APCO International

BROADBAND IMPLICATIONS FOR THE PSAP

ANALYZING THE FUTURE OF EMERGENCY COMMUNICATIONS

APCO

Broadband Implications for the PSAP

A Project 43™ Initiative

APCO International
351 N. Williamson Blvd.
Daytona Beach, FL 32114

www.apcop43.org

PROJECT 43™

BROADBAND IMPLICATIONS FOR THE PSAP

Analyzing the Future of Emergency Communications

Table of Contents

ACKNOWLEDGEMENTS: PROJECT 43™ CONTRIBUTORS

APCO sincerely thanks the following individuals who were members or leaders of the P43 working groups or otherwise contributed to this report. By sharing the benefit of their time, collaboration, experience, expertise, and dedication, each played a helpful role in formulating the content of this report, which required true vision to forecast the impacts of broadband technology. Without their collective input, this report would not have been possible.

Project Chair

Steven Proctor

Participants

Mindy Conner Adams, RPL*
Cory L Ahrens
Scott C Andrews
Dominick V Arcuri
Tami M Atkinson
Sandra Barfield
Gary A Bell, ENP
Cheryl Bledsoe
Angela R Bowen, RPL, CPE
Katie Braverman
Eddie Burchell
Kimberly Burdick, RPL, CPE
Michael Byrd
Kim Coleman Madsen
Mike Corbett
Jackie L Crotts
D Jeremy DeMar, RPL
Antonio DeSimone
Tony A Dolezal
William E Duggan, RPL, CPE
Gabe Elias
Jay English
Chris A Fischer*

Charlene A Fisk, RPL
Charlynn F Flaherty
Cheryl S Giggetts, PMP
Tammy L Goggia, ENP
Kevin J Harris
Vahram Havandjian
Peter J Howard
Vihang Jani
Brent Jensen
Jonathan L Jones
Frank J Kiernan, III
James Leyerle
Bob Little
Timothy J Lorello
Barry H Luke
Walt Magnussen
Fred McAnn
Tim McKee
Donald W Miller
Kristen Molander
Donald M Naccarato
Christine Pantoja-Young
Nicole Parrish

Eddie L Reyes*
Randy J Richmond
Dave Ripley
Doug Roberts, PhD
Harry Fritz Rote, III
Robert L Smith
Bradford S Smith
Steve Souder*
James T Soukup
Chuck Spalding
Mark Spross
Matthew J Stillwell, RPL
Matt Tooley, ENP
Joe Treglia
Steve Usher
Debbie Vance
Renee Vande Voort
Maureen A Will, RPL
Stephen C Williams*
Stephen J Wisely
Patrick J Woods

*Working Group Chairs

Staff Liaisons

Megan Bixler
Mark Cannon, CAE, CPE
Jeff Cohen
Lauren Corcoran

Stacy Hall
Kathy Lawrence
Steve Leese
Crystal McDuffie, RPL

Derek Poarch
Mark Reddish
Nicole Zimbelman

EXECUTIVE SUMMARY

INTRODUCTION

A number of major, broadband-based developments are leading to a paradigm shift in the role of the public safety answering point (PSAP). Implementation of a new, interoperable, nationwide public safety broadband network (NPSBN) will place broadband communications into the hands of first responders. Next Generation 9-1-1 (NG9-1-1) technology will enable PSAPs to utilize broadband data in ways that will transform how the public reaches 9-1-1 and how public safety telecommunicators (PSTs) interact with first responders.

APCO launched Project 43, Broadband Implications for the PSAP, in April of 2016. This report is the outgrowth of the work of nearly 80 member practitioners assisted by APCO professional staff arrayed across several working groups focused on the following major topical areas: operations, governance, cybersecurity, technology, training, and workforce. Each working group consisted of experienced public safety and industry professionals who met regularly over the course of a year. The goal of Project 43 is to help public safety telecommunicators, PSAPs, PSAP directors, 9-1-1 authorities, elected and appointed officials, and others in the public safety community better leverage existing technology capabilities and prepare for the evolving broadband communications technologies that will impact PSAP operations and, at the same time, improve support to field responders.

This is necessarily just a start, and not the final word. Technology changes quickly, as does the nature of threats to public safety. APCO will be undertaking a number of follow-up actions and welcomes the beginning of significant dialogue and collaboration triggered by this report, for the months and years to follow. Comments are welcome and may be sent to broadband@apcointl.org.

An analysis of broadband implications requires new or more comprehensive definitions of fundamental terms. The literal language of the term “PSAP” becomes outdated in a broadband environment. 9-1-1 centers are increasingly and appropriately being called emergency communications centers (ECC).[1] Further, job titles of 9-1-1 professionals vary widely, but trends show decreasing use of “dispatcher” and increasing use of variants of “telecommunicator.” The term “Public Safety Telecommunicator” fits better in a broadband environment because it encompasses call taking, dispatching, and other tasks associated with being responsible for mission critical communications during an emergency response. PST also better encompasses the diverse and complex technical nature of the various tasks performed by these professionals as a whole. And of course this term has been recognized at the national level since 1992 when Congress established National Public Safety Telecommunicators Week.[2]

NG9-1-1 must be defined in a way that ensures it is deployed in a comprehensive and uniform fashion nationwide. To truly achieve a full NG9-1-1 deployment, the definition must account not only for Internet Protocol (IP)-based network connectivity, but the functions and equipment necessary for broadband information to be received, processed, and acted upon at the PSAP. A common definition would help ensure that PSAPs across the country modernize 9-1-1 networks in a manner that to the public remains familiar. Further, policymakers at all levels, industry partners, and other stakeholders can all work in the same direction only if they share the same understanding of what is needed to accomplish NG9-1-1. Accordingly, NG9-1-1 should be defined as follows:

"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."

"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."

Defining NG9-1-1 in this manner is also essential to recognizing the central role of the PSAP in a fully broadband-enabled environment. Additional broadband technologies such as the NPSBN being implemented by FirstNet,[3] when fully integrated with NG9-1-1, will enable a seamless exchange of broadband communications between the PSAP and responders in the field.

PSAPs of the future will be a nerve center, managing data-rich communications via broadband technology with 9-1-1 callers and first responders.

IP-based technologies, including those supported through smartphones, tablets, and mobile apps, are widely prevalent throughout the general public and capable of sending an array of information to the PSAP. As a result, PSAPs of the future will be a nerve center, managing data-rich communications via broadband technology with 9-1-1 callers and first responders.

PUBLIC SAFETY COMMUNICATIONS TODAY

From the current ability of the public to stream services over multiple screens and devices to the complex, and compelling, world of cognitive enabled services,[4] broadband is already having an impact on public safety communications. As broadband transforms communications technology outside of public safety, it also impacts emergency communications. Geographic information systems (GIS) technology enabled a new way of mapping and tracking incidents and responders. Now, with broadband-enabled technologies and GIS-based, real-time location capabilities at the fingertips of smartphone users throughout the nation, there is a push towards more defined, comprehensive location technologies. High definition video streams are becoming available to PSAPs and responders, as well as other local governmental agencies and authorities from multiple sources, and in some cases in real time. Social media and mobile apps are also already impacting how PSAPs and responders communicate and receive information.

Smart cities, already in existence in various forms, are representative of how broadband is used in the current environment. A "smart city" is one that has developed technological infrastructure that enables it to collect, aggregate, and analyze real-time data to improve the lives of its residents.[5] Examples of smart city technologies with applicability to

PSAPs include fire detection (from public parks and wooded areas to buildings), gunshot detection, traffic conditions (for emergency vehicle routing and overall situational awareness), street lamp outages (for night safety), infrastructure sensors (such as at bridges, for damage), municipal vehicle tracking (situational awareness of public safety and support vehicles), connected drones, surveillance cameras, and responder body cameras. These networks are empowered by broadband connectivity, which is becoming increasingly widespread thanks to new and future generations of wireless technologies.

Each of these examples demonstrates how broadband is already changing public safety. In addition, a number of broadband-based services are available to the PSAP and other government agencies such as fusion centers, hospitals, and utility departments. Whether as part of an interconnected smart city, or via use of a combination of commercially available technologies such as automatic vehicle location data, mobile apps, or even unmanned aerial vehicles with broadband connectivity, communications during routine operations as well as during emergencies are already being redefined by broadband technologies.

VISION OF THE FUTURE

The following two scenarios help illustrate how broadband will alter emergency communications.

Scenario: MULTI-VEHICLE COLLISION, **CURRENT DAY**, Anywhere USA

Multiple 9-1-1 calls are received (voice only) about a multi-car pileup on Interstate 10, somewhere just outside a large metro area. There is reportedly a tanker truck involved, on its side with flames coming either from or nearby the tanker. At least two vehicles are reported to have people trapped in them. Callers differ on the exact location and number of vehicles involved. Callers are unable to see the placard on the tanker, and cannot see the condition of the vehicles with entrapment. There are multiple parties reported as injured.

Not knowing the type of hazardous material (HAZMAT) involved, the number or trauma level of the patients at the scene, or the precise location, PSTs continue to question the callers, and continue to receive mixed information. They select relevant information based on their training and experience, and pass that information along to a number of units for dispatch, including the two closest HAZMAT response teams. Multiple ambulances are dispatched, and several local air medical evacuation helicopters are put on standby in case they are needed. As responders go en route, they are provided with the latest available information via radio, and their onboard mobile data terminals receive computer-aided dispatch (CAD)-based text updates.

Scenario: MULTI-VEHICLE COLLISION**, THE FUTURE**, Anywhere USA

NG9-1-1 calls, with multimedia streaming audio and video, are received by the PSAP. The PSAP is a fully integrated, broadband-based, multimedia-capable command, control, and communications center. In its legacy version, the PSAP was limited by technology and less integrated with both the public and responders. Now, PSAPs around the country represent the “nerve center” of emergency response and serve multiple roles from integrated intelligence gathering (with fusion centers and federal, state, and local partners), to shared cybersecurity, communications, and incident management capabilities. The geo-tagged information received by the PSAP indicates the incident is located on Interstate 10, at mile marker 101. An orbiting public safety unmanned aerial vehicle (UAV) immediately shifts course, and begins obtaining live video of the scene. The video from the UAV, in conjunction with video and audio live from callers at the scene, conclusively show eight vehicles involved in the incident, including a tractor-tanker with a four sided, diamond shaped red placard clearly affixed onboard. The placard has the number “1203” printed in white letters in the middle, with a smaller number “3” underneath.

Along with a visual of the placard, received from multiple sources over broadband-enabled networks, the fully integrated CAD system performs a simultaneous lookup of the placard and presents both the video information and the listing of the United Nations Hazardous Material (UN HAZMAT) code definition. The information indicates that this placard represents a Class 3 flammable liquid, which is a flammable liquid with flashpoint of not more than 60.5°C (141°F), or any material in a liquid phase with a flashpoint at or above 37.8°C (100°F). In this specific case, based on the numbers “1203,” the liquid is gasoline.

The cognitive dispatch system makes immediate resource and dispatch recommendations to the PST, along with recommending tasking the UAV with orders for a new set of video information based on wind speed and direction also provided via broadband information services directly linked to the PSAP systems. Additionally, based on ground, airborne, and satellite imagery and audio, in combination with automatic crash notification and biometric data from callers’ wearables, streamed directly to the PSAP via broadband, the NG9-1-1 center’s systems determine there are at least two Level 2 trauma patients and one Level 1 trauma patient at the scene. Per local protocols, three airborne medical evacuation helicopters are dispatched at the push of a button by the tactical PST,[6] and immediately upon powering up onboard systems, the crew begins to receive common information about the scene and their patients.

The PSAP dispatches units, including specialty resources such as HAZMAT technicians, from multiple jurisdictions. Despite the disparity of devices and software used by the various agencies, all PSAPs and responding units including law enforcement, fire/rescue, and EMS agencies begin receiving real-time feeds of audio and video data via NPSBN-based systems from the host PSAP. Fully interoperable voice and data communications allow the units who arrive first on scene to provide up to date, real-time information to additional units responding to the scene regardless of which agency they are from. PSAPs, though they have different CAD and radio systems, can communicate and receive common updates via interoperable, standardized CAD interfaces. This is possible due to the interoperable nature of the NPSBN, and the fact that NG9-1-1 will enable transfer of data, in real time, from one PSAP to another. As a result, not only will the PSAPs be able to keep each other informed, each PSAP will be able to communicate the same data directly to responders. By design, FirstNet will enable subscribers to exchange incident data among agencies. Therefore, even if the responding agencies would be limited by having different radio systems (for voice communications) in today’s environment, in the broadband-based PSAP and responder agency of tomorrow FirstNet and NG9-1-1 have overcome proprietary limitations to afford both PSAPs and responding agencies data communications capabilities.

Upon arrival and establishment of command, the on-scene incident commander is immediately provided with control of the UAV, and can obtain a direct feed of incoming audio and visual data to the command vehicle or hand-held portable device and begin a size up and tasking of resources. In addition, the incident commander has a direct link to the company operating the tanker, and gathers specifics about the amount of fuel still in the truck, the type of vehicle, etc. while also gathering wind speed and wind direction data. Additionally, responding EMS units receive any updates available from patient telemetry linked directly to each individual’s smartphone or biometric device. Airborne medical resources arrive within minutes of the first responder arrival, and orbit waiting for landing instructions. A clear landing zone (LZ) has been identified by the orbiting UAV and communicated to the incident commander, who has already moved resources to that location to secure the LZ and begin patient evacuation. Throughout the incident, PSTs monitor biometric sensors on first responders, assisting the incident commander with resource management based on data analytics that assess exertion levels of fire/rescue personnel and exposure sensors on HAZMAT technicians.

As should be evident by now, the future holds great promise for public safety communications. The ability to link multiple systems, as illustrated by this scenario, is only one part of the future. Fully interconnected vehicle and patient sensors, cognitive systems in the PSAP, FirstNet-based broadband services to the responders, and the availability of almost any needed service at the touch of a button are possible. At the center of this future and critical to fully realizing this vision of a fully interconnected public safety world is the PSAP. Whether processing initial calls, texts, and multimedia feeds or making use of multiple "smart" resources, the PSAP and the professionals who make it function are truly the nerve center of every response. From routine calls to major events, it is the PSAP that represents not only the first link in the response chain, but the critical hub through which all communications flow from start to finish of any incident. The PSAP is now the focal point of a fully interconnected public safety communications landscape. No longer just an "answering point," the PSAP of tomorrow is an emergency communications hub, a tactical intelligence center, and a unified command and control entity for all responding agencies and personnel.

ACHIEVING THE VISION

As the previous examples illustrate, the broadband-driven future promises new opportunities for public safety communications professionals to vastly improve the efficiency and effectiveness of emergency response. APCO's vision of the future for public safety communications is where devices, people, and places are all interconnected in an interoperable, secure, real-time, location-defined environment with multimedia-based interactive communications.

To achieve this vision, Project 43 was established to identify the impacts of broadband technologies and develop recommendations to maximize the benefits and minimize the challenges for the public safety communications community.

In the sections that follow, the report presents findings and recommendations concerning the implications of broadband technology on operations, governance, cybersecurity, technology, training, and the workforce. Operations are the starting point because, notwithstanding any other factors, this report is focused on what is necessary to ensure an effective emergency response. PSAPs must have the resources needed to effectively incorporate and utilize broadband and NG9-1-1 technologies, including methods of processing and preserving the new data and information that will become available. This will require development of new or modified standard operating procedures, best practices, and protocols.

Ensuring interoperability from the outset is an essential component of successful adoption of broadband technologies. Interoperability requires use of widely deployed commercial standards,[7] and other standards approved through organizations such as the American National Standards Institute (ANSI)[8] (which accredits the procedures of standards development organizations to ensure openness, balance, consensus, and due process) and that are proven to achieve and maintain seamless interoperability among PSAPs, emergency services IP networks (ESInets), originating networks, FirstNet, and other government and public safety enterprise networks.

In addition to interoperability, success also depends upon establishing effective governance and cybersecurity foundations. Governance structures may take several forms, but with the right features can lead to well-planned, sufficiently-funded, and accountable deployments and operations. Cybersecurity is a present and evolving challenge that requires significant vigilance through training and best practices. Threat detection and prevention can be accomplished via shared resources, which can help to concentrate the expertise necessary for this complex field, reduce costs, and lead to more effective and efficient cybersecurity of NG9-1-1 and other public safety networks.

The technical implications of broadband are profound – PSAPs will be making a large leap from decades-old, legacy technology to current technologies enjoyed by consumers and soon by FirstNet users. From video, to hosted and cloud-based services, data analytics and cognitive technologies, the opportunities for broadband technology to enable a more effective and efficient emergency response are significant.

These technologies, accompanied by a new operational environment, updated governance and related laws and regulations, and cybersecurity awareness, all point to substantial emphasis on the need for training. Training requires initial and sustained attention and priority to ensure PSTs are best equipped to perform the increasingly complex and critical tasks they will confront and embrace. This includes the changed nature of stress that PSTs will face due to both the increased volume and intensity of data and imagery that will flow from the public and field responders into the PSAP.

To meet the new NG9-1-1 opportunities and challenges, the future PSAP workforce will need to evolve. While attributes such as professionalism and dedication to service will remain essential, PSTs will need new skills and training to manage the opportunities and challenges of a broadband environment.

Most findings and recommendations throughout the sections of this report focus on state and local stakeholders but a key recommendation is the opportunity for congressional action to assist with modernizing 9-1-1 networks throughout the country. Achieving NG9-1-1 is essential to the safety and security of the general public and first responders, and a national imperative. A significant federal grant program is needed to: provide the capital to upgrade legacy networks and equipment to IP-based, broadband-enabled, NG9-1-1 systems; provide incentives to achieve interoperability, economies of scale, and sustainable funding mechanisms by states and localities; and eliminate, once and for all, the practice of some states to divert fees collected for 9-1-1 to other purposes.

This report compiles the major findings and recommendations for achieving the stated vision. It concludes with summarizing next steps and particular commitments of APCO to begin addressing the broadband implications for the PSAP. ■

Notes

[1] For simplicity, "PSAP" is used throughout this document. One of this report's recommendations, however, is broader adoption of the term "ECC" to better encompass the nature of public safety communications centers.

[2] http://www.npstw.org/.

[3] www.firstnet.gov.

[4] Cognitive services analyze and interpret a wide variety of data, including unstructured text, images, audio, and video. Basically, they "learn" from each transaction and become capable of analyzing "big data" and differentiating actionable information from background information. In addition, if properly implemented, these services can provide advanced capabilities which would include recommendations based on learned "personalities," tone, and even emotion. Advanced solutions will utilize machine learning to grow knowledge in applications and systems and will also provide the benefit of advanced quality assurance capabilities.

[5] Trends in Smart City Development, National League of Cities (Jan. 5, 2017), http://www.nlc.org/find-city-solutions/city-solutions-and-applied-research/urban-development/trends-in-smart-city-development-report-landing-page.

[6] A "tactical PST" operates in the field as part of a critical incident management team to support tactical command staff.

[7] "Widely deployed commercial standards" means those that are proven to achieve and maintain seamless interoperability among the hundreds of millions of connected devices and networks in use around the globe, regardless of manufacturer, device, operating system, platform, etc. Examples include standards developed by the Third Generation Partnership Project (3GPP), the Institute of Electrical and Electronics Engineers (IEEE), the Alliance for Telecommunications Industry Solutions (ATIS), the Internet Engineering Task Force (IETF), and the International Telecommunications Union (ITU), and successfully implemented in truly interoperable, device and network agnostic fashion. These are the standards that have led to the notable success of the industries encompassing the current, planned, and future origination networks delivering voice and data to PSAPs, and that will be employed by FirstNet.

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

OPERATIONS

INTRODUCTION

Operations is where the stark reality of an emergency situation is confronted by public safety communications professionals. The day-to-day processing of emergency calls, which occurs at the local level, is the first layer of any response. Technical solutions will only work if they are interoperable, intuitive, and useful to 9-1-1 professionals staffing or managing PSAPs. Operational impact must be factored into all aspects of design and implementation of technology, and requires close coordination with technology and information services departments. Additionally, when grounded in a well-developed governance structure and cybersecurity framework, operational considerations will drive training and workforce requirements.

> *The time is now to embrace the opportunities and minimize the challenges that broadband will bring to operations.*

The receipt and processing of broadband data from NG9-1-1 and FirstNet will have a number of substantial impacts on PSAP operations. Policies must address all functional elements including call processing, CAD, GIS, location technologies, ESInet, records management system (RMS), recording, data processing, management and evidence retention, as well as dispatch console (radio and NPSBN) operations. Further, policies should address how staff interact with each of these elements, the capacity of the workforce and PSAP systems to handle the amount and type of data involved, the role of technology and service providers, and the different ways PSAPs will interface with the public, responders, third party providers, and other systems and databases. This requires an evaluation of a variety of potential policy solutions and areas of improvement to existing consensus-based standards and best practices.

> *The receipt and processing of broadband data from NG9-1-1 and FirstNet will have a number of substantial impacts on PSAP operations.*

The nation's 9-1-1 networks are among the last still entrenched in legacy technology, and are quickly becoming an island in the middle of advanced technologies available to the public and soon to come to first responders over the NPSBN. Like the experience in the private sector, broadband technology will completely revamp 9-1-1 and emergency communications. The time is now to embrace the opportunities and minimize the challenges that broadband will bring to operations. Interoperability, cost-effectiveness, innovation, and cybersecurity can and should be the goals to achieve at the outset.

THE OPERATIONS ROLE

The ability to share information across jurisdictions is limited today but also bound to grow significantly with use of IP and broadband technologies. Examples of how information sharing could be leveraged by public safety agencies and resources include but are not limited to:

- Home medical devices designed to store and share patient information with emergency responders.

- Electronic health records made available to doctors before the patient arrives at the hospital and soon to the responders in the field to assist with pre-hospital emergency treatment.

- Building records and floor plans could be sent through CAD to incident command.

- Broadband interfaces could connect on a much larger scale to numerous camera systems and detectors including at schools, public gathering places, and critical infrastructure facilities allowing for real-time situational awareness.

- Officer-worn body cameras will have the ability to transmit video to the PSAP and supervisors in real time for immediate situational awareness.

- Video from security surveillance systems at residences and businesses that are triggered by an alarm can be streamed live to PSAPs and shared with responders.

FINDINGS

Broadband technology will impact almost all aspects of operations. The following is a non-exclusive list.

Funding

Sufficient funding is essential for both the initial capital expenditure to purchase the networks, equipment, software, hardware, and applications needed to move from legacy to new technology, and the operating expense to sustain, maintain, and upgrade these technologies. Congress to date has established limited grant programs, but a more substantial grant program to modernize 9-1-1 services across the country is a national imperative. This would help ensure that PSAPs across the country have the resources needed to upgrade in approximately the same timeframe, while preserving the responsibility of state and local governments to address funding for workforce, training, and sustainability.

Policy Development

The current 9-1-1 environment supports a structured process with relatively clear delineation of responsibilities as defined by statutes, rules, standard operating procedures, and guidelines for call processing. Broadband-based NG9-1-1 introduces complexities into this structure requiring increased coordination and partnership with other stakeholders, including other local PSAPs, regional or consolidated 9-1-1 centers, fusion centers, real-time crime centers, hospitals, supporting agencies such as utilities, departments of transportation, federal agencies such as the Department of Homeland Security (DHS),[9] and the private sector such as alarm companies and private ambulance services. Not only will all of these entities serve as resources of data and information sharing, a connected, broadband-enabled network of PSAPs across the country will, for the first time, be able to act as a sensor network and indicator of developing trends and threats. This will necessitate reexamination of certain existing governance and policy structures and call flows, as well as new or modified APCO standards.

Standard operating procedures will be needed to address handling each type of broadband data (voice, text, photo, video, sensor, etc.). Procedures will also need to account for:

- Increased call or session times
- Errors made by the public
- Legitimacy of the information
- Potential for real-time text and video chatting with the public and responders

- Opportunities to send media back to 9-1-1 callers, including instructional materials and photos (such as to verify a suspect or location)
- New technological options for communications with non-English speakers, and hearing and visually impaired callers
- Hosted services including CPE, CAD, and RMS
- Sharing and exchanging data with first responders, hospitals, support agencies such as departments of transportation, utilities, and private companies such as alarm companies
- Management of the data (how received, analyzed, shared, retained, and stored)
- False or unconfirmed alarms from automated systems and sensors
- Implementing systems (such as the APCO ASAP program) that substantially reduce errors and delays

IP and broadband technology will make a marked improvement in the ability and ease of transferring information between PSAPs. Fully interoperable ESInets will be key to data exchange. However, policies will need to govern when and how to transfer a call to ensure seamless operations and to cover shifting responsibilities over the data such as for record management and liability.

Policies and procedures will also, for some time, need to address the transition period as IP connectivity and broadband technology are introduced. While this transition period ideally should be kept as short as possible, PSAPs will need to contend with the various stages of legacy, transitional, and fully deployed NG9-1-1 and broadband technologies.

Simultaneously Triaging Multimedia Data from Multiple Sources

Call processing times will vary depending on the type of information being received. For voice calls or text messages, call processing times are more readily established and managed. But with the introduction of multiple types and sources of data in addition to or in place of voice calls, and the need to process this information as part of an overall response, operations will need to make adjustments to measure and manage call flows and processing times. At the same time, PSTs will continue to perform many of the same fundamental tasks they perform today: triage (where is the emergency, what is the nature of the emergency, are weapons involved, number of injured, when the emergency occurred, what is the callback number), classification of the information received, and conveying information to field responders.

In the broadband environment, PSAPs may need to create a new position or function for a data or intelligence analyst.

In the broadband environment, PSAPs may need to create a new position or function for a data or intelligence analyst to triage multiple sources of information concerning the same or unrelated incidents, in order to determine what multimedia data is critical to forward to responders immediately, versus what data is more “background noise” or evidentiary rather than actionable. The work of the data or intelligence analyst may at times need to be coordinated with other public safety agencies.

The analyst function may require certain certifications or core competencies, and likely would be a specialty skill requiring cross training or additional staff positions. Particularly for data mining technology applied to social media outlets, data mining specialist positions may also be needed. It is becoming increasingly more common for a first report of an incident to be posted on social media before a 9-1-1 call is made.

