Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
	)	
Framework for Next Generation 911 Deployment	)	PS Docket No. 10-255
	)	
	)	
	)	
	)	
	)	
	)	

COMMENTS OF L.R. KIMBALL

L.R. Kimball, a CDI Company, of Ebensburg, Pennsylvania hereby submits comments in response to the *Notice of Inquiry* adopted by the Commission on December 21, 2010, in the above captioned proceeding.

L.R. Kimball is one of the nation's largest engineering/architecture/consulting firms, annually ranked among the top 200 design firms and the top 20 telecommunications firms by Engineering News Record. L.R. Kimball's Communications Technology Division has offered public safety and mission critical consulting services for more than 15 years. Our telecommunications and technology practice is focused on all facets of public safety, supporting operations and technologies; 911 networking, call delivery and call handling; radio communications; cyber security; and public policy.

COMMENTS

L.R. Kimball commends the Commission on initiating this comprehensive proceeding to address how Next Generation 911 (NG911) can enable the public to obtain emergency assistance by means of advanced communications technologies beyond traditional voice-centric devices.

DISCUSSION

A. NG911 Capabilities and Applications

1. Potential Media Types in a NG911 Environment

There are many potential current and future media types that can be used for NG911. These media types should all be reviewed, before they are included, to see how each type will benefit a person in need and the PSAP and responders that help. The primary media type should remain real time two way communications between the user and the PSAP.

2. Primary vs. Secondary Usage of Media Types

The degree to which each of the media types discussed above will be used as a primary versus a secondary form of communication on NG911 networks

The primary media type should remain real-time-two way communications between the user and the PSAP. Of the media types discussed in subsection A.1 of the NOI, Potential Media Types in a NG911 Environment, those that should be considered as primary media include "message-based text" and "real-time text." Both delivery methods provide for primary communications between the sender and PSAP personnel. These methods of communication are widely accepted and are the most likely method of initial contact with a PSAP. These methods would provide the basic information that would support secondary methods with the provision of additional references to the original contact.

Additional methods of communication, including still images, real-time video, telemetry data and auxiliary medical and other personal data, should be considered secondary media. These communication methods would support the primary media with the additional information that could be utilized by the PSAP and emergency responders. E-mail and other social media should not be considered a primary media as an alternative to message-based text or real-time text as they do not provide for immediate interaction and could cause confusion and delay in providing emergency services.

What primary and secondary media types PSAPs and service providers will likely support?

PSAPs and service providers will likely support message-based text and real-time text as primary media. Still images and real-time video could be accepted as secondary media to support the primary. PSAPs should be expected to support all primary media, but should have discretion with regard to accepting secondary media. Secondary media information has the potential to overload a PSAP and each PSAP should have the prerogative to define its capabilities to process such information. Different standards should apply to primary media types than apply for secondary media types. Primary media should have the same functional requirements as other voice-based media currently in place.

Privacy issues related to the delivery of secondary non-conversational media should have the same requirements that are currently defined by federal and state laws and regulations. The extension of those requirements to secondary media may require changes to current laws, regulations and tariffs. PSAPs need specific policies in place before being authorized to receive secondary media information. Liability and privacy issues should be addressed by federal and state statutes. Secondary media information of a medical or personal nature, including telemetry data, should also be addressed by federal and state statute.

3. SMS for Emergency Communications

The popularity and ubiquity of SMS text messaging and the expectations of the public require that SMS text messages to 911 be given careful consideration. L.R. Kimball supports the development of a SMS to 911 solution. The 4G AMERICAS TEXTING TO 911 paper referenced in the NOI points out many of the technical problems associated with SMS to 911 service. However, many of those issues are a consequence of the selected point-of-interconnection (POI) between the SMS system and 911, namely, at the store-and-forward service. Selecting a different point of interconnection between the SMS system and 911 may permit many of these problems to be resolved, and, if implemented properly, should not seriously or significantly impact the operation of the existing SMS system.

By requirement and design, SMS must have a message store-and-forward function because the cellular telephone that is the destination of a given SMS message may not be reachable at any given moment. The message store-and-forward function holds the message until the destination becomes available (if it ever becomes available) within a timeout period. If the destination becomes available, the message is forwarded. As a consequence, the SMS system is not a real-time system, and is not a reliable message delivery system. Therefore, from the perspective of 4G Americas and other industry parties, SMS to 911 should not be attempted.

However, a PSAP is considered to be online at all times, and should always be reachable. Hence, a store-and-forward function need not exist between the SMS originator and the PSAP, provided a suitable POI can be found ahead of the store-and-forward function. Furthermore, if 911 SMS messages can be extracted from the system ahead of the store-and-forward server, they can be directed to a 911-specific service that can mitigate most of the issues with the store-and-forward function and provide the additional special features required to make SMS to 911 a viable service.

The flow of a SMS message from a handset to the store-and-forward function follows this path: The handset sends the message to the mobile switch via the radio link. The mobile switch sends the message to a SMS store-and-forward server or service via the telephone industry standard Signaling System 7 (SS7) network. In fact, it is the SS7 network itself that determines the “short” in Short Message Service (SMS). The SMS design includes a requirement that a SMS message must be wholly contained in a single SS7 packet. After overhead and protocol information is provided in the SS7 packet, only 160 characters remain for the message payload.

