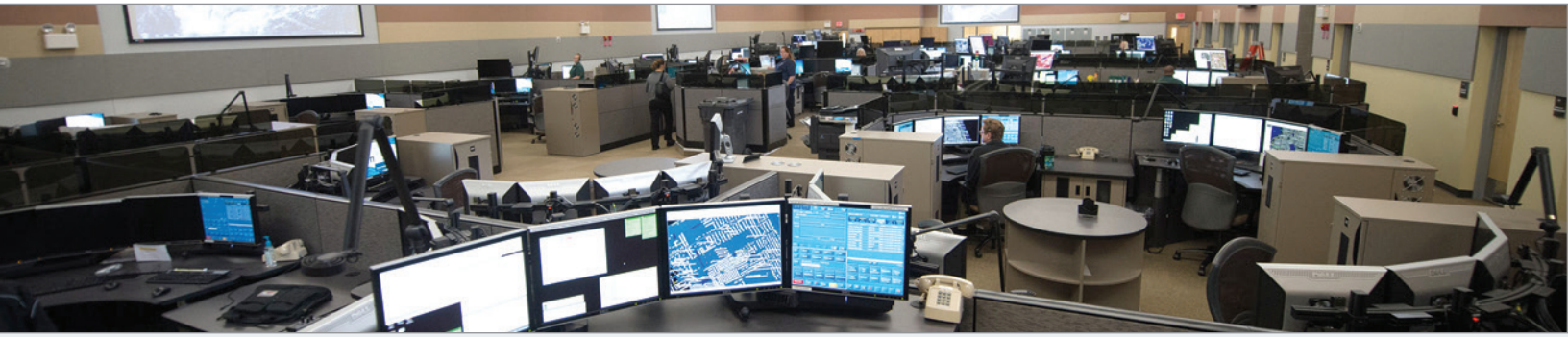
In order to reap the greatest benefit from a next generation architecture, PSAPs need fast, easy access to rich data as well as a reliable way to deliver that data in a useful way to the most appropriate place in the least amount of time. PSAPs that implement enhanced data features will increase situational awareness, improve first responder safety, and create valuable operational efficiencies.

With broadband connectivity, PSAPs have the opportunity to connect with other broadband-driven technologies such as IoT, smart cities, intelligent highways, vehicle telematics, and automated alarms.

In the legacy environment, ALI and ANI data is limited, usually including caller name, originating telephone number, caller location, and some basic caller and public safety data. In a next generation architecture, however, data will travel over a high-capacity, secure IP-based network. The type of information available may include:

- Social media
- Medical information (real-time and patient history)
- HAZMAT information
- Vehicle telematics
- Premises data
- Alarm monitoring
- Private/public databases
- Responder locations
- Weather alerts
- News feeds
- Language services

PSAPs may wish to forward some of the enhanced data directly to first responders. With that in mind, seamless interoperability across the entire PSAP ecosystem – for example from public IoT to CAD and RMS – will be necessary.



ASAP CASE STUDY[74]

The Automated Secure Alarm Protocol (ASAP) program is a good example of industry and public safety coming together to develop and implement a standard that facilitated interoperability and resulted in clear operational benefits.

Traditionally, the process for facilitating an exchange between an alarm monitoring central station and a PSAP was accomplished by the alarm company calling the PSAP's ten-digit non-emergency line. Once the call was answered, it could take anywhere from a minute-and-a-half to three minutes to relay the alarm information to the PST. Depending on the alarm company, the PST would be given information in varying formats, increasing data entry time and the risk of miscommunications.

In 2005, recognizing an opportunity to streamline, automate, and standardize this process, APCO and the Monitoring Association, an alarm industry trade association, partnered to develop an exchange standard. The goal was to reduce telephone call volumes to PSAPs from alarm monitoring companies, eliminate miscommunications, and

ultimately reduce emergency response times. The joint effort resulted in a voluntary, consensus-based American National Standard (ANS) that is vendor neutral, non-proprietary, and based on open commercial standards. The ASAP standard provides a data exchange specification for the automated transmission of alarm information between a PSAP CAD and an alarm monitoring company.