Priority must be given to information of an emergent nature, such as crimes in progress, HAZMAT situations, fire and medical emergencies, etc. Also, decisions need to be made as to what type of information can or should be sent based on the role of the particular responder receiving the information. For example, a police officer rushing to a scene, who is focused on speed of arrival and the immediate environment, cannot necessarily absorb an abundance of information. There are also practical considerations – if a fire response typically occurs within minutes of time, determining what information is most critical, at what particular moments, and to whom to send the information

to during the response will be necessary. Further, since responders using the NPSBN will have new options for receiving information, such as through touch screens, hands-free devices, messaging, etc., PSAPs will need to decide how and in what format to send information to responders. Many agencies are already deploying PSTs tactically to the field, whether for pre-planned events or major incidents. Similar to field responders, tactical PSTs will be afforded additional broadband-enabled means to communicate with the PSAP, and this too will require consideration.

Today, multiple reports to 9-1-1 can come from the same incident, such as a traffic accident. In a full NG9-1-1 environment, this would now include multiple photos, videos, and other data coming not only from the public, but from field responders, surveillance cameras, drones, as well as sensor data such as vehicle telematics, biometrics, gun shots, chemicals, etc. Further, these sources of multimedia are not necessarily fixed in time, but can yield continuous and dynamic information, requiring continued vigilance. The analyst and PST could be aided by systems being developed with data mining, intelligence, or cognitive (self-learning) capabilities that identify key indicators and provide dispatch recommendations. However, operations would always need to account for the human element in emergency response. The human element is the value that PSTs add regardless of the technology available to them, based on their training and interview skills (such as EMD questions, obtaining suspect descriptions, identifying fire exposures or entrapment data). Ultimately, it is the experience and expertise of PSTs that best ensure a successful response.

There will also be numerous sources of additional information from the public that will tax resources. With all of the potential ways that the public could communicate with 9-1-1, PSAPs large and small will also need to contend with reports made through mobile apps, social media, and crime tip portals. Many of these reports will not be emergencies and may be more numerous as compared to today's non-emergency voice calls. Further, with the consumer expectation for immediate response typical of their personal experience with texts, social media, and mobile apps, the PST will need to remain focused on emergencies while balancing the public's expectation for an immediate answer to their inquiries. At the same time, standard operating procedures will need to address how to handle, preserve, and store the information received from the public in a way that is compliant with relevant laws and regulations.

Ultimately, it is the experience and expertise of PSTs that best ensure a successful response.

Broadband technology will also provide new options for PSAPs to send alerts and notifications to the public. In addition to official outlets, such as the Emergency Alert System and Wireless Emergency Alerts, there are a number of alerting and Emergency Notification Systems (ENS) currently on the market. All require the input of information and selection of the area to be notified. Many PSAPs and state and local agencies have web pages and social media forums as well. Public alerts and notifications can be very helpful to reduce or focus 9-1-1 inquiries and reports. PSAPs need to establish procedures for coordination of these numerous alerting platforms, selection and timing of emergency notifications, and compliance with applicable laws and regulations including storage and retention. It may be best to identify a supervisory level position to originate and execute alerts to permit the PST to remain focused on coordinating the response to the emergency, processing incoming calls and information, and updating responders.

PSAPs also need to determine how operations will complement and interact with other entities such as fusion centers that manage multiple sources of information and data.

Data Storage, Retention, and Evidence Control

The recording and archiving of voice, text, audio, photographs, video, data, location information, etc. is going to be a major operational concern. Consideration must be given to the open records acts, privacy, and evidence retention related laws for each state. Local requirements for retention of data will drive agency requirements for equipment or services. In addition, with certain hosted solutions, records may be retained in more than one place (such as for redundancy and security reasons) and consideration must be given to identifying the responsible custodian of record, such as for subpoena purposes.

Standard operating procedures need to ensure that the handling, disseminating, and storage of the information received are compliant with all local, state and federal laws and regulations.

Standard operating procedures need to ensure that the handling, disseminating, and storage of the information received are compliant with all local, state, and federal laws and regulations while still maintaining an orderly and efficient flow of data. This extends to the need for tracking the flow of information, and flagging information for confidentiality, evidentiary, chain of custody, and investigative purposes.

Maximizing Staff Effectiveness in the Next Generation PSAP

With the new forms of data that will be available to the PSAP, PSTs will need to triage information in a fast-paced, high emotion environment. Incident-related photos and video messaging, in contrast to voice calls, will have a different and more disturbing impact on PSTs, potentially leading to additional stress-induced issues. Because PSAPs are the concentration point for incidents, the exposure to high volumes of information and disturbing content may be especially intense on staff. Further, the unique responsibilities of PSAP personnel mean that they cannot necessarily take a break before responding to the next call for service from the public, processing new information from other agencies, or assisting first responders facing life-threatening situations.

Preparing staff for this type and level of activity, and hiring the right personnel to begin with, is key. As detailed in the Workforce section, hiring processes will need to adapt to the broadband-driven, rapidly changing environment, including adding new positions and functions such as data analysts. Agencies are already being asked to do more with the same staffing, or find ways within existing or declining budgets to hire additional staff with enhanced skillsets. This is unsustainable and, with

the approaching impact of broadband on PSAPs, will require the attention of leadership at all levels.

Training will be a critical aspect of preparing for and implementing broadband-based technologies and services.

As detailed in the Training section, training will be a critical aspect of preparing for and implementing broadband-based technologies and services. This extends to new positions (e.g., analysts), new responsibilities (evidence documentation and retention), new forms of EMD, and resulting stress brought on by imagery normally only experienced by field personnel. It will be important for agencies to provide information to employees regarding access to and participation in critical incident stress management (CISM) and other programs including employee assistance, health and wellness, and stress management. With the potential for additional critical incident stress, this may require reconsidering twelve hour shifts and creating shorter shift hours or split shifts.

Cybersecurity Hygiene and Requirements for the PSAP

In the legacy environment, PSTs have for the most part been immune to cybersecurity issues. The Cybersecurity section goes into much greater detail, but this threat is only going to grow, and even with hosted or shared solutions, must be taken into account throughout all aspects of PSAP operations for prevention, detection, mitigation, and recovery from cyber threats.

The Impact of Mobile Apps on the PSAP

Mobile apps, such as those used on smartphones and tablets, will play an increasing role both in the use by the public to contact 9-1-1, and by responders in the field using apps including those to be made available by FirstNet. Apps can make emergency response more effective and efficient by incorporating useful information in an easy and intuitive way to the user. PSAPs in turn will be able to receive and process information that apps make possible.

Through its "Application Community" (www.AppComm.org) website, APCO has led the way in helping to ensure that apps used for public safety and emergency response purposes are as effective and efficient as possible. APCO has also produced a helpful Fact Sheet on Mobile Apps and 9-1-1,[10] and a White Paper on "The Status of 9-1-1 Apps."[11] In addition, APCO has been partnering with DHS on a pilot project to advance interoperability and security of mobile apps.[12] Standards including a common way for apps to provide data to PSAPs are critical.

Important considerations for mobile apps include the necessity of open APIs (to avoid proprietary, non-uniform solutions), interoperability among PSAPs and responder agencies including seamless integration with CPE, CAD, GIS, and RMS, and cybersecurity and reliability (particularly if the app uses networks, databases, and servers outside of the trusted 9-1-1 network). Cost is also a consideration, especially if the public comes to rely upon an app and the PSAP is faced with a lack of funding or a cost increase for using the app. Further, app developers must appreciate and accept the responsibility and commitment that comes from producing a product used for emergencies.

Operationally, PSAPs need to ask developers questions about costs, interoperability, commitment, etc. and plan on ensuring sufficient liability protection and training. ■

RECOMMENDATIONS: OPERATIONS

Operational Standards

Standards are critical to effective operations, and to ensure interoperability, cost effectiveness, and innovation. For operations, new ANSI standards should be developed to address data triaging; real time evidence management, retention, and control; and interoperable interactions with other agencies. With the advent of a major transformation within 9-1-1 and emergency communications, this will be a large but valuable undertaking.[13]

Best Practices

The nature of broadband technology to lead to uniform deployments and applications across the country, while allowing room for local customization and control, provides opportunity for model best practices development. APCO will develop an online repository for PSAPs to post and share next generation best practices.

Resources and Funding

PSAP managers and directors should work to build their cases for new or modified personnel positions and the funding needed to upgrade and maintain needed services and equipment. They should also engage in a broad dialogue with IT departments and other existing or developing intelligence analysis centers to frame out respective operations and division of responsibilities. APCO will advocate at the federal level for a sufficient, effective, and efficient grant program for the initial capital needed to modernize 9-1-1 networks and equipment across the country.

Public Messaging and Education

The impacts on operations, from today's legacy systems through the transition and eventual completion of NG9-1-1, can be mitigated by a better informed public. For example, public education campaigns for nascent text-to-911 services have been successful in reinforcing the concept to "call if you can, text if you can't." As the expectations of the public become increasingly disconnected from the actual capabilities of PSAPs, 9-1-1 authorities and PSAPs should convey what services they currently offer.

Quality Assurance/Quality Improvement (QA/QI)

One of the larger impacts broadband capabilities will have is on QA/QI. Not only will calls continue to require review in a systematic and objective manner, but new data types, requirements, capabilities, and stresses will all have to be taken into consideration.

The following are recommended updates to the QA/QI program:

- Set clearly defined minimum standards and expectations for processing SMS/text-to-911 and multimedia/MMS calls. The QA/QI program must be understood by PSTs.
- Update pre-scripted "interview" questions for each public safety discipline (police, fire, EMS).
- Set minimum expectations for gathering critical criteria particularly for callers sending multimedia information (address, callback telephone number, nature of emergency, etc.).
- Establish new requirements for objective scoring categories and supporting standard evaluation guidelines for the handling of broadband information (below expectations, meets expectations, exceeds expectations, etc.).

- Maintain a log of all incoming SMS/text-to-911 and multimedia/MMS calls which are subject to random or requested/special review in the QA program.

- Access and print transcripts of SMS/text-to-911 and record and store multimedia/MMS calls along with other associated information (CAD event, ANI/ALI data, etc.).

- Review data, photos, videos, etc. associated with incidents to assess how this information was utilized by the PST.

- Provide appropriate training for conducting reviews on SMS/text-to-911 and multimedia/MMS calls to QA evaluators.

- Establish timeline benchmarks for conducting QA reviews on SMS/text-to-911 calls and multimedia/MMS calls (e.g., weekly, monthly, etc.).

- Establish an accountability process, training, performance improvement plans, and/or corrective action specific to SMS/text-to-911 and multimedia/MMS calls as required.

- Align standard operating procedures (SOPs) with those areas identified for improvement so that the SOPs can be used in future training related to use of broadband technologies (in-service training, remedial training, training bulletins, etc.).

- Implement or expand Critical Incident Stress Debriefing to address Post Traumatic Stress Disorder experienced by PSTs exposed to disturbing multimedia/MMS data.

Notes

[9] DHS provides a number of resources to support a robust information sharing environment. See https://www.dhs.gov/topic/information-sharing.

[10] http://appcomm.org/wp-content/themes/directorypress/thumbs/FactSheet_911Apps.pdf.

[11] http://appcomm.org/wp-content/themes/directorypress/thumbs/WhitePaper_911Apps.pdf.

[12] http://psc.apcointl.org/2016/11/10/apco-partners-with-dhs-to-advance-interoperability-and-security-of-mobile-apps/.

[13] On the technical side, NG9-1-1 standards are needed to ensure seamless interoperability, connectivity, and data sharing, especially among and between CPE, CAD, RMS, and radio and broadband communications consoles. However, until standards are both developed and implemented in a manner that PSAPs can rely upon as being "build to" or "end state" in nature, PSAPs need to make important inquiries of their vendors. See the Technology section for a more detailed discussion of this issue.

GOVERNANCE

INTRODUCTION

Governance is the foundation upon which the vision of the future of emergency communications must be built. A workable governance model must be agreed upon and implemented in order for any technical solution to succeed.

An examination of governance revolves around the legal and regulatory framework (laws and regulations) needed to facilitate the adoption, use, and handling of broadband technology at PSAPs. This includes issues related to coordination, funding, resource and data sharing, mutual aid,[14] redundancy, interoperability, liability, privacy, and the use of memoranda of agreements, interagency agreements, and similar vehicles. This section contains recommendations for governance approaches based on a survey of existing governance structures and trends.

A number of states have developed legal and regulatory frameworks that enable the planning and implementation of NG9-1-1.[15] These activities include legislation establishing new or updated governance structures, deploying IP connectivity, crafting and re-crafting funding mechanisms, and promoting coordination, mutual aid, and information and resource sharing. Though deployment progress varies, a handful of states and counties have issued requests for proposals (RFPs) for ESInets and other NG9-1-1 components, and commenced or completed some implementation.[16]

States that have established governance structures for deploying broadband networks such as NG9-1-1 are making the most progress. Governance bodies do not need to follow a particular approach - they can be state-driven, decentralized and locally-driven, or another format. But the common hallmark of success is to actively engage with local stakeholders, including PSAPs.

Key characteristics for governance success include:

- An inclusive, participatory statewide and/or regional governance structure that promotes coordination and collaboration
- Governance structures at the local levels for day-to-day management of 9-1-1 networks
- Champions among key stakeholder groups
- A strategic vision for the entire 9-1-1 ecosystem
- Sufficient, long-term funding mechanism with strong oversight, including no fee diversion
- Grant-making authority with incentives to achieve statewide goals
- Training support
- Rulemaking authority
- Cost efficiencies
- Enforcement authority
- Outreach and education
- Mechanisms to promote coordination, mutual aid, and information and resource sharing, including among public safety radio communications and the NPSBN

On the legislative front, states need to remove existing or legacy barriers to 9-1-1 modernization, update legislation to promote technology adoption and broadband network implementation, and craft new provisions to address the legal, regulatory, liability, and privacy concerns of a broadband environment.

THE GOVERNANCE ROLE

Governance is a fundamental concept in public safety communications. A governance structure is the underpinning for all that follows in establishing a broadband-rich environment for PSAPs across the country. Absent a sufficient governance structure, it is nearly impossible for PSAPs to carry out their missions, regardless of the technology or human resources available.

State and local governing bodies can and should enact laws and regulations, and/or establish governance structures that help achieve certain goals afforded by broadband technology. States also need to remove existing legacy barriers to 9-1-1 modernization, update legislation to promote technology adoption and broadband network implementation, and craft new provisions to address the legal, regulatory, liability, and privacy concerns in a broadband environment.

Data-Driven Policy Development

Broadband technology presents opportunities to capture and analyze large amounts of data, which in turn can be used to inform policy development and strategic planning. A data-driven approach can help establish business cases for funding and resources, as well as measure the success of governance structures in promoting adoption of broadband technology, ensuring adequate staffing and funding, and meeting mission objectives. Accordingly, mechanisms should be put into place to capture and analyze the data flowing into and generated by PSAPs.

Most states today already collect data on expenditures of 9-1-1 fees, as evidenced by the requirement of the Federal Communications Commission (FCC) to report annually to Congress on 9-1-1 fee diversion practices, including the cost to provide 9-1-1 service, amount of 9-1-1 fees diverted to other purposes, and NG9-1-1 expenditures.[17] This kind of data could be helpful for 9-1-1 authorities to plan for NG9-1-1 and develop sustainable funding mechanisms. Unfortunately, not all states possess a capability to collect and provide data. The data contained in the FCC's fee report help to illustrate the governance features that would be conducive to detailed data collection in the broadband environment:

- Common definitions and terminology (for example, of "NG9-1-1" and "cybersecurity")
- Reporting through a common system to an entity that receives a centralized report
- Mandating or providing strong incentives for reporting by local governments
- Commonality in accounting systems across local governments
- Collecting data from all types of 9-1-1 service

Effective Coordination

Governance includes the laws and regulations enacted by state and local governments and regulatory agencies, as well as bodies and entities created by these governments that are charged with carrying out certain responsibilities.

> *Effective governance structures facilitate a more rapid and cost-effective transition to NG9-1-1.*

Governance Structures

Effective governance structures facilitate a more rapid and cost-effective transition to NG9-1-1, and can provide centralized support or oversight, technical and operational expertise, planning assistance, and requirements or incentives that foster broadband deployment. Governing bodies do not need to follow a particular model to be effective. They can be state-driven, decentralized and locally-driven, or a hybrid approach.

The following are some illustrative examples:

- Pennsylvania amended its emergency services statute, which modernized the duties of the Pennsylvania Emergency Management Agency (PEMA), created the 9-1-1 Advisory Board to assist PEMA, established a 9-1-1 Fund (previously the Wireless E9-1-1 Emergency Services Fund), required development of an NG9-1-1 plan, extended liability protection to providers of NG9-1-1 technology, and modernized statutory definitions, by adding definitions of NG9-1-1 service and NG9-1-1 technology among others.[18]

  PEMA can consult with the 9-1-1 Advisory Board to establish a statewide NG9-1-1 plan, including a statewide interoperable IP network using NG9-1-1 technology.[19] The 9-1-1 Advisory Board, which consists of diverse stakeholders including at the local level, can advise the agency on plans to deploy NG9-1-1 technology, and promote sharing of information among the agency, 9-1-1 systems, and other state and local agencies relating to the operation and improvement of 9-1-1 systems.[20]

- North Carolina enacted legislation that created an NG9-1-1 Reserve Fund, requires PSAPs to implement NG9-1-1, authorizes the 9-1-1 Board to establish purchasing agreements for statewide procurement, allows the PSAP grant account to be used for expenses to enhance the 9-1-1 system, amends liability for the 9-1-1 system, and updates the 9-1-1 statutes to include new technology.[21]

  The NC 9-1-1 Board has 17 members including eight local officials, eight vendors, and a Chief Information Officer of the Department of Information Technology (IT) or Designee as Chair of the Board, and has a Technology Committee with an NG9-1-1 focus.[22] The Board oversees statewide planning and implementation of 9-1-1. The Board is charged with (1) developing a 9-1-1 plan, (2) establishing policies, procedures, and standards for PSAPs and backup PSAPs, including for cooperative purchasing agreements or other contracts for the procurement of goods and services, and funding advisory services and training, (3) managing and distributing the 9-1-1 Fund, (4) investigating the revenues and expenditures associated with the operation of a PSAP to ensure compliance with restrictions on the use of 9-1-1 funds, (4) adopting rules necessary to perform its duties, and (5) producing or acquiring public education materials regarding the proper use of 9-1-1.[23]

- Indiana established the Statewide 9-1-1 Board to oversee 9-1-1 implementation, including the administration of fees to fund local PSAPs and the operation of the statewide ESInet.[24] The Board can also adopt and enforce rules, and develop, maintain, and update a statewide 9-1-1 plan.[25] The Board consists of 15 members, including a number of local stakeholders.

Planning

Several states have enacted legislation that requires a 9-1-1 modernization study or the development of an NG9-1-1 plan:

- California passed legislation requiring the Office of Emergency Services to develop a plan and timeline of target dates for the testing, implementation, and operation of an NG9-1-1 emergency communication system, including text-to-911 throughout California.[26]

- Colorado passed a law creating a Task Force on 9-1-1 Oversight, Outage Reporting, and Reliability for the purpose of studying issues surrounding and making findings and recommendations for the improvement and deployment of 9-1-1 service, which included studying and determining whether the current funding sources and amount of funding are sufficient for providing existing 9-1-1 service and transitioning to NG9-1-1 service.[27]

- Georgia passed a Senate resolution that created a Senate Study Committee on 9-1-1 System Modernization.[28]

Improving Operations

Resource and Data Sharing

Broadband technology, and NG9-1-1 by its nature, increases PSAPs' ability to share resources and data. For example, multiple PSAPs across a region or a state may share GIS, cybersecurity protection, or even their workforce and agency-managed data for mutual aid. Effective governance can:

- Allow, promote, or require infrastructure, equipment, technology, and data sharing among PSAPs
- Require the development of uniform technical and operational procedures and standards
- Promote the creation of multijurisdictional entities and mutual aid agreements
- Encourage PSAPs to share information across jurisdictions

Examples: California requires the NG9-1-1 system, where consistent with public safety and technologically feasible, to incorporate shared infrastructure and elements of other public safety and emergency communications networks;[29] Pennsylvania enables PEMA and the 9-1-1 Advisory Board to establish and publish uniform 9-1-1 technology standards and promote information sharing among agencies;[30] and the Oklahoma 9-1-1 Management Authority encourages sharing of equipment, technology, and information among PSAPs.[31]

Some PSAPs have used tools such as memoranda of understanding (MOUs) and interlocal agreements to facilitate resource and data sharing. For example, the Mendocino Next Generation 9-1-1 project in California, which aimed to provide a network-based NG9-1-1 service among three PSAPs, began with a MOU.[32] The Counties of Southern Illinois Next Generation 9-1-1 Project was formed through an interlocal agreement allowing a number of counties to share an NG9-1-1 system, including an ESInet.[33] In Ohio, counties that wanted to participate in the OARnet ESInet Test Pilot Program were required to sign MOUs.[34] In Wyoming, the Laramie County Combined Communications Center, the City of Laramie Police Department, and the Laramie/Albany County Records and Communications Center entered into a MOU in furtherance of the deployment of NG9-1-1 and an ESInet, which enabled the sharing of customer premise equipment to improve 9-1-1 call taking and dispatching services.[35] In its 2016 Statewide 9-1-1 Plan, Pennsylvania planned to develop and execute a MOU with any PSAP, public safety agency, or critical infrastructure facility that is requesting connectivity to the Commonwealth ESInet by the end of 2017.[36] The Michigan Upper Peninsula 9-1-1 Authority ESInet Project was formed by 15 counties entering into an interlocal agreement.[37] The Kansas 9-1-1 Coordinating Council stated a MOU will be "executed between the Council and any PSAP electing to subscribe to the NG9-1-1 System prior to ordering of related hardware, software, and connectivity."[38] And Southeast 911, a Nebraska Joint entity, formed an interlocal agreement that provides for a Regional Governing Committee "to facilitate the planning and coordinate the delivery of emergency communications services including Enhanced 9-1-1 (E 9-1-1) and emerging services such as next generation 9-1-1 (NG9-1-1)."[39]

Redundancy

The increased connectivity between PSAPs that will continue with the growth of broadband technology creates new opportunities to ensure redundancy. Some laws and regulations explicitly require NG9-1-1 systems to have redundancy built into the network or include redundancy as an element in the definition of NG9-1-1 or NG9-1-1 network.

Example: North Carolina requires the 9-1-1 Board to ensure individual PSAP plans incorporate a backup PSAP.[40]

Interoperability

Laws and regulations across all states should uniformly ensure seamless interoperability among PSAPs, ESInets, originating networks, FirstNet, and other government and public safety enterprise networks. This will be key to ensuring that all PSAPs have the technical capabilities for interoperability including for mutual aid, as well as for increasing competition, achieving economies of scale for the costs of equipment and services, and enabling public safety to keep pace with advances in the commercial sector.

Example: Virginia requires the 9-1-1 Services Board to establish standards for an ESInet and core NG9-1-1 services to ensure that enhanced public safety telephone services seamlessly interoperate within the Commonwealth and with surrounding states.[41]

Governance also has a non-technical role for achieving interoperability. State and local governments can encourage mutual aid capabilities through the formation of agreements between PSAPs, counties, municipalities, or other local entities.

State and local governments can encourage mutual aid capabilities through the formation of agreements between PSAPs, counties, municipalities, or other local entities.

Examples: In Pennsylvania, PEMA is "to cooperate with county and regional 9-1-1 systems to develop interconnectivity of 9-1-1 systems through the establishment, enhancement, operation and maintenance of an Internet protocol network."[42] Additionally, legislation empowers counties to execute mutual aid agreements and cross-service agreements necessary to implement their 9-1-1 plans.[43] According to Connecticut law, municipalities may enter into an interlocal agreement to jointly perform any function.[44] Oklahoma legislation states that PSAPs may enter into local cooperative agreements.[45] Kentucky law states that "any local government, or any combination thereof, may with the approval of their governing bodies enter into an interlocal cooperation agreement creating a joint 9-1-1 emergency service."[46]

Keeping Pace with Advanced Technology

Technology Adoption

As technology continues to evolve, coordinating entities can help by offering centralized support (at the state or regional level) to assist with planning or provide technical and operational expertise. Further, state coordinating entities typically solicit and reflect the input of a variety of key stakeholders, which helps drive adoption and buy-in of newer technologies throughout the 9-1-1 community. When technology solutions are developed and led by a coordinating body with stakeholder involvement, there is greater likelihood of technology adoption, particularly if the solution meets operational needs and is cost-effective.

On the other hand, outdated state laws and regulations can have the opposite effect by presenting obstacles to adoption of broadband technology including NG9-1-1. These tend to focus on legacy, circuit-switched technologies and processes, such as continued reference to tariffs and local access and transport areas (LATAs) as defined by the regulated telephone companies, and contain outdated or insufficient funding and liability protection schemes. Many state regulations still treat 9-1-1 service as a single-provider system accompanied by legacy requirements which do not translate well to a competitive NG9-1-1 market, and the resulting disincentives to new entrants can be significant.

Examples of legacy technology regulations include 9-1-1 system service provider (SSP) certification restrictions, and regulations that impede IP-based routing. These obstacles can impact a variety of stakeholders, including PSAPs, carriers, technology companies, and 9-1-1 SSPs. A 9-1-1 SSP certification requirement can delay entities that offer NG9-1-1 services to PSAPs for many months, or simply prevent some SSPs from providing broadband technology or services to PSAPs.

Additionally, a key feature of broadband and NG9-1-1 architecture is the IP-based routing of calls. IP-based routing assumes the presence of databases and servers to properly route the call and is completely different than the network components that support legacy 9-1-1 systems. Rather than using IP-based routing, legacy networks use selective routers owned and operated by incumbent local telephone companies. Thus, absent modification, existing laws and regulations may inhibit IP-based routing and thus NG9-1-1 architecture. In some cases, it may only take updating existing laws and regulations to account for NG9-1-1.[47]

Procurement

With the expanded range of technologies made available through broadband comes the opportunity for a much larger ecosystem of manufacturers and service providers. The FirstNet legislation embraced this opportunity for first responder communications by imposing a number of requirements on procurement practices and equipment.[48] Similarly, changes in state or local laws or regulations may be needed to ensure that procurement practices (such as requests for proposals) are fair, open, transparent, and competitive. In this way, states can expand the potential pool of vendors. Further, states and localities can use procurement vehicles to explore synergies among broadband networks purchased for other state agencies to meet the transport, capacity, and redundancy requirements for NG9-1-1.