The SS7 network interconnects three basic types of nodes: Signaling Switching Points (SSPs), Signaling Transfer Points (STPs), and Signaling Control Points (SCPs). The SS7 network provides out-of-band call setup and signaling functions for the public switched telephone network (PSTN).

The SS7 network provides an effective and convenient POI for interconnecting SMS systems with a new 911-specific SMS service.   Mobile telephone switches (themselves SSPs on the SS7 network) are able to route calls to specific SS7 node addresses based on the dialed digit strings.   Alternatively, calls with certain common destination prefixes may be routed to a STP which in turn performs further forwarding of the call. At the very least, a mobile switch forwards all of its incoming SMS messages to a specific SS7 address associated with the SMS store-and-forward function, which itself is a SS7 SCP.

There are several possible mechanisms that can be used to separate SMS to 911 messages from normal SMS processing. The mobile switch may be able to direct all SMS messages dialed to 911 (and to other appropriate codes, such as 112) to a specific SCP, which could be a SMS to 911 service with functions described below.

Alternatively, if the mobile switch itself is not able to perform this 911 SMS routing function, at least one commercial vendor of STP products claims to be able to route SMS to 911 messages differently than non-911 messages in one of its STP products. This would enable them to direct SMS to 911 messages to the SMS to 911 SCP, while forwarding non-911 messages through the standard SMS processes.

With SMS to 911 messages separated from the SMS system, it becomes possible to implement a dedicated SMS to 911 SCP. This SCP can address most, or even all, of the technical objections to a SMS to 911 service and can do so without impacting the SMS store-and-forward functions that are in widespread use today.

The SMS to 911 SCP can perform functions such as:

- Gateway and protocol conversion functions from SS7 to NG911, including signaling and media conversion as described elsewhere.
- Assigning a “session identifier,” so that successive SMS messages (from the same phone) reach the same dispatcher via the NG911 network.
- Providing acknowledgement or negative delivery text messages back to the originator of the emergency text message. In this way, the originator is provided with feedback on whether the text message did, in fact, reach an emergency telecommunicator.
- Querying the wireless carrier’s position determining system in an attempt to locate the originator’s location.

L.R. Kimball believes that there are no insurmountable technical barriers to a SMS to 911 service, and that it is possible to implement such a service with negligible impact on existing infrastructure. The key is to make the SMS to 911 interconnection at the right point in the process, namely at the SS7 transport of the message out of the mobile switch.

Currently, there is no business or regulatory driver to implement a SMS to 911 interconnection. Implementation and maintenance would be an additional cost to carriers and there is no process in place to recoup those expenditures. There are currently no regulations in place to drive carriers to implement a SMS to 911 interconnection.

Just as legislation was required to implement cell phone location services from the carriers and mitigate the associated costs, a similar process may be required for the implementation of SMS to 911 interconnection services.

How the increasing use of SMS may impact emergency communications and whether NG911 networks should be configured to support SMS emergency communications.

Implementation of SMS to 911 service as described above will require adherence to standards. The NENA 08-003 i3 specification document (draft), which provides Session Initiation Protocol (SIP) location conveyance via the Presence Information Data Format – Location Objects (PDIF-LO) (Internet Engineering Task Force [IETF] RFC 4119 and related) and location-based Emergency Call Routing Functions (ECRF), including a Policy Routing Function (PRF), should provide adequate SMS routing capabilities. All that is required is that the SMS to 911 SCP deliver the call to the NG911 system using the NENA i3 protocols, including the location information obtained from the wireless Position Determining Element (PDE). This location is coded in the PIDF-LO format and embedded in the SIP headers as Multipurpose Internet Mail Extensions (MIME) attachments. This process is well-documented in IETF and NENA publications.

The media choice for text communication has been discussed elsewhere in this response. The maintenance of session continuity should be the responsibility of the SMS to 911 SCP or associated gateway device(s.) Once the SMS “session” enters the NG911 network, it should be in compliance with NG911 protocols and look identical to other possible text applications utilizing NG911.

It is clear that had SMS been designed from the outset with emergency communications in mind, the system would have features that would improve this method of emergency communication. These issues have been considered in the design of more advanced systems, including IP-based 4G systems. The proceedings of the Emergency Services Workshops,[1] among others, have fostered awareness of emergency communications requirements among Standards Developing Organizations (SDOs) and have improved the newer, emerging technologies, including NG911 itself.

SMS is in widespread use and the public has come to depend upon it. Since it will not disappear in the near future, SMS to 911 should be implemented effectively for the public good and welfare.

Existing and future public expectations related to the use of SMS for emergency communications

Implementation of SMS to 911 will likely require a combination of regulatory pressure and reasonable limits to liability for the wireless carriers and implementers. From a business perspective, there are few drivers for SMS to 911. Carriers may be reluctant to implement unless the competitive playing field is level, meaning the carrier's competitors must also implement. In the end, timely implementation of SMS to 911 will likely require Commission mandates, much like the implementation of wireless Phase II 911 service.

