RESPONDING TO THE CALL FOR NEXT GENERATION 9-1-1

A white paper from FE/Kimball

Responding to the Call for Next Generation 9-1-1

GETTING INTO THE GAME

Initiating your plans for a Next Generation 9-1-1 (NG9-1-1) system is much like sitting down at a chessboard halfway through the match. Some of the pieces are available to you; others may be inaccessible because of challenges like budget or technology. Approaches taken by industry peers may be unclear, and the direction you must pursue may be vague. Your tendency may be to make the best of the pieces available to you and hope that you can somehow still achieve NG9-1-1's goal of "any call, anywhere, anytime."

A chess master understands, however, that above all else you must develop a concise strategy. You must be certain of the role assigned to every piece and maintain a view of the entire board. You can't afford simply to concentrate on one or two of the components, because all the pieces in your NG9-1-1 plan must work comprehensively for a successful implementation.

THE VALUE OF NG9-1-1

NG9-1-1 systems operate through Emergency Service IP Networks (ESInets) and are designed to dramatically shorten the time required to identify a caller's exact location. These systems can pinpoint calls from a wide variety of technologies, ranging from text messages to computers and photos.

Operating on an IP-enabled network, NG9-1-1 will permit calls to be easily transferred within networks and among regional networks in a state. The bandwidth of the network is, for all practical purposes, unlimited. It can be shared for all services, allowing interoperable communications and converged applications for all public safety departments in regions that are part of the IP backbone. When agencies converge many applications into a single communications link, they minimize the potential points of failure and reduce duplication of technology. In NG9-1-1 operations, servers handle the core functions, with the caller's location arriving with the call. The inherent flexibility, efficiency capacity and speed of NG9-1-1 can allow public safety agencies to achieve their "any call, anywhere, anytime" goal, but only if each aspect of the overall system has been appropriately considered.

Attaining a highly functional, reliable NG9-1-1 system, however, requires much more than the network and the technology within it. It begins with a vision for how highly intelligent applications, hardware and systems will enable emergency communications in new ways and in virtually all

HIGHLIGHTS

Every 9-1-1 center will should develop an NG9-1-1 strategy that has a unique starting point. From wherever you start, you must take a holistic look at all components of the strategy.

circumstances, and a look at the entire "game board" and its potential.

Each community in America is developing a NG9-1-1 strategy from their own unique starting point. Some are more advanced technologically; others have done a better job of establishing governance bodies and policies in anticipation of their move to NG9-1-1. From wherever you begin, as any good chess player is aware, you must take a holistic look at the positions of the pieces in the game and develop a strategy for all to work together. Neglecting any one piece can defeat an otherwise sound strategy. Strategizing with the resources at hand and calling on reinforcements from the community of public safety telecommunications experts, you can help ensure that your move toward NG9-1-1 will achieve your goals.

NINE PIECES, ONE OBJECTIVE

Whatever stage of development your NG9-1-1 network is in today, the pieces in play must assume nine specific roles in a comprehensive approach, as illustrated in Figure 1, the NG9-1-1 transition.