Funding

Insufficient funding mechanisms impede the deployment of NG9-1-1 systems, as does the current practice of some states in diverting fees collected for 9-1-1 purposes. Many state and local funding mechanisms do not adequately account for new services that offer emergency communications in an NG9-1-1 environment. For example, 9-1-1 funding mechanisms that are specific to legacy 9-1-1 access technologies would not apply to or sufficiently account for all types of services delivering broadband information to PSAPs including NG9-1-1. Moreover, once funding sources are established or expanded as the case may be, states may need to modernize allowable costs to account for broadband-based technologies.

A statewide funding mechanism can help ensure that NG9-1-1 service is provided and adopted throughout the state, in cities and rural communities, and everywhere in between. The authority to conduct audits and take enforcement actions can ensure that fees are being collected properly and actually spent on improving and enhancing 9-1-1 services, rather than being diverted to other non-9-1-1-related uses. PSAPs need a funding mechanism that is dependable, protected, and sustainable.

> *A statewide funding mechanism can help ensure that NG9-1-1 service is provided and adopted throughout the state, in cities and rural communities, and everywhere in between.*

Legal Protections

A broadband environment introduces a number of additional legal issues to PSAP operations. Action by federal, state, and local governments becomes increasingly necessary in order to permit proper use and adoption of broadband-enabled technologies and data. These matters can be addressed through legislation, regulations, or MOUs and other interlocal agreements.

Liability

As a matter of public policy, federal and state liability protection can encourage private companies to innovate and serve the 9-1-1 community. Some states have modernized their 9-1-1 legislation to explicitly extend liability protection beyond legacy service providers to voice over IP (VoIP) and NG9-1-1 providers.[49] Liability protections can address issues ranging from those related to 9-1-1 systems and services to the disclosure or release of subscriber information. Additionally, MOUs and interlocal agreements among cities and counties or PSAPs may also determine the extent of liability of each party to the agreement.

In the Next Generation 9-1-1 Advancement Act of 2012, Congress extended the parity of protection from liability to a provider or user of NG9-1-1 services, a PSAP, and the officers, directors, employees, vendors, agents, and authorizing government entity (if any) of such provider, user, or PSAP.[50] In other words, for NG9-1-1, the liability protection is to be not less than the scope and extent of immunity or other protection from liability that any particular state currently offers. Therefore, that still leaves open vulnerabilities where, for example, a state currently ties protection to telephone company tariffs that may be too inflexible to extend to NG9-1-1, or in states that presently have no liability protections.

Two recent examples of updated liability protections can be found in legislation passed by North Carolina and Connecticut. Under North Carolina law, liability is extended to NG9-1-1 system providers: “Except in cases of wanton or willful misconduct, a voice communications service provider, and a 9-1-1 system provider or next generation 9-1-1 system provider, and their employees, directors, officers, vendors, and agents are not liable for any damages in a civil action resulting from death or injury to any person or from damage to property incurred by any person in connection with developing, adopting, implementing, maintaining, or operating the 9-1-1 system or in complying with emergency-related information requests from State or local government officials.”[51] This includes but is not limited to “(1) The release of subscriber information related to emergency calls or emergency services. (2) The use or provision of 9-1-1 service, E9-1-1 service, or next generation 9-1-1 service. (3) Other matters related to 9-1-1 service, E9-1-1 service, or next generation 9-1-1 service.”[52]

Connecticut law extends liability protection to NG9-1-1 systems by stating: “No telephone company, certified telecommunications provider, provider of wireless telecommunications service, as defined in section 28-30b, as amended by this act, pursuant to a license issued by the Federal Communications Commission, provider of prepaid wireless telecommunications service, voice over IP service provider or the officers, directors, employees, vendors or agents of any such company or provider shall be liable to any person or entity for release of the information specified in this section or for any failure of equipment or procedure in connection with the enhanced 9-1-1 service, an emergency notification system, or the next generation 9-1-1 telecommunication system established under sections 28-25 to 28-29b.”[53]

Privacy

The introduction of multimedia content, mobile apps, social media, video (including video chatting), drone surveillance, etc. will lead to the collection and use of additional types and larger amounts of information than that collected and used in a legacy environment. New technologies will incorporate human recognition capabilities and a person’s location, enhanced with additional context that can predict future locations and add more personally identifiable data. Related to privacy is the cybersecurity of devices and data, which is addressed separately in this report.

A growing number of state laws and regulations address the disclosure of certain types of consumer data, and may also limit the types of data that can be collected and retained. The availability of broadband data from a growing number of potential sources will require a framework guiding what records may be relied upon or require authentication, and how the records are to be used, stored, protected, accessed, and disposed of by PSAPs. MOUs and interlocal agreements can be employed to address which parties are responsible for the collection, control, and retention of data, and which parties are responsible if a data disclosure occurs. Individual PSAPs may need to amend their privacy or data policies so that they are suitable for a broadband environment.

Public Records

The definition of a public record may need to be updated to include new forms of personal identification information other than name, address, and telephone number, such as pictures, video, and text. For example, Maine updated its confidentiality of system information law to include “personally identifying information of a caller to a public safety answering point,” meaning “any information that directly or by reasonable inference might disclose the identity of or personal information about a specific person or persons.”[54]

Other legal issues in a broadband environment that require renewed attention include chain of evidence, the Freedom of Information Act (FOIA), and the Health Insurance Portability and Accountability Act (HIPAA), etc.

FINDINGS

Governance Structures Can Facilitate NG9-1-1 Deployments

Many states have established NG9-1-1 governance structures, ranging from approaches that are top-down and state-driven to those that are decentralized and locally or regionally driven. Regardless of the approach, state structures typically include some level of local participation and provide for a 9-1-1 coordinating entity that is often charged with duties and responsibilities such as planning and implementing 9-1-1, administering and distributing 9-1-1 funds, establishing necessary policies, procedures, and rules, entering into contracts and agreements, monitoring and responding to technological change, assisting with training, and reserving to individual jurisdictions more localized management of 9-1-1 systems.

Outdated Laws and Regulations Impede NG9-1-1

Some states maintain outdated legislation and regulations that focus on legacy, circuit-switched technologies and processes or have outdated or insufficient funding and liability protection schemes, which present obstacles to adoption of broadband technology, and particularly NG9-1-1. A sufficient and enforceable funding mechanism is especially important to sustain an NG9-1-1 system and to promote broadband technology adoption and use. Additionally, lack of state or local laws that enable or at least permit establishment of appropriate governance structures can impede adoption of broadband technology and NG9-1-1 deployment.

State Laws and Regulations Need Updating

Before, during, and after the transition to an NG9-1-1 network, states will need to take steps to enact or modify laws and regulations. A number of states have already taken steps and updated or introduced 9-1-1 legislation to modify or include a 9-1-1 funding mechanism, encompass NG9-1-1 and broadband technologies, enable IP connectivity, and promote coordination, mutual aid, and information and resource sharing within and among PSAPs and other public safety entities.[55]

States Lack a Common Definition of NG9-1-1

Aside from the common reference to IP-enabled communications, state definitions and requirements for NG9-1-1 vary significantly. Some say NG9-1-1:

- Enables the user of a communications service to reach an appropriate PSAP by sending the digits 9-1-1 via any technological means[56]
- Must be designed to "provide access to emergency services from all connected communications sources and to provide multimedia data capabilities for [PSAPs] and other emergency services organizations"[57]
- Is a system that "provides standardized interfaces" and conforms to the federal definition of NG9-1-1 services[58]
- Provides "a hosted solution with redundancy built in"[59]
- Allows "immediate transfer of 9-1-1 calls, caller information, photos, and other data statewide"[60]
- Provides "a secure environment for emergency communications"[61]

The lack of common definitions creates confusion. Developing cost estimates, obtaining federal funding, procuring NG9-1-1 services through RFPs, and managing expectations are made more difficult as a result. ■

RECOMMENDATIONS: GOVERNANCE

States Should Establish a State-Level Coordinating Entity

- States should establish a coordinating entity that actively engages with local stakeholders, including PSAPs. The specific type of coordinating entity can vary. More important is that a governance structure exists to aid in the planning, implementation, and management of NG9-1-1 and broadband technologies, and that it incorporates local participation and local control. A statewide or regional coordinating entity will help to achieve economies of scale, cost savings, coordination, and interoperability, among other benefits.
- A coordinating body can also serve to establish a strategic vision for the entire 9-1-1 ecosystem. The vision should detail what the state wants to achieve and include a framework for conveying this vision to policymakers, PSAPs, and the public. Early-adopting states can create these frameworks to act as a blueprint for planning and deployment in later-adopting states.

States should establish a coordinating entity that actively engages with local stakeholders, including PSAPs.

- Congress should continue to provide incentives as conditions of NG9-1-1 related grant programs for states to establish a single officer or governmental body to serve as the coordinator of implementation of NG9-1-1 services (but not vest such coordinator with legal authority to implement NG9-1-1) and coordinate its grant application with the local PSAPs.[62]

States should ensure that diversion of 9-1-1 fees does not occur.

States Should Update 9-1-1 Funding Mechanisms

- States should establish and oversee a sufficient, enforceable, technology-neutral funding mechanism. During the transition period to NG9-1-1, states will need to continue to fund both the existing legacy 9-1-1 system and the costs associated with planning and implementing NG9-1-1 and other broadband-related systems. Funding mechanisms should also anticipate long-term needs such as maintenance, upgrades, new requirements, etc.
- States should ensure that diversion of 9-1-1 fees does not occur. Creating a separate 9-1-1 fund can help ensure that 9-1-1 fees are not commingled with other state monies and thus less likely to be diverted for other non-9-1-1 related purposes. It would be beneficial to specifically devote a portion of 9-1-1 spending to NG9-1-1 planning and implementation.
- Funding mechanisms will also benefit from legislation or regulations that specifically mandate what 9-1-1 funds may be used for, and empower a coordinating entity to audit the provision and use of 9-1-1 funds, and take enforcement action if funds are not being remitted properly or are not being utilized properly by receiving entities.

Other Roles for States or Coordinating Entities

- Provide training support to localities and PSAPs. This can be in the form of funding, training materials, training programs, etc.
- Have effective rule-making authority and enforcement authority.
- Ensure redundancy and interoperability in the NG9-1-1 system.
- Collect and analyze data, which in turn can be used to inform policy development and strategic planning.
- Promote coordination, mutual aid, and information and resource sharing within and among PSAPs. This can be accomplished in part by enabling the creation of interlocal and mutual aid agreements or memorandums of understanding between localities and PSAPs.
- Encourage PSAPs to develop or update operational, technical, security, privacy, and training policies for an NG9-1-1, broadband environment.
- Ensure that NG9-1-1 networks and equipment be built to widely deployed commercial standards, and other standards approved through organizations such as ANSI that accredit the procedures of standards development organizations to ensure openness, balance, consensus, and due process, that are commonly used in public safety communications, and that are proven to achieve and maintain seamless interoperability among PSAPs, ESInets, originating networks, FirstNet, and other government and public safety enterprise networks.

Outreach and Education

- States and coordinating entities should conduct outreach and education for policymakers, PSAPs, and the public to advance NG9-1-1 progress and adoption of broadband technology.
  - This could include explaining how technology is shaping the 9-1-1 landscape, the benefits of NG9-1-1, the funding and other challenges PSAPs face, and how FirstNet and other broadband technologies will be integrated into the 9-1-1 system.
- States and coordinating entities should also monitor changes and trends in NG9-1-1 and broadband technologies in order to continuously update outreach and education for policymakers, PSAPs, and the public.

Amend Laws and Regulations that Impede 9-1-1

- States should remove barriers to 9-1-1 modernization within existing legislation. This includes outdated, legacy-based regulations such as 9-1-1 SSP certification requirements and regulations that impede IP-based routing. Regulations should instead promote competition, IP connectivity, and broadband technologies.
- States should update legislation and regulations to promote technology adoption and NG9-1-1 implementation, and address new and existing legal, regulatory, funding, liability, security, and privacy concerns in a broadband environment. This could include creating legislation and regulations that comprehensively and uniformly define and promote NG9-1-1, create a coordinating entity, establish or expand a 9-1-1 funding mechanism, extend liability protection to NG9-1-1 service providers and systems, and address privacy, cybersecurity, and data security in an NG9-1-1 environment.

States should update legislation and regulations to promote technology adoption and NG9-1-1 implementation.

State Procurement

States should follow fair, open, transparent, and competitive procurement practices.

State Coordination

Where feasible, states should coordinate FirstNet and NG9-1-1 implementation.

Role of the U.S. Congress

Congress should establish a substantial grant program to modernize 9-1-1 services across the country as a national imperative. APCO will continue its efforts to achieve federal legislation that would help ensure that all PSAPs have the resources needed to upgrade in approximately the same timeframe, while leaving to the responsibility of state and local governments to address funding for workforce, training, and sustainability. A grant program can be used to serve certain objectives, such as to achieve and maintain seamless interoperability including through use of widely deployed commercial standards, promote information and resource sharing, drive cost efficiencies, require use of open and competitive procurement practices, ensure states create sustainable funding mechanisms to support continued operations, and prevent fee diversion.

Further, Congress has the opportunity to fund additional research and development to assist with the development of technologies to advance NG9-1-1. This can be patterned after the existing public safety wireless communications research and development program that the FirstNet legislation assigned to the National Institute of Standards and Technology (NIST).

Congress should establish a substantial grant program to modernize 9-1-1 services across the country as a national imperative.

Notes

14 Throughout this report, "mutual aid" is meant to be comprehensive, including the exchange of resources and services for field units as well as PSAP-centric practices such as 9-1-1 call overflow to another PSAP.

15 The research concerning actions occurring within the states towards NG9-1-1 is based on publicly available information, and is subject to change. Progress varies among states, and implementation of NG9-1-1 is a fluid process. States that have recently updated their legislation to account for NG9-1-1 include: Connecticut, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maryland, Minnesota, Montana, Nebraska, New Mexico, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, and Virginia. Other states such as California, Colorado, Georgia, and Ohio have enacted legislation that requires studies related to the modernization of the 9-1-1 system.

16 States in which some NG9-1-1 progress has occurred at either the state, regional, or local level include: Alabama, Alaska, Arizona, California, Colorado, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Washington, D.C., and Wisconsin.

17 Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges, Federal Communications Commission, at 13-18, 60-66, 70-80 (Dec. 30, 2016), at https://transition.fcc.gov/pshs/911/Net%20911/Net911_Act_8thReport_to_Congress_123016.pdf.

18 35 Pa. Cons. Stat. §§ 5302-14, 5398-99 (2015).

19 Id. at § 5303(a).

20 Id. at § 5303(b).

21 N.C. Gen. Stat. §§ 143B-1400-16 (2015).

22 911 Board and Committees, North Carolina Department of Information Technology, at https://it.nc.gov/about/boards-commissions/911-board/911-board-and-committees.

23 N.C. Gen. Stat. § 143B-1402.

24 Statewide 911 Board, at https://www.in911.net/911-board.html.

25 Ind. Code § 36-8-16.7-27.

26 Cal. Gov't Code § 53121(a) (2014).

27 Colo. Rev. Stat. §§ 29-11-301(1)(a), 302(1) (2016).

28 Ga. Senate Resolution 1203 (2014).

29 Cal. Gov't Code § 53121(b).

30 35 Pa. Cons. Stat. § 5303.

31 Okla. Stat. tit. 63 § 2864 (2016).

32 Mendocino Next Generation 9-1-1 Project, California Office of Emergency Services, at http://www.caloes.ca.gov/PublicSafetyCommunicationsSite/Documents/9-1-1%20Fact%20Sheet-%20Mendocino%20Next%20Generation%209-1-1%20Project.pdf.

33 Donny Jackson, Counties of Southern Illinois (CSI) Begin Operations on Next-gen 911 System Provided by Ng-911, Inc., Urgent Communications (Jul. 7, 2015), at http://urgentcomm.com/ng-911/counties-southern-illinois-csi-begin-operations-next-gen-911-system-provided-ng-911-inc; Counties of Southern Illinois Next Generation 9-1-1 Project, Jackson County 9-1-1, at http://jc911.org/index.php/nextgen-9-1-1-project.

34 Ohio 9-1-1 Newsletter, Ohio 9-1-1 Program Office (Apr. 2016), at http://911.ohio.gov/Portals/0/ESINet%20Steering%20Committee/April%202016%20Newsletter.pdf.

35 Memorandum of Understanding for Next Generation 911 Hosted Customer Premise Equipment for Laramie County Combined Communication Center and Laramie/Albany County Records and Communication Center, at https://www.cityoflaramie.org/AgendaCenter/ViewFile/Item/1236?fileID=1579.

36 Commonwealth of Pennsylvania Statewide 9-1-1 Plan, Pennsylvania Emergency Management Agency, at 26 (Jul. 2016), at http://www.pema.pa.gov/planningandpreparedness/Documents/9-1-1%20plans%20guides%20and%20templates/PEMA%20Statewide%209-1-1%20Plan.pdf.

37 Gary Johnson & Thom Sumbler, Upper Peninsula 9-1-1 Authority ESInet Project (2015), at https://www.michigan.gov/documents/msp/2015_Interop_Conference_UP_528924_7.pdf.

38 "The MOU establishes the expectations of the Council for the PSAPs, and the responsibilities of the Council to the PSAPs." Kansas Statewide NG911 System: the Technology and Cost, Kansas 911 Coordinating Council, at 14 (Mar. 2015), at http://www.kansas911.org/.

39 Second Amended and Restated Interlocal Cooperation Agreement Southeast Region 911 Communication Services Procurement and Delivery, at https://lincoln.ne.gov/city/council/agenda/2015/111615/15r231a.pdf.

40 N.C. Gen. Stat. § 143B-1402(a)(1).

41 Va. Code §§ 56-484.12, 56-484.14 (2016).

42 35 Pa. Cons. Stat. § 5303.

43 *Id.* at § 5304.

44 Conn. Gen. Stat. § 7-148cc (2001).

45 Okla. Stat. tit. 63 § 2849.

46 Ky. Rev. Stat. § 65.760 (2016).

47 Other examples abound. For instance, states that seek to deregulate retail IP-based services should exercise care to not inadvertently deregulate or remove incentives to promote IP-based networks serving public safety.

48 FirstNet is required to issue "open, transparent, and competitive requests for proposals," and "promote competition in the equipment market" by requiring equipment be built to "open, non-proprietary, commercially available standards" that are further capable of being used by any public safety entity and by multiple vendors. 47 U.S.C. §§ 1426(b)(1)(B), (b)(2)(B).

49 States that have updated their liability provisions include North Carolina, Connecticut, Pennsylvania, Montana, Tennessee, and New Mexico.

50 47 U.S.C. § 1472.

51 N.C. Gen. Stat. § 143B-1413(a).

52 *Id*.

53 Conn. Gen. Stat. § 28-28a(d).

54 Me. Rev. Stat. tit. 25, § 2929 (2015).

55 States that have recently updated their legislation to incorporate NG9-1-1 include: Connecticut, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maryland, Minnesota, Montana, Nebraska, New Mexico, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, and Virginia. Other states such as California, Colorado, Georgia, and Ohio have enacted legislation that requires studies related to the modernization of the 9-1-1 system. Michigan and New Jersey have legislation pending.

56 N.C. Gen. Stat. § 143B-1400(20).

57 Neb. Rev. Stat. § 86-471(1) (2016).

58 Okla. Stat. tit. 63 § 2862(a)(3).

59 50 Ill. Comp. Stat. 750/15.6b(a)(4) (2015) (lapsed).

60 *Id*. at 750/15.6b(a)(3) (lapsed).

61 N.M. Stat. Ann. § 63-9D-3(T)(6) (2017).

62 Note that incentivizing effective governance structures does not include the regionalization or consolidation of PSAP facilities, functions, equipment, or services. Regionalization and consolidation must be a local decision.

CYBERSECURITY

INTRODUCTION

Cybersecurity presents one of the most complex set of challenges for PSAPs in a broadband environment. Not only must each PSAP manage cybersecurity for its own networks and equipment, the networks and systems that interconnect with each PSAP must likewise be secured from intrusion and interference. PSAPs must account for the cybersecurity needs of other related networks and databases including criminal justice, investigative, and medical data for responding agencies, personnel, and the public. It is essential that cybersecurity is considered at the onset, and not treated as an afterthought, when adopting new technologies. In other words, cybersecurity must be "baked in," not "bolted on."

It is essential that cybersecurity is considered at the onset, and not treated as an afterthought, when adopting new technologies. In other words, cybersecurity must be "baked in," not "bolted on."

THE CYBERSECURITY ROLE

Cybersecurity risks have the potential to affect everything from national security to public safety communications networks and other critical elements such as financial institutions, electric power distribution, and even intrusions into vehicles. Even the most sensitive and proprietary information is subject to intrusion and attack from malicious cyber actors, criminal groups, and nation states. With public safety communications systems becoming ever more reliant on IP-based technologies, including in a legacy environment, the threat is real and potentially very consequential.

For these reasons, cybersecurity practices and policies must be established and applied to PSAP personnel and technology vendors. Key concepts include the need to identify vulnerabilities, detect anomalous behavior, respond to incidents, mitigate the damage, and recover from the event. A new culture of cybersecurity awareness must be fostered and integrated with technical and operational considerations to defend both legacy and next generation systems.

The Existing Threat

To date, thousands of Telephony Denial of Service (TDoS) attacks have been identified nationally, with an alarming amount of those attacks directed at public safety or related targets. 9-1-1 networks have traditionally been secure, with limited access and effective controls in place. CAD systems are typically designed and operated on closed, internal networks with little or no access to or from any system other than the 9-1-1 and radio systems maintained internal to the public safety entity. Despite this relatively secure environment, PSAPs and other law enforcement, fire/rescue, and even federal agencies have been successfully targeted and impacted by TDoS, Distributed Denial of Service (DDoS), and ransomware attacks.[63] These attacks can render PSAPs unable to receive, process, and respond to calls for service, and public safety data and records can become inaccessible or corrupted (including potentially without actual knowledge that records have been changed).

The scale and sophistication of cyber-attacks vary. For example, one DDoS incident in October 2016 resulted in widespread disruptions to some of the most used sites on the Internet.[64] This attack against Dyn, one of the companies that run the Internet's domain name servers, represented a successful manipulation of multiple Internet of Things (IoT) devices on a global scale to effect damage on a specific target. The Dyn attack represents a coordinated and complex approach with global impact.

In a separate incident, also in October 2016, a single actor perpetrated a multi-state TDoS attack against numerous PSAPs in twelve states in the United States.[65] The perpetrator was an 18 year old who developed a simple JavaScript (programming language) code that was spread through a popular web link and infected mobile phones, causing them to repeatedly dial 9-1-1 without the knowledge of the user. This actor did not require specialized knowledge of 9-1-1, but was nonetheless able to create a signficant disruption to 9-1-1 through an exploit that was extremely difficult for PSAPs to mitigate.

The Future Threat

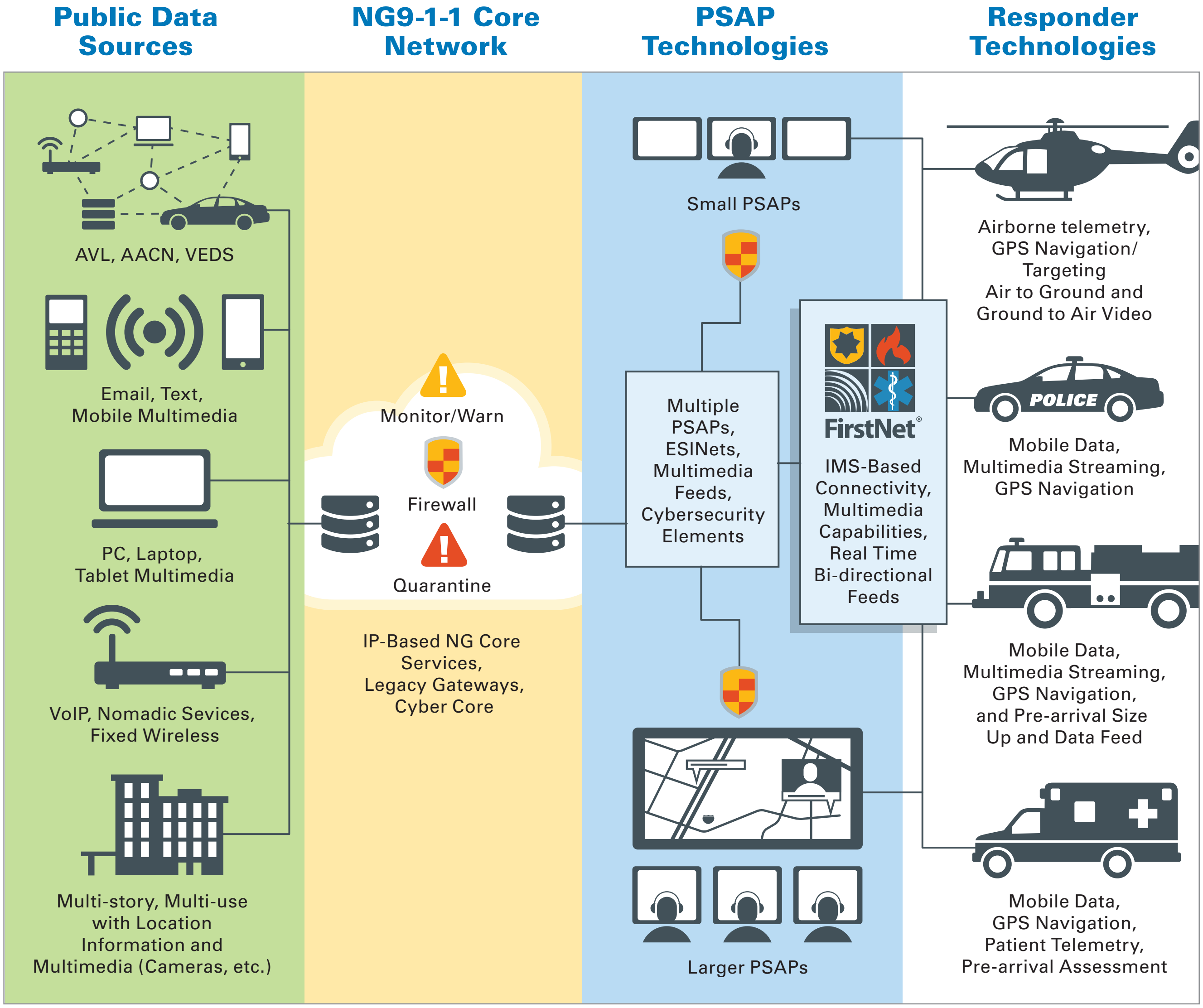
As public safety communications transition to IP-based technologies, PSAPs will experience more cyber-attacks. Broadband-based systems such as NG9-1-1, IoT, smart cities, intelligent highways, mobile apps in use by the public and responders, and next generation alerting platforms that may benefit PSAP operations also create new vulnerabilities. With the introduction of various new ways to access public safety communications networks, most of them in the relatively open Internet environment, the ability to secure networks and critical data from cyber-attack must be a primary consideration when designing and implementing any new solutions.