4. NG911 Applications for Persons with Disabilities and Special Needs

What media types and devices (e.g., text, video) persons with disabilities will likely use to make an emergency call in a NG911 environment?

[1] http://www.emergency-services-coordination.info/index.html

Deaf, hard-of-hearing, speech-impaired and other special needs persons and those who choose to use Real Time Text (RTT) should be supported with a Text over IP (ToIP) solution with the implementation of an IP-based NG911 infrastructure. This solution should adhere to the standards outlined in RFC 5194, Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP). These standards are compatible with Voice-over-IP (VoIP), Video-over-IP, and Multimedia-over-IP (MoIP) environments and support the needs of existing and future mainstream ToIP users. ToIP should be functionally equivalent to the services provided to individuals who do not have a disability.

Planning initiatives should include the eventual obsolescence of legacy technologies and address the removal of capabilities, as required, over a stated period of time. Security of ToIP packets should be a priority of proposed solutions, as the identity of individuals using other-than-voice emergency calls cannot be exposed to Ethernet packet sniffing. ToIP could potentially be secured by the utilization of SSL connections or through the inherent security features within IPv6.

What media types non-English speakers likely will use to make an emergency call in a NG911 environment

Many PSAPs utilize a language interpretation service when a call is received at a PSAP from a person with limited English ability. If the call taker knows the language being spoken, he or she can request a specific language interpreter. If the call taker does not know the language, typically, the call is transferred to a language interpretation service representative trained to help in language identification. Once the language is identified, the call is transferred to a language interpretation service representative with that language skill.

Once the interpreter joins the conversation, the PSAP call taker explains that this is a call for help to a 911 center and the call taker needed assistance. The call taker should take the lead in the conversation by giving the interpreter specific questions to relay. At no time should the call taker leave the caller alone with the language interpreter. The call taker must take the lead and provide the subject matter expertise. The interpreter, in turn, would relay the information back and forth.

These procedures for voice calls can be adapted to other call types entering the PSAP. If the technology being used to place the call to the PSAP has the ability to identify which language is being used as the call is placed, the PSAP can implement call handling procedures using this information to process the call.

Non- English speakers will still have access to traditional voice service but may also make an emergency call in a Next Generation environment using video, SMS text, or real time text. These services can be configured to identify the language being used and provide that information to the PSAP. The PSAP can establish procedures to contact a “text language interpretation service” or a “video language interpretation service” to assist with the call. These video and text conference calls can be established as calls enter the PSAP, or after the PSAP identifies the requirement.

B. NG911 Network Architecture

1. Transport Mechanisms in a NG911 Environment

It seems clear the language of NG911 is IP, which is “layer 3” in the Open Systems Interconnection (OSI) model of network protocol stacks. As this NOI points out, IP can be transported by many different low-level media (layer 1) including copper, fiber, and radio signals, and using many different media access control protocols (layer 2) such as Ethernet, WiFi, WiMax, and others. The choice and implementation of layer 1 and layer 2 protocols is largely driven by the marketplace and engineering considerations and should not have significant impact on either the PSAP or the users of NG911 because the handoff between the user and the PSAP is ultimately at the IP level.

NG911 PSAPs are and will be built using layer 1 and layer 2 transports appropriate to the task, which today is likely to be UTP-based Ethernet and possibly some WiFi. As these technologies evolve, our present layer 1 and layer 2 will be replaced gradually by the newest current technically and economically appropriate infrastructures. Economics, security, reliability, and similar concerns will play significant roles in these selections. Future layer 1 and 2 technologies will almost certainly have to be widely accepted and adopted in the marketplace before they could be incorporated in the PSAP. This should not present any special burden to the PSAP as technology replacements are part of normal equipment replacement cycles common in PSAPs and other enterprises.

IP itself is undergoing a profound change from IPv4 to IPv6.   Additional IPv4 address space allocations are not available from ICANN (Internet Corporation for Assigned Names and Numbers), so growth in the IPv4 network can occur only by reclamation, reassignment, or the use of private IPv4 addresses. Since construction of ESInet infrastructures is still at an early stage, new ESInet development going forward should be capable of supporting IPv6, even though the network may be implemented using IPv4. This may introduce higher costs at initial implementation time, but delaying IPv6 support will eventually incur even higher IPv6 implementation costs later. The future transition of the layer 3 protocol from IPv4 to IPv6 will be a significant cost, but will be a one-time cost.

The IETF ECRIT working group suggested SIP with location conveyance as the primary signaling protocol of NG911, and RTP as the primary media transport protocol in response to the issue of protocols running above layer 3 with respect to NG 911 services. NENA has followed these recommendations in the Detailed Functional and Interface Standards for the NENA i3 Solution, document 08-003 draft.

In a true i3 / NG911 design, there is no involvement of intermediate signaling and routing proxies and functions with the media streams. This arrangement leaves open a maximum amount of flexibility in accommodating new media formats while maintaining the overall architecture of NG911. The incorporation of a new medium type within the context of SIP and RTP requires that (within the IP network) the source and the destination both support the new medium. No other components are involved. Generally, changes in the NG911 architecture, SIP signaling protocol, call routing, or other structures should not be required.

