Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
International Comparison and Consumer	)	
Survey Requirements in the Broadband Data	)	**GN Docket No. 09-47**
Improvement Act	)	
	)	
A National Broadband Plan for Our Future	)	**GN Docket No. 09-51**
	)	
Inquiry Concerning the Deployment of	)	
Advanced Telecommunications Capability to	)	
All Americans in a Reasonable and Timely	)	
Fashion, and Possible Steps to Accelerate	)	
Such Deployment Pursuant to Section 706 of	)	**GN Docket No. 09-137**
the Telecommunications Act of 1996, as	)	
Amended by the Broadband Data	)	
Improvement Act	)	**DA 09-2133**

COMMENTS – NBP PUBLIC NOTICE # 8

NATIONAL EMERGENCY NUMBER ASSOCIATION

November 12, 2009

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY OF COMMENTS 2

II. CURRENT AND EXPECTED USE OF BROADBAND FOR EMERGECY SERVICES 4

III. PUBLIC SAFETY MOBILE BROADBAND NETWORKS 8

IV. NEXT GENERATION 9-1-1 10

NG9-1-1 Broadband Infrastructure Requirements 12

Early NG9-1-1/Pre-NG9-1-1 Deployments 14

Status of NG9-1-1 Standards 15

NG9-1-1 Equipment Development 17

Regulatory Roadblocks 18

Automatic Location Identification 21

V. CYBER SECURITY 24

VI. BEYOND NG9-1-1: THE BROADER NEXT GENERATION EMERGENCY COMMUNICATIONS ENTERPRISE 27

VII. CONCLUSION 29

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

In the Matter of	)	
	)	
International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act	)	**GN Docket No. 09-47**
	)	
A National Broadband Plan for Our Future	)	**GN Docket No. 09-51**
	)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act	)	**GN Docket No. 09-137**
	)	**DA 09-2133**

COMMENTS – NBP PUBLIC NOTICE # 8

NATIONAL EMERGENCY NUMBER ASSOCIATION

The National Emergency Number Association ("NENA")[1] respectfully submit these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Public Notice seeking additional comments on the public safety, homeland security and cyber security elements of the National Broadband Plan.[2] In response to the National Broadband Plan Notice of Inquiry, NENA submitted comments in June outlining a vision of broadband-enabled

---

[1] NENA is The Voice of 9-1-1.™ NENA promotes implementation and awareness of 9-1-1 as North America's universal emergency number and is the leading professional non-profit organization dedicated solely to 9-1-1 emergency communications issues. NENA serves its nearly 7,000 members in 48 chapters across the U.S., Canada and Mexico through policy advocacy, establishment of technical and operational standards, Next Generation 9-1-1 development, certification programs and a broad spectrum of educational offerings. More information about NENA is available at www.nena.org.

[2] *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, DA 09-2133 (Rel. Sept. 28, 2009).

Next Generation 9-1-1 and emergency communications systems.[3] NENA appreciates the opportunity to expand on our earlier comments and applauds the Commission for continuing to seek targeted data and perspectives on public safety broadband needs.

I. INTRODUCTION AND SUMMARY OF COMMENTS

It is essential that the National Broadband Plan's recommendations include concrete proposals and suggestions designed to facilitate the transition of our nation's 9-1-1 and emergency communications systems to broadband-enabled, IP-based platforms. The Plan should clearly articulate that it is the policy of the United States to foster the migration from analog, voice-centric 9-1-1 and emergency communications systems into a broadband-enabled 21st century, IP-based emergency services model.

To be effective, the Plan must address four fundamental issues. **First**, all public safety answering points ("PSAPs") and emergency services agencies must have access to both wired and wireless broadband networks. **Second**, access to broadband networks alone is insufficient; for 9-1-1 and emergency communications systems, the National Broadband Plan must recognize that there is a difference between (1) access to publicly available commercial broadband networks that can benefit public safety, and (2) privately managed Emergency Services IP networks ("ESInets")[4] specifically designed for emergency services that <u>utilize</u> such publicly available broadband networks. **Third**, there must be sufficient funding available on a recurring

[3] FCC 09-31, released April 8, 2009; NENA Comments of June 8, 2009, GN Docket 09-51.

[4] All emergency response agencies need to be connected to ESInets. ESInets are engineered, managed networks, and are intended to be multi-purpose, supporting extended public safety communications services, in addition to 9-1-1. ESInets use broadband, packet switched technology capable of carrying voice, video, and text, plus large amounts of varying types of data using Internet Protocols and standards. ESInets will ride on a mix of commercial and government-owned network infrastructure, but simply having a broadband network pass by emergency response agencies is insufficient. Commercial and government-owned broadband networks are a critical component of our nation's homeland security, but the vision of NG9-1-1 and emergency communications requires the further step of ensuring that all public safety agencies are interconnected on ESInets riding the broadband infrastructure.

basis for 9-1-1 and public safety access to broadband networks and the applications and services made possible by broadband.[5] **Fourth**, state and federal regulations and statutes must be clarified and interpreted in a consistent manner to enable IP-based Next Generation 9-1-1 and emergency communications systems. Suggestions on these overarching considerations are discussed below and in earlier NENA filings.[6]

In addition to policy issues related to the deployment of broadband-enabled NG9-1-1 systems designed to receive emergency assistance requests from the public, the FCC also needs to clarify the 9-1-1 responsibilities of wired and wireless broadband network providers and communications service providers in a new IP-based environment. For example, it is increasingly the case that the network over which a communication (voice, video, text, or other data) is travelling may be provided by a separate entity than the communications provider offering a service to consumers. This raises questions as to the 9-1-1 responsibilities of each entity - the separate network and communications service providers - that should be addressed by the Commission. This subject is an example of the fact that in addition to focusing on broadband issues related to deploying NG9-1-1 systems, the FCC also must simultaneously address the

---

[5] *See e.g.*, Written Testimony of Brian Fontes, National Emergency Number Association, before the House of Representatives, Committee on Energy and Commerce, Subcommittee on Communications, Technology, and the Internet (September 24, 2009) at pg. 5; available at http://www.nena.org/sites/default/files/Brian%20Fontes%20Testimony%209.24.09_0.pdf.