As public safety communications transition to IP-based technologies, PSAPs will experience more cyber-attacks.

Added to this, the implementation of the NPSBN, managed by FirstNet, will provide first responders with wireless broadband communications using a uniform technology and network design to ensure interoperability. Like NG9-1-1, the NPSBN will be an IP-based network of networks that will be subject to cyber risk. Given that NG9-1-1 and FirstNet networks will enable significant exchange of data, all stakeholders should pay close attention to the prospect of bad actors seeking to exploit one or both of these significant pillars of the future emergency response ecosystem. Figure 1 illustrates the flow of information and a number of the touch points of these two networks. See Appendix 1 for a detailed list of potential vulnerability points resulting from the interconnection of NG9-1-1 with the NPSBN.

The threat of cyber-attack cannot deter the progression into what may well be the most significant advancement in emergency communications since the advent of two-way radio or basic 9-1-1 services. Public safety must commit to deploying these new technologies in such a way that cybersecurity is incorporated by design into planning, implementation, and operations models at the onset. The resolve to combat cyber-criminals and cyber-activists on every front must be unwavering. Education and training, proper planning and design, and a unified approach centered on information sharing and collaboration will help to ensure success.

Figure 1. **Interconnected NG9-1-1 and FirstNet Networks**


Public Data Sources
NG9-1-1 Core Network
PSAP Technologies
Responder Technologies
AVL, AACN, VEDS
Email, Text, Mobile Multimedia
PC, Laptop, Tablet Multimedia
VoIP, Nomadic Sevices, Fixed Wireless
Multi-story, Multi-use with Location Information and Multimedia (Cameras, etc.)
Monitor/Warn
Firewall
Quarantine
IP-Based NG Core Services, Legacy Gateways, Cyber Core
Small PSAPs
Multiple PSAPs, ESINets, Multimedia Feeds, Cybersecurity Elements
FirstNet®
IMS-Based Connectivity, Multimedia Capabilities, Real Time Bi-directional Feeds
Larger PSAPs
Airborne telemetry, GPS Navigation/ Targeting Air to Ground and Ground to Air Video
POLICE
Mobile Data, Multimedia Streaming, GPS Navigation
Mobile Data, Multimedia Streaming, GPS Navigation, and Pre-arrival Size Up and Data Feed
Mobile Data, GPS Navigation, Patient Telemetry, Pre-arrival Assessment

Cybersecurity Concepts

While the purpose of this report is not to provide comprehensive educational material on cybersecurity, a brief overview of several important topics is essential for a discussion of the implications to PSAPs.

Identity, Credential, and Access Management (ICAM)

ICAM refers to the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources such as electronic files, computer systems, or physical resources such as server rooms and buildings.

Firewalls

Firewalls contribute to security by controlling the flow of information into and out of network entry points. By using a set of user-defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. For more guidance on the use of firewalls to control access, see Appendix 2.

User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by his or her role within the organization. User access can be restricted in various ways, such as by using solutions commonly deployed by IT departments, establishing authorization requirements for individual devices (e.g., routers, servers, embedded controllers, workstations), and by stronger authentication methods for critical host devices such as smart cards or USB tokens, biometric authentication, and two-factor authentication.

Remote Access

Providing access to remote users presents a unique set of security challenges. Addressing these challenges may require building additional protections into the network infrastructure, such as using secure connections and data transfer protocols, multi-factor authentication, and placing strict limits on who may remotely access the network.

Vendor Access

Virtually all organizations have networks, systems, and facilities that rely on outside vendors for service. Those vendors might require physical access, dedicated remote network access, network cloud access, or any combination of the three. When using a vendor, a level of risk is inherent in the relationship.

Vendor staff should meet the agency's security and background check requirements. The due diligence and negotiation processes should include a thorough vetting of the vendor's in-house cybersecurity practices, as well as the specific protections designed into its offering. It's important to inquire of employee continuity, both to limit those having access to PSAP systems, and to ensure continuity of support. The vendor company must be stable and financially sound. These factors should be addressed in vendor contracts.

PSAPs need to balance the risk to networks with the level of access needed for vendors to service their equipment. For example, remote access by vendors to the network can be accomplished through either a Secure Shell (SSH) Tunnel, Virtual Private Network (VPN), or dedicated communication link. Regardless of the access mechanism, security patches should always be kept up to date.

When a vendor accesses the agency network a strong password policy must be required. For example, single-use passwords for vendors are an effective means of minimizing the risk of vendor access.

Passwords

User passwords for public safety networks must balance security needs with burdens on the user. Unrealistic password policies can actually undermine cybersecurity if users develop workarounds (such as keeping a written list of passwords at a workstation). Password protection policies should apply to user-level, system-level, network equipment, web, email, and public safety application accounts, and include routine changing of passwords, careful storage of passwords, avoiding repetitive use of similar passwords, separate passwords for separate systems, and review of the password policy with employees. These measures can help ensure the public safety network remains secure and that all users (including employees, contractors, consultants, temporary workers, etc.) adhere to the password policy. See Appendix 3 for recommended guidelines and practices for password creation and protection.

Physical Security

Because a single point of intrusion such as a work station or server room can expose an entire system to cyber-attack, physical security is an essential component for mitigating cybersecurity risks. Physical security prevents unauthorized access to devices, networks, and information. Without it, intruders have the means to circumvent all of these otherwise restricted vulnerabilities. Physical security policies should address building security, workstation and individual program authorizations, visitor access, and other measures (such as security cameras). Regularly scheduled audits of physical security measures should also be conducted.

Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction, or malfunction of equipment. In order to minimize these risks, data must be stored in an appropriately secure and safe environment, and frequently backed up.

Removable media should not be the only place where data obtained for agency purposes is held. Copies of any data stored on removable media must remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

The Human Element

The people who interact regularly with an agency's network play a critical role in maintaining overall system security. Cybersecurity protections can easily be undermined, either knowingly or unknowingly, by a single individual. Policies and procedures must outline what is considered acceptable use of the agency's networks, proper email usage, and approved use of removable media.

Social engineering and phishing are two types of hacking techniques that are considered "low tech" methods of intrusion into a facility or network. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Phishing is an example of a social engineering attack, typically carried out by email, that is the favored method used by cyber-criminals. A phishing email might appear to come from a colleague or friend, using personal information for the appearance of authenticity, to deliver malware and ultimately gain access to secure systems.

Removable Media and Access Ports

Removable media is a well-known source of malware infections and has been directly tied to loss of sensitive information in many organizations. Open and unsecured network access ports on switches, routers, firewalls, etc. pose a similar threat as individuals can connect removable media to gain physical presence on the agency network.

Removable media include, but are not limited to:

- USB Memory Sticks (also known as pen drives or flash drives)
- CDs
- DVDs
- Optical Disks
- External Hard Drives
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and answering machines)

Removable media are helpful for processes such as backing up data, updating software, and transferring files without a network connection. However, removable media have historically been a source of spreading malware and viruses. A well-documented and closely followed removable media and access port policy helps ensure the integrity of the network, data, and computer systems of the agency. See Appendix 4 for guidance on removable media security and access port policy.

FINDINGS

Existing Educational Materials

Many organizations have developed resources that the public safety community can use to improve cybersecurity. This report need not attempt to replicate the work done in these documents, but the following may be of interest to public safety communications professionals seeking to learn more about cybersecurity issues:

- APCO's Cybersecurity Committee report, "An Introduction to Cybersecurity: A guide for PSAPs"[66]
    - This document can serve as a starting point to educate PSAP supervisors on identifying, preventing, and minimizing exposure to cybersecurity risks and vulnerabilities.

- The FCC Task Force for Optimal PSAP Architecture (TFOPA) report[67]
    - The TFOPA report includes a section entitled "Optimal Approach to Cybersecurity for PSAPs" with recommendations and a toolkit for use by PSAPs that includes a guide for evaluating cybersecurity capabilities and risks, a roadmap for creation of a cybersecurity strategy, and a list of potential resources for PSAPs and 9-1-1 authorities.

- The 2012 DHS "Emergency Services Sector (ESS) Cyber Risk Assessment"[68]
    - This document is intended to provide a risk profile that ESS partners can use to enhance the security and resilience of the ESS disciplines by increasing the awareness of risks across the public and private sector domains.

- The 2014 DHS primer on "Cyber Risks to Next Generation 9-1-1"[69]
    - The primer is an introduction to improving the cybersecurity posture of NG9-1-1 systems nationwide and provides an overview of the cyber risks that will be faced by NG9-1-1 systems. It is intended to serve only as an informational tool for system administrators to better understand the full scope and range of potential risks, as well as to recommend mitigations to these risks.

- The NIST Framework for Improving Critical Infrastructure Cybersecurity[70]
    - The NIST Framework is designed to help organizations manage cybersecurity risk, and a next version is under development.

- Industry best practices relevant to TDoS attacks[71]
    - As a result of a cooperative effort between federal authorities, public safety representatives, and commercial service providers, a checklist was developed to assist in the development of a continuity of operations plan for TDoS attacks.

The Key Role of Personnel

Training PSAP personnel about the role each person plays in maintaining security within an organization is critical. From basic cyber hygiene to more advanced network security training and programs (such as to recognize risks or actual attacks in progress), security begins and ends with the people who operate the systems and services that support the public safety mission.

Opportunities for Resource-Sharing

FirstNet and NG9-1-1

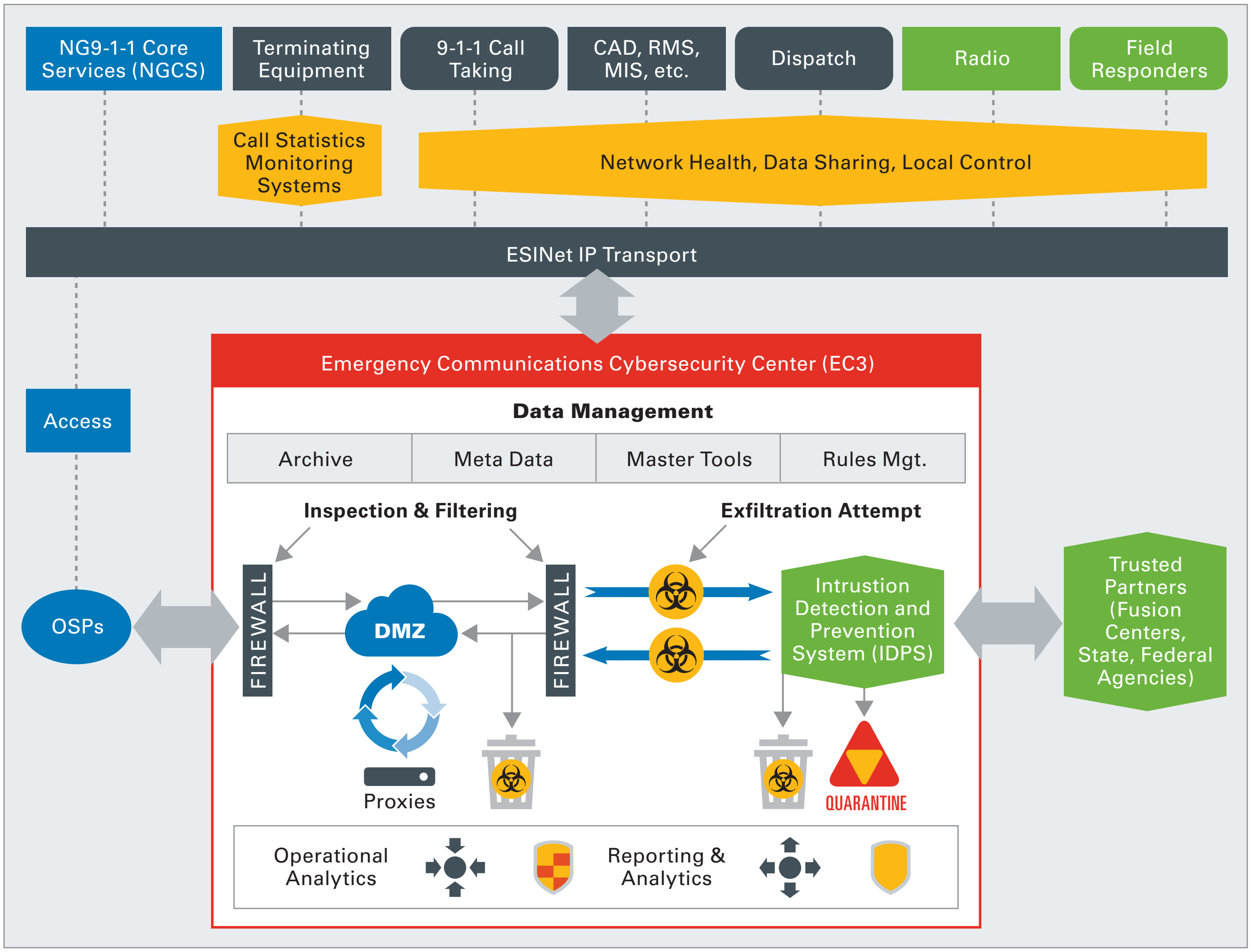
FirstNet and NG9-1-1 networks are both designed with IP technologies and therefore are susceptible to cybersecurity risks. They will constitute the twin pillars of the future emergency response ecosystem, frequently exchanging data and information and sharing a mutual, strong interest in protecting the integrity of public safety communications networks and data. As FirstNet implements its cybersecurity strategies, and approaches are being considered to protect NG9-1-1 networks, there could be benefits to a cooperative approach.

The Emergency Communications Cybersecurity Center

Intrusion Detection and Prevention Systems (IDPS) are network security/threat prevention technologies that examine network traffic flows to detect and prevent vulnerability exploits. By centralizing services such as IDPS, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place. The FCC's TFOPA developed a concept known as the Emergency Communications Cybersecurity Center (EC3), which would centralize IDPS for next generation public safety networks.

In the proposed architecture, the EC3 takes on the role of providing IDPS services to PSAPs and

Figure 2. **The Emergency Communications Cybersecurity Center**

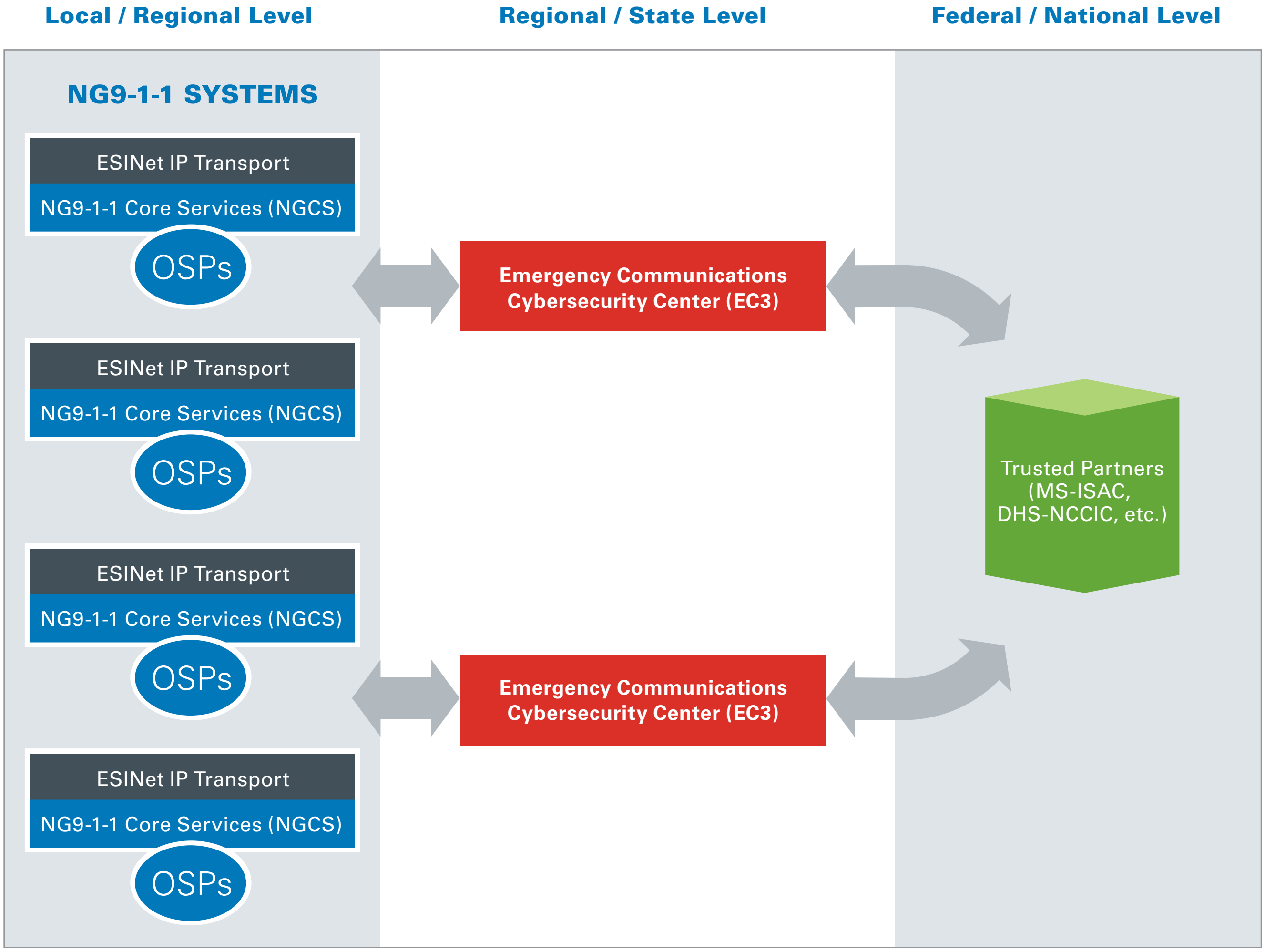


any other emergency communications service or system that would consider utilizing the centralized core services architecture proposed. For example, emergency operations centers could also connect to the EC3 service. This approach would allow public safety entities to build one infrastructure that serves many clients. EC3s could be designed to interconnect with other IDPS throughout the United States, for example if a large public safety entity wanted to manage its own EC3 but benefit from the analysis made possible from the larger ecosystem. This flexibility provides significant economies of scale, puts multiple resources into the same protection scheme, and allows for sharing of data, mitigation strategies, and recovery efforts across the public safety ecosystem.

As illustrated in Figures 2 and 3, the potential flow of this system would begin with the originating service provider (OSP) and NG9-1-1 core services elements, encompass the ESInet transport network between disparate PSAPs, and provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation, and recovery, while still allowing local agencies to maintain control of day-to-day operations.

Rather than requiring PSAPs to build and staff such facilities, the EC3 concept allows for PSAPs across all jurisdictions to interconnect to the core cybersecurity system and benefit from its capabilities. While not specified, the interconnect requirements would include cyber hygiene elements at the PSAP, single user sign-on and multi-factor authentication at the local level, and

Figure 3. **The EC3 Deployed**


Local / Regional Level
Regional / State Level
Federal / National Level
NG9-1-1 SYSTEMS
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
Emergency Communications Cybersecurity Center (EC3)
Emergency Communications Cybersecurity Center (EC3)
Trusted Partners (MS-ISAC, DHS-NCCIC, etc.)

some form of agreed upon, trusted connection (and relationship) from the local levels to the state or regional level EC3.

This architecture is intended to represent a scalable and customizable approach. This means for localities with larger than average emergency communications systems (such as major metropolitan areas) there is ample opportunity to construct a single EC3 to serve this individual customer. However, any EC3 should be designed and constructed in such a way that it will interconnect with other EC3s throughout the United States with the same functions and requirements. From the regional or state level, the information should flow to a centralized, trusted, federal repository with adequate service capabilities to support multiple clients and incidents in real time.

Increased Complexity and Risk from Interconnection

Individual networks are expected to maintain a heightened level of cybersecurity posture to protect from exposure to other networks that may have been compromised. It is reasonable to expect that each network will interconnect to its peers through a series of firewalls, intrusion detection systems, and border control mechanisms.

Following the FCC's TFOPA cybersecurity recommendations, an overall IDPS is needed to protect public safety networks as an enterprise, and individual networks should have specific security requirements to interconnect via IDPS to other networks. Security is needed at each end point, meaning at each user-termination node, such as a

PST workstation or CAD terminal. Stronger security protections should be in place at touch points with connections to non-secure networks and devices such as the citizen caller, external databases, web-based traffic, and other data connections to systems beyond the operational ownership of the modernized public safety network. Even interconnection points between internal public safety networks, such as between ESInets, legacy PSAPs, and next generation core services, and between FirstNet systems and NG9-1-1 systems, should have a certain level of cybersecurity rather than assuming that these networks are safe.

Land Mobile Radio (LMR)

When addressing security surrounding communications systems and infrastructure, it's easy to overlook traditional LMR. Today's radio system infrastructure no longer simply consists of a transmitter in an equipment shed with an outside antenna that may be considered immune to cyber-attack. Rather, LMR bears a closer resemblance to a traditional data center than that of the old "radio room." There are servers, routers, and firewalls as well as other IP-connected devices that need to be secured.

CAD, CPE, and GIS

The variety in approaches for implementing CAD, CPE, and GIS, including the concept of hosted solutions, adds to the complexity of addressing related cybersecurity challenges. It is important to keep in mind that all of these systems represent a method of accessing the PSAP and may be shared among several PSAPs, introducing a greater vulnerability and level of potential impact. Common cybersecurity approaches should include limiting access to these systems by other systems and software applications, and use of strong passwords.

Internet Access and Mobile Apps

PSAPs increasingly provide Internet access at PST work stations. This can be a useful tool for obtaining information such as real-time weather and news reports, but even when the connection is separated from CAD and other important systems, Internet access presents a cybersecurity threat. For example, a PST might receive a call over the PSAP's ten-digit line that was initiated through a mobile app advertised for use by the public during emergencies. The caller could be a representative working at the app's third party call center, claiming that an app user in the PSAP's jurisdiction reported an emergency and that further information is available through a website. With the cybersecurity vulnerabilities of mobile apps and the Internet, the information ultimately being received and recorded by the PST could be misleading or even malicious. To counteract this threat, some PSAPs limit access to only pre-approved ("whitelist") websites. Other PSAPs have established criteria for blocking sites that are not related to their positional duties or pose a potential security threat. As described in the Technology section of this report, APCO is continuing efforts to ensure public safety apps are as safe and effective as possible.

Other IP-Based Systems

Many systems within PSAPs are IP-based. It is imperative that centers consider all of the various systems which could be threatened by a cyber-attack. Some of these systems are:

- Power (uninterrupted power supply (UPS), climate controls, building monitoring systems, battery chargers, remote monitoring systems)
- Security cameras
- Fuel pump systems
- Any device with an assigned IP-address ■

RECOMMENDATIONS: CYBERSECURITY

There are a number of proactive steps that public safety agencies can take to plan and properly defend networks and systems. The following section represents some high level recommendations to help agencies begin this critical process.

Education and Training

APCO encourages agencies of all sizes, and personnel at all levels, to get engaged in the cybersecurity conversation, get educated about the threat, and become proactive in the defense of the public safety communications ecosystem.

APCO encourages agencies of all sizes, and personnel at all levels, to get engaged in the cybersecurity conversation, get educated about the threat, and become proactive in the defense of the public safety communications ecosystem.

The ability to defend networks and systems is directly related to the understanding of those systems. Even basic knowledge of the networks and systems, and the security risks and potential solutions available, will empower public safety leaders to ask relevant questions of their vendors who, in turn, can provide focused responses and design solutions for the safety and security of the PSAP.

Security training works best if participation is mandated and monitored for effectiveness, and made part of quality assurance/quality improvement programs. APCO will develop and offer a cybersecurity hygiene course for public safety communications professionals to assist with these challenges.

Sharing Cybersecurity Resources

APCO supports the concept of an EC3 as described by the FCC's TFOPA cybersecurity report.[72] APCO recommends becoming familiar with the EC3 concept and proposed architecture, as well as considering requirements for full IDPS capabilities in any forthcoming RFPs related to next generation systems and services.

APCO supports the concept of an EC3 as described by the FCC's TFOPA cybersecurity report.

Develop a Cyber Strategy

PSAPs should develop strategies for preventing and mitigating cyber-attacks. Individual approaches may vary. For example, strategies may entail conducting audits of cyber hygiene and unauthorized access on a monthly basis, or setting more stringent protection measures for systems based on cost and perceived need. Universally, however, these strategies should be comprehensive, recognizing that cybersecurity needs to be a group effort, with everyone made to feel they are part of the solution.

If a system is hit by a cyber-attack, having a plan available for immediate implementation and mitigation is essential. Establishing critical partnerships with technology partners and government resources will lessen the impact to the organization and increase the ability of enforcement agencies to locate and prosecute the actors. APCO currently participates in federally-coordinated response efforts by working with the DHS National Coordinating Center for Communications (NCC) to distribute information about potential cyber-attacks affecting PSAPs.