Figure 1
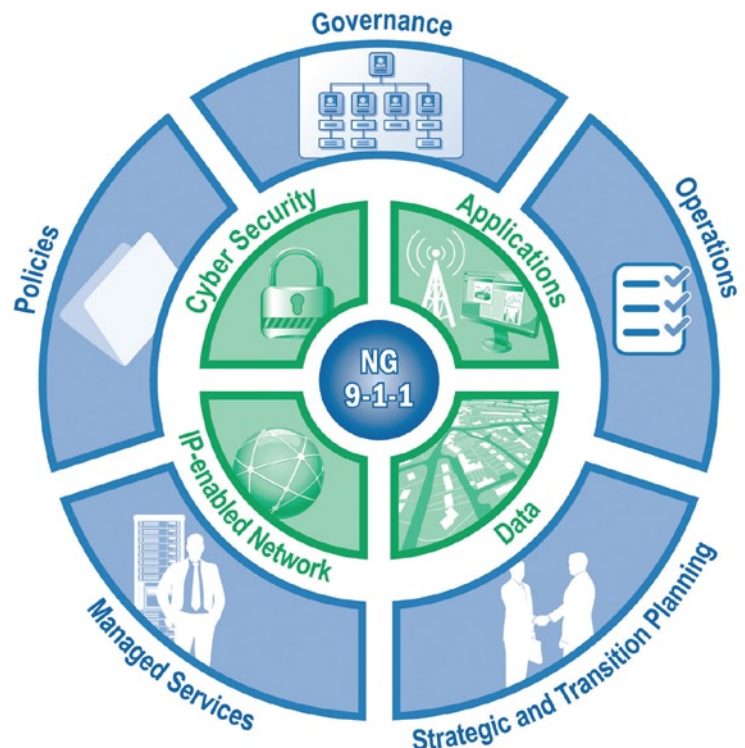
HIGHLIGHTS

The key elements in the NG9-1-1 transition include:
1.) an IP-enabled network
2.) data
3.) applications
4.) cyber security
5.) policies
6.) governance
7.) operations
8.) future roadmapping and planning
9.) managed services

From a technology standpoint, contained in the inner circle of the diagram, NG9-1-1 demands an integrated approach that incorporates four key elements:

- An IP-enabled broadband network
- Data to store and manage location information in new, more effective ways
- Applications that enable both traditional and advanced multimedia 9-1-1 services
- A foundation of cyber security hardware and software measures to protect the network from being checkmated by malicious opponents or accidentally taken down by users.

Surrounding the technology should be five operational components:

- Policies on how the network is to be used and not used, how applications are to be introduced and rolled out, and how the network will comply with government regulations.
- Governance procedures agreed upon by representatives of all stakeholders sharing the network
- Operations aligned with state regulations, which may need to be revised to accommodate NG9-1-1
- A roadmap for strategically planning and transitioning to NG9-1-1 systems
- Managed services that may be required for selecting and evaluating software, filling staffing needs maintaining network security and other purposes

Decisions on how to position each of these pieces may require coordinated efforts with telecommunications experts. For example, Greater Harris County, Texas, which includes the Houston area, initiated plans to build an NG9-1-1 network that integrated PSAPs for 48 cities and two counties into a single NG9-1-1 IP backbone. It relied on FE/Kimball to write the RFP for systems, gather and evaluate the responses, and negotiate with the chosen vendor. FE/Kimball then performed similar roles for creation of a fully redundant microwave network to back up the Internet-based system. When the Michigan State Police wanted to migrate from a fixed, landline-based system to NG9-1-1, FE/Kimball conducted a statewide feasibility study and assessed options from technical, operational, economic, policy and political standpoints to recommend the best strategy for the agency.

With careful consideration of your next moves, each of the pieces begins to assume a critical role in your holistic strategy for achieving NG9-1-1, both in technical and operational arenas.

HIGHLIGHTS

Calls from today's 21st century communications devices, such a mobile phones, struggle through analog systems routed through wireline carriers and their CAMA trunks.

## TAKING THE RIGHT STEPS WITH TECHNOLOGY

The IP-Enabled Network

Current enhanced 9-1-1 systems are served by analog CAMA (Centralized Automatic Message Accounting) circuits (trunks), which pull identification information on callers from the telephone company's billing database. The data is updated when service activity relating to individual phone numbers occurs. The functionality of these analog CAMA trunks and the reliability of the identification data is limited. Information about callers often resides in very low speed automatic location identification (ALI) databases operating through serial RS232, a standard for transporting data that was created in 1962 for electromechanical devices. Calls from today's 21st century communication devices, such as mobile phones, still must struggle through these analog systems, routed through wireline carriers and their CAMA trunks. Even voice-over-IP and calls from vehicle-based systems like OnStar must navigate through the landline carrier's selective router to the public safety answering point (PSAP).

A Secure, Resilient and Redundant IP-Enabled Network with 99.999 Percent Uptime

To begin on the path toward NG9-1-1, most PSAPs install an IP-enabled network among sites, regionally and statewide. 99.999 percent uptime should be guaranteed through a secure network with resiliency and redundancy. Standards from the National Emergency Number Association (NENA) direct that IP-enabled networks should not completely mirror the peer-to-peer connectivity that the Internet provides. NG9-1-1 is to operate in an IP-system with clearly defined redundancy and resiliency that meets service levels required for the delivery of 9-1-1 information. Service levels on most peer-to-peer networks do not meet these criteria. For example, calls received in one PSAP that should be routed to another county are sent up to an ESInet and then directed back down to the proper PSAP for response. This methodology ensures that PSAPs using hardware or software from different vendors can still communicate, using the ESInet to relay calls nearly instantaneously.