[6] For additional background and supporting information, we recommend that the Commission closely review, and formally include in the record of the National Broadband Plan, a recent report to Congress from the National E9-1-1 Implementation and Coordination Office ("ICO") titled, "*A National Plan for Migrating to IP-Enabled 9-1-1 Systems*," ("*ICO NG9-1-1 Migration Plan*") available at http://www.e-911ico.gov/NationalNG911MigrationPlan_sept2009.pdf. In addition, numerous other important reports from the Department of Transportation's Next Generation 9-1-1 Project are available at http://www.its.dot.gov/ng911/ng911_pubs.htm.

9-1-1 location acquisition, routing and delivery responsibilities of originating service providers[7] in an IP-based 9-1-1 environment.

II. CURRENT AND EXPECTED USE OF BROADBAND FOR EMERGENCY SERVICES

To assist the Commission in its request for data from parties involved in the National Broadband Plan proceeding, NENA recently conducted a public safety broadband survey of PSAPs and other emergency services agencies.[8] The survey was designed to gather high-level information on the availability of wired and wireless broadband networks for public safety agencies, as well as the current and expected use of broadband for 9-1-1 and emergency communications.[9] Before responding to the specific questions in the Public Notice, an overview of the findings in the preliminary responses to the NENA broadband survey is provided to give some insight into current and expected public safety broadband uses.[10]

The survey results represent initial responses from nearly 650 respondents in 40 states and the District of Columbia. Overall, survey results indicate that broadband, where available, plays an important role in everyday PSAP and emergency services operations and will continue to do so in the future as broadband-enabled applications and services are deployed. Of those

---

[7] In this filing, the term "Originating Service Provider" (OSP) refers to any communications service provider that enables a caller, whether human-initiated (e.g. a 9-1-1 call or text message) or non-human-initiated (e.g. automated sensor communication) to submit an emergency call or message to 9-1-1 systems.

[8] Survey results available at http://www.nena.org/sites/default/files/Broadband%20Usage%20SurveySummary_11122009.pdf.

[9] For the survey, the following definitions were used: WIRELINE BROADBAND: Broadband provided via a hard-wired Internet Protocol access method that supports high-speed data communications between the network and the PSAP/emergency services agency. These are commonly known by their commercial marketing names, such as DSL, Cable Modem, T-1/DS-3 lines (or similar); WIRELESS BROADBAND: Broadband provided via a wireless Internet Protocol access method that supports high-speed data communications between the network and the PSAP/emergency services agency, or mobile response unit. Not to be confused with WiFi, these are commonly known by their commercial marketing names, such as mobile broadband or 3G or 4G wireless data services (or similar); SATELLITE BROADBAND: Broadband provided via a satellite Internet Protocol access method that supports high-speed data communications between the network and the PSAP/emergency services agency.

[10] Note: the survey did not seek information concerning fixed wireless (microwave).

with access to broadband, nearly 85% of responding agencies utilize wireline broadband and approximately 55% utilize a wireless broadband network. Almost four percent of total respondents stated that no form of broadband is available in their geographic area.

For those entities indicating that they do not currently use any form of wireline broadband (approximately 15% of total respondents), the top three reasons given for not using available broadband services were that the service is too expensive (38%), broadband is not a permitted expense under the current budget (29%), and there is little or no perceived value for broadband (28%). Similarly, for entities indicating that they do not currently use any form of wireless broadband (approximately 45% of total respondents), reasons provided were that the service is too expensive (31%), there was little or no perceived value for broadband (29%), insufficient network coverage (25%), insufficient reliability (23%), broadband is not a permitted expense under the current budget (23%), and lack of availability (17%).

The survey also includes information on local law enforcement, fire and EMS use of wireless broadband services. A high percentage of respondents indicated they rely on commercial wireless broadband networks (police: 88%; fire: 85%; EMS: 89%). A significantly lower percentage of respondents indicated that local police, fire and EMS agencies rely on government-run wireless broadband networks (police: 25%; fire: 29%; EMS: 19%). Respondents identified numerous services provided via wireless broadband connections. The two primary reasons provided for those police, fire, and EMS agencies that do not use any form of wireless broadband service were insufficient network coverage and cost. Interestingly, the survey revealed that concerns over insufficient bandwidth and reliability of wireless broadband networks were comparable for both commercial and government-run wireless broadband

networks. In some cases, commercial networks were deemed to have superior bandwidth and reliability, while in other cases the opposite is true.

Commercial Wireline Broadband Use By PSAPs

Respondents indicated that commercial wireline broadband service is used by PSAPs for numerous applications and services, including administrative purposes (88%), monitoring weather information (67%), connecting to law enforcement data networks (66%), downloading large map files (60%), emergency alerting (42%), dispatch service (39%), and several other applications/services. When asked about bandwidth and reliability, 66% of respondents indicated that the bandwidth of their commercial wireline broadband network is sufficient and 70% were satisfied with network reliability.

Government-Run IP Wireline Broadband Use By PSAPs

While only 42% of PSAPs responding to the survey indicated that they use a government-run wireline broadband network, the uses of such networks were similar to commercial wireline broadband networks. The majority of respondents use government-run IP wireline broadband networks for connecting to law enforcement data networks (74%), with other uses including administrative purposes (67%), downloading large map files (49%), dispatch service (42%), emergency alerting (30%), and several other applications/services. Regarding bandwidth and reliability, 65% of respondents indicated that the bandwidth of their government-run IP wireline broadband network is sufficient and 71% were satisfied with network reliability.

Commercial Wireless Broadband Use By PSAPs

Approximately 55% of PSAP respondents rely on a wireless broadband network, with 77% of agencies using a commercial wireless broadband service and 26% relying on a government-run wireless broadband network. For those depending on commercial wireless

broadband networks, uses include administrative purposes (69%), connecting to law enforcement data networks (56%), dispatch service (56%), monitoring weather information (41%), downloading large map files (39%), emergency alerting (35%), and other uses. When asked about bandwidth and reliability, 65% of PSAP respondents indicated that the bandwidth of their commercial wireless broadband network is sufficient and 63% were satisfied with network reliability.