As of June 2017, there were 19 ASAP active alarm monitoring companies, 22 participating PSAPs in nine states and Washington, DC, with even more in the testing or onboarding phase.[75] To participate, PSAPs must work with their CAD provider to implement the ASAP interface solution. Once the interface is in place, the PSAP is able to receive alarm information from participating alarm monitoring companies directly to the CAD and send response updates, such as resources dispatched and requests for information, back to the alarm company. No telephone call with the alarm monitoring company is necessary.

The benefits of ASAP were proven soon after implementation. During one county's pilot test for example, in four instances the reduced processing time enabled police to arrive at the site of a burglar alarm in time to capture the suspect.[76] As PSAPs adopt broadband technologies and are able to receive additional enhanced data, this ANSI standard can serve as a model for achieving interoperable technology that results in improvements to public safety operations.

Nationwide Public Safety Broadband Network (NPSBN)

Many public safety agencies have deployed MDTs that run on commercial wireless broadband networks. This allows PSAPs and responders in the field to share incident-related information. MDTs allow field responders to view maps for routes to the scene, hydrant locations, incident pre-plans, suspect information, incident location histories, a list of dispatched units, assignments, etc. They allow responders to receive visible incident and suspect information in the field as well as to create records allowing for a more efficient response that eliminates the need for responders to leave the field to complete incident information. The introduction of smartphones has opened the door to new features at the personnel-level, rather than the vehicle-level. Now, individual responder locations may also be tracked for responder safety. Field responders can leverage broadband data capabilities throughout an incident.

As a result of the technology differences between traditional private mission-critical voice communications systems and shared commercial data systems, as well as the concern over security and availability, there has traditionally been very little interoperability or coordination between these systems. However, there are currently opportunities for progress in this area with migration to IP-based systems and with the upcoming introduction of mission-critical data communications via FirstNet.

When combined with fully deployed NG9-1-1 networks, the NPSBN and the NG9-1-1 PSAP will serve as twin pillars of the greater emergency response ecosystem, enabling the exchange of broadband-rich data between PSAPs and NPSBN users.

The NPSBN will be a major driver of broadband technology for communications between and among field responders and PSAPs. The FirstNet legislation recognized the need for the NPSBN to be integrated with PSAPs. When combined with fully deployed NG9-1-1 networks, the NPSBN and the NG9-1-1 PSAP will serve as twin pillars of the greater emergency response ecosystem, enabling the exchange of broadband-rich data between PSAPs and NPSBN users.

Mobile Apps

Mobile apps are already being used to improve public safety operations for features such as location tracking, resource management, and accessing incident pre-plans. Eventually, push to talk apps may substantially alter the way many agencies depend on traditional LMR-based systems for mission critical voice.

Recognizing that apps hold great potential, APCO has been working to ensure they are as effective and safe as possible. This work includes a variety of past and ongoing collaborations with public and private sector partners, including FirstNet, DHS, NIST, the Public Safety Communications Research (PSCR) program, as well as a number of state and local government IT and public safety professionals.[77] APCO's efforts have included:

- Establishing an online forum focused on public safety apps
  - In 2013, APCO launched the Application Community (www.AppComm.org), a forum for learning about existing apps and contributing ideas for new ones.[78]

- Identifying the Key Attributes of Effective Apps for Public Safety and Emergency Response
  - APCO published the Key Attributes to provide public safety professionals, app developers, and the general public with an outline of important considerations for apps that include public safety or emergency response features.[79]

- Developing an app testing program for public safety
  - Working with private and public sector partners, APCO conducted pilot testing programs to evaluate app efficiency and security.[80] Subsequently, APCO partnered with the DHS Science & Technology Directorate to refine an evaluation program designed to ensure interoperability and security for public safety apps.[81]

- Convening experts to address public safety requirements, app security, and interoperability
  - APCO has hosted multiple workshops to address app-related issues, partnering with organizations with significant expertise in apps, including DHS, NIST, PSCR, and FirstNet. These events gathered public safety professionals, app developers, cybersecurity professionals, and other subject matter experts to address issues such as security requirements, data classifications, and interoperability for public safety apps.[82]

- Issuing specific guidance on 9-1-1 apps
  - In 2015, APCO published a White Paper and Fact Sheet[83] to educate the general public and the app development community on the state of the 9-1-1 system and the role that apps can play currently and in the future.