The broadband IP backbone is simply the first step toward NG9-1-1.

Without making further changes, calls may still ingress to the IP-network from gateways that terminate existing analog-technology CAMA trunks and that convert the call to some sort of IP technology. CAMA trunks use multi-frequency tones to perform signaling, such as the transfer of the calling party's phone number. CAMA signaling is slow and very limited in what information can be transmitted, compared to modern all-digital signaling technologies.
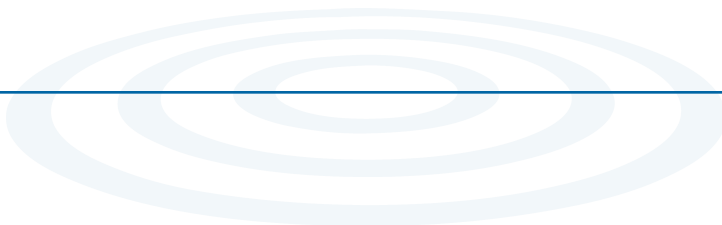
HIGHLIGHTS

Real world experience with IP-enabled networks and other all-digital signaling networks has shown call setup reductions of nearly half or more.

While CAMA trunks may carry over digital facilities, unless the CAMA signaling is converted to some other digital signaling method, the CAMA signaling technology and the time required to signal, is identical to CAMA trunks carried on analog facilities.

As PSAP migrate to newer equipment that can accept 9-1-1 calls in an IP-format, CAMA signaling conversion needs to occur only at IP-network ingress points where CAMA signaling is the only format available. If a digital signaling format is available at the IP-network ingress point then CAMA signaling can be eliminated entirely, at least for those calls terminating to an IP-capable PSAP.

As a result, only some additional functions are added at this stage of network development. PSAPs on the ESInet, are now able to share GIS mapping information and updates, as well as computer-aided dispatch information once the IP connections have been established. The IP network also offers a path if the public safety departments want to integrate radio into the new backbone. It would enable a PSAP damaged by a tornado, for instance, to transfer calls to another PSAP to dispatch responders.

Very long call setup times, especially for wireless 9-1-1 calls, are fairly common in traditional 9-1-1 systems that contain multiple CAMA signaling segments. This can cause issues because most 9-1-1 callers dial 9-1-1 infrequently and therefore do not expect the long interval time that could elapse before they hear a ring-back signal or before the dispatcher answers. Eliminating or reducing CAMA signaling segments in the call path can significantly improve call setup times. Real-world experience with IP-enabled and other all-digital signaling networks has shown call setup interval reductions of one half, or more.

The Questions to Ask about IP Networks

Among the questions agencies should consider when planning the installation of an IP-enabled network are these:

- Who will install and maintain the IP lines?
- Who will host the system? Should it be co-located at a carrier's facility to be managed?
- How will the network be configured? Who will manage the firewalls and routers—existing staff or outsourced experts?
- What functions will be placed on the IP network and what will be the resulting demands for bandwidth allocations? Will mapping or radio integration be integrated into the network before the region goes to full NG9-1-1?
- Who should share a full NG9-1-1 network?

HIGHLIGHTS

With NG9-1-1, GIS plays a much larger role than in traditional 9-1-1 systems and is used to route calls to the proper emergency response agency.

- How will you ensure that PSAP traffic always maintains top priority in the network when it is shared among agencies? How will you establish a separate, secure prioritized network for 9-1-1 calls?

Data

The IP network is an enabler for all the basic and advanced features of NG9-1-1. Among the most important of these functions are the storage, maintenance and retrieval of data that allows a caller to be identified quickly. In the current traditional 9-1-1 systems, geographic information system (GIS) data comes into play at the dispatcher's end of an emergency call. When a 9-1-1 call reaches a dispatcher, it is associated with an address or coordinates. The information is then plotted on a map in the computer-aided dispatch system to assist the dispatcher in locating the caller.

