Whitepaper: Harnessing the NPSBN and NG911

WHAT'S INSIDE

This whitepaper discusses the range of technical impacts PSAPs will need to address in order to fully leverage the enormous capabilities of the Next Generation 911 (NG911) and Nationwide Public Safety Broadband Network (NPSBN) platforms.

The Technical Evolution of the PSAP in a NG911 and FirstNet Environment

Background

The Federal Bureau of Investigation (FBI) reports that 4,091 bank robberies occurred in the United States in 2015. In the future, after the nationwide public safety broadband network (NPSBN)—which is being implemented under the auspices of the First Responder Network Authority (FirstNet)—and Next Generation 911 (NG911) systems are implemented, the manner in which public safety answering points (PSAPs), aka 911 centers, respond to such events will be dramatically different.

Today, the PSAP might receive an alert from the bank's alarm system and a 911 voice call—assuming it was safe for the teller to trip the alarm and the patron to place the call. Even if the call is placed, the amount of information that is provided to the telecommunicator likely will be severely limited, in large measure because the patron will want to end the call quickly given the danger of being discovered by the perpetrators.

It is expected that, sometime in the future, the number of data inputs that stream into a PSAP will increase significantly, largely driven by the fact that both the NPSBN and NG911 systems are Internet Protocol (IP)-based and broadband-enabled.

A Hypothetical Example of the New Emergency Response

The following is a *hypothetical* example of how such an event might play out after these vital communications platforms are operational:

- The bank's alarm system is tripped, which puts into motion several events. One involves triggering a protocol that results in real-time video streams from the bank's internal surveillance system and the city's fixed surveillance system flowing into the PSAP; this video is pushed out to law enforcement officers within a geofenced area surrounding the bank's location, so that they can see what is happening both inside and outside the bank.
- The alarm also prompts the PSAP to leverage the geofencing capability and social media to push out alerts to citizens advising them to stay out of the area until further notice; various social media platforms also are monitored to gain additional situational awareness.
- In addition, the alarm triggers a protocol that prompts the telecommunicator to utilize the traffic-light-control system to turn all stoplights red within the geofenced area around the bank, effectively locking

MissionCriticalPartners

down the area to prevent vehicular traffic from entering—in turn keeping citizens out of harm's way and clearing a path for emergency vehicles.

- Multiple patrons send text messages to 911, and several of them transmit video or images; in some, the perpetrators are clearly visible and the telecommunicator engages facial-recognition software to identify them.
- A patrol car equipped with an automatic license plate reader (ALPR) system receives a hit on a stolen car parked outside the bank; this information is relayed to the telecommunicator.
- The city's gunshot-alerting system informs the telecommunicator that shots have been fired inside the bank.
- The telecommunicator dispatches the appropriate emergency response, which includes patrol officers, SWAT, hostage negotiators and a helicopter that hovers over the bank and live streams additional video into the PSAP.

The data inputs described above will raise situational awareness in the PSAP to levels that were unimaginable only a short time ago given the limitations of today's public safety communications systems—such is the power of the NPSBN and NG911, particularly if they are converged, which will be essential if data is to flow between them seamlessly. However, much work needs to be done by the nation's 911 centers if they want to harness the full potential of these networks.

Technical Impacts PSAPs will Need to Overcome

Technical Impact 1: Interface Development

The technical impacts on the PSAP that will spin out of the implementation of the NPSBN and NG911 systems are considerable. The first concerns establishing the interfaces that will be needed to allow the myriad data streams to flow into the 911 center and then to enable telecommunicators to interact with them. While these interfaces are crucial—they provide the translation necessary for disparate systems to communicate with each other—developing them is not particularly complicated, and a burgeoning marketplace of application developers exists that can be tapped for this purpose; some toil for vendors that long have served the public safety community, while others work for third-party entities.

The more-critical consideration is that a great many interfaces will be needed. Some will connect the PSAP directly to data-generating systems, such as the city's video surveillance system or the bank's alarm system. Others will be machine-to-machine based; an example is the interconnection between the bank's alarm system and the geofencing solution, as well as the traffic-light-control system, which in the above scenario automatically changed signals to red when the alarm was triggered. Some of these interfaces will reside within the PSAP, while others will be hosted in cloud-based solutions.