Interoperability and Standards

NG9-1-1 Use Cases

Seamless interoperability is an imperative that will improve emergency response operations and expand the market so that public safety benefits from the competition and innovation enjoyed in the commercial sector. Seamless interoperability means avoiding expensive integrations or specialized interfaces for every NG9-1-1 use case:

- PSAP-to-PSAP: seamless hand-off of calls such as for transfers, overloads, or mutual aid
- ESInet-to-ESInet: seamless exchange of data between connecting networks, including across state boundaries, to facilitate mutual aid, disaster recovery, or data sharing
- ESInet-to-origination networks: a seamless way for the public and other sources of data (including smart city, IoT, and intelligent highway networks) to flow into NG9-1-1 networks
- NG9-1-1-to-FirstNet: one network cannot fully function without the other, and a seamless interface to exchange data between these two vitally important public safety networks is a must

While it would be natural to expect seamless interoperability given the value to public safety's mission, NG9-1-1 deployments are on course to lack

end-to-end interoperability, at least without costly after-the-fact integrations. Adherence to widely deployed commercial standards, and any other standards approved through organizations such as ANSI that accredit the procedures of standards development organizations to ensure openness, balance, consensus, and due process, will be critical to achieving public safety's interoperability goals.

Adherence to widely deployed commercial standards, and any other standards approved through organizations such as ANSI that accredit the procedures of standards development organizations to ensure openness, balance, consensus, and due process, will be critical to achieving public safety's interoperability goals.

ANSI Accreditation

ANSI coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. ANSI accredits standards development organizations (SDOs).

To produce an American National Standard, an ANSI-accredited SDO must adhere to certain due process requirements that ensure openness, balance, and consensus in standards development, which are designed to help make standards development in the U.S. an equitable and open process that serves both U.S. business and the public good.[84] In other words, ANSI-accredited standards are to be developed through a process designed to prevent standards from narrowly favoring a particular interest. As an ANSI-accredited SDO, APCO values and honors these due process requirements in its standards development role because that is in the best interests of our members and colleagues throughout the 9-1-1 profession.

Public Safety Standards

In addition to commercial standards, there are a number of complementary efforts underway by the public safety community and industry to improve interoperability and flexibility for NG9-1-1. Standards are also in progress to address NG9-1-1 network architecture.

Emergency Information Data Document (EIDD)

In early 2017, APCO and NENA received final approval for an American National Standard that identifies standard specifications for the exchange of NG9-1-1 emergency data between disparate manufacturers' systems (CAD, RMS, etc.) located within one or more public safety agencies.[85] Proprietary CAD systems pose a significant challenge for seamless interoperability. The EIDD provides standardized, industry-neutral National Information Exchange Model (NIEM) conformant (XML-based) specifications for exchanging emergency incident information to agencies and regions that implement NG9-1-1 and IP-based emergency communications systems.

The EIDD is intended to support a full complement of interoperable emergency incident data exchanges between a variety of public safety systems (CAD-to-CAD, CAD-to-RMS, CAD-to-mobile data, etc.).

The Integrated Justice Information Systems (IJIS) Institute will provide a conformance and certification platform and will work to encourage agency adoption of the specification during the acquisition process to foster broader adoption.[86] The EIDD should be adopted as a method of exchanging cross-jurisdictional public safety communications data.[87]

The Future Standard for an NG9-1-1 Architectural Framework - NENA i3

The NENA i3 Vision for NG9-1-1, while not yet an accredited, consensus-based American National Standard, seeks to establish an end-state architectural solution for NG9-1-1. Accordingly, at the time of this report, i3 is not intended to be a "build-to" specification for a complete NG9-1-1 system. APCO realizes the importance of these architectural concepts and fully supports NENA's stated intent to pursue having i3 accredited via the ANSI process with the next version of i3. While the functional elements derived from this vision are helpful in describing certain elements of NG9-1-1, until i3 is a complete, accredited American National

Standard, APCO will continue to recommend pursuing an approach that is based on completed standards. This is especially important because at the present time, it is uncertain whether current NG9-1-1 deployments are on course to achieve seamless interoperability without costly after-the-fact integrations.