With NG9-1-1, GIS data comes into play at the front end and is used to route calls to the proper emergency response agency. Calls are routed through the state or regional ESInet to the most appropriate PSAP, police, fire or ambulance service. In this situation, location information—a street address or latitude/longitude coordinates—comes along with the call from the very beginning. Such a system resolves problems posed today by the many new technologies of mobile devices from which a 9-1-1 call can originate.

The latest standards require each telephone company, Internet service provider and local service provider to store customer location information in its own location information server (LIS). Customer addresses are pre-validated against a location validation function so that their accuracy is assured when customers initiate 9-1-1 calls. The location validation function accesses GIS datasets to perform the validation of customer address information.

GIS is the Heart of a NG9-1-1 System

With GIS at the heart of NG9-1-1's database, safety agencies need to review four key considerations to keep this data timely and accessible:

1. Accuracy. GIS uses road center lines, the addresses of buildings and jurisdictional boundaries as guides for deciding to which safety agency a call should be routed. Ensuring the accuracy of this information in the GIS database is crucial to prevent erroneous routing. Neighboring jurisdictions need to work together from the beginning to review boundaries to ensure that GIS mapping corresponds to on-the-ground locations.
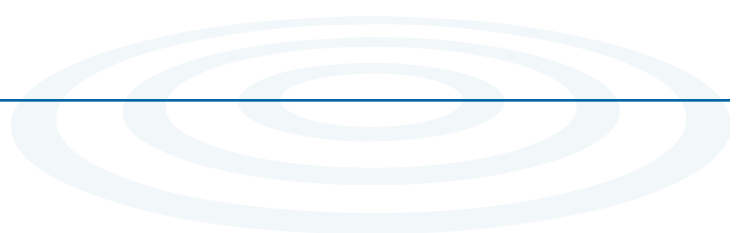
HIGHLIGHTS

Key data terminology for NG9-1-1:

ECRF: Emergency Call Routing Function

LoST: Location to Service

TranslationMSAG: Master Street Address Guide

LIS: Location Information Server

LVF: Location Validate Function

ALI: Automatic Location Identificaiton

2. Maintenance. Address information must be updated and maintained regularly at the local level and then be pushed up to an Emergency Call Routing Function (ECRF) database server in the ESInet. The ECRF, which stores precise location data, communicates with another server that uses Location to Service Translation (LoST) protocol to determine the best route for the call, based on the location of the calling device. If the address information is not up to date, the whole routing process can degrade.

3. Standards. In an NG9-1-1 network, data is likely to be received from a large number of agencies, PSAPs, counties and other jurisdictions that all operate within the same ESInet. This data must be standardized so it can be integrated into the ECRF. For example, NENA requires the name of a street such as "West Main Street" to be stored in three separate fields: "W," "Main" and "St.", with "W" being the pre-directional, "Main" being the street name and "St" being the street suffix or type. If a local agency stores it as "West Main" and "Street," the ECRF may not recognize its meaning as it is not adhering to the expected standards for addressing. Information must be entered consistently in all the database fields.

4. Policy and governance. Each jurisdiction must examine their policies on maintenance, workflow and assignment of new addresses and ensure that staff members who update GIS data are following those policies. Decisions need to be made in policy documents regarding how frequently information is updated and who is responsible for carrying out this task. In some smaller communities, addresses might be assigned within a planning department without GIS, and the street names and addresses are not integrated within the datasets of surrounding areas that have complete GIS addressing. These smaller communities can work with surrounding jurisdictions to develop policies and procedures to hand off the address-assignment responsibility to a neighboring or overarching jurisdiction, such as a county or council of government that has the GIS capabilities for a NG9-1-1 environment and can provide the necessary data requirements to an ECRF.

With detailed location information now stored in the databases for the ECRF and Location Validation Funciton (LVF), traditional ALI systems and the master street address guide (MSAG) can be decommissioned. Calls arriving at a PSAP no longer need to dip into the ALI database to find a customer's name, address and community, send it to the MSAG

HIGHLIGHTS

The major data difference in an NG9-1-1 environment is that calls no longer need to dip into an ALI database to find a customer's name, address and community. Instead, they are pre-validated against GIS data using a location validation function.

and find the emergency service number for the right response unit. Instead customer records are pre-validated against the GIS data using LVF, and 9-1-1 calls come in with an address or coordinate attached to them and the GIS data in the ECRF ensures that the call is routed to the most appropriate responder.