Report Suspicious Activity, Threat, or Attack

PSAP personnel having reason for concern of a cybersecurity issue should report the event as soon as practical after attending to any operational priorities. This helps situational awareness particularly if the attack is widespread. Complaints can be filed with the Internet Crime Complaint Center, www.IC3.gov, which is co-sponsored by the Federal Bureau of Investigation and the National White Collar Crime Center.

PSAP personnel having reason for concern of a cybersecurity issue should report the event as soon as practical.

Notes

[63] "In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software."
Incidents of Ransomware on the Rise - Protect Yourself and Your Organization, Federal Bureau of Investigation, at https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

[64] https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

[65] http://securityaffairs.co/wordpress/52895/cyber-crime/911-service-attacks.html.

[66] https://www.apcointl.org/resources/cybersecurity/cyber-security-guide-for-psaps/file.html.

[67] https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf.

[68] https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf.

[69] https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20FINAL%20508C%20(003).pdf.

[70] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. For the NIST Framework and documents related to an updated version, see https://www.nist.gov/cyberframework/draft-version-11.

[71] http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/.

[72] https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf.

01 11001 11
101 111 0001
1100 00 0001
01 11001 11
101 111 0001

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**

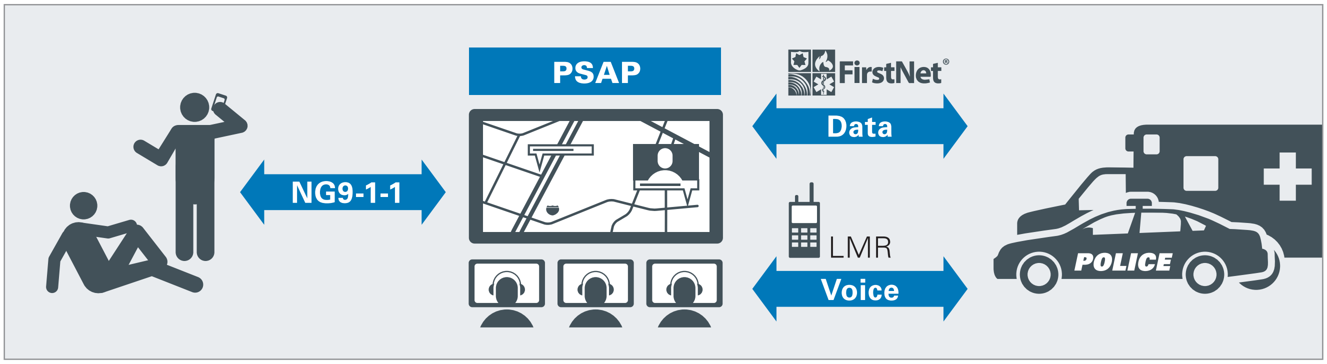
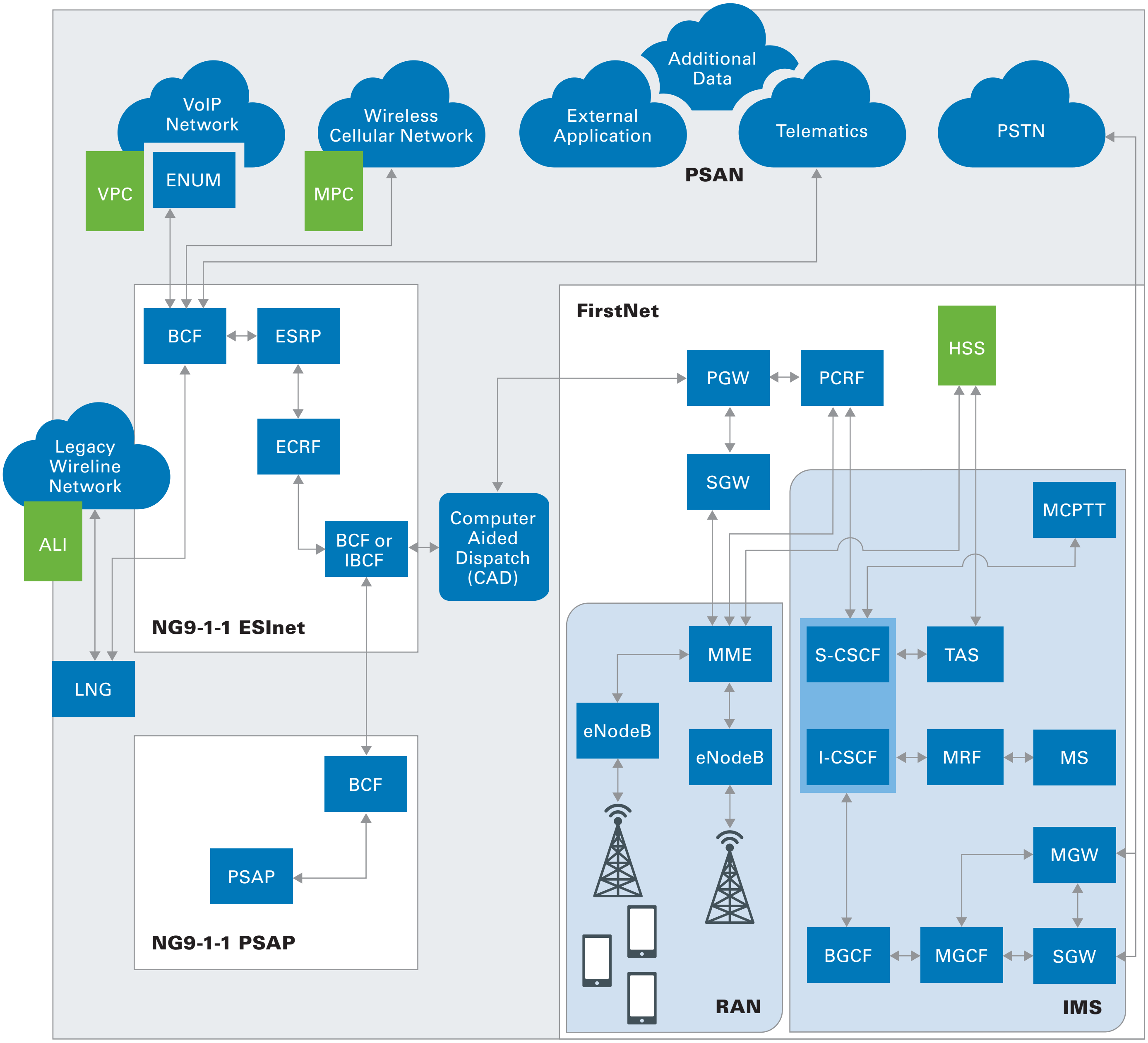


Figure 5. **Conceptual Diagram for Integration of NG9-1-1 and the NPSBN**[73]



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.

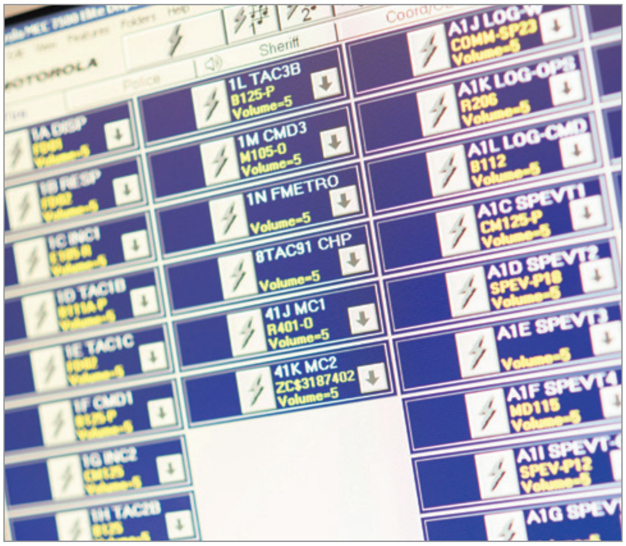
Customer Premise Equipment (CPE)

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.

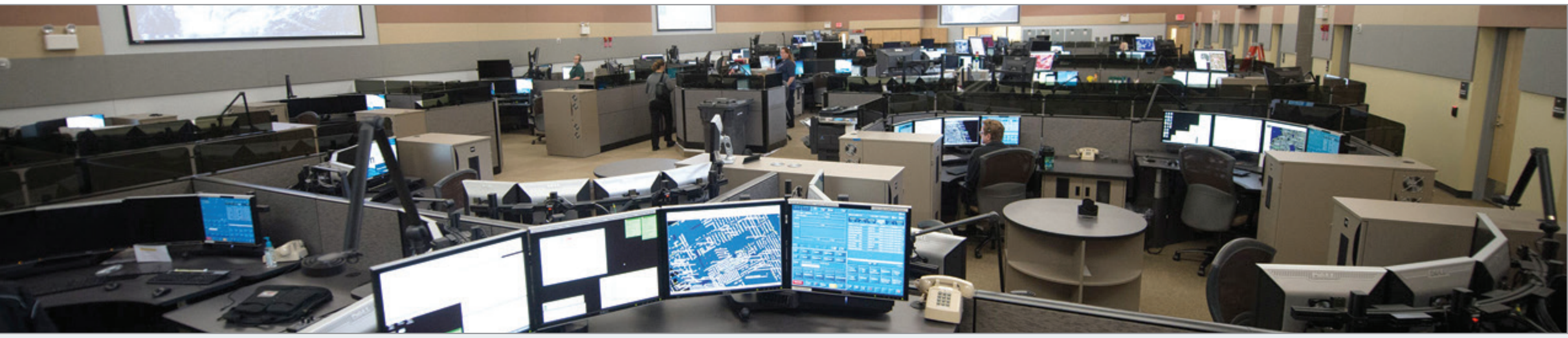
In order to reap the greatest benefit from a next generation architecture, PSAPs need fast, easy access to rich data as well as a reliable way to deliver that data in a useful way to the most appropriate place in the least amount of time. PSAPs that implement enhanced data features will increase situational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

TRAINING

INTRODUCTION

Training, while too often the victim of budget cuts and realignments, is absolutely key in the success or failure of any public safety operation. The ability to maintain quality services for both the public and emergency responders is dependent upon the ability to provide both initial and ongoing training to PSAP personnel. Without adequate training, at the operational level even the best technical solution will fail. Training is fundamental to the success of any public safety operation, and PSAPs are no exception. 9-1-1 authorities and relevant decision-makers should prioritize funding for the initial and ongoing training that PSTs deserve, as an investment that is necessary to provide quality services to the public and emergency responders.

9-1-1 authorities and relevant decision-makers should prioritize funding for the initial and ongoing training that PSTs deserve, as an investment that is necessary to provide quality services to the public and emergency responders.

The training needs for personnel in a broadband PSAP environment include what's currently needed for PSTs as well as what's needed to develop and maintain skills in an environment with new capabilities and rapidly evolving technology. The capacity for broadband technology to be ubiquitous and intuitive to the user can be leveraged to create model training programs for states while preserving flexibility to meet particular requirements and governance approaches. The varying sizes of PSAPs will be a differentiating factor in training approaches. However, in an IP-connected, interoperable environment powered by broadband technology, training should include sufficient commonality because, particularly in mutual aid situations, PSAPs must be prepared to understand and appropriately respond to the expectations of the public and emergency responders using widely deployed broadband technologies.

Current training standards and best practices would benefit from a number of specific language changes (for example, the term "call for service" is far too limiting in a broadband environment), and new definitions (such as for "broadband," "NG9-1-1"). Further, public safety can leverage lessons learned from technologies already in use, such as mobile apps and social media platforms deployed at universities and enterprise environments. Ongoing training to maintain competence will be even more important in a rapidly evolving broadband environment accompanied by increased stress due to processing more information and exposure to live video from incidents.

THE TRAINING ROLE

To set the stage for a discussion of the training-related impacts of broadband technology, consider the potential changes for PSTs of the future. The scenarios described in the Executive Summary concerning the response to a multi-vehicle traffic crash today compared to the response in a fully broadband-capable public safety environment can help illustrate the role of training.

Without broadband, PSTs:

- Receive calls of an automobile accident with entrapment and question the callers about the

location, number and type of vehicles involved, number of patients, and injuries
- Dispatch field responders according to their SOPs
- Perform emergency medical dispatch to assist with patient care before field responders arrive
- Once field responders are on scene, assist with communications and dispatch additional resources as requested

With broadband:

- PSTs receive real-time video from the scene from members of the public and an agency-operated UAV
- PSTs can see a vehicle placard and identify potential HAZMAT concerns
- When the PSAP is overwhelmed by callers from the scene, PSTs transfer calls with all related information to a partner agency for assistance with call processing and emergency medical dispatch
- Biometric devices on victims transmit data such as pulse and medical history along with the 9-1-1 call
- Video, corroborated by biometric data, indicates that one of the patients is a Priority 2 trauma, leading the PSTs to dispatch a medevac helicopter and additional fire/rescue units to establish a landing zone
- PSTs can share video and other data with field responders to provide information before they reach the scene and improve situational awareness throughout the incident

To fully take advantage of these advanced capabilities for the benefit of public safety, PSTs will need additional training. For example:

- How to incorporate live video, whether from a caller or an agency-operated source, into call processing and dispatching
- How to manage PST support from a partner agency that may have different capabilities
- How to incorporate more detailed patient information into an assessment as part of emergency medical dispatch
- How to manage the increased stress that will come from exposure to images and increased operational involvement that have traditionally been limited to field responders

Consistent with the list of additional training considerations for broadband-capable PSAPs provided above, this report offers several considerations for PSAPs, PSTs, and training program developers as part of their planning for the adoption of broadband technology.

FINDINGS

Training for Broadband

The impacts to training requirements from broadband technology will be varied. Some technology used at the next generation PSAPs might not require significant training if it is similar to technology already in use by consumers (e.g., social media interfaces). Other technologies will be natural extensions of tools already available to PSAPs. For example, real-time video feeds and 3D location tracking of field responders will provide much more situational awareness to PSAP personnel than what's afforded by automatic vehicle location systems used today to track the location of public safety vehicles.

The information made available to PSTs by broadband will present an opportunity for PSTs to play an enhanced role during emergency operations, especially for incidents in which this real-time situational awareness information can be lifesaving, such as active shooter responses, and firefighter MAYDAYs. The nature of a PST's role will change dramatically. Whereas today, a PST might be the first to notice a MAYDAY or a critical background noise that indicates first responders are in danger, having more sophisticated situational awareness tools will further erode the physical separation from the scene. PSTs will require significant additional training with advanced technologies to prepare for a greater role in incident operations.

Lessons learned from existing technology deployments will assist with anticipating the impacts of broadband technology and developing training programs. Even today, a variety of mobile apps that enable broadband communications are being used in enterprise environments and universities for public safety functions. For example, apps can create a video link with real-time location tracking between students and campus police officers as part of a virtual escort. Students know to rely on traditional 9-1-1 for emergencies but can pioneer apps that have advanced features for non-emergency public safety needs. At the same time, lessons learned from these environments can help shape the training for use of similar technologies inside the PSAP.

Public safety professionals know that they cannot be trained for every scenario they will encounter so the philosophy has been to establish a core skillset that will allow personnel to effectively respond to any situation. The unpredictability inherent in emergency operations will be further complicated by the fact that PSTs will be impacted by technology they may not have had exposure to. Both first responders and the general public alike will have tools at their disposal, such as mobile apps, or access to intelligent databases, that they will use during emergencies and will look to rely upon this information as they contact PSTs. For example, a consumer-facing mobile app might keep track of AED locations and provide instructions for administering CPR. During a cardiac arrest call, PSTs might then need to determine whether to direct a caller to an AED (based on the caller's report of the app's suggestion) that may conflict with the agency's list of available AEDs.

There will be continuous innovation producing technologies that PSAPs cannot anticipate. Thus, adaptability, already a key trait of successful PSTs, will be even more important as broadband technologies change emergency communications because the technology may be developed and introduced more rapidly than training programs can keep up with.

For a broadband environment, PSTs will need to be trained in new subject areas. PSTs will need at least a basic level of training in cybersecurity awareness and hygiene because employees at every level impact cyber vulnerabilities and mitigation. Further, training should provide a broad knowledge of digital, IT, and broadband-based technologies that may impact public safety communications, some of which can be patterned off of training provided at IT departments, and emergency management, real-time crime, 3-1-1, and fusion centers.

Training to Manage Increased Stress

Training PSTs to effectively recognize and manage stress in themselves and their colleagues is important today and will become even more important with broadband technologies. The capacity for broadband to create a more immersive experience for PSTs with increased situational awareness and exposure to images and live video from incidents, as well as new opportunities for monitoring field responders' safety, can all lead to a more effective response but also serve as additional sources of stress.

> *The capacity for broadband to create a more immersive experience for PSTs with increased situational awareness and exposure to images and live video from incidents, as well as new opportunities for monitoring field responders' safety, can all lead to a more effective response but also serve as additional sources of stress.*

Training programs should therefore include an awareness of basic concepts related to stress, and the following strategies should be considered (some of which are already part of stress management programs).

Train Personnel to Use Active Coping as a Stress Management Tool

Active efforts to resolve problems or reduce distress yield better outcomes for workers' psychological health. Active coping includes a broad range of activities such as problem-solving, exercise, diet, and seeking social support. The key is that the person takes action rather than avoiding, denying, or passively accepting the troublesome situation. If PSTs can be trained to critically appraise a video call for specific information (presence of a weapon or other safety hazards, for example), this may offer them a protective sense of having taken control, as well as gleaning practical information to relay to responders. Additionally, research has shown that the impacts of viewing traumatic material can be lessened with certain mitigation interventions.[90] For example, distracting tasks (such as playing a video game) and cognitive reappraisal[91] have been shown to reduce intrusive memories and other traumatic effects.

Conduct Team-Oriented Training

The social context in which a potentially traumatic event unfolds and is processed plays an important role in a PST's psychological health. In general, social support and interpersonal variables are important factors for the impacts of stress. Leaders perform a key role in supporting resilience training, creating a culture of support, and implementing stress exposure mitigation policies. But, training the entire agency on what to do and what not to do when communicating with each other after traumatic events will be an important part of a stress-management program.

Train Personnel to Provide Peer Support

Peer support teams should be trained, at a minimum, to identify stress and provide or assist with basic peer counseling. Whenever possible, peer supporters should be professionals with broad public safety experience to offer a comprehensive perspective, and it could be beneficial to include representatives from other public safety agencies to offer support from someone other than immediate coworkers. Teams should partner with a licensed mental health professional to provide adequate training of the team and serve as an ongoing resource. Peer supporters should be familiar with local counseling resources.

Training lessons could also be learned from other sectors that already employ training programs focused on stress management, particularly involving trauma exposure (such as disaster response teams, military). Further, the impact to PSAP personnel of exposure to significant data and imagery would likely benefit from additional, focused research.

Training Differences Across PSAPs

Variation in PSAP capabilities and training is often attributed to differences in PSAP size. However, the size of a particular PSAP is not necessarily dispositive of the type of training required. While some impacts will vary by size alone, factors such as funding, age differences across the workforce, and general availability of resources will be more useful predictors.

Broadband technology, by raising the ceiling of what's possible, will result in a wide disparity of technologies across PSAPs, leaving some with more advanced capabilities than others. At the same time, it will increase connectivity between PSAPs and therefore lead to more collaboration between agencies with different training levels and capabilities. Training for all PSAPs should thus include a baseline commonality because, particularly in mutual aid situations, PSAPs must be prepared to understand and appropriately respond to the expectations of the public and emergency responders using disparate technologies. This might mean that personnel in PSAPs with relatively more technological resources are trained to use their agency's tools, as well as the tools available to any agency they might interact with that uses less sophisticated tools.

For example, suppose firefighters at Agency A have a mobile app that can automatically retrieve hazardous material information from a placard and immediately relay the pertinent information to the PSAP and to the mobile data computers of other units via wireless broadband. Firefighters from Agency B provide mutual aid, but lack these particular broadband tools. PSTs at Agency A, having been trained to communicate effectively for a response that uses traditional resources, use basic voice communication and a paper copy of the Emergency Response Guidebook to coordinate with firefighters from Agency B.

This example also introduces a related training need - to maintain proficiency with legacy technology even as broadband enables the use of more sophisticated tools. Over-reliance upon sophisticated technology can lead to serious problems if these technologies fail and PSTs are no longer proficient with legacy backups.

Training Regardless of Resource Limitations

PSAPs with more training resources are more likely to manage the related impacts of broadband successfully. For example, assistance from IT departments, in-house instructors and classrooms, and staffing flexibility make training on new technology easier. The following training strategies may be useful to PSAPs regardless of resource availability.

Address Training Requirements in RFPs

When procuring broadband technology from various vendors, PSAPs should consider addressing training needs in their RFPs. Sample RFP language is included in Appendix 6 for a variety of options for user and administrator training.

Resource Sharing

All agencies, particularly smaller ones and agencies with strained budgets, may want to consider sharing training costs with the other agencies in their region. Those agencies using the same vendors/technology may be willing to assist with training employees of a neighboring agency, and even without using the same vendors/technology there could be a benefit to training on shared concepts. The benefits of such a collaborative strategy could be compounded by coordinating technology enhancements at a regional level.

Budget for Training Beyond the Scope of Anticipated Upgrades

As PSAPs adopt standards-based broadband technologies, tools may be enhanced at a rapid pace that surpasses traditional PSAP upgrade cycles. PSAPs will need to look ahead and plan for additional training expenses to ensure staff maintains competence without being limited to advances that are part of a traditional procurement cycle.

Skill-Focused Trainer Selection

Rather than looking to supervisors or training coordinators as the exclusive options for training, any staff with an aptitude for embracing and understanding new technology should be considered. This may be especially helpful as age-related differences in comfort with technology increases with the introduction of broadband and more proficient but junior staff are better-suited to provide or at least assist with training.

Updating Existing and Creating New Training Standards

An important factor in improving training for broadband-capable PSAPs is the ability of training programs to reflect the characteristics of the fast-paced and ever-evolving nature of broadband technology. Several current consensus-based standards could benefit from modification in order to adapt to a broadband environment. This includes revising commonly used standards language such as “calls for service” to include text, video, audio, or photographic messages, and the need for new and consistent definitions for major new terms such as “broadband” and “NG9-1-1.”[92]

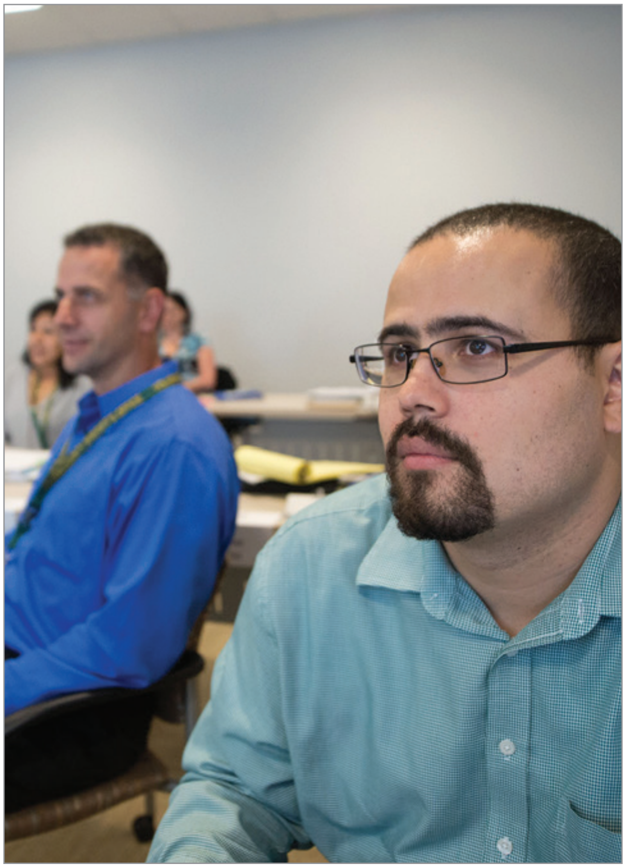
As noted above, new training programs will be needed for PSTs in areas such as cybersecurity and digital, broadband, and IT. Training models and strategies will also need to continually adapt, taking into account generational differences of PSTs in the workforce. Consider, for example, a situational awareness app that provides live video feeds, real-time location tracking, and biometric data from field responders to the PSAP. Today’s newest PSTs may have grown up with smartphones, tablets, gaming platforms, intuitive touch-screens, and high-speed technology, accompanied by a culture of little need for, and intolerance of, extensive training. Therefore, what’s intuitive to some personnel may not be intuitive to others. This again points to the need for public safety to leverage technology used in the commercial sector to benefit from the intuitive approach required by the consumer market. The capacity for broadband technology to be widespread and intuitive to consumers can be leveraged to create model training programs for PSTs while preserving flexibility to meet requirements specific to varying workforce compositions.

Existing consensus-based training standards need to be updated to reflect the expanded scope and flexible terminology of a broadband environment.

Existing consensus-based training standards need to be updated to reflect the expanded scope and flexible terminology of a broadband environment. New training standards will be needed to address needs for general aspects of broadband technology, as well as target differences among the workforce in terms of the level of intuition with emerging technologies.

Training New Stakeholders

Outside of the emergency response community, educating other constituencies including IT departments, app developers and other innovators, the general public, and elected and appointed officials would benefit PSTs and PSAPs.



Training IT Departments

When IT departments support the broadband-enabled PSAP, whether for training, technology deployments, or ensuring continued performance, it would be helpful for IT professionals to have a basic understanding of the emergency response structure. Understanding the roles and responsibilities of public safety communications professionals will improve IT personnel's communications with PSTs and overall approach to carrying out their complementary duties.

Training App Developers and Other Innovators

The broadband ecosystem makes it possible for a much wider range of innovators to develop truly helpful solutions for PSTs and PSAPs. The more familiar they are with the particular requirements and limitations of an emergency response center and public safety operations, the better able they will be to produce intuitive, effective, and efficient products and services.