Additionally, SIP provides for the negotiation of compatible media types between the endpoints, so fallback to a common medium is built into the design of the i3 compatible system. For example, if a new video format is introduced into the ESInet, and a PSAP does not support that video format, there should be a standard “common denominator” media types in widespread use and implemented at all PSAPs so the call can still be completed. . Therefore, there must be a list of “standard” codecs and protocols that all PSAPs should support, and which call sources must also support as appropriate to that source. These common codec requirements, such as ITU G.711 (for voice), have been listed in the work of ATIS, NENA, and others. But this list should be only a minimum requirement, allowing both PSAPs and call sources to expand on the list of available protocols if such new protocols become widely adopted.

In addition to SIP and RTP, it is likely that ESInets and NG911 will utilize widely deployed Internet protocols, such as http (via off-the-shelf web browsers) and related protocols, formats, and encodings, such as mpeg, gif, wav, and others. These should pose no special burden on PSAPs because these technologies are widely deployed and economically available as part of commercial off-the-shelf products.

Concerns have been raised that the use of IP as the NG911 transport opens the PSAP to a flood of new protocols and communication requirements that the PSAP may not be equipped to support. However, NG911 as envisioned by ECRIT, NENA, and others, is based on SIP and RTP, and other widely adopted Internet protocols, while allowing for non-disruptive evolution of the system, and should not impose a special burden on PSAPs.

2. NG911 Participants

The participants of new services are vastly different than in the past. In today's environment, anyone can use commercially available equipment to provide services to anywhere in the world. This environment has changed the traditional role of the telecommunications provider. Traditionally, a user would go to the local telecommunications service provider and be given service. Now, consumers can pick and choose which service they want, how it is delivered to them, what type of device they want to use, and even where they use it.

Many of these new providers have not operated in a regulated environment before and have the flexibility to adjust to the changing needs of users. This has led some providers to feel that they do not need to be a part of the solution. The impact of these providers should be studied and an initiative should be established to work with these providers to develop guidelines. Some of these providers may require regulation by the Commission or other state or federal agency, and still others may not be able to be regulated.

The development of guidelines and possible regulations should begin by looking at the functional flow of information from the service's users to public safety personnel, and the information that is needed by public safety agencies to properly perform their life-saving functions. The information that agencies *need* to perform their functions is what should drive future guidelines and regulations rather than business models. It will be important to keep in mind that the best solution may be difficult or costly.

Today's consumers have a choice of devices to use to communicate with public safety. In a NG911 environment, these devices for public safety should be limited to those that can perform real-time communication. Non-real-time communication devices or services will leave users believing that 911 does not work when they encounter inevitable delays in communication with 911.

Devices and services that have the capability to provide their users with access to 911 should follow a set of standards, but certification may slow innovation. There should be a way to stop the marketing of devices that do not meet the standards for public safety. Certifying and labeling devices could mislead users to believe that they have the ability to reach 911 with the device when that is not always the case (as occurred in the early days of VoIP deployments).

3. Interoperability and Standards

Interoperability is a major requirement of public safety. Several vendors offer their version of NG911, but not all of them use the same processes and interoperability interfaces. For effective interoperability, all systems should use a standard interface that will work with all other systems. That interface should include all information, or references to all of the information, that is associated with the call and caller, to include location.

Standards development is underway and many standards have been developed. Adoption of these standards by an authoritative entity will reinforce the importance of the standards and speed their implementation. There has been discussion that standards that are not developed through the American National Standards Institute (ANSI) process may not be standards. This belief should be addressed. SDOs that are not affiliated with ANSI are developing important standards for NG911. These organizations use open processes and gather consensus to develop their standards, and should be used when appropriate.

The Commission should continue to promote open, consensus-based development of standards. The National Technology Transfer and Advancement Act of 1995 and the United States Standards Strategy support this approach.

4. PSAP Functions in a NG911 Environment

The concept of a virtual PSAP has great potential, but from an operational perspective it needs more review because there are some critical issues that need to be resolved. For example:

- How does an authority protect data and information outside of its controlled facilities?
- How does an authority protect access to a virtual PSAP workstation when it can be located anywhere?
- How will the call taker at a virtual PSAP dispatch responders?

This latter issue is extremely important to NG911; the system must include processes and technologies to allow a call taker at a virtual PSAP to contact or send information to the responders. There would be significant liability exposure if this issue were not resolved before a virtual PSAP is implemented.

NG911 will be deployed across the country in a variety of ways. Some states may deploy several regions within the state. Some may deploy a single statewide system. Still other states may join with neighboring states to deploy a multi-state NG911 system. All these systems will need to be interconnected. A national infrastructure will be important to interconnect all of the various NG911 systems around the country. This interconnection will allow calls to be transferred anywhere, and the use of virtual PSAPs capabilities could be used to help in a disaster. One way to accomplish this could involve the development of a non-profit organization made up of the various NG911 systems, similar to what NLETS accomplished for law enforcement data sharing.

C. Other Specialized NG911 Applications

The use of automated devices to contact 911 has long been debated. Several states have laws that prohibit automated systems from sending alerts to the 911 system. Careful study of these devices and services must be performed before they are granted direct access to the 911 system. In the current E911 system, these devices typically are connected to a third-party screening center, which may subsequently forward the information to 911. Such non-human-initiated alerts should be given consideration for NG911, but better links from the device/service’s third-party answering centers to the 911 system should be developed. The success of the Virginia pilot project to directly connect alarm monitoring centers to 911 systems would be a good model to review.