Synchronizing the ALI, MSAG and GIS Data

Currently, local public safety agencies are in a variety of stages for development of an NG9-1-1 database. Most have GIS data, but in different phases of development. For example, they may have road center lines, but no data maintenance plan in place or they may not have the appropriate jurisdictional boundary data nor the individual structure point address point data that can provide detailed address location information. It's important for local jurisdictions to ensure that addresses are verified in a comprehensive manner.

As an initial step for communities, FE/Kimball recommends comparing their GIS data with their ALI and MSAG databases and identifying discrepancies. FE/Kimball can provide a roadmap for assembling the data—synchronizing it, creating address points and working with surrounding jurisdictions to update boundary maps.

NENA's goal is to elevate data to a 98 percent accuracy level. Working with GIS and data management experts, communities should put together a complete maintenance plan and policies to reach this goal. They should also adopt GIS software tools to help efficiently maintain data.

The importance of accurate data cannot be overstressed. With accurate information:

- Local agencies minimize risks of incorrectly routing responders
- The number of seconds to locate the scene of an emergency may be reduced, which in the 9-1-1 environment even a few seconds can help save a life or property
- The dispatcher can gain a good ground reference of the surroundings to see topological or structural barriers to responders

Applications

As a digital network with greatly increased capacity, NG9-1-1 presents the opportunity for deploying many applications that are not possible with current analog networks.

Ultimately, NG9-1-1 will enable video, photos, text messages and a variety of other communications to analyze emergency situations and promote a speedy response. Emergency centers can use photos and video to obtain better situational awareness, seeing situations in real

HIGHLIGHTS

Far greater application flexibility will be possible with NG9-1-1 such as video-based calls from deaf residents, sensors, and common-operating-pictures across jurisdictions.

time. Camera-equipped phones at the sites of emergencies could be controlled by the 9-1-1 center, pulling in video of the scene. A location database also will align bank or street security cameras with the scene to provide a wider view to inform a fire truck or police cruiser, for example, of the best way to navigate to the scene. Video-based calls from deaf residents can be routed anywhere in the network to an operator who understands sign language or can conference in a sign-language expert as the call comes in.

Sensors can be used more extensively within emergency management. For example, river gauges can be tied into NG9-1-1. If river levels reach a certain height, the emergency operations center (EOC) can examine real-time information to determine whom to evacuate. EOC officers can even visualize the kind of flooding that is likely to occur by using 3D-elevation information in the GIS.

An EOC will be able to switch to any CAD position and view all current 9-1-1 calls on a map at the same time. A mobile command center 100 miles away can connect remotely with the EOC and view the same systems and data. In a disaster situation, PSAPs, neighboring safety departments, state agencies, FEMA, Homeland Security personnel, the National Guard and other agencies all can look at the same information and have a common operating picture to make decisions.

With such expansive potential in their NG9-1-1 systems, jurisdictions must be diligent in selecting the vendors that will supply the network and the applications that will be installed. Certifiedtechnology systems and applications must be evaluated and the right applications chosen to enable reception and sharing of wireline, text, mobile, VoIP, video, e-mail and other forms of messaging. For example, the State of Indiana deployed an IP-enabled network in 2007 to route and deliver all wireless 9-1-1 calls statewide. FE/Kimball assessed the network's feasibility prior to developing a strategic plan for the network and provided procurement assistance and implementation oversight. The network enabled all of Indiana's 167 9-1-1 centers to receive 9-1-1 calls originating from wireless phones. It provides faster call processing times as well as quicker data delivery of vital caller location data. The State was able to reduce connectivity points by greater than 90 percent, thereby significantly lowering costs and providing for complete redundancy and diversity. FE/Kimball is currently helping the State route Voice over Internet Protocol (VoIP) and other IP-device calls on the network to make the network NG9-1-1 capable.

HIGHLIGHTS

NG-SEC standards were released in early 2010 by the National Emergency Number Association. They help to reduce the risk of service interruptions that could threaten 9-1-1 call centers with viruses, denial of service attacks and hardware and software failures an other security issues.