Government-Run IP Wireless Broadband Use By PSAPs

Only 26% of PSAPs responding to the survey indicated that they use a government-run wireless broadband network. The majority of respondents use government-run wireless broadband networks for connecting to law enforcement data networks (68%), with other uses including administrative purposes (58%), dispatch service (52%), downloading large map files (47%), emergency alerting (35%), and several other applications/services. Regarding bandwidth and reliability, 62% of respondents indicated that the bandwidth of their government-run wireless broadband network is sufficient and 73% were satisfied with network reliability.

Expected Future Use of Broadband

Respondents identified the following broadband-enabled services and/or applications not currently in use that agencies will (or would like to) use in the future: Next Generation 9-1-1 (87%), direct receipt of images and/or video from 9-1-1 callers (76%), direct connection to video services used by the deaf and hard of hearing (71%), inter-agency information sharing (68%), PSAP to responder image/video communications (65%), first responder image/video communications (62%), radio-over-IP (62%), direct receipt of advanced automatic crash notification data (60%), real-time video-enabled training (57%), remote virtual PSAPs (53%),

direct receipt of sensor/alarm data (47%), hosted software services/applications (43%), and receipt/distribution of electronic medical records information (26%).

III. PUBLIC SAFETY MOBILE BROADBAND NETWORKS

While not providing technical details on public safety bandwidth and capacity requirements, NENA's public safety broadband usage survey described in Section II above does provide some insight into the current and expected device and application needs for mobile broadband. The survey also indicates that PSAPs and emergency services departments are currently relying significantly on commercial wireless broadband networks. While there is a strong desire to have wireless broadband networks designed and built for public safety use, a recent report of the National Public Safety Telecommunications Council ("NPSTC") indicates that reliance on commercial wireless broadband networks will continue for many years. The NPSTC 700 MHz Broadband Task Force Report states that, "a nationwide, interoperable wireless broadband network…for public safety will not be built overnight and it will take many years to even approximate ubiquitous coverage. During that period, the ability of public safety users to roam on commercial networks will be essential."[11] This is primarily due to the reality that there is a lack of identified funding to build public safety broadband networks, a central fact that has driven the Commission's discussion on innovative public/private partnerships to ensure public safety access to wireless broadband.

Even if broadband networks expressly designed for public safety become available, NENA believes that conservative network design principals that recommend multiple network technologies, from multiple providers would argue for continuing use of commercial wireless

[11] National Public Safety Telecommunications System, 700 MHz Public Safety Broadband Task Force Report and Recommendations (September 4, 2009) at pg. 32; available at http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf.

networks within public safety systems. The ubiquity of Internet Protocol deployments on all these networks allows public safety to use many different networks to build its overall communications enterprise, providing much greater reliability than any single network could offer.

The general lack of funding and recognition that in many areas public safety will continue to rely on commercial wireless broadband networks for a long time leads to three overall conclusions: **First**, it is essential that a reliable, recurring funding source is established for public safety access to, and use of, broadband.[12] **Second**, the Commission should continue to seek innovative public/private partnerships to ensure public safety access to wireless broadband networks. **Third**, given the continued reliance on commercial wireless broadband networks, it is important to look at what additional steps the Commission can take to ensure that current and planned commercial networks can meet the bandwidth, coverage and reliability needs of public safety. It will always be desirable to have specialized networks that meet the critical needs for public safety communications, but it will not always be efficient or cost effective. Therefore, the Commission may be able to address public safety challenges by taking specific actions to enhance commercial networks and devices, in conjunction with the construction of public safety networks.

Regarding actions the Commission can take to ensure interoperability among public safety broadband systems, NENA urges the Commission to ensure that its rules require a nation-wide public safety wireless broadband network (or network of networks) based on a single standard and technology platform consistent for all users of the system with interoperability and

[12] Comments of NENA on 700 MHz broadband public safety waiver requests, Docket 06-229, October 16, 2009.

roaming requirements.[13] Requiring all entities to commit to deploying a common technology standard (*e.g.* LTE), and ensuring that public safety entities are continually operating on the most current version of the standard, is essential. NENA encourages the Commission to review the significant work and recommendations on interoperability and roaming made in the recent report of the NPSTC 700 MHz Public Safety Broadband Task Force. To ensure interoperability, the FCC should require a commitment by operators of public safety wireless broadband networks to those applications identified as essential to interoperability and roaming, such as the recommendations in the NPSTC report currently being reviewed by the Public Safety Spectrum Trust ("PSST").

Finally, consistent with previous NENA filings, we urge the Commission and stakeholders involved in the D Block debate to consider how all the components of a national wireless public safety broadband network, including the wired portion of such a network that joins the wireless access points, can be a part of a national "internetwork" backbone interconnecting state and regional ESInets.

IV. NEXT GENERATION 9-1-1

There are four fundamental purposes of Next Generation 9-1-1 (NG9-1-1): (1) fully replace Enhanced 9-1-1 (E9-1-1) with all core functionalities and capabilities of the current E9-1-1 system; (2) add capabilities to support 9-1-1 access in multiple formats for all current and new types of originating service providers; (3) add increased system flexibility for PSAPs and 9-1-1 governing authorities; and (4) add capabilities to integrate and interoperate with entities involved in emergency response beyond the PSAP.

[13] NENA, APCO, NPSTC and the PSST have all endorsed LTE as the preferred technology platform for the national public safety wireless broadband network.

NG9-1-1 systems are not being designed as dedicated, closed, single purpose systems. They will be shared systems comprised of multiple entities. 9-1-1 will be only one part of a much larger system shared with general government, private sector entities and other public safety services and agencies. The amount and type of information (voice, text or video) received by PSAPs and shared with emergency response agencies will greatly surpass current E9-1-1 systems. NG9-1-1 makes it possible to push and pull video, still images, medical information and a host of other data with a 9-1-1 call. Additionally, the architecture of NG9-1-1 systems will significantly increase the amount of information, equipment and services contained in shared databases and networks. For example, the same emergency services IP network that is used to route all forms of voice, video and data to PSAPs could be shared with other emergency response entities to enable IP-based voice and data applications utilized by first responders (e.g. radio over-IP).