Educating the General Public and Policymakers

There is an existing and growing divide between public expectations and the reality of today's PSAPs in terms of technology adoption and availability. As time goes by, this gap will only lead to more confusion on the part of the general public and government officials responsible for enacting laws and regulations and providing resources and funding impacting PSAPs. The better educated the general public is about the capabilities of the 9-1-1 system, the safer they will be, and the more efficient PSTs can be in addressing their emergency response needs. Similarly, decision-makers at all levels of government would benefit from appreciating limitations that exist at PSAPs and thus the resources needed for PSAPs to meet public expectations and keep the community as safe as possible. This applies to legacy, transitional, and fully broadband-enabled stages. ■

RECOMMENDATIONS: TRAINING

Increased Situational Awareness

Training programs should account for the significant increase in situational awareness that new technologies will afford PSTs.

Training developers should leverage university and enterprise experiences with safety-related technologies for a testing ground for enhanced features and lessons learned to inform training programs.

Training on Cybersecurity

Agencies should consider adopting the training recommendations of APCO's best practices guide to implementing effective cybersecurity policies and procedures in PSAPs, "An Introduction to Cybersecurity: A guide for PSAPs,"[93] as well as training standards, best practices, and courses from other sectors such as IT, emergency management, real-time crime centers, and fusion centers.[94]

Stress Management Training

PSAPs should place greater emphasis on stress management training, especially in anticipation of increased sources of stress brought on as a result of broadband-based technologies. Stakeholders should also participate in research to identify lessons learned in other sectors, and evaluate PST stress and the efficacy of strategies and interventions to prevent or mitigate stress. This would help ensure that any new training standards and programs are informed by existing experience and empirically-driven.

New Baseline Training and Non-Traditional Methods

A common baseline training should be adopted so that regardless of resource and training differences among PSAPs, PSTs are prepared to understand and appropriately respond to the expectations of the public and other emergency responders, particularly in mutual aid situations. Further, PSTs must be trained to use backup (legacy) tools in the event that advanced technologies fail.

In addition to traditional training programs, agencies of all sizes and resources can employ a number of options to educate their workforce, including addressing training requirements in RFPs, sharing resources with other PSAPs, budgeting for continued training needs, using skill-focused trainer selection, and taking advantage of no or low-cost media.

Updated Training Standards

APCO will update its existing standards to reflect the new scope and terminology of a broadband environment and will develop new broadband-related training standards and programs as appropriate.

Notes

90 Holmes EA, James EL, Kilford EJ, Deeprose C (2010) Key Steps in Developing a Cognitive Vaccine against Traumatic Flashbacks: Visuospatial Tetris versus Verbal Pub Quiz. PLoS ONE 5(11): e13706.

91 The meaning or appraisal of an event appears to play a large role in whether a potentially traumatic event will actually lead to traumatic effects. After traumatic calls, a PST's immediate appraisal of the incident may be "I am responsible for that person's death because I wasn't fast enough to save him," even if the PST performed perfectly. Instead, the PST can be trained to immediately reappraise that thought, to look at the event through a different lens, and replace the initial appraisal with a more accurate and adaptive one, such as "I wish I could have helped save him, but when I really think about it, I know I did my best." This strategy will help reduce or prevent traumatic effects.

92 For both general considerations and specific redline changes to existing standards, see Appendix 7.

93 https://www.apcointl.org/doc/911-resources/669-introduction-to-cyber-security-a-guide-for-psaps/file.html.

94 For a list of training courses related to Fusion Center and Emergency Operations Center Coordination, see Appendix 8.

WORKFORCE

INTRODUCTION

Broadband-enabled technologies will lead to an unprecedented amount of data available for emergency response, and PSAPs will be the nexus between the general public and field responders. This creates several workforce challenges at a time when recruiting and retaining quality personnel has never been more difficult. The stress levels, work environments, expectations, and requirements of the job are sometimes overwhelming for both the veteran staff members and newcomers. Developing strategies to address the impacts of broadband on the PSAP workforce will be critical.

THE WORKFORCE ROLE

The workforce in a fully broadband-enabled PSAP will require the expertise needed to analyze, process, and transmit many new forms of communications, including text, video, photo, telemetry data, and more. This will entail an expanded set of knowledge, skills, and abilities as well as new staffing models to manage the heightened impacts of broadband technology, including critical incident exposure, workforce burnout, retention challenges, and generational differences.

> *The workforce in a fully broadband-enabled PSAP will require the expertise needed to analyze, process, and transmit many new forms of communications, including text, video, photo, telemetry data, and more.*

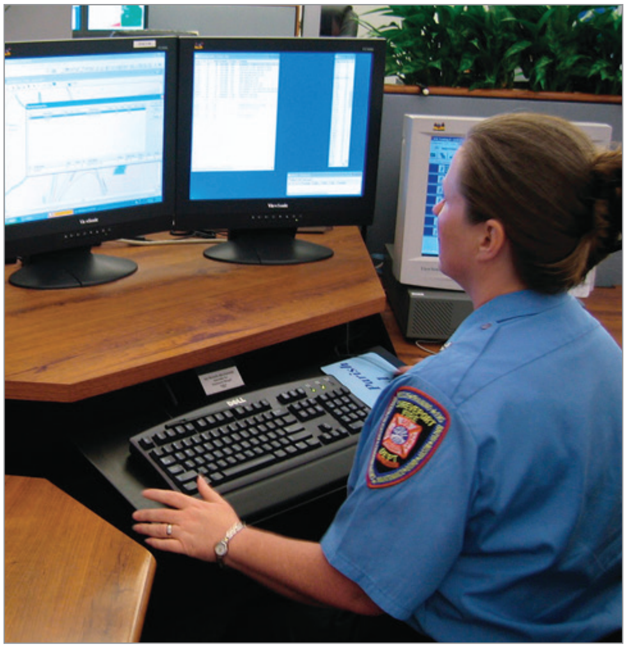
Recruitment and Retention

Recruitment and retention are already significant workforce challenges for PSAPs. Research has shown that the national average turnover rate is 17% and can be as high as 56% even at large PSAPs.[95] High turnover rates result in unnecessary costs in terms of overtime needed to make up for staffing shortages and inefficient use of hiring and training resources. More importantly, recruitment and retention difficulties can ultimately impact operations when PSAPs lack the personnel needed to perform during emergencies.

The Necessary Core Competencies, Knowledge, Skills, and Abilities

Today's PSAP workforce already requires a unique set of core competencies, knowledge, skills, and abilities (KSAs) spanning technical, operational, and legal subject areas. The critical life or death nature of the public safety communications profession distinguishes its workforce from many others, requiring a special type of individual to succeed and thrive in such an environment. Knowledge and experience with emergency operations and today's technologies will remain essential.

A broadband environment will introduce new technologies and an influx of much more data than can easily be managed with the same core competencies required in today's workforce. Data analytics tools can help to detect trends and key pieces of information. But once this data enters the PSAP, the workforce will need to cope with the challenges and seize the opportunities for making use of this information. In many ways, the differences will be in the magnitude of the new technologies and complexity and volume of the data that will be available in the future. For example, the PST may view video of a fire or select the best image of a bank robbery suspect before first responders



are able to reach the scene, placing more emphasis on the need to effectively manage resources with situational analysis and critical decision-making responsibility. More emphasis will be placed on using or quickly learning technical skills, synthesizing large amounts of data from a wide variety of sources, and analyzing the value of the information. Having a basic level of IT skills will be necessary in order to troubleshoot minor technical problems, stay on mission, and be alert to cybersecurity threats.

Examples of Existing KSAs:

- Knowledge of local features and geography, applicable laws, statutes, and codes, specialized systems and equipment, standards, policies, and procedures
- Calmness under intense pressure, multitasking, critical thinking, rapid decision-making, problem solving, active listening, interviewing, triaging, and prioritization
- Ability to comply with government or professional requirements, identify and properly utilize agency resources, and effectively use available communication tools and technologies to meet operational needs

New KSAs in the Broadband PSAP:

- Knowledge of IT systems, technology administration, GIS, and related mapping tools
- Proficiency with social media tools
- Examining data (including multimedia content, sensor information, GIS and related mapping tools, etc.) for quality, authenticity, and reliability
- Interpreting the meaning of the data and deciding what is actionable
- Determining what to tag and store, consistent with state or agency public access, privacy, and evidentiary requirements and sharing rules
- Collaborating effectively with counterparts in complementary sectors such as IT, fusion centers, and public information offices

PSAPs will need a workforce capable of handling a wide range of calls for service, from “basic” 9-1-1 calls (e.g., voice-only) to calls containing incident-related pictures and video. Appendix 9 describes the likely staffing impact with the adoption of broadband technology by comparing staffing considerations before and after broadband implementation. These charts are designed to reflect job tasks rather than specific job titles.

Increased Job Complexity and Stress

Research has shown that as the number of tasks for PSTs increased, satisfaction and retention decreased.[96] Job complexity is therefore one of the most important factors for retention in PSAPs and will be a critical issue with the introduction of broadband. In addition to today’s communications channels, broadband-enabled PSAPs will need to contend with platforms that may or may not be integrated into NG9-1-1 networks but can be relevant to emergency response. Public alerting systems such as the Integrated Public Alert and Warning System (IPAWS) will have the potential of an expanded role during emergency events in a broadband environment. Additional platforms will also be available such as reverse 9-1-1 systems, social media platforms, and mobile apps that are deployed specifically for public safety purposes or that are consumer-oriented but play an indirect role in emergency response. Balancing these platforms will be a complex task for PSTs.

PSTs will also be exposed to graphic images and videos, significantly amplifying the already stress-inducing voices and sounds they contend with today. The workforce will need to incorporate staff with the mental and emotional resiliency to handle stressors with greater frequency and severity.

Agency programs such as employee assistance programs, CISM, and debriefings will play a more vital role in protecting the workforce in a broadband environment.

Staffing Options in a Broadband Environment

Broadband technology will provide a number of useful tools that offer new opportunities for managing and meeting staffing needs.

Workforce Sub-Units

Past experience has shown that turnover can be dramatically reduced by splitting operational functions – call taking and dispatching – into separate roles.[97] Broadband technologies create new opportunities, and in some cases necessities, for specializations. For example, in order to handle the amount of new information that broadband technologies will enable for the PSAPs, and then be able to deliver the best and most relevant of this information to field responders, PSAPs may need to employ or share experienced police and fire investigators, medical professionals, and data analysts to triage incoming data. These specialized units can then pass information along to a different portion of the workforce that focuses solely on communicating with the responders. States or regions can provide opportunities for hosted functions benefitting all PSAPs in those jurisdictions, such as a multimedia analysis center or fusion center. Shared services or specialized staff can also help address or mitigate variations in sizes and resources of PSAPs, such as the number of positions, call volume, or population served.

> *In order to handle the amount of new information that broadband technologies will enable for the PSAPs, and then be able to deliver the best and most relevant of this information to field responders, PSAPs may need to employ or share experienced police and fire investigators, medical professionals, and data analysts to triage incoming data.*

Use of Other Governmental Agencies and Departments

Certain aspects of broadband technology are common to multiple state and local governmental functions, such as technology administration and support. PSAPs can leverage existing CIO, CISO, and CTO departments at local or state levels for many of their basic IT needs. Similarly, cybersecurity centers staffed with experts can be centralized and serve multiple PSAPs.

Leveraging Broadband Connectivity

A fully IP-enabled PSAP will be able to extend all NG9-1-1 call receipt and dispatch functionality to other locations, and may support the establishment of virtual PSAPs. This provides new, dynamic opportunities for mutual aid, workload sharing, call overflow management, and workload expansion. These capabilities can also enhance continuity of operations and disaster management, and increase information sharing and coordination among PSAPs.

Generational Differences

Aging in the PSAP brings its own challenges that may be manifested in a broadband environment. Each incoming generation will bring native abilities matching each leap in innovation, at a higher rate of change. Newer generations of PSTs have attained a native cognition of digital technologies, including intuitive, touch-screen, high-speed, and multitasking features. They are generally more data-centric than voice-centric. This impacts the way newer generations learn and interact in team settings.

Along with this potentially greater comfort level with new technology, younger generations bring recruitment and retention challenges. Relatively speaking, the younger segment of today's workforce desires a mobile work environment, changes jobs more readily, and expects rapid career progression.

Retaining the "aging" workforce must remain a priority. While some in this category may have a difficult time adapting to the broadband environment, they will remain essential to PSAP operations. The mature segment of the PSAP workforce has experience, as well as knowledge of existing technology that the younger segment may have no experience with.

FINDINGS

New Workforce Roles

The workforce of the future will need to expand upon existing knowledge, skills, and abilities to include cybersecurity awareness, familiarity with digital, broadband, and IP-based technology, and the ability to sift through and prioritize increased volumes and types of data, including unsettling imagery. Agencies will need to account for the following new job functions as they implement broadband technologies. Many of these duties may be absorbed by existing staff while other functions may require the creation of a new position such as a data or intelligence analyst.

> *The workforce of the future will need to expand upon existing knowledge, skills, and abilities to include cybersecurity awareness, familiarity with digital, broadband, and IP-based technology, and the ability to sift through and prioritize increased volumes and types of data, including unsettling imagery.*

Operational

- Triage/evaluate incoming data, including video from fixed systems, vehicle and body worn camera systems, and NG9-1-1 callers.
- Receive and process information coming in from sensors and analytical systems. This could include devices that are used by first responders (e.g., biometric telemetry from firefighters working on HAZMAT scenes or a gunshot detection sensor on an officer's vest).
- Collect, analyze, and distribute data from a variety of new sources made available by broadband technology. For example, a PST may need to review multiple incoming video or picture images to determine which (if any) should be forwarded to responding units, flagged for review by investigators at a later date, or stored.
- Liaise between the PSAP and external entities who are managing data on behalf of the agency. For example, a PSAP may elect to initially dispatch EMS units and then route all video calls needing pre-arrival medical care to a third party center that specializes in that function.
- Monitor or analyze social media feeds to identify information critical for first responders. Some PSAPs are already using data mining filters to monitor Twitter message traffic to obtain intelligence at large events, including the location of disturbances and other problems being noted on social media.
- Manage the equipment, software, and network components.

Administrative

Human Resources

Implementation of broadband technologies will result in a dramatic change for PSAP operations and a resulting change in the needs of the PSAP workforce. Human resource departments supporting PSAPs will need to manage a host of new issues and employee requirements. These changes will likely impact the recruiting and hiring process, including the introduction of new candidate testing methodologies. Expected changes in job functions, organizational span of control, and employee training will require a comprehensive review of position classifications and benefits. Promotion and salary structures will need to be reassessed. Each PSAP must make these changes based on its own workforce and agency needs. Additionally, policies will need to be developed regarding employees who cannot cope with the new requirements. If a PSAP adopts broadband technologies in phases, there could be a gradual shift in the workforce.

Critical Incident Stress Management (CISM)

PSTs will be exposed to an increased level of stress due to the changing nature of the PSAP environment, the likelihood of an increase in workload, and the possibility of critical incident stress once live video and other potentially graphic displays are introduced to the PSAP. Each PSAP should develop or amend their CISM intervention plan to accommodate these new risks.

Public/Media Information Management
The implementation of broadband technologies will have a number of different impacts with regard to social media and information management. As more data is made available to the PSAP through the implementation of broadband technology, there will be more pressure on the public safety organization to acknowledge the presence of that data following a major incident. Each PSAP should organize its workforce to ensure responsibilities and policies are clear.

Recruitment and Retention Issues

Recruitment and retention of tech-savvy personnel will be beneficial to deal with the ongoing evolution of technology in PSAPs. This presents a variety of challenges for PSAPs that are either new or different from what they face today.

Aging in the PSAP

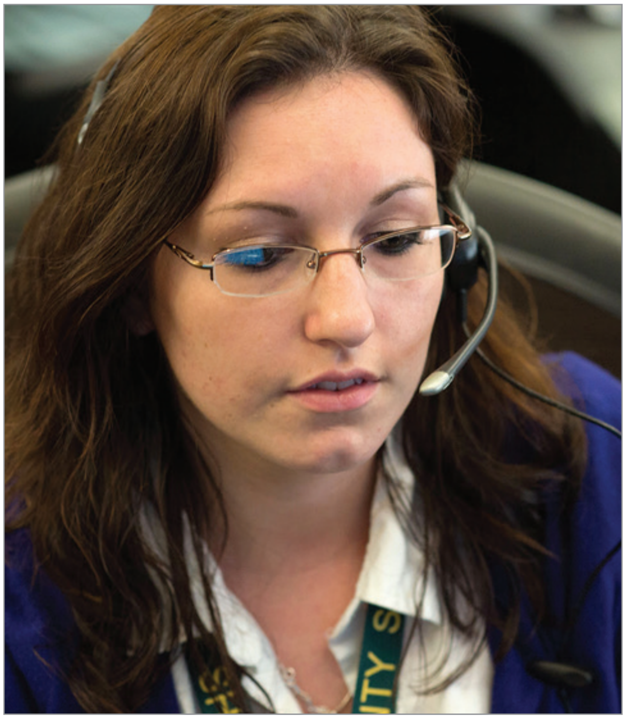
Generational differences in the workforce will become more evident as the complexity and speed of implementation of technology increases. It will be critical to address training and operational issues to retain personnel with substantial experience in emergency communications despite challenges adapting to new technologies.

Appropriate Recognition for PSTs

The nature of PSTs' work generally keeps them out of the public eye. Consequently, they often do not receive appropriate recognition for their sacrifice, dedication, and public service. The lack of recognition, and often respect, translates to a challenge for morale, as well as salary and other benefits. This ultimately creates a substantial recruitment and retention issue.

Staffing Levels

Technology adoption and staffing levels are intertwined. If a PSAP is dealing with a staffing shortage, adding the challenge of adopting new technology could be more difficult and even detrimental to operations. Conversely, broadband technology has the potential to help PSAPs deal with staffing shortages, for example, by creating connections to other PSAPs for failover during high call volumes. According to APCO's research, the vast majority of PSAPs lack sufficient staff to comfortably handle the workload, stress is worse without adequate staffing, the workload for PSTs has been increasing, and staffing is the most important factor in predicting retention rates.[98] As discussed further below, APCO Project RETAINS and the accompanying tool kit to assist PSAPs with estimating staffing needs are currently being updated.



Quality Assurance Programs

In conjunction with the challenges of broadband technologies, PSTs will continue to face pressure to keep call processing times as short as possible, while balancing the value of the information at hand. Comprehension of primary versus secondary or supplemental information will continue to play an integral role in the PSAP. In other words, knowing what baseline information is necessary to trigger a dispatch and with some incidents, modify a response based on additional information received. In some instances more time may be required to process broadband-based information, but the result may lead to a much more effective response. Agencies should give careful consideration to establishing a quality assurance program that accounts for the use of broadband information as well as developing a comprehensive training program for new and experienced staff members. ■

EVAC

RECOMMENDATIONS: WORKFORCE

New Recruitment and Retention Strategies

PSAPs should consider a variety of recruitment and retention strategies to grow and maintain a workforce having skills in new technologies.

New Focus on the PST Career

The future PSAP workforce will involve the same passion for serving to protect the safety of the public and responders, coupled with an interest and talent for embracing new broadband and information technologies. This is a profession that deserves more attention for its importance to saving and protecting lives, and, in a broadband environment, it will be a profession with more options for growth and advancement. Accordingly, governments at all levels should drive interest in and development of post-secondary educational programs to produce graduates trained in IT, PST, and related emergency response skills.

> *Governments at all levels should drive interest in and development of post-secondary educational programs to produce graduates trained in IT, PST, and related emergency response skills.*

For example, federal and state scholarship programs could create or expand upon public service programs to include NG9-1-1. There are already programs that offer scholarships to attract much-needed talent for public service. In recent years, such programs have been expanded to improve the cybersecurity workforce in government.[99] These educational programs could also incorporate simulated PSAP environments, to help prepare candidates for the exposure to the at times intense nature of emergency communications.

> *The future PSAP workforce will involve the same passion for serving to protect the safety of the public and responders, coupled with an interest and talent for embracing new broadband and information technologies.*

Job Exposure During Recruitment and Training

A common problem for PSAP retention is losing new PSTs soon after they finish initial training because the job proved more difficult than expected. This results in a significant loss of investment in terms of training resources and the lost opportunity of another potential hire who might have remained. To address this issue, PSAPs could increase the amount of exposure candidates receive prior to or early in the application process, which could eliminate candidates who will not stay before further investment is made in their hiring and training. For example, the application process could include listening to several emotionally difficult calls that have been handled by employees in that center. A realistic demonstration of actual incidents and how they were processed may be necessary to portray the type of work an applicant may need to perform, and additional consideration should be given to strategies that would include longer exposures so potential hires have a sense of what it's like to work a full shift.

Researching New Hiring Models and Incentives

The lack of budget and hiring flexibility makes it hard for PSAPs to maintain adequate staffing. Many PSAPs must manage staffing shortages for long periods between hiring cycles, and the shortages can get worse the longer they go on due to the increased workload on PSTs in an understaffed PSAP. Some agencies over-hire to create a buffer against anticipated attrition. Agencies could also consider more flexibility in hiring, including looking to other public safety disciplines for candidates that did not end up completing the recruitment process but may be interested in a PST career.

Agencies should also consider offering incremental years of service incentives as part of recruitment and retention. Pay bonuses based on years of service – x% for one year, 2x% for two years, etc. – could offer a more compelling incentive to remain through a minimum length of service than non-binding commitment agreements which are widely used today. Additionally, where agencies lose personnel to neighboring jurisdictions that offer better salary or benefits, agencies could offer a deferred signing bonus that is not awarded until the completion of the minimum service term.

Professional Development

Retention, particularly of the younger segment of the workforce, could be improved through increased training and professional development opportunities. As described in the Training section of this report, PSAPs can leverage broadband technology for online classes and interactive training, which could increase job satisfaction as well as performance. PSAPs can also expand career opportunities by crafting new positions and staffing options. Plus, the additional functions required in a broadband-enabled PSAP will most likely require a restructuring of the normal recruitment practices, work hours and shifts, pay grades, job responsibilities, and promotion track. During this restructuring, managers could be creative with job titles and levels of responsibility. If there are more promotion opportunities, chances to cross train, diverse operational roles, and increased levels of responsibility, personnel could be more likely to stay with an organization.

Research New Staffing Models

As discussed above, PSAPs have a number of options to meet the future workforce demands of a broadband environment. This can include a combination of specialized workforce sub-units, using other agencies and departments, and leveraging broadband technology to improve connectivity and thereby enable human resource sharing for mutual aid, periods of high volume, continuity of operations, etc. Further research is needed into the technology, training, and governance issues associated with these dynamic approaches.

Increase Recognition of PSTs

APCO will continue its efforts to ensure PSTs receive the respect and recognition they deserve. One strategy for increasing the public's understanding and appreciation of the life-saving work performed by PSTs is to encourage more widespread reporting of 9-1-1 stories. This in turn could help raise awareness of the value of serving in such a public safety capacity, along with the new options and opportunities that broadband technology will enable at PSAPs. Accordingly, APCO will investigate creating a new award that recognizes a journalist, anchor, or news organization for admirable coverage of 9-1-1 operations.

Continued Research and Support for Staffing and Retention Issues

APCO Project RETAINS was launched to address staffing issues for PSAPs. As part of the Project, APCO conducted a national study of staffing and retention issues, the results of which informed an Effective Practices Guide.[100] Current models that aid in determining adequate staffing are available; however, updates will be needed in the future for accurate calculations in an NG9-1-1 environment. For example, some current staffing formulas require the input of incident types such as domestic violence and emergency medical dispatch to help compute staffing recommendations. It will be necessary to re-examine these and make additions to adequately capture the challenges that NG9-1-1 incidents will bring and the time it takes to process them. APCO is updating the research for Project RETAINS and the accompanying tool kit to assist PSAPs with estimating staffing needs and addressing retention issues, mainly focused on the current environment. It will be a few years before full NG9-1-1 can be realized. At that future point, APCO will consider a next (third) iteration of Project RETAINS to incorporate broadband-specific inputs to help address NG9-1-1 staffing issues.

Notes

[95] Staffing and Retention in Public Safety Communications Centers, APCO Project RETAINS (Aug. 2005), https://www.apcointl.org/doc/conference-documents/personnel-human-factor/283-project-retains-effective-practices-guide-2005/file.html.

[96] *Id.*

[97] *Id.* at 34, describing how one agency reduced PST turnover from 40% to 8-13%.

[98] *Id.*

[99] For example, see the Commonwealth of Virginia's Cybersecurity Public Service Scholarship Program, http://schev.edu/index/tuition-aid/financialaid/state-student-aid/cybersecurity-public-service-scholarships. Also, the National Security Agency (NSA) and DHS jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/.

[100] For more information on APCO Project RETAINS, visit http://retains.apcointl.org/.

CONCLUSION AND NEXT STEPS

The introduction of broadband technologies will be an evolution, not a discrete change for PSAPs. It is APCO's intent that this report serves as a starting point to guide additional efforts to serve the public safety communications community at all levels and in all sectors.

ESSENTIAL FINDINGS AND RECOMMENDATIONS

While every finding and recommendation in this report warrants consideration, the following require the most immediate attention.

Appropriate Recognition for Public Safety Telecommunicators

Public safety communications professionals are and will remain essential to emergency operations. As communication methods evolve, the skill and professionalism of PSTs will remain constant, serving as a lifeline for members of the public and first responders. Garnering financial support and attention from industry and decision-makers in government, whether for upgrading technology or supporting the workforce, depends on understanding the emergency communications ecosystem. Accordingly, PSTs deserve appropriate respect and recognition at the federal, state, and local levels.

Building a Shared Vision for the Future of Emergency Communications

With the transition to broadband technologies, PSAPs have a chance to break the cycle of proprietary, one-off solutions for public safety. The time has come to think outside of the box and reject the assumption that public safety products require costly enhancements to achieve interoperability. With CPE, network elements, RMS, GIS, CAD, mobile apps – every element of public safety communications – the community must demand interoperability as a baseline expectation. The vision must be end-to-end, meaning from the initial report of an emergency, whether from a member of the public making a voice call or another input, to PSTs and onto first responders in the field, every element of the ecosystem must be interoperable with other components.

A common definition of NG9-1-1 is essential for achieving this vision: "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."

Emergency Communications Centers as the "Nerve Centers" of Emergency Response

Rather than serving a primary purpose of receiving and processing 9-1-1 calls, PSAPs will quickly morph into fully integrated command, control, and communications centers with capabilities that include basic intelligence collection and monitoring, 9-1-1 multimedia traffic processing, full scale dispatch, and incident command capabilities. Communications centers will increasingly be the "nerve centers" of public safety operations. "Public Safety Answering Point" fails to convey the important operational role. Accordingly, stakeholders should adopt the term "Emergency Communications Center."