Cyber Security

9-1-1 call centers have traditionally been isolated, stand-alone networks. With this configuration, these centers and their data have been fairly secure. NG9-1-1, however, interconnects PSAPs, local public safety departments, regional agencies and federal agencies using IP-enabled networks so that they can share information to provide a more effective response. The downside of such a network is that it can expose the agencies within it to more viruses, denial-of-service attacks, hardware and software failures, intrusions by malicious hackers, data loss and system downtime than previously. Furthermore, 9-1-1 systems are particularly attractive targets for hackers and others who seek publicity for bringing down a highly visible network.

Therefore, every NG9-1-1 effort must include a comprehensive cyber security component during planning and implementation to reduce the risk of service interruptions. In particular, NG9-1-1 planning efforts should plan for compliance with the National Emergency Number Association's (NENA) NG9-1-1 Security, or NG-SEC, Cyber Security standards which was released in early 2010. Recognizing the need for tightly securing NG9-1-1 networks and systems, FE/Kimball formed the nation's first unbiased, vendor-neutral cyber security consulting service for public safety departments. In fact, two FE/Kimball security experts co-chaired the NENA working group that developed the NG-SEC security standards for NG9-1-1 systems. The cyber security offerings cover a wide range of client needs including:

- Security readiness assessments
- Security audits
- NENA security for NG9-1-1 audits/planning
- Vulnerability assessments
- Penetration testing
- Security architecture planning and consulting
- VoIP security
- Security policies
- Security software and hardware selection and installation
- Staffing augmentation
- Managed security services

It's important to realize that security for 9-1-1 mission critical applications must be handled differently than that of standard computer systems, because
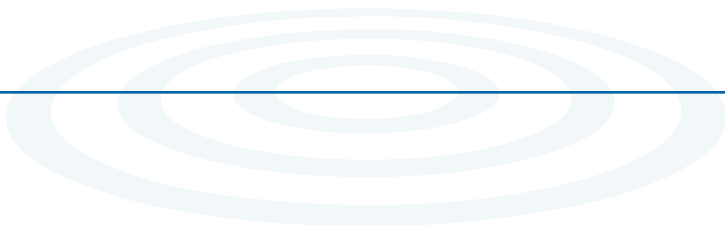
HIGHLIGHTS

Mission critical applications must be handled differently than those of standard computer systems when it comes to security because sporadic rebooting is not possible.

9-1-1 operations should avoid downtime during installations and upgrades. For example, rebooting sporadically during the installation of security patches is not tenable in 9-1-1 enviroment where it might be in a traditional commercial organization. Therefore it's important to ensure that cyber security experts understand 9-1-1 when implementing security countermeasures.

Determining Your Readiness for NG-SEC

For those undergoing NG9-1-1 planning an important first step is for agencies to conduct an NG9-1-1 security (NG-SEC) readiness assessment to determine gaps in their compliance capabilities and the additional measures they will need to take. Experts like those at FE/Kimball can advise agencies on appropriate budgeting for the new standards, how the standards might impact procurement and how to ensure that the right language is included in requests for proposal for NG9-1-1 systems. Similarly, vendors building products with NG9-1-1 capabilities should ensure those devices work and comply with the NG-SEC standards, and telecommunications providers need to recognize how these standards affect their contracts and support models.

Testing Your Network's Vulnerability

An integral part of any cyber security program is periodic vulnerability testing. A vulnerability assessment can help determine the degree of vulnerability of a 9-1-1 system and identify key areas to focus improvement efforts.

With advanced software tools and highly trained security experts, the process involves a thorough and comprehensive examination of networks and systems. The experts will plug specialized equipment into the network and conduct an unobtrusive scan. Weaknesses, vulnerabilities and areas that cyber criminals might try to exploit will be identified.

VoIP Security

Voice-over-IP phone networks introduce new threats to the voice communications. These threats are often similar to those experienced on traditional IP-enabled, networks. Of primary concern is dealing with a denial-of-service attack in an NG9-1-1 environment. Public safety agencies should develop a comprehensive plan for identifying and mitigating VoIP security risks in a manner consistent with overall cyber security plans and policies.