To reiterate, NG9-1-1 is not simply an extension of E9-1-1. While a full NG9-1-1 system must support all E9-1-1 functions and features, NG9-1-1 is IP-based, and software and database controlled in fundamentally new ways, enabling many new technical and operational capabilities to further enhance the coordination and delivery of emergency services nationwide. NG9-1-1 is designed to:

- provide standardized interfaces from all call and message services
- process all types of emergency calls including non-voice (multi-media) messages
- acquire and integrate additional data useful to call routing and handling
- accurately locate and deliver calls/messages and data to the appropriate PSAPs and other appropriate emergency entities
- support data and communications needs for coordinated incident response and management
- provide a secure environment for emergency communications

Finally, NENA believes that it is in the nation's best interest to foster interconnection of ALL public safety agencies, and specifically, to provide shared, reliable, managed private

networks connecting all public safety agencies. Building one network for 9-1-1, another for police, another for fire, another for EMS, etc, is too costly, too hard to manage and protect, and fosters silos of communication that we cannot afford. The FCC should discourage single purpose networks and encourage all public safety agencies to share common networks, services and management where feasible. See Section VI below for further discussion in Next Generation emergency communications beyond NG9-1-1.

NG9-1-1 Broadband Infrastructure Requirements

It is important to acknowledge that access to broadband networks alone is insufficient. For 9-1-1 and emergency communications systems, the National Broadband Plan must recognize that there is a difference between (1) access to publicly available commercial broadband networks that can benefit public safety, and (2) privately managed ESInets specifically designed for emergency services that utilize such publicly available broadband networks. NG9-1-1 systems will not be run over the public Internet. As with any IP network, the networks used for public safety will be constructed of routers and links between those routers. The links will be a mix of commercial and government owned networks, wireline and wireless. Each link can be a physical circuit/wire/radio, or it can be a "virtual" connection which is provisioned over a public broadband network. Any discussion about bandwidth, capacity, reliability and other requirements for NG9-1-1 refer to the managed private network as a whole, and not the portions of a public broadband network that may provide components of that managed private network. Nevertheless, when designing public broadband networks, the needs of public safety should be taken into account, and are detailed in the following paragraphs.

It is impractical to provide a single definitive answer concerning the requirements for NG9-1-1 infrastructure. Numerous factors will impact such requirements, including the number

and type of users, identified uses, and geographic coverage area of the system. Another critical factor is whether the system is designed specifically for 9-1-1 or if it is a system in which numerous entities share the IP backbone infrastructure, as recommended by NENA, for efficiency and cost purposes. NENA offers the following guidance regarding broadband infrastructure:

Access - When planning public broadband networks, wired or wireless, attempts should be made to include all public safety agencies within the service area of the network. If the route comes within 1 mile of a public safety agency of any kind, it should be routed so it passes by such agencies. Access to the network should be provided to public safety agencies on reasonable terms.

Bandwidth - 2MBit per PSAP plus 2MBit per call taker position is a reasonable total bandwidth requirement. This estimate is also valid for the dispatch part of a responder agency. Unlike most users, public safety usually requires symmetric bandwidth agreements (same upload and download rates). For the communications to responder units, our estimates are 1Mbit per agency and 1Mbit per responding unit for a small agency, 5Mbit per agency and .5Mbit per responding unit for a medium (5-20 units) and 20Mbit per agency and .25Mbit or perhaps .33Mbit per responding unit for a large agency. We expect that responder units may often use more upload bandwidth than download bandwidth for sustained times, although planning for symmetric bandwidth use will probably suffice. As with most uses for broadband, bandwidth needs for public safety will grow quickly as more broadband-enable services and applications become available.

Diversity – Diversity of physical infrastructure is of critical importance to public safety and is often not considered when planning broadband networks. Care must be taken to assure that there

are multiple paths into and out of the physical buildings housing public safety agencies such that normal incidents like backhoe digging, or car vs. power pole accidents do not sever all connections to the facility. Also, for reliability, the networks used by public safety need bandwidth from several sources, so that if one or more sources fail, connectivity can be maintained. As above, NENA believes that public safety networks will be constructed from a mix of commercial and government owned networks, and diversity must be taken into account when planning such networks. At least 3 physical links with at least 2 completely diverse paths (no common facilities, poles, conduits, rights of way, power sources, etc) are recommended.

Connection types - Often, commercial broadband networks are constructed on top of "sub-IP" technologies such as SONET rings, MPLS networks or Frame Relay systems. Public safety is better served if access is provided at the sub-IP layer, in which the infrastructure enforces separation between uses of the physical connection. Failing access to the sub-IP layer, it will be necessary to use "Virtual Private Network" ("VPN") techniques that use IPsec or similar technology to get secure connections across a public network.

Reliability - Because networks are being engineered with multiple connections with physical diversity, the reliability of any one connection need not be the same as the reliability of the network as a whole. In general, public safety will probably require service level agreements of 99.95% availability from its broadband suppliers.

Early NG9-1-1/Pre-NG9-1-1 Deployments

Many states and sub-state regions are planning and implementing IP networks that may provide a foundation for the transition to NG9-1-1. In general, NENA refers to such developments as "pre-NG9-1-1." NENA's NG9-1-1 project includes active tracking of state and sub-state initiatives to implement IP networks capable of supporting NG9-1-1 functions in the

future, or specifically being designed for NG9-1-1 system deployment. NENA maintains a spreadsheet of counties/regions/states that are either considering or in the process of implementing an IP backbone network in preparation for NG9-1-1.[14]

According to NENA's ongoing research, the state of Vermont has made significant progress in the initial stages of NG9-1-1 deployment at a state-wide level. Several other states have deployed or are in the planning stages of deploying state-wide and/or regional IP backbone networks that can be utilized for ESInets necessary for NG9-1-1. These states include, but may not be limited to, Indiana, Texas, Washington, Minnesota, Alabama, Connecticut, Illinois, Pennsylvania, Kentucky, Florida, California, Delaware, Louisiana, Maryland, Montana, Missouri, New Jersey, New Mexico, North Carolina, Oklahoma, Oregon, Tennessee, and Washington, D.C.[15]

Status of NG9-1-1 Standards

Major NENA functional NG9-1-1 technical standards are being finalized and are planned to be released in the fourth quarter of 2009 and the first quarter of 2010. These include the core IP functions and interface standards (known as "i3"), and the first of two major security standards. Standards work outside of NENA is progressing as well. For example, the Internet Engineering Task Force ("IETF") Emergency Context Resolution with Internet Technologies ("ECRIT") working group has developed the Location to Service Translation Protocol ("LoST") to route IP-enabled 9-1-1 calls to the appropriate PSAP. NG9-1-1 related standards work is also being done by the Alliance for Telecommunications Industry Solutions' (ATIS) Emergency

---

[14] Spreadsheet available at http://www.nena.org/ng911-project/ip-network-status.