Interoperability and Standards

Standards are critical, and the public safety community needs mechanisms to ensure that NG9-1-1 systems meet the interoperability goals described in the use cases above, 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.

The Need for Federal Action to Support 9-1-1

Congress should establish a substantial grant program to modernize 9-1-1 services across the country as a national imperative. This would help ensure that all PSAPs have the resources needed to upgrade in approximately the same timeframe. A grant program can drive objectives such as seamless interoperability, promote information and resource sharing, drive cost efficiencies, require use of open and competitive procurement practices, ensure states create sustainable funding mechanisms to support continued operations, and potentially prevent 9-1-1 fee diversion.

APCO has and will always advocate for local control. The recommendations contained in this report, and those to come as the result of future work, in no way diminish that support or alters APCO's position. To the contrary, APCO believes that broadband technology will enable the ECC to enhance local capabilities via shared services like cybersecurity and call delivery, improve information flow, and increase interoperability.

Cybersecurity

Cybersecurity already presents major challenges for PSAPs, and the threats will only increase with the continued introduction of broadband technologies. PSAPs need additional support to address these challenges. APCO will continue working with expert organizations in the public and private sector to develop educational materials, strategies, and partnerships to give PSAPs the resources they need to prepare for and respond to cyber incidents.

APCO'S NEXT STEPS COMMITMENT

There are a number of steps that APCO will take pursuant to the findings and recommendations of this report. APCO will:

- Undertake an analysis to determine what new or modified standards may be needed as a result of this report, and make recommendations accordingly to APCO's Standards Development Committee
- Review existing training and certification programs and explore the need for changes to address emerging broadband technology
- Create a Task Force on Public Safety Apps that will undertake a number of activities to support and expand upon APCO's efforts by providing subject matter expertise and engaging with public safety professionals and app developers
- Develop an online repository for sharing next generation best practices for PSAPs
- Perform an occupational analysis of the work performed by the next generation PST when appropriate
- Develop and offer a cybersecurity hygiene course for PSAP personnel
- Review existing best practices and guidance related to GIS for opportunities to support PSAPs implementing next generation services
- Update existing and develop new curricula related to broadband implications for the PSAP
- Advocate for federal funding for modernizing 9-1-1
- Consider a next (third) iteration of Project RETAINS to incorporate broadband-specific inputs to help address NG9-1-1 staffing issues

This is a crossroads for the public safety communications profession, and APCO is committed to moving both the technology, and the profession, forward as one. With the continued support of its members, industry and government partners, and innovative thinkers, APCO believes that the ECC of tomorrow is not only possible, but it is absolutely essential to the safety and well-being of every citizen in the United States. Together, this community will transform the PSAP of today into the Emergency Communications Center of tomorrow. ■

APPENDICES

Appendix 1. Potential Vulnerabilities of NG9-1-1 Interconnection with the NPSBN

Given that NG9-1-1 and FirstNet networks will enable significant exchange of data, all stakeholders should pay close attention to the prospect of bad actors seeking to exploit one or both of these significant pillars of the future emergency response ecosystem. The following is a detailed list of potential vulnerability points resulting from the interconnection of NG9-1-1 with the NPSBN.

- Compromised citizen devices impacting FirstNet
  - Traffic interception
    Over The Top (OTT) or IP next generation apps are vulnerable to traffic interception, particularly when utilizing the public Internet
    - Extraction of Personally Identifiable Information (PII), especially in the case of calls involving medical information exchanged with the EMS responder
    - Information passed from a PSAP to a caller may not be suited for wider consumption, especially with regards to police interactions
    - The caller information going to a first responder can be spoofed, risking false responses, response testing (reconnaissance), or denial of service attacks
    - First responder information could be intercepted, allowing future attacks on the identified device (now known to belong to a first responder)
  - Malware – caller
    Malware (worm) on an end-user device could infiltrate other systems or devices
    - Citizen device could pass malware into FirstNet
    - Citizen device could pass malware into first responder device
  - Denial of service
    Citizen devices could be used to generate DDoS attacks
    - Citizen devices could generate DDoS attack into FirstNet
    - Citizen devices could generate DDoS attack on first responder device(s)

- Compromised Originating Network impacting FirstNet
  - Traffic Interception
    Compromised Originating Network could intercept traffic interacting with FirstNet
    - Extract PII
    - Extract inappropriate information
    - Intercepted traffic in Originating Network is spoofed
    - Intercepted traffic in Originating Network identifies first responder device
  - Malware – network
    Malware in Originating Network could infiltrate other systems or devices
    - Originating Network could pass malware into FirstNet
    - Originating Network could pass malware into first responder device
  - Ransomware – network
    Ransomware in Originating Network could infiltrate other systems
    - Originating Network could pass ransomware into FirstNet
  - Denial of service
    Compromised Originating Network could generate DDoS attacks
    - Originating Network could generate DDoS attack into FirstNet
    - Originating Network could generate DDoS attack on first responder device(s)

- Compromised Internet server, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on Internet server could infiltrate other systems or devices
    - Internet server could pass malware into FirstNet
    - Internet server could pass malware into first responder device
  - Ransomware – network
    Ransomware in Internet server could infiltrate other systems
    - Internet server could pass ransomware into FirstNet
  - Denial of service
    Compromised Internet Server could generate DDoS attacks
    - Internet server could generate DDoS attack into FirstNet

    - Internet server could generate DDoS attack on first responder device(s)

- Compromised Government server, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on Government server could infiltrate other systems or devices
    - Government server could pass malware into FirstNet
    - Government server could pass malware into first responder device
  - Ransomware – network
    Ransomware in Government server could infiltrate other systems
    - Government server could pass ransomware into FirstNet
  - Denial of service
    Compromised Government Server could generate DDoS attacks
    - Government server could generate DDoS attack into FirstNet
    - Government server could generate DDoS attack on first responder device(s)

- Compromised LMR network/devices, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on LMR network could infiltrate other systems or devices
    - LMR network could pass malware into FirstNet
    - LMR network could pass malware into first responder device
  - Malware – devices
    Malware on LMR devices could infiltrate other systems or devices
    - LMR devices could pass malware into FirstNet
    - LMR devices could pass malware into first responder device
  - Ransomware – network
    Ransomware in LMR Network could infiltrate other systems
    - LMR network could pass ransomware into FirstNet
  - Denial of service
    Compromised LMR network could generate DDoS attacks
    - LMR network could generate DDoS attack into FirstNet
    - LMR network could generate DDoS attack on first responder device(s)

- Compromised NG9-1-1 PSAP impacting FirstNet
  - Malware – network
    Malware in NG9-1-1 PSAP could infiltrate other systems or devices
    - NG9-1-1 PSAP could pass malware into FirstNet
    - NG9-1-1 PSAP could pass malware into first responder device
  - Ransomware – network
    Ransomware in NG9-1-1 PSAP could infiltrate other systems
    - NG9-1-1 PSAP could pass ransomware into FirstNet
  - Denial of service
    Compromised NG9-1-1 PSAP could generate DDoS attacks
    - NG9-1-1 PSAP could generate DDoS attack into FirstNet
    - NG9-1-1 PSAP could generate DDoS attack on first responder device(s)

- Compromised legacy PSAP impacting FirstNet
  - Malware – network
    Malware in legacy PSAP could infiltrate other systems or devices
    - Legacy PSAP could pass malware into FirstNet
    - Legacy PSAP could pass malware into first responder device
  - Ransomware – network
    Ransomware in legacy PSAP could infiltrate other systems
    - Legacy PSAP could pass ransomware into FirstNet
  - Denial of service
    Compromised legacy PSAP could generate DDoS attacks
    - Legacy PSAP could generate DDoS attack into FirstNet
    - Legacy PSAP could generate DDoS attack on first responder device(s)

- Compromised Next Generation Core Services (NGCS) element impacting FirstNet
  - Malware – network
    Malware on NGCS element could infiltrate other systems or devices
    - NGCS element could pass malware into FirstNet

    - NGCS element could pass malware into first responder device
  - Denial of service
    Compromised NGCS element could generate DDoS attacks
    - NGCS element could generate DDoS attack into FirstNet
    - NGCS element could generate DDoS attack on first responder device(s)

- Compromised Emergency Services IP Network (ESInet) element impacting FirstNet
  - Malware – network
    Malware on ESInet element could infiltrate other systems or devices
    - ESInet element could pass malware into FirstNet
    - ESInet element could pass malware into first responder device
  - Ransomware – network
    Ransomware on ESInet element could infiltrate other systems
    - ESInet element could pass ransomware into FirstNet
  - Denial of service
    Compromised ESInet element could generate DDoS attacks
    - ESInet element could generate DDoS attack into FirstNet
    - ESInet element could generate DDoS attack on first responder device(s)

- Compromised FirstNet device impacting NG9-1-1
  - Traffic Interception
    - Compromised FirstNet device could intercept traffic interacting with citizen
    - Extract PII
    - Extract inappropriate information
    - Intercepted traffic in FirstNet is spoofed
  - Malware – network
    Malware in FirstNet network could infiltrate NG9-1-1 network
    - FirstNet network could pass malware into NG9-1-1 network
    - FirstNet network could pass malware into interconnected network (Government server or Internet server)
    - FirstNet network could pass malware into Originating Network
    - FirstNet network could pass malware into citizen device
  - Malware – device
    Malware in FirstNet device could infiltrate NG9-1-1 network
    - FirstNet device could pass malware into NG9-1-1 network
    - FirstNet device could pass malware into interconnected network (Government server or Internet server)
    - FirstNet device could pass malware into Originating Network
    - FirstNet device could pass malware into citizen device
  - Denial of service – network
    Compromised FirstNet server could generate DDoS attacks
    - FirstNet network server could generate DDoS attack into NG9-1-1 network
    - FirstNet network server could generate DDoS attack into interconnected network (Government server or Internet server)
    - FirstNet network server could generate DDoS attack into Originating Network
    - FirstNet network server could generate DDoS attack on citizen device
  - Denial of service – device
    Compromised FirstNet device could generate DDoS attacks
    - FirstNet network device could generate DDoS attack into NG9-1-1 network
    - FirstNet network device could generate DDoS attack into interconnected network (Government server or Internet server)
    - FirstNet network device could generate DDoS attack into Originating Network
    - FirstNet network device could generate DDoS attack on citizen device

Appendix 2. Use of Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. By using a set of user defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. The following provides more guidance on the use of firewalls to control access.

Firewall Basics

A firewall is either a stand-alone device or a software application running on a host with the following characteristics:

- Supports at least one internal and one external connection
- Filters information in the following ways:
  - Service control
  - Direction control
  - Behavior and content control (email, web)
- Functionality ranges from basic to complex:
  - Packet filtering
  - Application level – proxy server
  - Deep packet inspection
- Requires special expertise for proper selection and configuration

Selecting Components - Security Features that Matter

Consider the following best practices when selecting system components:

- Choose devices and protocols that support encryption, integrity, and nonrepudiation whenever possible. Encryption protects the information traversing a network by making it unreadable to unauthorized users. Integrity checks determine if any changes have been made to a network message. Nonrepudiation verifies the identity of an information source.
- Give preference to devices with logging capability, such as Syslog support. Event logging is available in a wide range of devices including routers, firewalls, backup systems, and access control systems. Logs can aid in early threat detection by recording significant network events, changes to firewall configuration, or user access to an area or device. Syslog is a logging standard that can be used to consolidate log information from multiple devices on a network.
- Look for tamper proofing, built-in locks, and other access control features when selecting mission critical components.

Wireless Technology

- Choose wireless devices with built-in firewalls and support for the highest level of encryption available.
- Harden wireless access devices by following these steps:
  - Replace the default administrator name and password with strong alternatives.
  - Follow the device's "Before You Begin" protocols.

Configuring Security Features

The goal in this phase of the process is to properly configure the security features of each system component. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic. A typical approach is:
  - Create rules that explicitly deny access
  - Add rules to permit only the required access
  - Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP "SYN-flood" attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

Appendix 3. Recommended Guidelines and Practices for Password Creation and Protection[101]

User passwords for public safety networks must balance security needs with burdens on the user. Password protection policies can help ensure the public safety network remains secure and that all users (including employees, contractors, consultants, temporary workers, etc.) adhere to the password policy. The following provides recommended guidelines and practices for password creation and protection.

Password Creation

- Strong passwords:
  - Contain at least 8 alphanumeric characters.
  - Contain both upper and lower case letters.
  - Contain at least one number (for example, 0-9).
  - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:”;’<>?,/).

- Poor, or weak, passwords have the following characteristics:
  - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
  - Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
  - Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
  - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
  - Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1, or 1secret).
  - Are some version of “Welcome123,” “Password123,” or “Changeme123.”

Additional Considerations:

- Never write down a password. Instead, try to create passwords that can easily be remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation.
- Do not use the same password for business accounts as for personal access.
- Where possible, users must not use the same password for various business access needs.
- User accounts that have system-level privileges granted through group memberships must have a unique password for all other accounts held by that user to access system-level privileges.

Password Protection

- Regularly Change Your Password:
  - All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
  - All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months, preferably every four months.
  - Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

- To Protect Your Password, Do Not:
  - Share with anyone. All passwords are to be treated as sensitive, confidential information.
  - Insert into email messages or any other form of electronic communication.
  - Reveal over the phone to anyone.
  - Reveal on questionnaires or security forms.
  - Hint at the format of a password (for example, “my family name”).
  - Share business passwords with anyone, including administrative assistants, secretaries, managers, coworkers, and family members.
  - Write passwords down and store them anywhere in the office, including in a file on a computer system or mobile devices (phone, tablet) without encryption.
  - Use the “Remember Password” feature of applications (for example, web browsers).

- In Administering User Accounts and Passwords:
  - Maintain a simple and usable password management structure, which can be administered by the fewest number of personnel possible.
  - Grant rights only to those who need them.
  - Adhere to the policy of least privileged user level, meaning if a basic user can perform all of the tasks necessary, don't grant administrator access to them.
  - Limit the number of administrator accounts and only use them for administrative work, use a regular log on for day-to-day work.
  - Disable or rename built-in administrator accounts.
  - Deny anonymous or guest accounts as these typically can be exploited.
  - Periodically run audits against the users to determine what is actually their effective rights and permission. If a user is a member of several security groups, it is possible for that user to have elevated privileges that were not intentional.

Note

[101] For additional discussion of password policy, see "Password Construction Guidelines," the SANS Institute, at https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines.

Appendix 4. Removable Media and Access Port Security Policies

Removable media are helpful for processes such as backing up data, updating software, and transferring files without a network connection. However, removable media have historically been a source of spreading malware and viruses. A well-documented and closely followed removable media and access port policy helps ensure the integrity of the network, data, and computer systems of the agency. The following provides guidance on removable media security and access port policy.

Security of Data

- In order to minimize physical risk, loss, theft, or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. At least one storage copy should be located offsite.

- Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way while in their care or under their control.

- All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all protected, restricted, or controlled data held must be encrypted.

- Virus and malware checking software approved by the agency must be operational on both the machine from which the data is taken and the machine onto which the data is to be loaded. The data must be scanned for viruses and malware before the media is loaded onto the receiving machine.

- Only data that is authorized and necessary to be transferred should be saved onto the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.

- Special care must be taken to physically protect the removable media device and stored data from loss, theft, or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Restricting Access to Removable Media

- Some policies prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media. Therefore, clear business benefits that outweigh the risks must be demonstrated before approval is given.

- Requests for access to, and use of, removable media devices must be made to the department supervisor. Approval may only be given by a department manager.

Procurement of Removable Media

- All removable media devices and any associated equipment and software must only be purchased and installed by IT. Non-agency owned removable media devices must not be used to store any information used to conduct official agency business and must not be used with any agency-owned or leased IT equipment.

- Only agency purchased and IT-approved equipment and media should be used to connect to any agency equipment or network.

Network Port Access

- All open, and unused, network ports must be turned off through the management console of the respective switch, router, or firewall.

- The network device should be secured itself by adhering to password creation and protection policies.

- Any ports which will not be used for an extended period of time, for example when an employee goes on extended leave or retires, should be turned off and not accessible until it is needed again.

Appendix 5. Functional Elements Associated with NG9-1-1 and the NPSBN

Functional elements describe how NG9-1-1 will operate and integrate with origination networks and FirstNet. What follows is a more detailed description of the functional elements associated with the integration of NG9-1-1 and the NPSBN.

NG9-1-1 Functional Elements

- User Element – This is either the caller's device or a proxy for that device. This device is responsible for obtaining its current location and inserting it into the SIP call setup header to be used for call routing.
- Location Server (LS) – This element tracks and reports the current location of the 9-1-1 caller. The LS can be a static database for fixed locations, the Mobile Positioning Center (MPC) for wireless callers, or the VoIP Positioning Center (VPC) for mobile VoIP systems.
- Emergency Services Routing Proxy (ESRP) – This is a policy-based emergency call routing platform that routes a call to a PSAP based upon location, congestion, availability, language, caller impairment, PSAP capability, and other parameters.
- Emergency Communications Routing Function (ECRF) – This is a location-based emergency call routing function that provides information about the appropriate PSAP.
- NG9-1-1 PSAP – A PSAP that can handle a next generation formatted call.
- Border Control Function (BCF) – This is a combination of a session border controller (SBC) that provides security filtering SIP transactions, and a firewall that provides security filtering of all other types of transactions. There may be several BCFs to support all ingress and egress points of the ESInet.
- Legacy Gateways, Legacy Network Gateways (LNG), and Legacy Selective Router Gateways (LSRG) – These functional elements provide translations between legacy signaling (SS7) and next generation signaling (SIP) allowing calls to be transferred between legacy PSAPs and NG9-1-1 PSAPs.
- IP Multimedia Subsystem (IMS) support – At this time it is uncertain as to whether the ESInet will require a full IMS core, or just an IMS border proxy. This element would manage authentication and Quality of Service (QoS).

FirstNet

- Home Subscriber Server (HSS) – This server manages authentication at the LTE device level.
- Policy and Charging Rules Function (PCRF) – This element is responsible for managing resources for end users based upon end user role and application requirements.
- Mobility Management Element (MME) – This functional element manages call handoff between LTE cell sites when the user is in transit.
- Signaling Gateway (SGW) – This device supports a secure channel to the end user's device. A separate channel is provided and prioritized for each application.
- Packet Gateway (PGW) – The gateway provides Internet connectivity for the applications.
- eNodeB – These are the LTE cellular nodes.
- User Element (UE) – These are the end user devices.

Interconnection Between NG9-1-1, FirstNet, or IMS

- Home Subscriber Server (HSS) – The HSS manages authentication at the SIP or VoIP level.
- Proxy Call Session Control Function (P-CSCF) – This proxy either sits at the edge of the home network (FirstNet, in this case) or at the edge of the visiting network (NG9-1-1, in this case). It manages call flows between the two networks, including authentication and prioritization.

- Interrogating Call Session Control Function (I-CSCF) – This proxy serves as a central forwarding point for all external SIP service requests. It manages call flows between outside proxies and internal IMS proxies.

- Serving Call Session Control Function (S-CSCF) – This functional element is responsible for SIP client registrations, determining the appropriate application servers to use, and provides routing (typically ENUM) lookups.

- Telephony Application Server (TAS) – This application server manages advanced call features. These features include services such as conference bridging, voice mail, call forwarding, and other telephony features.

- Public Switched Telephone Network (PSTN) Gateway – This element is used when a SIP call needs to be connected to the PSTN.

- ENUM Servers – ENUM is a system that supports using the Internet DNS structure to support call routing of SIP calls to other domains without having to transit the PSTN.

Appendix 6. Sample Training Language for RFPs

When procuring broadband technology from various vendors, PSAPs should consider addressing training needs in their RFPs. The following provides sample RFP language for a variety of options for user and administrator training.

User Training and Administrator Training Options

User Training and Administrator Training programs will be provided for the system. User training shall be a minimum four hours in length and be conducted at locations within the State. Administrator training shall be a minimum six hours in length and be conducted at a central location within the State. All training documentation shall be provided prior to any PSAP installation. The Contractor must provide cost information for each training option. The State reserves the right to choose one or more options.

Training Option 1 - Just In Time Training
Contractor shall provide training to PSAP no less than three days prior to installation of the new software platform at each PSAP. Sufficient training classes at each PSAP will be provided to ensure that personnel from all shifts can be trained (no less than two classes will be conducted at each PSAP). Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training for all PSAP personnel. Training will be conducted in a training room outside of the active PSAP area of the answering point.

Training Option 2 - Regional Training Offsite from PSAPs
Contractor will provide training classes in dedicated classrooms offsite from the PSAPs. Sufficient classes will be conducted to ensure that all PSAP personnel are trained prior to the installation and activation of the new software platform. No less than 60 classes of 25 students each will be conducted. Contractor will provide for no less than two concurrent classes during the installation and activation period. Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training in the classroom. Classrooms will be provided by the State.

Training Option 3 - Train the Trainer
Contractor will provide training classes in dedicated classrooms offsite from the PSAPs. Sufficient classes will be conducted to ensure that representatives from each PSAP are trained as trainers prior to the installation and activation of the new software platform. Sufficient training will be provided to ensure that trained trainers can successfully train their respective PSAP call takers and dispatchers. Online and phone-based help desk services must be provided to ensure that all trainers can resolve training questions and problems. No less than eight classes of 25 students each will be conducted. Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training for trainers in the classroom. Classrooms will be provided by the State.

Training Option 4 - Self-Paced Online or CD-Based Training
Contractor will provide the capability for all users to utilize online or CD-based self-paced training. Sufficient capability or number of CDs must be provided to ensure that all training can be acquired prior to the installation and activation of the software platform. Online and phone-based help desk services must be provided to ensure that all users can resolve training questions and problems.

Administrator Training

There shall be administrator training that will provide the Department and PSAPs with any information needed to administer/manage the system. Please explain in detail the training to be provided.

Appendix 7. Suggested Modifications to Existing Training-Related APCO Standards

An important factor in improving training for broadband-capable PSAPs is the ability of training programs to reflect the characteristics of the fast-paced and ever-evolving nature of broadband technology. For the most part, APCO's standards are written to have broad applicability – both with regard to agency resources and, whenever possible, with regard to technology. Thus, many don't require modification to accommodate broadband capabilities. However, several standards could benefit from modification, described below as general considerations related to the impacts of broadband technology, followed by specific recommendations for language to change.

General Considerations

- Many APCO standards include a phrase such as "Information contained in calls for service," without specifying the type of information. In some cases, adding language such as "including text, video, audio, or photographic messages" or "NG9-1-1 and other broadband technologies" could be beneficial. Further review is suggested of the following standards:
    - Minimum Training Standards for Public Safety Telecommunicators APCO ANS 3.103.2.2015
        - Sections 3.10, 7.2.3, 8.4, 9.3.1, 9.3.3, 10.3.1, 10.4
    - Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator APCO ANS 3.104.1-2012
        - Sections 3.11.2, 3.11.3, 4.3.17
    - Core Competencies and Minimum Training Standards for Public Safety Communications Instructor APCO ANS 3.108.1.2014
        - Sections 3.11.2, 3.11.3
    - Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor APCO ANS 3.102.1-2012
        - Sections 3.11.2, 3.11.3
    - Core Competencies and Minimum Training Standards for Public Safety Communications Manager / Director APCO ANS 3.109.2.2014
        - Sections 3.11.2, 3.11.3, 4.3.10
    - Core Competencies and Minimum Training Standards for Public Safety Communications Technicians APCO ANS 3.107.1.2015
        - Sections 3.11.2, 3.11.3

- It may further be helpful to define terms such as "broadband" and "NG9-1-1" in the glossary of each standard.

- Some standards may require more comprehensive modification. For example, the Standard for Public Safety Telecommunicators When Responding to Calls of Missing, Abducted and Sexually Exploited Children APCO ANS 1.101.3-2015 may require modification to include operational considerations for PSTs who have the capability to ask callers reporting child abductions to send recent photos or videos of the child that could then be sent to field responders.

Specific Recommendations

- Minimum Training Standards for Public Safety Telecommunicators APCO ANS 3.103.2.2015
    - Modify Section 4.2:
        - "4.2 General Knowledge of the Telecommunicator The following general areas of knowledge have been identified for the Telecommunicator regardless of their area of public safety expertise:
            - 4.2.1 An awareness of and respect for diverse populations,
            - 4.2.2 Comprehension of jurisdictional boundaries and geography,
            - 4.2.3 Proper application of Agency terminology,
            - 4.2.4 The ability to identify and properly utilize Agency resources, and
            - 4.2.5 Comprehension of their role in:
                - 4.2.5.1 Incident Command Systems (ICS),
                - 4.2.5.2 National Incident Management Systems (NIMS), including, but not limited to required training, Tactical Interoperable Communication Plan (TICP), and
                - 4.2.5.3 State or local emergency operations plans, and
                - 4.2.5.4 Use and development of emerging technologies."

- Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO) APCO ANS 3.101.2-2013
  - Chapter 3 – Organizational Integrity:
    - “3.15 The CTO shall demonstrate comprehension and application of the Agency’s confidentiality policies and rules regarding the discussion or release of information acquired in the workplace to the public, the media, or others. Such information should include, but is not limited to:
      - 3.15.1 Data systems accessible through local, state, or federal networks,
      - 3.15.2 Information contained in calls for service, including but not limited to information obtained through text, video, audio, or photographic messages to the PSAP,
      - 3.15.3 Information gained through the 9-1-1 or E9-1-1 system,
      - 3.15.4 Records Management Systems, and
      - 3.15.5 System security.”