Security Policies

The security of a system depends equally on people, products and policies. Security policies are as crucial to an organization's safety as any piece of equipment or the personnel who use the system. A security policy documents specific goals and objectives for a security program, helps

HIGHLIGHTS

Some state's current legislation actually prohibits NG9-1-1 style operations. Before you begin the transition or define your governance structure, investigate this potential issue.

define the kinds of behaviors that are allowed and provides enforceability. For example, an acceptable-use policy specifies the kinds of activities that are permissible with an organization's computer systems and those that are not (like inappropriate use of the Internet, playing games, personal use of the computer while on duty, etc). Policies also can be used to provide clear requirements for how systems should be configured or hardened (network security policy) or furnish parameters for hiring practices and background checks. Experts can help the agency develop these policies, as well as build incident-response plans, business-continuity plans and policies for data classification, data backup, outsourcing, passwords, remote access and other actions.

MAKING THE RIGHT MOVES WITH OPERATIONAL CONSIDERATIONS

Policy, Governance and Operations

The issues surrounding policy, governance and operations are intertwined and are closely associated with the statutory and regulatory framework. Before an agency can establish policies, begin transitioning to NG9-1-1 or define a governance structure, some overriding questions must be addressed:

- **Is the state allowed to implement NG9-1-1?** In many instances, modifications to existing legislation will be required, because existing legislation may actually forbid NG9-1-1-style operations. For example, does the law allow a state or region to build an ESInet in the way it is defined nationally? NG9-1-1 is a service on a shared, multipurpose network; but state law may dictate that 9-1-1 networks must be single-purpose, closed systems and that only 9-1-1 calls can be transmitted on them. Statute may also provide that only the incumbent telephone company can provide 9-1-1 service. In these cases, an ESInet would be illegal and the statutes would need to be refreshed to permit a shared backbone.

- **How will NG9-1-1 be funded?** Traditional 9-1-1 systems are funded through a surcharge or tax on phone service. That fee applies only to 9-1-1 system components—such as the network, database and terminal equipment—and (typically) not to radio dispatch and other elements of an integrated NG9-1-1 network. In a shared ESInet for NG9-1-1, a number of stakeholders use the backbone, and a method must be developed to determine how each pays its fair share. Agreements and a governance structure must be set in place, and this can become a complicated matter.
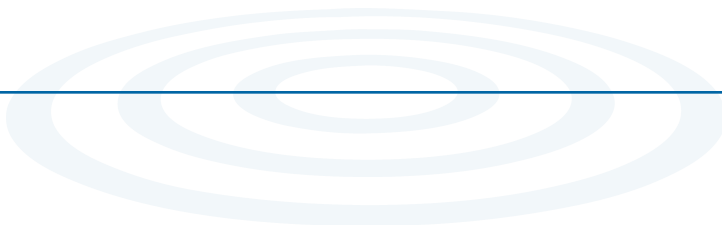
HIGHLIGHTS

The first step when organizing the operational structure of NG9-1-1 is looking at the legal and statutory framework with your state.

Therefore, the first step in organizing the operational structure of NG9-1-1 is to look at the legal and regulatory framework existing in each individual state. It's essential to understand the scope of authority that exists for those who operate 9-1-1 systems and what it needs to be to operate in an NG9-1-1 environment.

Regional or State ESInets

Because of the interconnected nature of NG9-1-1, it can't be administered on a county-by-county basis as previous 9-1-1 operations have been. PSAPs are no longer islands. While it is possible and in most instances desirable that multiple counties band together to form a regional ESInet and thereby leverage the economies of scale that NG9-1-1 makes possible, someone has to ensure that those regional ESInets are interconnected to provide seamless statewide and interstate coverage. That is best done at the state level. That requirement raises two more questions regarding governance:

- Is the state organized with a 9-1-1 authority at the state level?

- What is the scope of that entity's statutory responsibilities? If it has no authority to coordinate or implement NG9-1-1 or set and enforce standards, then there exists a serious barrier to compatible, interoperable NG9-1-1 communications.