Allowing social media sites to access 911 may be beneficial as more people use them in their daily communications. It is critical that social media access to 911 be provided the same level of service as other access types, i.e., communications must be two-way and in real-time accompanied by accurate location information. The major issue with this is the security of the social media sites. Adequate security must be required to prevent these sources from launching attacks on the 911 system.

All requests for emergency help should have access to the 911 system, whether from dedicated providers, third-parties or others. For example, many N11 services have public safety roles and can be the initial input of information in an emergency, such as a gas pipeline breach that was first reported to 811. Developing processes to enable this critical interoperability is important.

Many other data sources would benefit 911 users and responders. Access to these data sources will vary greatly from state to state, and even PSAP to PSAP. Some of the factors that will need to be addressed by each 911 authority are:

- Impact on PSAP staffing (will the PSAP have time to process this information).
- Level of automation to process the data.
- Importance of the data. Many items may be useful, but not critical; the deciding factor should be whether this new information would change the way the request is handled by the PSAP or responder.
- Ability to pass on the information to the responders. If the information cannot get to the responders, is it useful?

- Ability for the responders to process the information. Does an agency want a responding unit trying to navigate through traffic while also trying to watch an incoming video or read other incoming data?
- Protecting the information and ownership becomes an issue. Many states have open records laws that include all 911 information. If the data source is an entity that needs to protect its data, or whose data is already protected by law, that entity may not be willing to provide the information. Once it is delivered to 911, who owns that data? To ensure equal service nationwide, this may need to be addressed at the national level.

D. Issues Related to NG911 Implementation/Transition

1. Disparate PSAP Capabilities in a NG911 Environment

Disparate PSAP capabilities have existed since the advent of 911 and will certainly continue in the NG911environment. A PSAP's decisions regarding what to provision have been traditionally based on two factors:

- Funding – What are allowable uses of 911 funding, and what is not allowable?
- Usefulness – Many authorities have to fight the local culture of opinions based on the thought, "we don't need that to do our job."

Many states' 911 statutes limit the use of funds to only a portion of the system – typically everything up to the point of dispatch. This common limitation requires local 911 authorities to use other funding sources to pay for everything else.

2. 911 Competition

The Commission should weigh the benefits of competition against the critical nature of public safety.

A competitive NG911 environment has the potential to benefit users by driving down costs. Competition also has the potential to give a choice of System Service Providers that could offer a variety of service capabilities and options at competitive prices. A competitive environment would also promote innovation. With more System Service Providers competing to maintain their market share, there would be more incentive for System Service Providers to update and improve their service offerings. The updated and improved service offerings available in a competitive environment would, in turn, give users even more choices.

Alternatively, a competitive environment poses potential risks to public safety. Protections must be established and implemented to guarantee the level of service required for 911. A competitive environment could draw new types of System Service Providers into the market who have not provided 911 system services before. New 911 SSPs have the potential to fail and close up shop without warning, potentially leaving the 911 system vulnerable. Increasing the procurement requirements of SSPs could help to protect the system by ensuring that SSPs are committed to service delivery. A provider of last resort would need to be established for each geographical area in order to protect the system and ensure the continued availability of 911 services in a competitive environment. New types of services and SSPs would need to interoperate with one another. This interoperability will require the implementation of guidelines or standards for interoperability as a prerequisite to offering services.

The current regulatory environment would need to change to enable the NG911 environment to become truly competitive. Incumbent 911 SSPs do not have sufficient incentives to upgrade their technology or to interconnect and interoperate with new 911 SSPs. Numerous examples from across the nation illustrate this, many of which have become part of a Commission proceeding. Revisions to or the elimination of older laws and tariffs would be necessary in order to require interconnections. Or, negotiations between incumbent 911 SSPs and competitive 911 SSPs would need to be incentivized. Either way, the 911 regulatory environments at both the federal and state level will need to be overhauled to promote competition. References to older technologies that could prevent the use of newer services and technologies in the NG911 environment will need to be replaced with technology-neutral language that promotes technological innovation and interconnectivity between different types of service providers.

3. Liability Concerns

The Commission should extend its liability protection to cover any service or device capable of accessing 911. Additionally, current liability statutes should be modified to be technology-neutral and extend to all forms of information pushed to a PSAP or pulled from external sources by a PSAP, regardless of the platform over which information travels.[2] More specifically, 47 U.S.C. § 615a[3] should be amended to include protection when a party is using any device capable of placing a 911 request for emergency service.

The Commission should review its requirement that all 911 calls be routed to the "geographically appropriate" PSAP to ensure that nothing prevents 911 calls from being intelligently routed to the appropriate PSAP, even if it is not the geographically closest PSAP.

[2] *See* National Emergency Number Association, Next Generation 9-1-1 Transition Policy Implementation Handbook, A Guide for Identifying and Implementing Policies to Enable NG9-1-1, at 23 (Mar. 2010)

[3] *See* 47 USC 615 - § 615a. Parity of protection for provision or use of wireless service

The reason has to do with the new capability local 911 authorities will have to configure their systems to route calls differently based on call type, e.g, calls from non-English speakers or from non-human-initiated devices.