[15] *See ICO NG9-1-1 Migration Plan* at pg. 6-9 for further information on pre-NG9-1-1 trial deployments in the states of Vermont and Indiana; Galveston County, TX Emergency Communications District; Hamilton County, OH; and Greensboro, NC (Guilford Metro 9-1-1).

Services Interconnection Forum (ESIF), the 3rd Generation Partnership Project (3GPP), and the Organization for the Advancement of Structured Information Standards (OASIS).[16] Results from testing, such as the recent NENA NG9-1-1 Industry Collaboration Event ("ICE")[17] developmental testing, will provide feedback to cause some detail adjustments in NENA and other standards. However, other technical standards and technical transition guidelines remain to be completed through the second quarter of 2010.

Several NG9-1-1 standards have been adopted already. Currently completed and published standards include the following[18]:

- 08-502: NENA Generic E9-1-1 Requirements, Issue 1, July 2004 (baseline for NG9-1-1)
- 08-751 i3 Requirements for NG9-1-1 (Long Term Definition) v1
- 08-752: Location Information to Support IP-Based Emergency Services, Issue 1, 2006 (Technical Information Document)
- 08-002: Functional and Interface Standards for NG9-1-1 (i3) v1 (Definition level)
- 71-501: Synchronizing GIS with MSAG & ALI v1
- 70-001: NENA Registry System v1
- 04-001: NENA Recommended Generic Standards for NG9-1-1 PSAP Equipment, Version 1

Pending documents that are expected to be available the first quarter of 2010 include:

- Revision to 58-001: NENA IP-Capable PSAP Minimum Operational Requirements Standard, Issue 2, June 9, 2007
- 08-003 IP Functions and Interfaces (i3) Stage 3 Design
- NG9-1-1 PSAP Technical Requirements
- NG9-1-1 Security Standard
- Guidelines for Managing Policy Rules in NG9-1-1

Technical architecture requirements and standards are only the start to successful NG9-1-1 implementation. While such requirements and standards can enable production of equipment for NG9-1-1, the parallel standards for operation of databases that control system

[16] *See ICO NG9-1-1 Migration Plan* at 5-8 (Box 5-1).

[17] Information on ICE available at http://www.nena.org/ng9-1-1/ice.

[18] Available at http:/www.nena.org/standards-recommendations-information.

functions, and resolution of policy issues that limit the transition to NG9-1-1 are equally critical. Examples of these system operations/database standards that are currently being addressed, and are planned for completion in the first and second quarters of 2010, include:

- Building Policy Rules for Call Routing and Handling in NG9-1-1
- Human Machine Interface (HMI) Specifications for PSAP Equipment
- Guidelines for Managing NG9-1-1 Databases
- Error Management and Auditing for NG9-1-1 Databases
- Physical Systems Transition
- Service Transition Planning[19]

NG9-1-1 Equipment Development

Because NG9-1-1 is primarily an IP software and database controlled system, NG9-1-1 at the hardware level is largely customer-off-the-shelf ("COTS") equipment. Many of the call handling and data flow software components are being produced or finalized as of fourth quarter 2009, and examples from 16 vendors were recently tested for interface interoperability at the first NENA Industry Collaboration Event. This was a developmental testing event, and while a number of standards were used for reference, it was not a formal standards testing process. Future ICE events are expected to formally utilize NG9-1-1 standards as baselines.

The status of the related database systems that are critical to control of and successful use of the software components is less clear. Since the standards for these parts of the NG9-1-1 system necessarily trail the definition and design of the NG9-1-1 call handling software, so does the development of products that can be successfully utilized by public safety organizations. Most of these database-related and system operations standards and products for users in the 9-1-1 Authority and PSAP environments are not yet completed.

Roll out of IP-capable 9-1-1 system components are going on today, usually in a transitional layout, with full NG9-1-1 coming as transition and full standards convergence take

[19] Note that some of the working titles above will be modified as development work continues.

place over the next few years. Leading 9-1-1 network, CPE and applications providers are investing significant energy and resources into IP-based 9-1-1 technologies and services. These efforts are accelerating the transition to NG9-1-1 and helping to guide the NG9-1-1 standards and policy development process.

Regulatory Roadblocks

The ICO *National Plan for Migrating to IP-Enabled 9-1-1 Systems* accurately states that, "[a]s NG9-1-1 deployment begins, current roles and responsibilities among all entities involved in providing 9-1-1 services will change and the existing legal and regulatory environment will likely not effectively accommodate new technologies."[20] While a particular state or region may be prepared to transition to NG9-1-1, some state and/or local rules and regulations in their current form may not fully enable the transition. Many existing laws, regulations and tariffs specifically reference older technologies or system capabilities and consequently could be interpreted to prohibit the implementation or funding of IP-based 9-1-1 systems. At a minimum, current regulations and rules may raise questions about the legality of some capabilities enabled by NG9-1-1 which could slow progress unless such questions are addressed. For example, by statute, some jurisdictions only permit access to PSAPs via the telephone network – which may not be interpreted to include an IP network. Laws and regulations for 9-1-1 must be updated to be technology and competitively neutral, to facilitate 9-1-1 access for the communication devices already used by the public and those on the technological horizon.

During the transition to NG9-1-1, as state and local jurisdictions seek to implement IP-based 9-1-1 systems, rights and obligations are unclear for those companies that are providers of IP services and seek to provide complete systems or components of 9-1-1 systems. This

[20] *ICO NG9-1-1 Migration Plan* at pg. 1-3.

regulatory uncertainty applies both to state and federal statutes, regulations, and tariffs. While companies are in the initial stages of deploying IP systems in the states, with many issues being considered by state public utilities commissions, a lack of clarity on how federal interconnection statutes should be interpreted in a more competitive 9-1-1 environment is slowing the pace of IP-enabled E9-1-1 system deployment. This ultimately slows the pace of NG9-1-1 implementation.