Beyond the organization of an NG 9-1-1 structure, special attention must be directed toward confidentiality. The NG9-1-1 network carries calls, messages, documents and other data from multiple organizations. State legislation may define what information can and cannot be shared among safety agencies, made public or used outside the actual response to an emergency. Provisions relating to disclosure, data retention and confidentiality must be incorporated into policies and governance. Liability issues need to be addressed as well. The new provider ofNG9-1-1 service needs the same immunity that traditionally has been granted to telephone companies. If players with data vital to the NG9-1-1 network feel they are not protected from liability, they won't join the game.

Strategic and Transition Planning

Once a state-level authority is in place, with all the legal provisions it needs to build and direct an NG9-1-1 network, safety agencies can take the next step, toward strategic and transition planning. The agency should develop policies regarding the use and operation of the network and identify how it will roll out procurement of the necessary hardware, software and integration services. Will the agency handle this step with its own staff, or will it need expert advice from a managed-services organization?

HIGHLIGHTS

NG9-1-1 is increasing the demand for 24x7 managed services because of their increased technical complexity and more systems.

Some additional, basic questions remain to be resolved:

- How the system will be run? Will it be a statewide network, or will the state simply facilitate interconnections among regional systems?

- Will there be a geographical structure to the rollout?

- How will statewide coverage be achieved?

- Is a state-level entity in place to manage the NG9-1-1 system, or must a separate governance structure be created? State law may require a new layer of governance that includes individuals from the state, each region, responders and other stakeholders who share the backbone network.

- How will the agency ensure that 9-1-1traffic maintains top priority within the IP network if it is shared with other government functions?
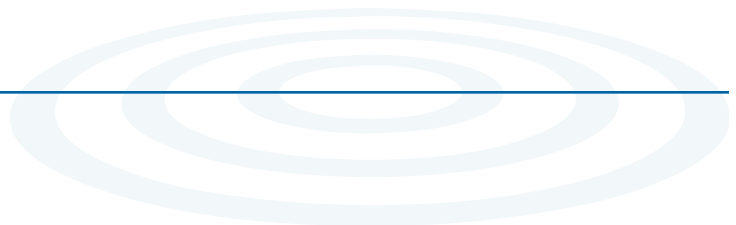
It's vital to get the planning process started early, with all stakeholders at the table, so the desired environment can be defined and it can be determined what governance structure is needed and what authority it needs to make effective decisions about these and other operational policies and procedures.

Managed Services

With the advent of NG9-1-1, the 24x7 managed (outsourced) services become especially important. This is primarily due to the increasing number of systems public safety agencies have to deal with, increased technical complexity, and reduced budgets/staffing. These factors intersect to create a definitive need for managed services in a NG9-1-1 environment. For NG9-1-1, managed services can include such tasks as:

- Network monitoring and maintenance

- Technical support for work stations and servers

- Providing a new breed of security services for telecommunications, including antivirus software, software updates, patch management, and backup and recovery of files

- Management of 911 authoritative databases, including scrubbing and updating GIS addressing data

Many PSAPs have small staff, with few fulltime IT or security personnel who can do all that is required from an NG9-1-1 technology standpoint. At the same time, budgets are shrinking while demands increase. Public safety agencies can save money and gain the insights of NG9-1-1

experts by outsourcing different aspects of their IT maintenance and support, security, or database management thereby allowing internal staff members can focus on their primary mission—answering and dispatching calls for assistance.

A managed services organization can provide other technology services, as well. For example, counties can host their Web sites on the servers of a company offering managed services. This option allows the county to avoid spending for servers, bandwidth, operating-system updates, new licensing and IT staff.

In considering a managed services firm, agencies should above all else review the company's experience and history in 9-1-1 development. Thru also should ensure that the provider offers a pricing model with maximum flexibility and minimum complexity.

For a fraction of the cost of employing staff to manage all these technology needs, a public safety agency can outsource them to a managed services organization and remain focused on lives instead of lines.

Conclusions

The next generation of 9-1-1 technology and operations will certainly revolutionize emergency services in the same way that the Internet transformed the operations of businesses, schools and governments. NG9-1-1 will improve the analysis of emergency situations, response times and response accuracy, thereby saving lives. While integrating all the aspects of this new environment may be complex, firms with a high level of 9-1-1 experience, such as FE/Kimball, are ready to offer guidance and assurance as regional and state agencies make their next moves in responding to the call for Next Generation 9-1-1.