It would be beneficial for the Commission to anticipate the addition of new technologies that will arise in the development of NG911 and to offer broader liability protections once the details and scope of these technologies are better understood.

4. Confidentiality and Privacy Concerns

NG911 systems will be shared systems comprised of multiple entities, and the amount and types of information that are available to PSAPs will be much greater than in current E911 systems. In addition, more of this data will be stored in shared databases on a network, rather than locally housed databases, and the data may be shared with parties not directly involved in the local response to an emergency. Current policies are inconsistent with regard to sharing this information with non-911 government agencies to facilitate an emergency response. This inconsistency can adversely affect access to 911 databases.[4]

To avoid restricting the availability of information that NG911 is designed to receive, current federal and state privacy laws that allow exceptions for emergency purposes need to be extended to cover all types of data, not just the traditional customer record information. Limitations contained in 47 U.S.C. § 222[5] should be addressed so that it does not impede the reasonable exchange of necessary information.[6] Additionally, the definition of a "911 call" in statutes and rules should be uniform and broad enough to cover any type of 911 request for

[4] *See* National Emergency Number Association, Next Generation 9-1-1 Transition Policy Implementation Handbook, A Guide for Identifying and Implementing Policies to Enable NG9-1-1, at 18 (Mar. 2010)

[5] *See* 47 U.S.C. § 222 Privacy of customer information

[6] *See* Intrado*, Next Generation 9-1-1 Cooperative Governance*, at 16 (2010)

assistance. Additionally, applicable regulations will need to make clear who is responsible for 911 information that is stored in shared databases and networks. As NG911 is deployed, the Commission needs to monitor developments and be prepared to take action when issues arise concerning the distribution and storage of data in separate systems.

5. Location Capabilities

The Commission is well aware that the percentage of 911 calls made from wireless devices has been increasing steadily, and the need to locate these callers makes the accuracy of location information vitally important. There are still issues with the accuracy of location information provided with wireless 911 calls, even after 15 plus years. In September of 2010, the Commission released an Order in PS Docket 07-114 Wireless E911 Location Accuracy Requirements. That Order holds wireless carriers accountable to accuracy standards at either the county level or PSAP level. This change will help to increase accountability for the accuracy of location information provided within county or PSAP jurisdictions. However, there will need to be continued focus on improving wireless location technologies. With either global positioning system (GPS) or network triangulation as the current means to derive coordinate-based location information, telephone manufacturers and carriers should continue to improve their technology to more accurately locate their customers.

As we transition to NG911 it will be imperative that the accurate location of callers is provided with the 911 call. Routing the call to the appropriate PSAP will be dependent on the coordinate-based location sent with the call. If the location provided within the call is not accurate and is off by hundreds or thousands of feet, it is possible that a call could get routed to the wrong PSAP. If that occurs, it will take longer for the call to get to the correct PSAP and responders will be delayed in providing emergency services. As other media are included in 911 call delivery, such as texting, videos, photos, telematics, etc., this information must be tagged with accurate location information. With that information, call takers will know from where the text message or photo is coming. Again, because location information will be used to route calls to the correct PSAPs, it is imperative that the technology and devices provide an accurate location.

There is no room for technology that provides limited or sporadic accuracy. Location accuracy requirements need to be established *before* new types of media can be delivered to PSAPs in a NG911 environment. Setting a low threshold for location accuracy just to get technology to work will compromise service to the public. The industry needs to be incentivized or required to develop devices and/or technology that provide the accuracy needed to properly route calls. If the accurate location requirement is not established at the outset of implementing new 911-capable devices and media, it will be more difficult for these policy changes later.

The industry needs to continue to improve location accuracy within buildings. Future location technologies should provide elevation information to locate the caller in a multi-story building. Again, it is imperative that these technologies be thoroughly tested and accuracy metrics established before they are deployed in the marketplace. Unreliable, inconsistent location information can delay response and is as detrimental as having no location information.

All devices and media that send requests for assistance to 911 with coordinate-based or civic address information should have established testing procedures defined prior to initial implementation and should require regular maintenance testing for accuracy reliability over time.

In NG911, geographic information system (GIS) data will be used to route and validate location information through the ECRF and the Location Validation Function (LVF), respectively. It will be important to have clear guidelines on data accuracy and data maintenance metrics for local jurisdictions responsible for providing regular updates of GIS data to the ECRF/LVF.

The LVF will be used by providers to pre-validate addresses or new subscribers. It will be important to review and implement effective policies to provide adequate rules that define pre-validation procedures. Call takers that enter new subscribers into the Location Information Server (LIS) and pre-validate the address against the GIS data using the LVF will need to follow procedures on how to handle addresses that do not validate against any data through the LVF. An address forced into the system could lead to a non-routable call when a subscriber needs to dial 911. Associations such as NENA are reviewing the potential location information discrepancies that may arise in the NG911 environment along with report mechanisms and system metrics that will be necessary to the development of standards related to discrepancy reporting. There will also be the need for a review of policies and guidelines to administer the appropriate accountability and metrics to assure the highest possible accuracy within the call routing and validation functions.

