Whitepaper: ESInet Deployment

WHAT'S INSIDE

This whitepaper examines the advantages and disadvantages of three approaches to provisioning an emergency services Internet protocol network—which not only provides the foundation of a Next Generation 911 system, but also performs other important functions.

Unlocking the Power of the ESInet

Background

Next Generation 911 (NG911) systems represent a quantum leap forward for the public-safety community and the citizens that it serves. Internet Protocol (IP)-based and broadband-enabled, such systems are capable of considerably more than legacy 911 systems—which is why many emergency communications centers (ECCs) from coast to coast are clamoring to implement them.

KEY CONSIDERATIONS

NG911 BENEFITS

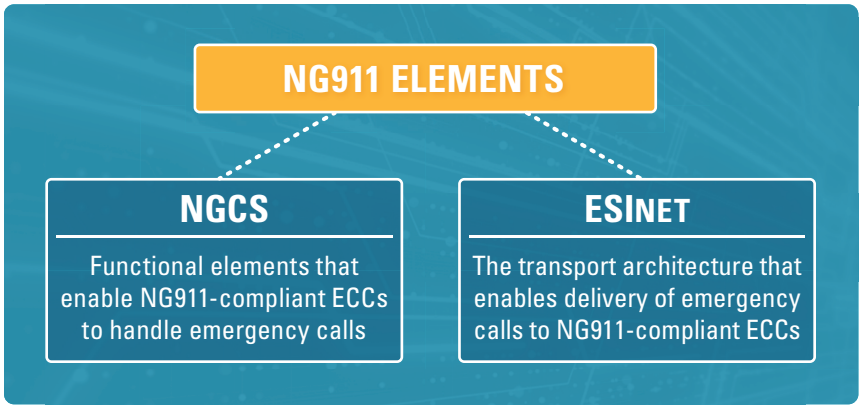
- More actionable data
- More accurate caller location information
- Less misrouted 911 calls
- Faster 911 call transfers with data intact

The broadband capabilities of NG911 systems enable large volumes of data to reach ECCs for the first time, because legacy 911 systems traditionally have been voice-centric, with very modest data capabilities. Moreover, NG911 systems enable transmission of high-bandwidth files, such as video and building floorplans. When this enormous volume of data is analyzed and contextualized effectively, it becomes actionable. In that form the data dramatically enhances situational awareness, which in turn enables emergency responders to do their jobs more effectively and keeps them safer, resulting in more lives and property saved. In addition, there is a great need in today's emergency response environment to share data between NG911 systems and with other broadband networks, for example public safety broadband networks being implemented by the First Responder Network Authority (FirstNet) and others.

Moreover, NG911 systems rely upon geospatial data generated by geographic information systems (GIS) to route 911 calls to the appropriate ECC. This is a huge improvement because geospatial data is much more accurate than the information contained in the legacy automatic location identification (ALI) and master street address guide (MSAG) databases. This dramatically reduces the number of misdirected 911 calls. Even when calls are misdirected, an NG911 system can transfer them to the correct ECC much faster than legacy 911 systems—and with the call information intact, which is something that legacy systems often cannot do.

MissionCriticalPartners

In the legacy environment, a telecommunicator who receives a transferred 911 call often must contact the sending ECC to receive the call information verbally or reacquire information from the calling party—in contrast, in an NG911 environment, the receiving ECC would receive the transferred call and its relevant information directly into its call-handling system and possibly even its computer-aided dispatch (CAD) system. The former approach introduces the possibility of error, and it takes seconds, sometimes minutes, for the call information to be captured by the ECC that received the misdirected call—if it can be captured at all. Both are bad outcomes in a scenario when lives are on the line and every second matters.



An NG911 system consists of two essential elements: next generation core services (NGCS) and one or more emergency services IP networks, or ESInets. The former are the functional elements that enable emergency calls to be handled by a NG911-compliant ECC. The latter provides the transport architecture required to deliver calls in an NG911 environment. Three ways exist to implement an ESInet: contract with a commercial entity, such as a telecommunications service provider, to provision the network; self-provision it, which means that the network users would own, operate and maintain the network; or leverage a hybrid approach.

This whitepaper explores the advantages and disadvantages of these very different approaches.

Commercially Provisioned ESInets

Traditionally, public-safety agencies have provisioned their 911 systems by contracting with commercial entities. In the legacy environment this often meant their incumbent local exchange carrier (ILEC), if the ILEC also provided the agency's selective router; if it didn't, then the agency contracted with the selective-router provider that had contracted with the ILEC for circuits delivery. There are several reasons for this. First and foremost, the agency doesn't have to worry about implementing the system or maintaining it—it is a "one-stop shop, set it and forget it" scenario. In addition, commercial carriers already have miles of fiber-optic cable embedded to support their own communications networks.