For example, numerous state public utility commission,[21] at least one federal court,[22] and the FCC's own Wireline Competition Bureau[23] are each considering issues revolving around interpretations of existing interconnection laws (*e.g.* Sections 251 and 252 of the Communications Act[24]) and rules related to telecommunications in the context of emerging broadband-enabled IP-based 9-1-1 systems. While all regulatory classification issues for IP technologies in the larger communications law context may not be resolvable in the near future, a clarification of rules impacting the delivery of 9-1-1 and emergency services is needed in the near term.

---

[21] *Cf.*, In re: Petition by Intrado Communications, Inc. for arbitration of certain rates, terms, and conditions for interconnection and related arrangements with BellSouth Telecommunications, Inc. d/b/a AT&T Florida, pursuant to Section 252(b) of the Communications Act of 1934, as amended, and Sections 120.80(13), 120.57(1), 364.15, 364.16, 364.161, and 364.162, F.S., and Rule 28-106.201, F.A.C., Order No. PSC-08-0798-FOF-TP, Docket No. 070736-TP; Intrado Inc., Petition for Arbitration pursuant to Section 252(b) of the Communications Act of 1934, as amended, to establish an Interconnection Agreement with Verizon North, Inc. and Verizon South, Inc., Docket No. 08-0550; In the Matter of the Petition of Intrado Communications Inc., for Arbitration Pursuant to Section 252(b) of the Communications Act of 1934, as Amended to Establish an Interconnection Agreement with Verizon New England Inc. d/b/a Verizon Massachusetts; In the Matter of the Petition of Intrado Communications Inc. for Arbitration Pursuant to Section 252(b) of the Communications Act of 1934 as amended, to Establish an Interconnection Agreement with the Ohio Bell Telephone Company dba AT&T Ohio.

[22] The Ohio Bell Telephone Company d/b/a AT&T Ohio v. Public Utilities Commission of Ohio, Case No. 2:09-cv-918, Complaint for Declaratory and Injunctive Relief (U.S. District Court for the Southern District of Ohio, Eastern Division) (Oct. 15, 2009).

[23] WC Docket Nos. 08-33 and 08-185, "Comment Sought on Competitive Provision of 911 Service Presented by Consolidated Arbitration Proceedings" DA-09-1262 (June 4, 2009).

[24] 47 U.S.C. §§ 251-252.

This is especially the case in the context of NG9-1-1 because there will likely be a long transition period where NG9-1-1 systems need to interoperate with legacy telecommunications and 9-1-1 networks. In addition, unlike other areas of communications where the lack of clarity over regulatory treatment of certain services may only involve the resolution of largely financial matters, for 9-1-1 and emergency services such issues may impact whether these lifesaving services may even be deployable and available to meet the increased consumer needs and expectations associated with new IP broadband services.

To help promote the expedited and consistent deployment of NG9-1-1 systems, the FCC should address and resolve federal regulatory framework issues that include, but are not limited to, (1) interconnection responsibilities for legacy and new 9-1-1 system service providers, (2) the joint federal and state regulatory authority or appropriate division of federal and state regulatory authority associated with using IP-based NG9-1-1 systems, (3) whether and how, if at all, the transition to NG9-1-1 systems impacts other FCC rules and requirements associated with 9-1-1 emergency services; and (4) location determination and overall 9-1-1 requirements for all current and emerging systems that will need to be capable of connecting to 9-1-1 systems. These issues need to be resolved in a technological and competitively neutral manner. As we have previously urged, the FCC should put out for comment and adopt a comprehensive "local competition" type Order on 9-1-1 network services and IP-based E9-1-1 and NG9-1-1 systems[25]. Such an Order would provide support to state efforts to avoid unnecessarily continuing lengthy case-by-case disputes currently being debated in the states that are each largely based on an interpretation of federal interconnection rules.

---

[25] *See e.g.*, Comments of the Texas Commission on State Emergency Communications, the Texas 9-1-1 Alliance, the Texas Municipal Emergency Communication Districts Association, the National Emergency Number Association, and the Association of Public-Safety Communications Officials International, Inc. on the Competitive Provision of 9-1-1 Service, Docket Nos. 08-33 and 08-185, July 6, 2009.

Additionally, the Federal Communications Commission should examine its use of the term "wireline E9-1-1 network" as defined in section 9.3 of the Commission's rules.[26] It could be argued that this definition would not allow for the routing of 9-1-1 calls via an IP-based NG9-1-1 system. The Commission should clarify that wireless, VoIP, and other types of 9-1-1 calls/messages can be routed over NG9-1-1 systems that achieve the functions of the current wireline E9-1-1 network, or that such systems are included within the meaning of the term "wireline E9-1-1 network."

Automatic Location Identification

New forms of communications, from cell phones to Internet-based calling services to text messaging, have consistently forced public safety to adapt. Indeed, it is these very advances that have exposed some of the limitations in our 9-1-1 infrastructure, and have provided an impetus for NG9-1-1. Innovations are rapidly coming to market, such as femtocells,[27] dual-mode handsets,[28] softphones,[29] and devices not yet envisioned. As noted in the recent ICO *NG9-1-1 Migration Plan*, there is an increased demand for location services and technologies, yet at the same time, the decoupling of originating service providers from network operators will make the delivery of real-time, automatic location information more challenging.[30] For example, access to communications services such as instant messaging or VoIP (whether fixed, nomadic, or a

---

[26] 47 C.F.R. § 9.3 (Wireline E9-1-1 Network is defined as: "A dedicated wireline network that: (1) Is interconnected with but largely separate from the public switched telephone network; (2) Includes a selective router; and (3) Is utilized to route emergency calls and related information to PSAPs, designated statewide default answering points, appropriate local emergency authorities or other emergency answering points."

[27] Femtocell: Femtocells are in-home cellular access points that connect to a mobile operator's network using residential DSL or cable broadband connections. (source: Femto Forum)

[28] Dual-mode handset: a calling device with both cellular and WiFi (802.11x) capability. The device typically rolls over to the subscriber's WiFi network when in the home.