6. Network and Data Security Concerns

What additional security concerns will be implicated by the transition to NG911 as compared to the legacy 911 security functionality?

The legacy 911 environment was afforded a small amount of protection from cyber attack by the nature of its architecture. Comprised of essentially closed network systems, the attack surface of a legacy 911 system was effectively minimized to local or physical attacks. In the unlikely event that a legacy PSAP was infected by a virus, it would have been contained to the local PSAP. However, the architectural model by which NG911 is built is an IP-enabled, interconnected and networked environment. PSAPs that were previously not connected must now join well-connected IP networks. This means that their attack surface exponentially increases. Traditional cyber threats like viruses, hacking, and denial of service (DoS) attacks now must be considered.

In the legacy 911 environment, it is easy to find PSAPs that have little to no protection against cyber threats. Simple and affordable measures, like antivirus software, are typically nonexistent (although this has been slowly changing over the past few years). It is L.R. Kimball's position that the greatest threats to NG911 are not some new or yet to be crafted threat that specifically targets NG911 (although such attacks will be created eventually). Instead, basic security threats that *all* IP-enabled networks face pose the greatest risk. Additionally, the scope scale and effectiveness of an attack in NG911 can be larger. Unlike the legacy 911 environment, a cyber attack in one PSAP could affect all PSAPs connected to the NG911 system.

PSAPs should begin the planning process prior to the implementation of NG911. Additionally, all NG911 planning efforts should include a cyber security element.

How can the NG911 network be protected against viruses, cyber attacks, fraudulent or harassing transmissions, and other unwarranted intrusions and interruptions?

NENA recently released the public safety industry's first comprehensive cyber security standards. These standards, known as NG911 Security, or NG-SEC, are specifically designed for PSAPs in a NG911 environment. NG-SEC standards provide a starting point for protecting the NG911 system from the effects of cyber attack. L.R. Kimball recommends that NG911 planning efforts integrate not only cyber security, but more specifically, compliance with NG-SEC in addition to other federal, state, or local requirements.

However, as previously noted by L.R. Kimball's comments in response to the Commission's September 28, 2009 Public Notice seeking additional comment on public safety, homeland security, and cyber security elements of National Broadband Plan, the release of the NG-SEC standards present a challenging question to the industry, particularly the PSAPs:

How will we fund the significant and costly activities necessary to ensure that the cyber security levels of these mission critical networks, including broadband, which our society depends on in time of need, are met and maintained?

Current funding mechanisms do not explicitly account for these new and necessary requirements. Local and state 911 budgets would need to be expanded to include items such as hiring or outsourcing cyber security staff, or introducing basic security countermeasures like firewalls, patch management solutions, vulnerability assessments, etc. There is an open question regarding whether the industry would be less likely to implement these standards without an effective means to fund them. There is a vitally important question that impacts our homeland security: If there is no standardized and mandated requirement for cyber security, how would a PSAP be able to interoperate with federal agencies like the Department of Homeland Security, the Federal Emergency Management Agency (FEMA), the National Guard, and others, during a time of crisis? What will be the ramifications of a failure to fund and implement these critical cyber security measures?

These questions serve as an important call to action for federal, state and local governments to actively and forcefully address the funding issue. Broadband initiatives aimed at increasing the effectiveness of public safety capabilities must include funding mechanisms specifically for cyber security. Funding explicitly targeted for cyber security in a NG911 environment is a necessary and important component to protect the NG911 network.

7. Education

What role will public information campaigns play in the transition to NG911?

Public information campaigns will play the same important role in the transition to NG911 as they did during the transitions to E911 and wireless E911. Public information has always been viewed as an important avenue to get people to think twice before burdening the 911 network with non-emergency calls. Although it is prudent to make an effort to set public expectations regarding local system capabilities, people will assume that the level of service they have at home is the level of service that exists everywhere. There is an expectation that the 911 system will work everywhere, every time. Disparate capabilities from one place to another can be expected to have the same potential for tragedy with NG911 as it did with wireless E911: callers may not be able to get through to 911, and callers may not be able to be located.

How can the Commission ensure that public safety personnel, consumers, and carriers are aware of NG911 deployments?

The Commission could ensure that public safety personnel, consumers and carriers are aware of NG911 deployments in the same manner it did during wireless deployments – by requiring them to report. The Commission would face a unique challenge, however, in that NG911 service providers may not always be regulated utilities and the Commission's ability to command them to report would be limited absent a rule change.

What entities should lead and contribute to consumer education?

State and local entities should lead and be the primary contributors to consumer education. The Commission also should provide consumer advisories similar to what it provided with its wireless E911 and VoIP brochures.

Should the Commission foster common terms and terminology to facilitate the deployment of NG911?

The Commission should not create entirely new terms and terminology, but should adopt those that have been established by NENA and are now commonly used within the industry.