KEY CONSIDERATIONS

COMMERCIALLY PROVISIONED ESINETS

- One-stop shop, "set it and forget it" ownership model
- Bandwidth capacity might be inadequate
- Bandwidth scalability and flexibility might be issues
- Strong service-level agreements with provider are needed
- Agency has little control over ESInet's hardware, software and fiber
- Lack of visibility into the ESInet

Two ways exist to implement an ESInet: Contract with a commercial entity or self-provision.

MissionCriticalPartners

In this scenario, the commercial entity controls all aspects of the network: hardware, software and connectivity, which nearly always is fiber-optic cable given the broadband requirements of NG911 systems. The fiber either is owned by the carrier or leased from other commercial entities.

A few challenges exist when provisioning an ESInet via a commercial entity. In an NG911 environment, bandwidth-intensive multimedia files likely will traverse the network. Consequently, one of the biggest challenges concerns the amount of bandwidth that is available to the agency. Moreover, a public-safety agency's communications needs evolve over time, which means that the bandwidth available to its NG911 system needs to be scalable and flexible. Many commercial carriers are adept at scalability and flexibility. They might allow agencies to dynamically adjust their bandwidth via an online customer portal, though restrictions often apply. They also might offer a sliding scale pertaining to the cost of the additional bandwidth; often the per-megabit cost will decrease in proportion to the amount of additional bandwidth being used.

Other carriers are less adept at scalability and flexibility, which makes provisioning additional bandwidth more challenging and complex. In such circumstances, the agency might need to renegotiate its services agreement with the carrier. Sometimes the carrier will lack the network infrastructure needed to meet the agency's bandwidth request. In some cases, the agency might be able to address this by leasing dark fiber from independent third-party providers; but doing so would require the agency to "light" the fiber. This requires the agency to implement, operate and maintain necessary hardware—e.g., routers, switches—which carries with it a certain amount of cost.

Another challenge is that any agency that has contracted with a commercial entity for its ESInet will have very little control over the network—hardware, software and fiber—if any. This includes network monitoring and troubleshooting. Commercial entities generally are focused solely on one question—is the network operating? If it's not, the commercial entity will resolve the issue, of course, but the critical question concerns how long that will take. The 911 systems operated by public-safety agencies are mission-critical, meaning that they must be operational continuously, because lives are on the line. While commercial entities typically monitor their networks via automated processes, the concern is whether its network monitoring center (NOC) and security monitoring center (SOC)—which will handle any cybersecurity-related issues—are robust enough to address promptly any alerts that the monitoring systems generate.

A corollary concern is the lack of visibility into the ESInet when the network is provisioned via a commercial entity. This visibility is essential to identifying the root cause of the problem, which in turn enables preventive measures to be taken to ensure that the problem doesn't occur again. Often, issues are lurking beneath the surface that could explode into a service-affecting problem. Consequently, agencies should consider hiring a third-party entity to monitor independently the network and all systems that connect to it—e.g., CAD, call-handling equipment (CHE) and land mobile radio (LMR)—as well as the interfaces that connect the network to those systems, to achieve the requisite visibility that the commercial entity likely is not providing.

Finally, it is imperative that the agency negotiates strong service level agreements (SLAs) into its contract with the commercial entity. The SLAs need to be airtight; they need to define how the commercial entity will respond to various scenarios; and—perhaps most importantly—they need to define how the commercial entity will be held accountable for its response. However, it should be acknowledged that it often is difficult to get commercial carriers to perform according to the SLA's terms, even when those documents are airtight; moreover, getting them to do so can take weeks, months, even years of badgering, which is a tremendous drain of resources.

The biggest advantage to self-provisioning is that it gives the agency complete control over the network—and thus its destiny.

MissionCriticalPartners

Self-Provisioned ESInets

Another way to implement an ESInet is for the agency to assume responsibility for all aspects, i.e., financing, hardware and software deployment, governance, operation and maintenance, and network monitoring and troubleshooting. The biggest advantage to this approach is that it gives the agency complete control over the network—and thus its destiny.

For example, if the agency needs more bandwidth for its ESInet, and it is leasing its fiber connectivity, then it simply instructs the fiber provider to expand the service (at increased cost, of course). In the case of a dark-fiber network, the agency can increase the bandwidth on its own by upgrading the network interface cards (NICs) or increasing their number.

KEY CONSIDERATIONS

SELF-PROVISIONED ESINETS

- Ideal for regional networks, enabling resource and cost sharing
- Agency has complete control over network hardware, software and fiber
- Agency controls network monitoring, troubleshooting and security postures
- Network can support other applications such as CAD, CHE, and LMR to generate economies of scale and enhanced capabilities
- Requires strong IT management and assets, including cybersecurity
- Strong governance is a must, especially for regional networks

Also in this scenario, the agency can set up its network-monitoring and -troubleshooting posture in any manner it chooses to ensure that the root causes of problems are identified. Doing so gives the agency a better chance of discovering and resolving issues and, better still, preventing them from occurring.