- Minimum Training Standard for TTY/TDD Use in the Public Safety Communications Center APCO/NENA ANS 3.105.1-2015
  - Section 2.2.7:
    - “The Agency shall provide the Telecommunicator with practical instruction on identifying and processing TTY/TDD calls including:
      - 2.2.7.1 The importance of recognizing silent or open line TTY/TDD calls, and
      - 2.2.7.2 Using proper syntax, abbreviations, and protocol when responding to TTY/TDD,
      - 2.2.7.3 Recognizing when an individual who is communications impaired (i.e. deaf, deaf-blind, hard of hearing, or a person who has a speech disability) is using text-to-911 or text-to-TTY based on the language of the message or how the call is presented to the Telecommunicator.”
  - Section 2.2.12.4:
    - “The Agency shall evaluate the trainee on use TTY/TDD protocol, such as:
      - 2.2.12.4.1 Abbreviations,
      - 2.2.12.4.2 Etiquette, and
      - 2.2.12.4.3 Language,
      - 2.2.12.4.4 Recognizing when an individual who is communications impaired (i.e. deaf, deaf-blind, hard of hearing, or has a speech disability) is using text-to-911 or text-to-TTY based on the language of the message or how the call is presented to the Telecommunicator.”
  - Section 5.3:
    - “The Telecommunicator shall demonstrate the ability to receive, process and initiate calls of an emergency and non-emergency nature utilizing the agency’s primary and backup TTY equipment, detection equipment, telephony equipment, records management system, and other related tools or equipment all appropriate tools, equipment, and technology they may be expected to operate within the public safety communications center and/or training facilities.”
  - Chapter 7 – Core Competencies of the Telecommunicator
    - Section 7.3: “The Telecommunicator shall demonstrate the ability to process emergency and nonemergency calls for service for individuals who are communications impaired (i.e. deaf, deaf-blind, hard of hearing or have a speech disability or other disabilities).”
      - Add: “7.3.4 The Telecommunicator shall demonstrate the ability to communicate directly and indirectly with callers via all appropriate tools, equipment, and technology.”

Appendix 8. Training Courses from Other Sectors with Applicability to PSAPs

Standards and best practices related to IT, Fusion Centers, Real-Time Crime Centers, and Emergency Management are worth considering for PSAPs implementing broadband technology. The following is intended to be a non-exhaustive selection from each sector.

Information Technology

The FCC's TFOPA, particularly its cybersecurity working group, conducted a review of IT standards and best practices and made recommendations for the public safety community. Among other things, TFOPA reviewed the NIST Cybersecurity Framework, a voluntary framework of standards and best practices, and recommended implementation of appropriate elements to PSAP operations. Regardless of the approach a PSAP takes to managing IT challenges, employees will benefit from understanding IT basics so that they can have a productive collaboration. The following best practices and standards should be considered:

- PSAP employees should have at least a basic level of IT training, which may include awareness of a cybersecurity plan to protect data and lower the risk of cyber incidents.
- PSAPs should have a basic understanding of cyber hygiene, meaning steps computer users can take to improve cybersecurity and protect their systems and data. This includes:
  - Establishing strong passwords by using a combination of numbers, letters of varying sizes, and symbols,
  - Having a strong firewall,
  - Installing and consistently updating antivirus protection software,
  - Updating computers and programs regularly,
  - Physically securing laptops, cell phones, and other electronics,
  - Using encryption software,
  - Backing up data regularly,
  - Being wary of emails, instant messages, and downloads from the web,
  - Limiting and managing the number of people who have administrative privileges to change, bypass, or override security settings,
  - Limiting and monitoring any devices that physically or wirelessly connect to the system,
  - Reporting on IT issues and suspected cyber incidents at all levels, and
  - Regularly reviewing and updating policies and standards.

Real-Time Crime Centers

Real-Time Crime Centers (RTCCs) leverage a variety of data to prevent and respond to crime. This can include live video feeds, social media, 9-1-1 call information, incident mapping, historical data, license plate readers, arrest information, and other sources of information. While RTCC training information was not readily available, publicly-available material reveals the following best practices:

- Training will vary based on the complexity, breadth of technology, and data used/gathered by the RTCC, but given the complex nature of the tools used in a RTCC, training may require six to nine months.
- Training should address information sharing and storage policies, as well as legal requirements.
- Depending on the software, there could be an operational benefit to training even non-programmers in structured query language (SQL), a special-purpose programming language designed for managing data held in a database management system or for relational data stream management, to enable them to fully leverage the capabilities of the available systems.
- Field units may require education and training on the RTCC to make them aware of its capabilities and increase the likelihood of collaboration and use for field operations.

Fusion Centers

Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial, and private sector partners. The U.S. Department of Justice and Department of Homeland Security developed guidelines for developing and operating a fusion center within a state or region. These guidelines include several considerations for training that may be relevant to PSAP operations:

- Identifying training needs of center personnel.
- Providing specialized training, as appropriate.
- Providing training on the fusion center operations, NCISP, intelligence cycle, and the fusion process.
- Providing information collection training for fusion center participants.
- Providing training in tactical and strategic intelligence.
- Seeking accredited or standards-compliant training programs for government personnel.
- Utilizing private security entities for subject-matter training (e.g., cybersecurity).
- Emphasizing analysis and its link to intelligence-led policing.
- Developing materials and integrating outreach efforts.
- Adhering to other training mandates.
- Ensuring that personnel assigned to specific crime desks receive crime-specific training.
- Utilizing scenario-based training, simulations, games, and tabletop and field exercises.
- Participating in public safety and private sector tabletop, functional, and full-scale exercises.
- Participating in college- and university-sponsored intelligence and analyst training programs.

Emergency Management

The U.S. Department of Justice and Department of Homeland Security have issued “Considerations for Fusion Center and Emergency Operations Center Coordination,” which includes a list of training courses relevant to PSAPs.[102]

Note

[102] https://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf.

Appendix 9. Likely Impacts on Job Tasks Following Adoption of Broadband Technology

PSAPs will need a workforce capable of handling a wide range of calls for service, from "basic" 9-1-1 calls (e.g., voice-only) to calls containing incident-related pictures and video. The following describes the likely staffing impact with the adoption of broadband technology by comparing staffing considerations before and after broadband implementation. These charts are designed to reflect job tasks rather than specific job titles.

SMALL PSAP (1-15 employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Moderate
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Moderate
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Minor
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Minor
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Moderate
Dispatching: Management of First Responder Sensors	N	Y	Minor
Dispatching: Management of Interoperable Data	N	Y	Minor
Supervising: Support to Telecommunicators	Y	Y	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Moderate
Supervising: Coordination with Agency PIO on Data	Y	Y+	Moderate
Admin: Database and Table Maintenance	Y	Y+	Moderate
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Moderate
Admin: Creation of CAD Records for Release	Y	Y+	Moderate
Admin: SOP Documentation	Y	Y	Moderate
Admin: GIS Maintenance	Y	Y+	Moderate
Training: Length/Complexity for New Employees	Moderate	Extended	Moderate
Training: Length/Complexity for Recurring Training	Moderate	Extended	Moderate
IT: Equipment, Application, Network Management	Minor	Significant	Moderate
IT: Physical and Cybersecurity Management	N	Y	Moderate

KEY: Y = Yes; N = No; Y+ = Yes, but will increase

MEDIUM PSAP (16-75 employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Significant
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Moderate
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Moderate
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Moderate
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Moderate
Dispatching: Management of First Responder Sensors	N	Y	Moderate
Dispatching: Management of Interoperable Data	N	Y	Moderate
Supervising: Support to Telecommunicators	Y	Y+	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Moderate
Supervising: Coordination with Agency PIO on Data	Y	Y+	Moderate
Admin: Database and Table Maintenance	Y	Y+	Significant
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Significant
Admin: Creation of CAD Records for Release	Y	Y+	Significant
Admin: SOP Documentation	Y	Y	Moderate
Admin: GIS Maintenance	Y	Y+	Significant
Training: Length/Complexity for New Employees	Moderate	Extended	Significant
Training: Length/Complexity for Recurring Training	Moderate	Extended	Significant
IT: Equipment, Application, Network Management	Minor	Significant	Moderate
IT: Physical and Cybersecurity Management	N	Y	Moderate

KEY: Y = Yes; N = No; Y+ = Yes, but will increase

LARGE PSAP (76+ employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Significant
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Significant
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Significant
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Significant
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Significant
Dispatching: Management of First Responder Sensors	N	Y	Significant
Dispatching: Management of Interoperable Data	N	Y	Significant
Supervising: Support to Telecommunicators	Y	Y+	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Significant
Supervising: Coordination with Agency PIO on Data	Y	Y+	Significant
Admin: Database and Table Maintenance	Y	Y+	Significant
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Significant
Admin: Creation of CAD Records for Release	Y	Y+	Significant
Admin: SOP Documentation	Y	Y	Significant
Admin: GIS Maintenance	Y	Y+	Significant
Training: Length/Complexity for New Employees	Moderate	Extended	Significant
Training: Length/Complexity for Recurring Training	Moderate	Extended	Significant
IT: Equipment, Application, Network Management	Minor	Significant	Significant
IT: Physical and Cybersecurity Management	N	Y	Significant

KEY: Y = Yes; N = No; Y+ = Yes, but will increase

GLOSSARY

3GPP Third Generation Partnership Project. Unites seven telecommunications standards development organizations, known as “Organizational Partners” and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies.

ACN Automatic Crash Notification (aka Automatic Collision Notification). A system which enables an automated notification when a vehicle is involved in a severe crash. Such a system, for instance, may initiate a transmission when an airbag is deployed, or when an installed accelerometer detects an impact exceeding a given magnitude.

AED Automated External Defibrillator. A device that analyzes the heart rhythm in victims of sudden cardiac arrest and delivers an electrical shock to restore normal rhythm.

ALI Automatic Location Identification. The automatic display at the PSAP of the address/location of the device that called 9-1-1.

ANI Automatic Number Identification. The automatic display at the PSAP of the telephone number associated with the line that called 9-1-1.

ANS American National Standard. A standard that has been sponsored by an ANSI-accredited SDO and met ANSI’s Essential Requirements.

ANSI American National Standards Institute. A private, not-for-profit organization that oversees the creation, promulgation, and use of thousands of norms and guidelines that directly impact businesses in nearly every sector. ANSI facilitates the development of American National Standards by accrediting the procedures of SDOs. These groups work cooperatively to develop voluntary national consensus standards.

APCO Association of Public-Safety Communications Officials International. APCO is the world’s oldest and largest organization of public safety communications professionals. It serves the needs of public safety communications practitioners worldwide - and the welfare of the general public as a whole - by providing complete expertise, professional development, technical assistance, advocacy, and outreach.

API Application Programming Interface. A set of routines, protocols, and tools for building software applications.

ASAP Automated Secure Alarm Protocol. A national program for processing information from alarm monitoring stations to PSAPs. The protocol was founded through the joint partnership of APCO, the Monitoring Association, and the National Law Enforcement Telecommunications System.

ATIS Alliance for Telecommunications Industry Solutions. A forum where information and communications technology companies convene to find solutions to their most pressing shared challenges. ATIS is accredited by ANSI and is the North American Organizational Partner for 3GPP.

AV Audio Visual. Used as a generic term for the audio and video components and capabilities in any system.

AVL Automatic Vehicle Location. A system for automatically determining and transmitting the geographic location of a vehicle.

BCF Border Control Function. Provides security filtering of all types of transactions with an ESInet. There may be several BCFs to support all ingress and egress points of an ESInet.

CAD Computer Aided Dispatch. A computer-based system that assists PSTs with activities such as call input, dispatching, call status maintenance, event notes, field unit status and tracking, and call resolution and disposition.

CAMA Centralized Automated Message Accounting. A type of analog transmission protocol that transmits a telephone number via multi-frequency encoding.

CIO Chief Information Officer. An executive-level position focused on overseeing the people, processes, and technologies within an IT department in order to support the department goals.

CISM Critical Incident Stress Management. An adaptive, short-term psychological aid process that can include pre-incident preparedness, acute crisis management, and post-crisis follow-up.

CISO Chief Information Security Officer. The senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

CPE Customer Premise Equipment. Enables the delivery of a voice-generated request for assistance from a 9-1-1 caller to a PST.

CPR Cardiopulmonary Resuscitation. An emergency procedure that combines chest compressions with artificial ventilation in an effort to manually preserve intact brain function until further measures are taken to restore spontaneous blood circulation and breathing in a person who is in cardiac arrest.

CTO Chief Technology Officer. An executive-level position focused on technological issues within an organization.

DDoS Distributed Denial of Service. A cyber-attack whereby multiple systems are used to flood a targeted server with traffic in an attempt to overwhelm its resources (bandwidth, memory, processing power, etc.), making it unavailable to respond to legitimate users.

DHS Department of Homeland Security. A federal agency designed to protect the United States against threats. Its wide-ranging duties include aviation security, border control, emergency response, and cybersecurity.

DHS NCCIC DHS National Cybersecurity Communications Integration Center. A 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

E9-1-1 Enhanced 9-1-1. A system that enables the delivery of a caller’s phone number and location information to the PSAP receiving the call.

EC3 Emergency Communications Cybersecurity Center. In the proposed NG9-1-1 cybersecurity architecture, the EC3 would provide IDPS to PSAPs and any other emergency communications services that would benefit from utilizing centralized, core cybersecurity services.

ECC Emergency Communications Center. A facility with capabilities that include intelligence collection and monitoring, 9-1-1 multimedia traffic processing, full scale dispatch, and incident command capabilities.

ECRF Emergency Call Routing Function. A component of an NG9-1-1 system that accurately routes 9-1-1 calls to the appropriate PSAP based on the caller's location.

EIDD Emergency Incident Data Document. Provides a standardized, vendor-neutral NIEM conformant (XML-based) specification for exchanging emergency incident information to agencies and regions that implement NG9-1-1 and IP-based emergency communications systems. Emergency incident information exchanges supported by the EIDD include exchanges between disparate manufacturers' systems located within one or more public safety agencies and with other incident stakeholders.

EMD Emergency Medical Dispatch. A systematic program of handling medical calls. Trained PSTs, using locally approved guide cards, quickly and properly determine the nature and priority of the call, dispatch the appropriate response, then give the caller instructions to help treat the patient until the responding EMS unit arrives.

EMS Emergency Medical Services. A type of emergency service dedicated to providing out-of-hospital acute medical care, transport to definitive care, and other medical transport to patients with illnesses and injuries which prevent the patient from transporting themselves.

ENUM Proposed Standard RFC 2916 from the IETF for a domain name system-based method for mapping telephone numbers to URLs. This protocol will assist in the convergence of the PSTN and the IP network; it is the mapping of a telephone number from the PSTN to Internet services — telephone number in, URL out. ENUM was developed as a solution to the question of how to find services on the Internet using only a telephone number, and how telephones, which have an input mechanism limited to twelve keys on a keypad, can be used to access Internet services.

EOC Emergency Operations Center. A central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management functions at a strategic level during an emergency, and ensuring the continuity of operation of a company, political subdivision, or other organization.

ESInet Emergency Services IP Network. An IP-based network used for emergency communications.

ESN Emergency Service Number. A designation that identifies the appropriate PSAP to receive the call as well as the responding emergency service agencies based on the caller's geographic location.

ESRP Emergency Service Routing Proxy. A functional element that selects the next hop routing within the ESInet based on location and policy.

FCC Federal Communications Commission. Regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories. An independent U.S. government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications laws and regulations.

FEMA

Federal Emergency Management Agency. A federal agency with the mission of supporting citizens and first responders to prepare for, protect against, respond to, recover from, and mitigate all hazards.

FOIA

Freedom of Information Act. A state or federal law that grants the public access to information possessed by government agencies. Typically, upon written request, agencies are required to release information unless it falls under an exemption.

FirstNet

First Responder Network Authority. The Middle Class Tax Relief and Job Creation Act of 2012 created FirstNet as an independent authority within the National Telecommunications and Information Administration to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety.

GIS

Geographic Information System. A system designed to capture, store, manipulate, analyze, manage, and display all kinds of spatial or geographical data.

GPS

Global Positioning System. A satellite-based global navigation system that transmits signals that are used for three-dimensional (latitude, longitude, and elevation) global navigation (position determination) and for the dissemination of precise time. GPS-derived position determination is based on the arrival times, at an appropriate receiver, of precisely-timed signals from satellites.

HAZMAT

Hazardous Material. A material (such as flammable or poisonous material) that would be a danger to life or to the environment if released without precautions.

HIPAA

Health Insurance Portability and Accountability Act. A federal law that, among other things, requires the protection and confidential handling of protected health information.

HSS

Home Subscriber Server. This server manages authentication to support IMS network entities.

ICAM

Identity, Credential, and Access Management. Represents the intersection of digital identities, credentials, and access control into one comprehensive approach.

ICS

Incident Command System. A standardized on-scene incident management concept designed specifically to allow responders to adopt an integrated organizational structure equal to the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries.

I-CSCF

Intermediate-Call Session Control Function. Used for exchanging messages between IMS and external IP networks.

IDPS

Intrusion Detection and Prevention System. A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

IEEE

Institute of Electrical and Electronics Engineers. A non-profit, global association of professionals working toward the development, implementation, and maintenance of technology-centered products and services.

IETF

Internet Engineering Task Force. One of the task forces (with more than 40 working groups) of the Internet Architecture Board, responsible for solving short-term engineering needs of the Internet.

IJIS

Integrated Justice Information System. A computer network, system, or architecture that allows entities to electronically access and share information between systems and across jurisdictional lines.

IMS	IP Multimedia Subsystem. An architectural framework for delivering IP multimedia services.
IoT	Internet of Things. Refers to the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.
IP	Internet Protocol. A standard protocol designed for use in interconnected systems of packet-switched computer communication networks.
IPAWS	Integrated Public Alert and Warning System. Established by Presidential Executive Order 13407, IPAWS is an integrated alerts system that allows the President to send a message to the American people quickly and simultaneously through multiple communications pathways. IPAWS is also available to federal, state, local, territorial, and tribal government officials as a way to alert the public via the Emergency Alert System, Wireless Emergency Alerts, NOAA Weather Radio and other National Weather Service dissemination channels, the Internet, existing unique warning systems, and emerging distribution technologies.
IT	Information Technology. The study or use of computers for storing, retrieving, and sending information.
ITU	International Telecommunication Union. A specialized agency of the United Nations that is responsible for issues that concern information and communication technologies.
LATA	Local Access Transport Areas. A term in the U.S. for a geographic area covered by one or more local telephone companies, which are legally referred to as local exchange carriers.
LMR	Land Mobile Radio. A wireless communications system intended for use by terrestrial users in vehicles (mobiles) or on foot (portables).
LNG	Legacy Network Gateways. An NG9-1-1 functional element that provides an interface between a non-IP originating network and a next generation core services enabled network.
LSRG	Legacy Selective Router Gateway. Provides an interface between a 9-1-1 selective router and an ESInet, enabling calls to be routed and/or transferred between legacy and next generation networks.
LTE	Long Term Evolution. An international standard for high-speed wireless communication for mobile phones and data terminals developed by 3GPP.
LZ	Landing Zone. An area where aircraft can land.
M2M	Machine-to-Machine. A broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.
MAYDAY	An emergency procedure term used as a distress signal in voice radio communications.
MDT/C	Mobile Data Terminal/Computer. A computerized device used in emergency vehicles, such as police cars, to communicate with a PSAP. They are also used to display mapping and information relevant to the tasks and actions performed by the vehicle such as CAD drawings, diagrams, and safety information.
MOU	Memorandum of Understanding. A formal agreement between two or more parties. Companies, organizations, and governmental entities can use MOUs to establish official partnerships.

MPC Mobile Positioning Center. A functional entity that provides an interface between the wireless originating network and the emergency services network. The MPC retrieves, forwards, stores, and controls position data within the location services network.

MSAG Master Street Address Guide. A database of street names and house number ranges within their associated communities defining Emergency Service Zones and their associated ESNs to enable proper routing of 9-1-1 calls.

MS-ISAC Multi-State Information Sharing and Analysis Center. A focal point for cyber threat protection, response, and recovery for the nation's state, local, tribal and territorial governments.

NCC National Coordinating Center for Communications. A component of DHS that continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes.

NCISP National Criminal Intelligence Sharing Plan. An intelligence-sharing initiative that links the computer databases of local, state, regional, and tribal law enforcement agencies with those of the federal government.

NENA National Emergency Number Association. An organization whose mission is to work with 9-1-1 professionals nationwide, public policy leaders, emergency services and telecommunications industry partners, like-minded public safety associations, and other stakeholder groups to develop and carry out critical programs and initiatives, to facilitate the creation of an IP-based Next Generation 9-1-1 system, and to establish industry leading standards, training, and certifications.

NG9-1-1 Next Generation 9-1-1. 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.

NGCS Next Generation Core Services. The base set of services needed to process a 9-1-1 call on an ESInet.

NIEM National Information Exchange Model. An XML-based information exchange framework for sharing data between communities of interest.

NIMS National Incident Management System. A systematic, proactive approach to guide departments and agencies at all levels of government and the private sector to work together seamlessly and manage incidents involving all threats and hazards - regardless of cause, size, location, or complexity - in order to reduce loss of life, property, and harm to the environment.

NIST National Institute of Standards and Technology. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST is a non-regulatory federal agency within the U.S. Department of Commerce.

NPSBN Nationwide Public Safety Broadband Network. A nationwide wireless data network dedicated to public safety.

OSP Originating Service Provider. A communications provider that allows its users or subscribers to originate 9-1-1 voice or non-voice messages from the public to the 9-1-1 authority.

OTT Over the Top. OTT generally refers to applications that operate on IP-based mobile data networks and that consumers can typically install on data-capable mobile devices.

PCRF Policy and Charging Rules Function. This element is responsible for managing resources for end users based upon end user role and application requirements.

P-CSCF Proxy-Call Session Control Function. The first contact point for user equipment within the IMS core network.

PII Personally Identifiable Information. Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PIO Public Information Officer. The communications coordinator or spokesperson of certain governmental organizations (i.e. city, county, school district, state government, and police/fire departments).

PSAP Public Safety Answering Point. A facility equipped and staffed to receive emergency and non-emergency public safety calls for service via telephone and other communication devices. Emergency calls for service are answered, assessed, classified, and prioritized.

PSCR Public Safety Communications Research. Located within NIST, PSCR provides research, development, testing, and evaluation to foster nationwide communications interoperability.

PST Public Safety Telecommunicator. An individual employed by a public safety agency as the first of the first responders whose primary responsibility is to receive, process, transmit, and/or dispatch emergency and non-emergency calls for service for law enforcement, fire, emergency medical, and other public safety services via telephone, radio, and other communication devices.

PSTN Public Switched Telephone Network. The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.

QA/QI Quality Assurance/Quality Improvement. Actions taken to ensure that standards and procedures are adhered to and that delivered products or services meet performance requirements.

QoS Quality of Service. A measurement of latency, packet loss, and jitter in data transmission.

RFP Request for Proposal. A document that solicits proposals, often made through a bidding process, by an agency or company interested in procurement of a commodity, service, or valuable asset, to potential suppliers to submit business proposals.

RMS Records Management System. A system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files.

RTCC Real Time Crime Center. A centralized technology center that leverages a variety of data to prevent and respond to crime. This can include live video feeds, social media, 9-1-1 call information, incident mapping, historical data, license plate readers, arrest information, and other sources of information.

SBC Session Border Control. A functional element regularly deployed in VoIP networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

S-CSCF Serving-Call Session Control Function. The element in the IMS core network that handles the session states.

SDO Standards Development Organization. An entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users.

SGW Signaling Gateway. A network component responsible for transferring signaling messages between nodes that communicate using different protocols and transports.

SIP Session Initiation Protocol. A communications protocol for signaling, for the purpose of controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, private IP telephone systems, as well as instant messaging over IP networks.

SMS Short Message Service. A service that allows the user to send and receive short (maximum 160-character) messages independently of voice calls.

SOP Standard Operating Procedure. Written procedure prescribed for repetitive use as a practice, in accordance with agreed upon specifications aimed at obtaining a desired outcome.

SS7 Signaling System Number 7. A set of protocols used to provide basic routing information, call set-up, and other call termination functions.

SSH Secure Shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SSP System Service Provider. Provides systems and support necessary to enable 9-1-1 calling for one or more PSAPs in a specific geographic area. It is typically, but not always, an Incumbent Local Exchange Carrier.

TAS Telephony Application Server. Manages advanced call features. These features include services such as conference bridging, voice mail, call forwarding, and other telephony features.

TCP Transmission Control Protocol. A communications protocol used to connect to an external database, perform a query of the database, and retrieve information.

TDoS Telephony Denial of Service. A flood of unwanted, malicious voice calls designed to disable the telephone system of a target entity.

TFOPA Task Force on Optimal PSAP Architecture. An FCC task force that provided findings and recommendations regarding actions that PSAPs can take to optimize their security, operations, and funding as they migrate to NG9-1-1, including approaches for PSAP cybersecurity, NG9-1-1 architecture implementation, and NG9-1-1 resource allocations.

TICP Tactical Interoperable Communication Plan. A tool used for incidents and planned events that is intended to document the interoperable communications resources available within the county.

TTY/TDD Teletypewriter / Telecommunications Device for the Deaf. A machine that uses typed input and output, usually with a visual text display, to enable individuals with hearing or speech impairments to communicate over a telecommunications network.

UAV Unmanned Aerial Vehicle. An aircraft piloted by remote control or onboard computers.

UN HAZMAT United Nations Hazardous Material Number. Commonly used for materials in commerce and can be found on shipping papers.

VoIP Voice over Internet Protocol. Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks. Communication services that originate or terminate via IP networks rather than the circuit-switched PSTN.

VPC VoIP Positioning Center. The element that provides routing information to support the routing of VoIP emergency calls, and cooperates in delivering location information to the PSAP over the existing ALI database infrastructure.

VEDS Vehicular Emergency Data Set. A uniform data set for the transmission and collection of advanced automatic collision notification data.

VPN Virtual Private Network. A method employing encryption to provide secure access to a remote computer over the Internet.

XML eXtensible Markup Language. A trimmed specification or version of the Standard Generalized Markup Language that allows web developers to create customized tags for additional functionality.

ABOUT APCO

APCO International is the world's oldest and largest organization of public safety communications professionals and supports the largest U.S. membership base of any public safety association. It serves the needs of public safety communications practitioners worldwide – and the welfare of the general public as a whole – by providing complete expertise, professional development, technical assistance, advocacy and outreach.

APCO International
351 N. Williamson Blvd.
Daytona Beach, FL 32114

www.apcop43.org