[29] Softphone: A software program for making telephone calls over the Internet from a general-purpose computer (including applications on wireless smart phones), rather than a dedicated calling device.

[30] ICO *NG9-1-1 Migration Plan* at 6-11.

mobile application) are network agnostic. As long as they are connected to an IP access network, the service can generate calls/messages. In this situation, the communications service/application provider has a direct connection to the calling/messaging consumer, but it is the separate network provider that is likely aware of the location of the device/application within the access network.

NENA points the Commission to the findings of the FCC's Network Reliability and Interoperability Council ("NRIC") VII Working Group 1B, which NENA fully supported. The Report articulated that location is critical to the E9-1-1 system, but newer technologies sometimes make it impractical for the entity providing communications services to know where the user is. The NRIC 1B final report advocated that every Access Infrastructure Provider (AIP), wireline or wireless, supply location information to endpoints. Specifically, the final report states, on page 29:

> "Where the AIP is the voice service provider, the information can be supplied directly. Where the AIP is not the voice service provider, but is the data provider (the "Internet Service Provider" or equivalent), it can supply endpoints with location, and the endpoints can provide this location on the call signaling when placing an emergency call. Where the AIP is neither the voice or data provider, it would need to have a relationship with the party who was, and can supply location data to that provider. Note that PSTN and wireless telephony providers would meet this requirement already."[31]

NG9-1-1 policymaking efforts and investment have largely focused on the infrastructure side of 9-1-1. Emphasis must also simultaneously be placed on the location determination and routing requirements of communications and applications providers whose services and applications enable the public to access 9-1-1. Within the current 9-1-1 system, there are services today that do not provide automatic location (e.g. interconnected VoIP services) and

[31] NRIC VII Focus Group 1B, Long Term Issues for Emergency/E9-1-1 Services, Report 4, at pg. 29, September, 2005. Available at http://www.nric.org/meetings/docs/meeting_20051019/NRICVII_FG1B_Report_September_2005.pdf.

there are new and emerging IP-based calling services for which the 9-1-1 location capabilities and requirements are unclear. Thus, such location determination and routing issues are not unique to NG9-1-1. However, NG makes it possible for more calling/messaging services and applications to connect to the 9-1-1 system and therefore increases the need to resolve location determination and routing issues.

It is a fundamental technical requirement of NG9-1-1 that the calling device or service must be aware of the caller's location for the call to be routed to the proper answering point. Therefore, it must be a policy objective to ensure all communications devices capable of accessing 9-1-1, or those in which the customer reasonably expects to be able to do so, can be automatically and accurately located. This is true for current devices/services and for new consumer communications platforms when they come to market.

As discussed above, originating service providers and access network providers have typically been one and the same, but this is no longer the case in many instances as communications devices[32] become more heterogeneous. In theory, any device with voice and data inputs and IP communications capability can become voice and data "calling" devices. The same device is likely able to have multiple location detection and routing capabilities depending on the network to which it is connected. Thus, devices (including applications downloaded on devices) will need to be able to determine or acquire their own location regardless of who provides the network connectivity. Similarly, network providers must be able to assist in enabling devices not uniquely designed for a specific network technology to acquire location and provide caller location information to 9-1-1 systems and public safety agencies. All of the issues above apply to current E9-1-1 systems and NG9-1-1 systems.

[32] As used in this filing, the term "devices" include a physical device and also separate software applications that are downloaded to the device that enable voice or data communications.

Consistent with the NRIC VII recommendations, NENA believes that all broadband networks must be configured to provide location to their client devices for use in placing emergency calls, regardless of what services the network provider offers, using consensus industry standards. All devices that may be capable of making emergency calls, or that allow applications on their devices that can separately make 9-1-1 calls, must implement similar consensus industry standards to supply location information with the calls. Further, since devices may be purchased anywhere in the world, and the services used to place calls may permit nomadic or roaming operation, the standards that such devices and services conform to must be international standards.

The Commission needs to address these issues to provide clarity as to the 9-1-1 location responsibility of the many types originating service providers, application providers, and network providers. A full record should be developed by the Commission taking into account policy considerations and technical challenges/limitations that impact the 9-1-1 capabilities and requirements of all providers of communications services, applications and networks. The results of such a process should make clear which services and applications are required to provide 9-1-1 service and what the different responsibilities are of service/application providers and network providers.

V. CYBER SECURITY

With the impending transition of traditional 9-1-1 systems to NG9-1-1, the need for comprehensive and robust cyber security countermeasures has never been greater. In the past, 9-1-1 systems have, for the most part, run on standalone networks which limited their threat vectors. Entry into the 9-1-1 system was limited to voice telephone calls. NG9-1-1 opens the door to allow numerous new devices and applications from multiple pathways to connect to the

9-1-1 system. In NG9-1-1 systems, entities are interconnected together with IP-enabled networks. This dramatically increases the scale and types of threats now facing the public safety industry. PSAPs will face traditional cyber security threats that include viruses, hackers, denials of services and many more. However, such threats are manageable.

NENA is committed to ensuring that 9-1-1 systems, and the entities operating systems and equipment on behalf of PSAPs, are secure during and after the transition to NG9-1-1. To that end, NENA has established a Security for NG9-1-1 Working Group specifically focused on addressing the important subject of cyber security within NG9-1-1 systems. The Security for NG9-1-1 Working Group is in the final stages of creating the industry's first comprehensive Cyber Security standards. These standards, known as Security for Next-Generation 9-1-1 (NG-SEC) will apply to all entities participating in NG9-1-1, including PSAPs, Computer Aided Dispatch (CAD) systems, customer premise equipment (CPE) and other 9-1-1 vendors, communications service providers, content providers and any other entity participating in NG9-1-1. These standards offer a means to achieve a specified level of security and will take a large step towards improving the overall cyber security posture of the industry—if adopted by all.

Further, NENA core NG9-1-1 IP functions and interface standards (i3) include stringent requirements for secure communications and access controls within public safety networks, and specify specific mechanisms for achieving them. NENA is concerned that the security mechanisms specified in its standards get implemented by vendors, and deployed by public safety agencies and their contractors. The FCC should encourage full implementation of these standards.