The Benefits of Commercial Standards

In the commercial sector, interoperability is taken for granted. For example, consumers can freely exchange multimedia content and data with each other, regardless of device, manufacturer, operating systems software, service provider, etc. This is because the consumer marketplace uses commercial standards – such as those created by 3GPP (including IMS), ANSI, ATIS, IETF, IEEE, etc. – and because the market generally demands it.

Across the globe and in the U.S., standards already support fully interoperable IP-based wireless and fixed networks.

In addressing the communications needs of first responders, Congress sought to leverage the opportunities afforded by the innovation, experience, expertise, infrastructure, and breadth of the commercial marketplace. In particular, by defining and requiring use of commercial standards in all network components, the FirstNet legislation is achieving the following for the NPSBN:

- Substantially expanded range of companies producing innovative solutions
- Seamless interoperability and data sharing without the need for additional interfaces or costly integration
- Significant economies of scale

NG9-1-1 can and must benefit from these same commercial standards and expectations.

Across the globe and in the U.S., standards already support fully interoperable IP-based wireless and fixed networks. This is what enables the sharing of multimedia content including audio, video, text, and photos regardless of the device, service provider, or network that is used. NG9-1-1 can and must benefit from these same commercial standards and expectations.

Location Information

Caller Location

In the legacy network, individual telecommunication service providers deliver basic information relative to their wireline customers to a 9-1-1 service provider. This data includes the name and service address associated with individual phone numbers. When the information is received, the 9-1-1 service provider utilizes an enhanced 9-1-1 (E9-1-1) database management system to confirm the data in a process known as address validation. The validation process runs the data through a set of rules based on the master street address guide (MSAG). Once the data is verified, the telephone number is tagged with the appropriate 9-1-1 attributes called the emergency service number (ESN). This designation identifies the appropriate PSAP to receive the call as well as the responding police department, fire department, and ambulance service based on the physical address of the telephone number.

Locations delivered for mobile 9-1-1 calls follow the same basic path, except for the additional services and equipment deployed by wireless service providers to determine a mobile position estimate.

It is estimated that more than 70 percent of 9-1-1 calls nationwide come from wireless devices.[88] Locating these devices is a challenge, especially indoors, because existing location network-based and even GPS-based location estimates can be too uncertain to be useful for public safety. Presently, the wireless industry, in concert with APCO and NENA, is implementing new FCC rules[89] and technologies to determine a more precise location fix, including inside of buildings and other structures. For example, access points from wireless routers and Bluetooth beacons, when aggregated and validated, can be used to deliver a "dispatchable location" to PSAPs.

With improvement in location technologies, particularly for calls made from indoor locations, combined with NG9-1-1 technology, calls can be routed based on the location of the caller, rather than the location of the cell tower or sector that handles the call. Further, NG9-1-1 will support policy-based call routing, such that PSAPs can specifically manage how a call is routed based on a number of factors such as call volumes.

Geographic Information Systems (GIS)

Mapping displays have become a fundamental element of effective public safety emergency response. Geographic information systems are the data management tools behind map displays as well as many of the advanced services coming with NG9-1-1. The legacy wireline 9-1-1 GIS systems are primarily based on textual (or civic/postal) addresses while newer mobile-based communications provide geographic (or X/Y) coordinates. The introduction of NG9-1-1 systems that require location information is leading to the association of X/Y coordinates with other address information, also known as geocoding. With the increasing focus on nationwide NG9-1-1 deployment, the potential of GIS as a powerful life-saving and decision-making tool is becoming more apparent, though current GIS systems will need to expand in order to reach their full next generation potential.

In the context of legacy 9-1-1, public safety agencies have been collecting tabular GIS information for decades in order to populate the information found in ALI and MSAG databases and to assign ESNs. This data is collected at the street level based on specific boundaries and street ranges with some interpolation to achieve address information. When a wireless emergency call comes into a legacy GIS-equipped PSAP, associated X/Y coordinates are delivered, though the coordinates are meaningless on their own. In order to be valuable, this data must be mapped in the call-handling environment. Once plotted, the information can be applied to perform dispatch functions. In this way, GIS is a supplemental tool used solely to verify location.