Moreover, by assuming control over the network, the agency more easily can ensure that it receives desired solutions that might not be available from commercial entities. The agency will be able to select network hardware and software, transmission media—dark and/or lit/leased fiber, or microwave and/or T1 circuits in underserved areas—and managed services, all based on its unique wants and needs. The agency can procure each of these individually to achieve the most cost-effective solution, and can leverage other procurements—such as ESInet applications, e.g., CAD, CHE, LMR—to achieve desired efficiencies.

Often, implementing an ESInet that is agency-controlled makes it easier to do so regionally or statewide. Such arrangements enable the numerous agencies that will share the network to also share in its implementation and ongoing care. It makes even more sense if the entities are able to leverage the ESInet to share applications that are not being shared currently.

A common misconception is that ESInets solely transport NG911-related data traffic generated by emergency calls, such as the data generated by a CAD system. In reality, if the ESInet is properly designed and implemented, it can perform myriad additional functions—for example, it can be used to backhaul radio traffic from the tower sites to the LMR system core, and to interconnect multiple agencies in a region. This latter capability enables the regional sharing of systems, e.g., CAD, CHE and LMR, which creates economies of scale and often results in enhanced capabilities, especially for smaller agencies that typically lack the resources of larger agencies. It should be noted, however, that any regional ESInet implementation would require strong governance, to ensure that all user needs are met, as well as equitable sharing of costs and operations/maintenance responsibilities.

In some cases, a hybrid approach to ESInet deployment makes sense, especially as a means of avoiding network outages.

MissionCriticalPartners

Yet another tradeoff concerns the information technology (IT) assets that the agency possesses. Effective network monitoring and troubleshooting—as well as cybersecurity-related mitigation and prevention—require a considerable amount of IT acumen, and many agencies lack such acumen. An ESInet is an IP-based network and such networks are particularly prone to cyberattacks—and such attacks against government entities, including public-safety entities, are exploding in number and increasing in sophistication, thus requiring an equally sophisticated cybersecurity posture. Here too a regional approach would be beneficial, because it enables multiple agencies in the region to pool their resources to do the job.

Another aspect that demands contemplation concerns what happens in the aftermath of a network outage that results in a significant injury or even loss of life, for example if the 911 system is unavailable, even for a short time period. Commercial carriers have ample experience in mitigating wrongful death lawsuits. While such a possibility should not deter an agency from pursuing an ESInet that it owns wholly or in concert with other regional entities, it is something that should be well-contemplated by the appropriate legal team(s) before a decision to procure the network is made.

The Hybrid ESInet

In some cases, a hybrid approach to ESInet deployment makes sense, especially as a means of avoiding network outages. We know of one state, for example, that transports 911 traffic into ECCs over a network path provided by the commercial carrier and over a path provided by the state-level ESInet. The dual-path approach is designed to provide network diversity, resiliency and redundancy. Of course, this could be achieved simply by provisioning both network paths from the commercial carrier. But leveraging a state-level ESInet offers two big advantages.

KEY CONSIDERATIONS

HYBRID ESINETS

- Ideal for state-level networks
- Greatest opportunity for network diversity, resiliency and redundancy because of dual-path approach
- Opportunity to enhance bandwidth capacity compared with commercially provisioned ESInet
- Reduced cost compared with commercially provisioned ESInet

One involves cost—an agency that leverages a state-level ESInet typically will be able to do so at a cost that is less expensive—often far less expensive—than what the agency would pay if provisioning that path from the commercial carrier. The second involves bandwidth—a state-level ESInet typically is a much bigger pipe. So, an agency not only can transport much more data over that path, in many cases—where allowed by the relevant procurement laws and policies—it also can transport data generated by myriad other systems. Again, think CAD, LMR and even logging/recording systems.

Conducting a needs assessment is one of the first things to do when deciding whether to contract with a commercial entity to deploy an ESInet or to build your own. If the latter option is selected, then the network will need to be designed with scalability in mind, and strategies developed for governing, monitoring, maintaining and securing the network once it is operational. If the former is selected, a contract will need to be negotiated with the commercial entity that not only includes strong SLAs, but also gives the agency as much control as possible over its destiny.

Conducting a needs assessment is one of the first things to do when deciding whether to contract with a commercial entity to deploy an ESInet or to build your own.

Regardless of the road taken, a request for proposals will need to be crafted, including technical specifications, and governance will need to be developed, including policies and standard procedures for operating and maintaining the network, as well as allowing agencies to connect to it. SLAs will need to be developed, vendor proposals will need to be evaluated and scored, and contracts will need to be negotiated.

Regardless of the road taken, a request for proposals will need to be crafted and governance will need to be developed.

Conclusion

An emergency services IP network, or ESInet, is a critical component of a Next Generation 911 system, as well as the entire public-safety ecosystem. Implementing such a network can take two very different paths, and each has unique advantages and disadvantages. The path an agency chooses will depend heavily on its financial and information technology resources, whether it can coalesce regional support, and the level of commitment it can and is willing to lend to the project.

Mission Critical Partners
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.8.MCP.911 or 888.862.7911
Fax: 814.217.6807

March 2021 | Doc # NTWKSWP030521

MissionCriticalPartners