The 9-1-1 industry should immediately adopt the new NG-SEC cyber security standards when released and the i3 standard when NG9-1-1 is deployed. As appropriate, the standards should be included in future procurements and referenced in state and local laws/policies where applicable. Moreover, the FCC and other federal agencies should support and promote NENA's NG9-1-1 cyber security efforts. Additionally, the 9-1-1 industry faces a unique funding challenge with regard to successfully implementing the upcoming standards. Most PSAPs and other public safety entities have not traditionally had a need to budget for cyber security, but that is no longer the case for NG9-1-1 systems. Therefore, it is critical that the industry as a whole, including the federal government, consider cyber security as an eligible use of 9-1-1 funds.

The nation's 9-1-1 system has to be considered critical infrastructure, and is clearly a potential target for cyber attack. As we move from current 9-1-1 systems to NG9-1-1, we simultaneously open new possible attack vectors, and provide a much wider array of defenses against attack. While the present system is built on highly reliable telephone networks, the reality that the telephone network and the Internet are interconnected in many ways allows cyber attack on the present system, for which we do not have adequate defenses. Moving to NG91-1, while opening the door to bigger and more sophisticated attacks, does provide the opportunity to harden the 9-1-1 system against attack that we cannot do with the current networks. Rapid deployment of standards-based NG9-1-1 is critical to protecting the 9-1-1 system against attack.

As we can predict with certainty that the 9-1-1 system will be attacked, the nation needs a Community Emergency Response Team (CERT) specifically charged with monitoring and reacting to attacks on the 9-1-1 system. The FCC could facilitate creation and operation of it.

VI. BEYOND NG9-1-1: THE BROADER NEXT GENERATION EMERGENCY COMMUNICATIONS ENTERPRISE

Beyond the focus on NG9-1-1, the National Broadband Plan should call for a broad, multi-dimensional effort to deploy next generation emergency information and communications technology ("ICT"), starting with broadband access for all 9-1-1 and emergency response agencies, broadband backbone networks connecting them, and multiple services and applications enabled by such broadband access. The Commission's focus here on NG9-1-1 is welcomed. However, it is also important to recognize that IP-based broadband networks and applications increasingly make possible the integration of 9-1-1 and other emergency communications systems. Thus, technology convergence necessarily requires policymakers and public safety leaders to think holistically about the overall emergency response enterprise, rather than each of our individual domains.

In summary, for the overall 9-1-1 and emergency communications "enterprise", the Broadband Plan should:

- ensure that every agency involved in emergency response has appropriate broadband connectivity, ideally to shared state and regional backbone networks;
- ensure the establishment of secure, shared state and regional backbone emergency service IP networks (ESInets) for emergency response;
- ensure the establishment of a secure national "internetwork" backbone to provide the (mostly application layer) connections between state and regional backbone networks;
- adopt an "everything over Internet Protocol" and open architecture approach;
- focus on industry-based, open standards development and use;
- focus not just on individual agencies (the "end points"), but also on the "middle", the network-centric applications and core services (e.g. security, access control and data rights management) that can be accessed and utilized by all authorized public and private entities involved in emergency response;

- broaden the traditional "pipes" (communications transport) focus to broadband, and the focus on "pipes" to include attention to the Application (IP) Layers; and

- Encourage the development of new services and applications for emergency response enabled by access to broadband, particularly the provision of managed/hosted services and applications for 9-1-1 and emergency communications. For example encourage mapping and computer aided dispatch systems or records management systems that can be hosted in the network and shared by multiple agencies across a region.

In this regard, NENA was pleased to lead the formation of a new Next Generation Safety Consortium. The Consortium brings together national organizations involved in emergency response, academic institutions, government leaders, and technology partners in a broad, multi-dimensional effort to facilitate the deployment of next generation emergency ICT. The Consortium was formed to promote broadband access for all 9-1-1 and emergency response agencies, robust and secure broadband backbone networks connecting them, and the multiple services and applications enabled by such broadband access. More information is available at www.nextgensafety.org.

Effective emergency response and emergency healthcare delivery in the United States are products of the combined efforts of the public, emergency response organizations, non-governmental and academic institutions, the private sector, consumer and social service agencies and all levels of government (local, state, tribal and federal). Before, during and after an emergency of any magnitude, citizens depend on the coordinated efforts of all of these entities. Yet, each of these sectors has their own unique responsibilities, governance structures, information sharing policies and communications technologies. And each sector has thousands of independent entities, making intra and inter-sector information sharing difficult.

Organizational structures are in place today to manage the tactical mobile interoperability issues of first responders, primarily focused on voice communications. However, there is no

national organizational effort to address the shared ICT needs of each of these sectors to enable organization-to-organization information sharing. Thus, while significant effort has been devoted to the ICT needs of the endpoints in the chain of response (9-1-1, police, fire, EMS agencies, hospitals, etc.), there is currently a lack of focus in the middle, on the organizational and technological meeting points of all of these sectors and their member organizations – governance structure, information sharing policies, and shared technologies and services that enable the interconnection of all of these organizations.

Advancements in modern networks, services and applications offer a significant opportunity for the multitude of organizations involved in emergency response to "meet in the middle" through the use of standards and shared modern ICT. As communications technology advances, public and private organizations responsible for the delivery of emergency response in America must come together to understand and take advantage of this opportunity. A major national effort is needed to organize the shared use of technologies and services, increase organizational information sharing, and develop the shared governance structure to manage "the middle." The Next Generation Safety Consortium was formed to address these issues which should be addressed in the National Broadband Plan.

VII. CONCLUSION

In conclusion, NENA encourages the FCC to articulate in the National Broadband Plan that it is the policy of the United States to foster the migration from analog, voice-centric 9-1-1 and emergency communications systems into a broadband-enabled 21st century, IP-based emergency services model. NENA offers the recommendations above to assist the Commission in the development of recommendations to achieve this critical national policy objective.

Respectfully Submitted,

Brian Fontes
CEO
National Emergency Number Association
4350 North Fairfax Dr., Suite 750
Arlington, VA 22203
703-812-4600
703-812-4675 (fax)

November 12, 2009