Next generation GIS has moved beyond basic coordinate-based capabilities. It is an integral tool used to guide and enhance response strategies, and geographic information is the basis for many advanced service capabilities. In an NG9-1-1 environment, the tabular data, or flat files, of ESNs, ALI, and MSAG databases will transition into geospatial intelligence in the form of GIS databases that can render maps and information for sophisticated emergency response services. While the determination of X/Y coordinates will remain a key function, next generation GIS are designed to capture, store, manipulate, analyze, manage, and present a wide variety of geographical data. In this type of geospatial environment, every piece of data about a geographic area can be represented using layers of information on a map or site plan. As more information is collected, additional layers of data can be created. Ultimately, layers of information will correlate with a specific PSAP, police department, fire department, medical response agency, poison response, and so on. If a call originates in a specific geographic area, the call will be routed and the response will be dispatched according to the rules assigned within the geographic information database. The big difference with NG9-1-1 is that these relationships will be determined dynamically at the time of a 9-1-1 call versus pre-staged in complex data management tools.

Moving forward, GIS data will become more refined and will correlate with other data sources to support the continuing evolution of next generation capabilities. PSAPs will need precise GIS databases that are accurate, up-to-date, and synchronized at the local, regional, and state level. Typical sources of GIS information must be supplemented with 9-1-1 attributes and modified to support the special

needs of public safety applications and processes. Additionally, workflows and processes will need to be created to collect, verify, correlate, maintain, and manage the vast amount of data that is associated with these systems.

FINDINGS

Confusion About NG9-1-1

Some states and localities are making progress towards NG9-1-1 by replacing legacy networks with ESInets. To be fully deployed, NG9-1-1 has to mean an end-to-end, all-IP network that includes not only the connectivity afforded by ESInets but also the equipment and services needed to enable every PSAP to process new forms of data. To illustrate, this means when a member of the public can send a multimedia message such as a photo or video to a PSAP that in turn is capable of receiving, analyzing, and forwarding this information to a field responder to render an emergency response.

Defining NG9-1-1 in this comprehensive manner will best ensure that all stakeholders work in unison to effectively implement NG9-1-1 across the United States. This includes innovators, technology companies, federal, state and local government officials, and 9-1-1 professionals. It also helps better identify the need and urgency to modernize 9-1-1 particularly for elected officials, and mitigate confusion on the part of the general public, whose expectations about the capabilities of 9-1-1 are increasingly far from reality.

To be fully deployed, NG9-1-1 has to mean an end-to-end, all-IP network that includes not only the connectivity afforded by ESInets but also the equipment and services needed to enable every PSAP to process new forms of data.

Confusion About Standards

There is confusion in the public safety community about what standards cover and what it means to comply with a standard. Historically, the 9-1-1 industry has produced standards that describe how originating service providers and 9-1-1 system service providers deliver and route 9-1-1 calls along with location information to PSAPs. SDOs like APCO and NENA produce ANSI standards that are specific to 9-1-1 operations. In a broadband environment, and as being experienced now with the NPSBN, widely deployed commercial standards will play a role for NG9-1-1 that was not possible previously, setting PSAPs on a course to benefit from interoperability, economies of scale, competition, and innovation matching the consumer marketplace. Yet until there are well-defined standards and implementation

guidelines, each vendor could implement a standard differently, defeating achievement of these goals. Practically speaking, this confusion can mean products being held out as "compliant" with a "standard" are misunderstood to be interoperable with one another.

For example, compared to the broadband technologies that will be available to PSAPs, text-to-911 is less complex. Yet, even several years into the adoption of text-to-911, for which industry rallied around a single standard, PSAPs face interoperability issues and are not always able to transfer texts between PSAPs.

The 9-1-1 community may not have the bargaining power, on its own, to match the economies of scale and innovation prevalent in the commercial marketplace and ensure needed interoperability for NG9-1-1.