A consideration as critical as the sheer volume of interfaces that will be needed is that they all need to be based on open, non-proprietary standards to ensure interoperability; if they are not, none of these systems will be able to communicate with each other, which will strip them of their utility.

Technical Impact 2: Data Analytics

Another key technical impact concerns managing the tsunami of data that will flow into the 911 center. No human is capable of simultaneously juggling the number of data streams that will be generated when a major incident occurs, whether it is a bank robbery, multivehicle pileup on the freeway or terrorist bombing. Consequently, PSAPs will need to deploy one or

---

Enabling and managing it all

New data systems will deliver new and different capabilities for emergency response. Some opportunities we see in a NG911/NPSBN environment:

- Real-time video streams
- State-of-the-art surveillance systems
- Geofencing
- Video communication with first responders
- Social media alerts and monitoring
- Traffic-light-control systems
- Text-to-911; Video-to-911
- Facial recognition software
- Automatic license plate reader (ALPR) systems
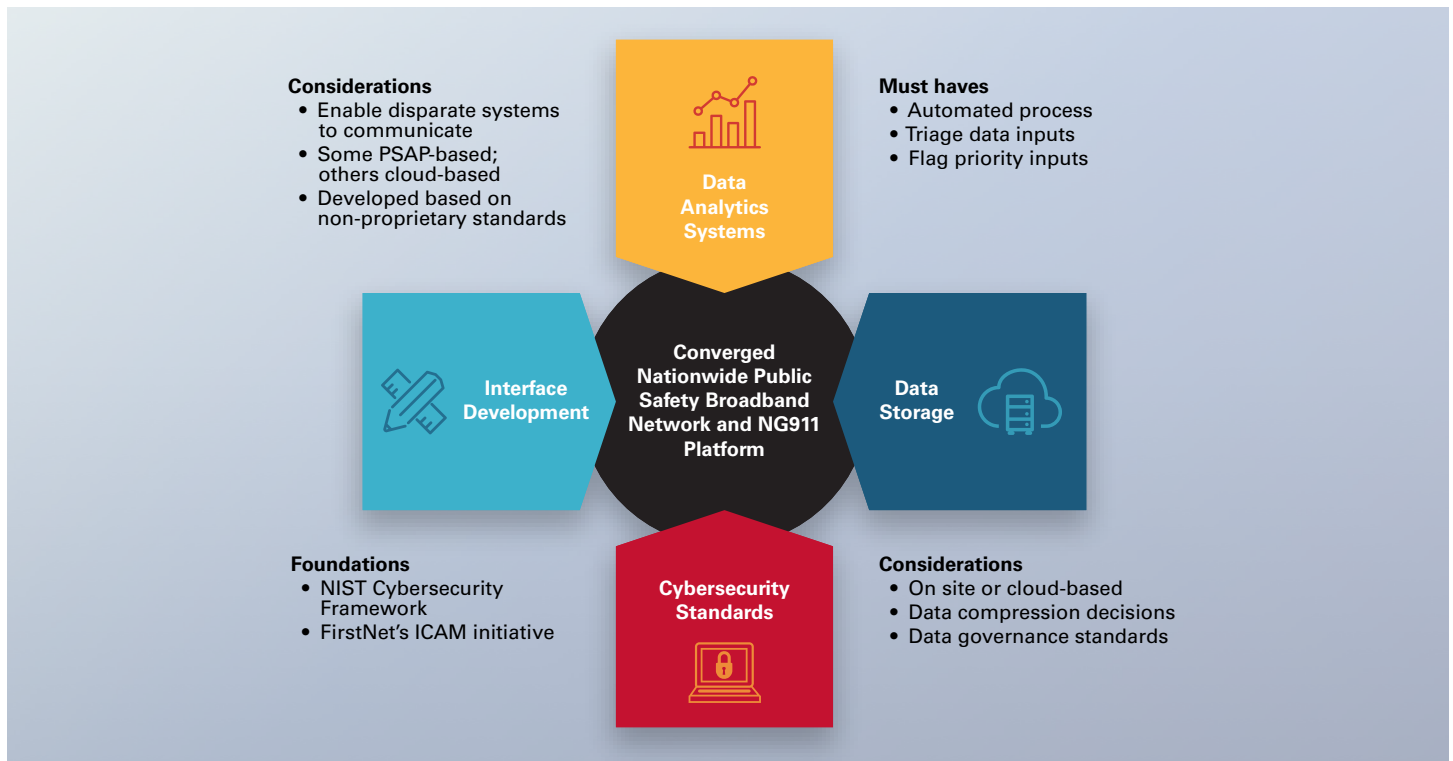- Gunshot-alerting systems