8. Unidentified Caller Access to NG911

Increased access to the 911 network will commensurately increase access for unidentified calls. Whether a caller is unidentified due to equipment or network failure, is unintentional, or is a prank or malicious call, anything that impedes access to the 911 system could become a liability and/or moral issue. A PSAP's ability to determine the intention of the call is unknown until the caller is queried and even then may not be known. For example, a voice call could arrive without voice or a text without a message. Creating authorization models that will provide the PSAP with caller, provider and location information from the closest point to a caller’s entrance to the NG911 network will help eliminate prank or malicious calls, while providing a point of reference for an actual emergency response. Facilitation of these authorizations or standards would have to be at the federal level as most states will not provide regulation of the service providers.

9. International Issues

International issues are faced today with VoIP. These issues should be carefully studied to determine the best options for addressing them. Will it be technically possible for the access provider to reroute international calls to a local Application Service Provider (ASP)? This would require application-aware networks that may be costly; but it is worth consideration because the secured networks that may be needed to support those calls are similar to what access providers need to provide location information in the first place.

Another option would to look at the role of ASPs in the provisioning of telecommunications and their impact on this critical service. If the routing of international calls is found to be telecommunications services, this may be able to be addressed with international coordination such as through the ITU, the leading United Nations agency for information and communication technology issues.

Other international issues that impact 911 are wireless services. The location of a wireless service provider’s tower is used to determine the proper routing of a call. This has international implications for states that border Mexico and Canada. In the NG911 environment, these issues will remain. The use of a national infrastructure to interconnect to other nations clearly needs to be addressed. International interconnection will require federal action.

E. Jurisdiction and Regulatory Roles

Should each state designate an organization that will be responsible for planning, coordinating, and implementing the NG911 system in that particular state?

Federal policy, as reflected in existing 911 statutes and regulations, promotes and/or requires statewide planning and coordination and specifically recommends the establishment of a state entity to lead such planning and coordination. Other federal statutes and regulations that govern public safety interoperability grant programs also establish the principle of statewide planning and coordination. L.R. Kimball views the policy direction coming from the federal government to be clear in this regard.

Many states have established state-level 911 programs, but there is considerable diversity in the nature, organization and scope of those programs. Some states have made provision for limited statewide coordination, some programs are simply advisory, others can coordinate only on specific technologies (i.e. wireless), while yet others have full responsibility for planning, coordinating and funding their respective state 911 systems.

The historical record reveals that states that provided some level of coordination and oversight in the deployment of wireless E911 were more successful than those that did not. The body of work that has been done at the national level is clear about the nature of NG911: it involves interconnection to a degree that ultimately will result in a nationally interoperable ESInet with functionality far beyond the capability of today's E911 systems . The level of coordination and partnership this will require simply cannot come about on its own. Statewide planning and coordination mechanisms must be in place or it will not happen.

L.R. Kimball recommends that Congress require each state that does not already have a statewide 911 coordinator and oversight body to create one. In making this recommendation, we want to be clear: we are not advocating that states "take over" 911 services in states where said services are provided at local initiative and operation. We are advocating that all states have an effective mechanism to ensure interconnectivity between locally- or regionally-initiated NG911 systems and to bring NG911 to geographic areas that are not served by one of the local/regional systems. From a planning, funding and coordination perspective, we envision a mutually supportive arrangement in which all parties understand and strive toward the goal of achieving statewide coverage in a manner that is technologically and operationally feasible.

Should a single federal entity be established to oversee the transition to NG911?

L.R. Kimball is of the opinion that a single federal entity could not be established to oversee the transition to NG911. There are simply too many components involved in NG911 for centralized federal government involvement. One agency could not take on all aspects of NG911.

However, an entity should be established to coordinate efforts among federal agencies; it is L.R. Kimball's recommendation that the National E-911 Implementation and Coordination Office (ICO) established by the Ensuring Needed Help Arrives Near Callers Employing 911 Act of 2004 (ENHANCE 911 Act) be given this responsibility.

While the ICO may be the most practical choice for federal oversight, it should be noted that this would require statutory change to expand the duties of ICO. We note that the ICO will ultimately require reauthorization through an Act of Congress, as the ENHANCE 911 Act provided a sunset date of October 1, 2009 for the termination of the office. In 2010, the Next Generation 9-1-1 Preservation Act (H.R. 4829/S 3115) was introduced to sustain the functionality of this office. This legislation should be supported as the office provides an essential role in the advancement of NG911.

Should there be a national policy established by the Commission or another Federal entity to ensure consistent regulation?

L.R. Kimball believes that the Federal government should exert its authority in a positive manner that is beneficial to the advancement of 911 as a whole. The Federal government should not tell states what to do and what not to do, rather, it should develop models for cooperative agreements and establish rules, as with wireless E911, to require such things as specific location standards and to promote open, shared network policies to ensure that NG911 is not prohibited in any way by outdated policies.

What statutory or regulatory changes, if any, would be necessary for the Commission, other federal agencies, states, Tribes, or localities to facilitate and oversee NG911?

L. R. Kimball recognizes that NG911 is significantly different than E911 in scale and scope, and therefore recommends that federal, state, and local governments adopt statutory and regulatory changes that properly facilitate and oversee NG911. This includes adopting statutes and regulations that provide a state-level authority; support open, shared networks; provide that the implementation of NG911 be kept at the appropriate level; and provide for the needs of local PSAPs.