NG9-1-1 and FirstNet are the two main pillars of the nation's future emergency response capabilities. Accordingly, and similar to how the FirstNet legislation achieved these goals for first responder communications, the opportunity exists for Congress to provide strong incentives for NG9-1-1 implementation to use commercial standards and achieve full interoperability. For example, Congress can help ensure use of commercial standards and ongoing interoperability as a condition of federal grants.

Interoperability

Broadband technology creates new opportunities to think of NG9-1-1 in terms of interoperability. The devices that consumers use to contact 9-1-1 are already interoperable and innovative. FirstNet is setting the NPSBN on the same path. With the nation's NG9-1-1 systems poised to be right in the middle of these public-facing and responder-facing networks, they too need to be fully interoperable. Thus, establishing interoperability as a primary objective would in turn help to focus the technical solutions and standards that are needed. ■

RECOMMENDATIONS: TECHNOLOGY

Promote a Common Definition of NG9-1-1

NG9-1-1 must be understood to mean an end-to-end, all-IP network that includes not only the connectivity afforded by ESInets but also the equipment and services needed to enable every PSAP to process new forms of data. This means when a member of the public can send a multimedia message such as a photo or video to a PSAP that in turn is capable of receiving, analyzing, and forwarding this information to a field responder to render an emergency response. As described in the Executive Summary:

"NG9-1-1 is a secure, nationwide, interoperable, standards-based, all-IP emergency communications infrastructure enabling end-to-end transmission of all types of data, including voice and multimedia communications from the public to an Emergency Communications Center."

Mechanisms for Ensuring Seamless Interoperability

Standards Development and Adoption
APCO will continue to support the development of and adherence to standards that ensure seamless interoperability for public safety communications. As a specific near-term goal, APCO will continue collaborating with NENA to develop an ANSI-accredited standard for transporting EIDDs between systems and encourage adoption of the EIDD standard.

As a specific near-term goal, APCO will continue collaborating with NENA to develop an ANSI-accredited standard for transporting EIDDs between systems and encourage adoption of the EIDD standard.

Grants and RFPs

Standards are critical, but the public safety community also needs mechanisms to ensure that NG9-1-1 systems meet the interoperability goals described in the NG9-1-1 use cases on page 56, both when they are deployed and on an ongoing basis. APCO recommends that RFP language and federal grant programs call for the use of widely deployed commercial standards to ensure seamless interoperability among and between PSAPs, ESInets, states, jurisdictions, originating networks, and the NPSBN. Any standards used in addition to widely deployed commercial standards should be approved through organizations such as ANSI that accredit the procedures of standards development organizations to ensure openness, balance, consensus, and due process. Further, federal grant programs should require that any failure to maintain commitments to seamless interoperability results in forfeiting funds.

For those states and jurisdictions that have deployed, or are seeking to deploy, ESInets or other NG9-1-1 elements, APCO recommends asking the following questions of existing or prospective vendors and putting these questions into requirements in RFPs:

- Can you guarantee that our ESInet and other IP-based equipment will be seamlessly interoperable with other ESInets and equipment, including across state boundaries?
- Can you guarantee that our ESInet will be seamlessly interoperable with origination networks? With FirstNet?
- If a solution complies with a particular standard, how have you ensured that your implementation of the standard aligns with others in the industry to achieve interoperability?
- Will you guarantee your solution to be interoperable without additional upgrades and new costs to the PSAP?
- Will your CPE, CAD, RMS, GIS or mobile app product be able to seamlessly share and exchange data with other equipment, without the need for special interfaces, additional costs?

Collaboration with FirstNet

Given FirstNet's mandate to promote integration between the NPSBN and NG9-1-1, and the tremendous potential of seamless integration between these systems, APCO will seek to collaborate with FirstNet to help bridge this gap, such as through development of relevant standards. Further, APCO will continue to promote use of lessons learned from the FirstNet legislation to achieve similar goals in the development of NG9-1-1 systems and policies.

Notes

73 Diagram courtesy of the Texas A&M University Internet2 Technology Evaluation Center.

74 This case study describes what is today known as the ANS Standard for Alarm Monitoring Company to PSAP CAD Automated Secure Alarm Protocol. See ANSI/APCO/CSAA 2.101.2-2014 Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (August 5, 2014) at https://www.apcointl.org/doc/911-resources/apco-standards/527-alarm-monitoring-company-to-psap-cad-automated-secure-alarm-protocol-asap/file.html.