MissionCriticalPartners

Considerations
- Enable disparate systems to communicate
- Some PSAP-based; others cloud-based
- Developed based on non-proprietary standards

Data Analytics Systems

Must haves
- Automated process
- Triage data inputs
- Flag priority inputs

Interface Development

Converged Nationwide Public Safety Broadband Network and NG911 Platform

Data Storage

Foundations
- NIST Cybersecurity Framework
- FirstNet's ICAM initiative

Cybersecurity Standards

Considerations
- On site or cloud-based
- Data compression decisions
- Data governance standards

Figure 1: The technological evolution of the PSAP

more data-analytics solutions to automate the process of triaging the data inputs and then flagging for the telecommunicator those that are most relevant and require their attention. Along such lines, researchers at the Massachusetts Institute of Technology's Lincoln Lab—in a joint project with the New Jersey Office of Homeland Security and Preparedness—are working on a video-analytics platform that is designed to identify persons of interest based on certain physical attributes, such as their apparel. Such solutions will be integral to ensuring that the NPSBN and NG911 reach their full potential, because without them telecommunicators quickly will become overwhelmed by the amount of data that flows through them into the PSAP.

Technical Impact 3: On-Site or Cloud-Based Data Storage
Thought also must be given to storing and securing the data. Regarding storage, the key question involves whether the storage will be accomplished onsite or in the cloud, though decisions also will need to be made concerning the type of data compression that is used, which in the case of video could have a bearing on whether the data will be court-admissible.

Technical Impact 4: Cybersecurity Risks
It is critical that any data that flows into and out of the PSAP is secure. This is particularly true of any information that might be subject to the provisions of the Health Insurance Portability and Accountability Act (HIPAA), for instance, video and images of wounds suffered by the victim of a traffic accident captured by first responders and/or citizens and transmitted to the PSAP. The National Institute of Science and Technology's *NIST Cybersecurity Framework* provides an excellent resource to get PSAPs started. Another option is the Identity, Credential and Access Management (ICAM) initiative that is being developed for the NPSBN; ICAM considers technology, governance, and best practices for managing access to secure networks and data. It seems logical that FirstNet and the 911 community would take similar, if not identical, approaches to cybersecurity.

MissionCriticalPartners

Preparing for the data flood that will ensue once the NPSBN and NG911 are converged needs to begin now, if only to plan, because these will be time-consuming endeavors. They also will be costly, which is why it is imperative that Congress provides financial support, as it did when it enacted the Middle Class Tax Relief and Jobs Creation Act of 2012. This legislation not only created FirstNet, but also provided $7 billion in seed money for implementation of the NPSBN.

The 911 community needs similar support, not only to implement NG911 from coast to coast, but also to deploy the technology that PSAPs will need to take full advantage of this breakthrough. 911 funding is a huge issue—there simply is not enough of it. Due to the lack of funding, many PSAPs today are struggling to provide basic services and to keep their legacy systems operational. Ergo, it is unthinkable that they would be able to find the resources necessary to accomplish the initiatives described in this whitepaper without the support of the federal government. Earlier this year, Senators Amy Klobuchar (D-Minn.) and Bill Nelson (D-Fla.) introduced legislation that seeks to make NG911 implementation a national priority— providing meaningful funding would be a leap in the right direction.

Conclusion

The data streams made possible by the NPSBN and NG911 will provide PSAPs with unprecedented situational awareness that will make telecommunicators and first responders more effective. But to fully leverage this capability, PSAPs will need to address a variety of technical impacts, from interfacing with myriad data-generating systems to managing, storing and securing the data. Their ability to do so will depend largely on the level of financial support the 911 community receives from the federal government.

About Mission Critical Partners

Mission Critical Partners is a professional services firm that helps clients enhance and evolve their public safety systems and operations through extensive experience, knowledge and resources. By providing insight and support every step of the way, our clients are able to transform their mission critical operations, maximize the value of their investments and ensure optimal performance and success.

For more information, visit **MissionCriticalPartners.com**

MissionCriticalPartners