75 ASAP Activity, The Monitoring Association (June 6, 2017) at http://tma.us/asap-status/.

76 Automated Secure Alarm Protocol Reduces 9-1-1 Processing & Response Times, Bill Hobgood (August 2, 2011) at http://psc.apcointl.org/2011/08/02/automated-secure-alarm-protocol-reduces-9-1-1-processing-responses-times/.

77 See, e.g., APCO Enters Into Memorandum of Understanding with FirstNet Regarding Mobile Apps (Aug. 21, 2013) available at https://www.ntia.doc.gov/press-release/2013/apco-enters-memorandum-understanding-firstnet-regarding-mobile-apps; Partnering to Improve Public Safety Apps (Nov. 2, 2015) at https://www.apcointl.org/tabletopx/partnering-to-improve-public-safety-apps/; APCO Partners with DHS to Advance Interoperability and Security of Mobile Apps (Nov. 10, 2016) at http://psc.apcointl.org/2016/11/10/apco-partners-with-dhs-to-advance-interoperability-and-security-of-mobile-apps/.

78 APCO Launches Application Community (AppComm) Website (Apr. 23, 2013) at http://psc.apcointl.org/2013/04/23/apco-launches-application-community-appcomm-website/.

79 APCO Identifies Key Attributes of Effective Apps for Public Safety and Emergency Response (Aug. 19, 2013) at http://appcomm.org/article/apco-identifies-key-attributes-of-effective-apps-for-public-safety-and-emergency-response/.

80 Partnering to Improve Public Safety Apps (Nov. 2, 2015) at https://www.apcointl.org/tabletopx/partnering-to-improve-public-safety-apps/.

81 APCO Partners with DHS to Advance Interoperability and Security of Mobile Apps (Nov. 10, 2016) at http://psc.apcointl.org/2016/11/10/apco-partners-with-dhs-to-advance-interoperability-and-security-of-mobile-apps/.

82 APCO Holds Workshop to Identify Initial Public Safety Requirements for Mobile Apps (Feb. 25, 2014) at http://appcomm.org/article/apco-holds-workshop-to-identify-initial-public-safety-security-requirements-for-mobile-apps/, which resulted in a NIST Interagency Report, Public Safety Mobile Application Security Requirements Workshop Summary (Jan. 2015) at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf; APCO Convenes Experts to Advance Security of Public Safety Apps (June 2, 2015) at http://psc.apcointl.org/2015/06/04/apco-convenes-experts-to-advance-security-of-public-safety-apps/, which resulted in a NIST Interagency Report, Identifying and Categorizing Data Types for Public Safety Mobile Applications (May 2016) at http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8135.pdf; APCO Gathers Experts to Advance Public Safety App Interoperability (Oct. 31, 2016) at http://psc.apcointl.org/2016/10/31/apco-gathers-experts-to-advance-public-safety-app-interoperability/.

83 The Status of 9-1-1 Apps (Apr. 27, 2015) at http://appcomm.org/wp-content/themes/directorypress/thumbs/WhitePaper_911Apps.pdf; APCO, Fact Sheet: Mobile Apps and 9-1-1 (Apr. 27, 2015) at http://appcomm.org/wp-content/themes/directorypress/thumbs/FactSheet_911Apps.pdf.

84 https://share.ansi.org/shared%20documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2017_ANSI_Essential_Requirements.pdf.

85 http://psc.apcointl.org/2017/01/10/apco-announces-approval-of-apconena-standard-ng9-1-1-emergency-incident-data-document-eidd/.

86 http://c.ymcdn.com/sites/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/ijis_wp_IPSTC_CAD-to-CAD_Data_Sharing_-_Standards_20170317.pdf.

87 https://www.apcointl.org/doc/911-resources/apco-standards/694-apco-nena-2-105-1-2017-ng9-1-1-emergency-incident-data-document-eidd/file.html.

88 https://www.fcc.gov/consumers/guides/911-wireless-services.

89 https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf.