AS PREPARED FOR DELIVERY

National Association of Counties
Annual Conference
2010

Remarks by
James Arden Barnett, Jr., Rear Admiral (ret.)
Chief of the Public Safety and Homeland Security Bureau
Federal Communications Commission

July 20, 2010

Reno-Sparks Convention Center
Reno/Washoe County, NV

Slide 1 - Introduction

Good morning and thank you for the invitation to speak to you today about the opportunities and challenges we face in helping local communities enhance public safety and security. This conference presents a great and timely opportunity to share with you the details of the FCC's plans for advancing public safety and homeland security through broadband technologies and innovations. Much of our effort is tied to the FCC's National Broadband Plan, which is the culmination of a comprehensive and open process that generated a substantial input from all sectors. These are important issues to the counties and communities you represent, and they are an important focus at the FCC as well. I feel particularly privileged to talk to you about the work we have been engaged in to establish a nationwide interoperable public safety wireless broadband network.

Slide 2 – Promote Public Safety (Bureau Overview)

As Chief of the Public Safety and Homeland Security Bureau, I am responsible for carrying out the Commission's public safety mission, focusing on the development of rapid, reliable, and ubiquitous communications technologies to promote public safety and homeland security. Created in 2006 following Hurricane Katrina, the Bureau focuses on areas such as broadband technologies, 9-1-1 services, interoperability, protecting communications infrastructure, cyber security, ensuring the availability of communications as part of emergency preparedness and disaster response, and outreach on communications issues to the public safety community. To accomplish these tasks, we work closely with the first responder community, including police, fire and emergency medical agencies; emergency operations centers; public safety answering points; hospitals; state, tribal, and local governments; and other Federal agencies.

We interact on a daily basis with public safety personnel that operate state, local, and tribal police, fire, and emergency medical radio systems. We also play a role in emergency preparedness and response. Partnering with FEMA, we deploy FCC staff in advance of or following disasters to assist with communications assessments and recovery.

Slide 3 - PSHSB Key Priorities

While we have made tremendous strides on a number of fronts, as we approach the ninth anniversary of 9/11, the nation is still challenged by many of the same interoperability issues that hampered emergency responders on that very tragic day. Multiple counties along the Gulf Coast are dealing with an epic environmental catastrophe that is pushing the limits of their communications systems and emergency personnel. All of these emergencies have highlighted that, despite expending billions of dollars and substantial man-hours public safety communications still face significant interoperability challenges, jeopardizing the ability of the public safety personnel to communicate during emergencies. Further, many first responders do not have access to the advanced data communications capabilities required to do their jobs effectively and efficiently. We know these are issues that concern you and your communities, and we are working daily to close this gap and ensure the availability of and utilization of 4G tools for public safety.

Slide 4 – National Broadband Plan

When the FCC unveiled its National Broadband Plan in March of this year, it recommended a comprehensive strategy to create a nationwide public safety broadband network which includes:

- An administrative system for ensuring that public safety users have sufficient capacity, coverage where they need it, and access to commercial technologies at reasonable rates;
- A request for public funding to support the network's construction and operation;
- The creation of an Emergency Response Interoperability Center (ERIC) to ensure nationwide interoperability and operability of the network;
- Recommendations for improving cyber-security and securing our nation's critical infrastructure; and
- Proposals for accelerating the development of Next-Generation 911, and for promoting next-generation alerting.

Slide 5 – Broadband Network Strategy

However, the envisioned network will not become a reality unless we embark on a comprehensive plan now. This includes public funding to construct a 4G broadband network that leaves behind no jurisdiction, from the most crowded urban street to the most rural road. This means timely action, and the ability to catch the technological wave as commercial networks are built. Without both of these components, America will not be able to afford a nationwide, interoperable public safety network. To achieve an interoperable network, we must start at the very inception of 4G technology. There is no time to waste.

After substantial written input from public safety and hundreds of meetings, telephone calls, workshops, technical forums and, of course, e-mails, the consensus was that a public safety broadband network must include the following attributes:

1. The network must be **nationwide**, providing coverage for public safety in all the locations where Americans live, work, and play, whether rural or urban, with the goal of at least 99% population coverage.

2. The network must be **interoperable**, functioning across geographies and public safety agencies. We must move away from the fragmented public safety networks that currently define the norm.

3. The network must be **viable and resilient,** having the required capacity and performance to support public safety reliably and dependably on a day-to-day and emergency basis, as well as provide contingencies for operations during the worst disasters.

4. The network and its devices must be **cost-effective** – it must be affordable for the Nation and for public safety to deploy, operate, utilize and upgrade.

5. And the network must be **technologically advanced**, exploiting the latest technology and having a clear path for technological evolution – a system easily upgradable without considerable expense. We cannot afford for public safety to be trapped in expensive, old technologies unable to adapt to the changing times.

This approach provides an achievable roadmap for deployment and operation of this system. It has been endorsed by public safety leaders, including the Chair and Vice Chair of the former 9/11 Commission. The public safety community has expressed agreement, in most respects, with the National Broadband Plan’s comprehensive concept for the public safety broadband network. There is broad consensus on the need for use ofLTE technology, on the need for priority access for public safety, and on the need for roaming onto commercial networks and other public safety networks.

We agree that the public safety network should not be an isolated technological island, but that it must continue to evolve as commercial technology improves. We agree that there must be public funding for the network to ensure that it is built, that it is hardened, that it is upgraded, that it works inside buildings and that it extends to rural areas. These are all significant points of consensus with the FCC’s approach, and reflect the fact that we have listened closely to the public safety community on these issues.

The only point of disagreement by the public safety community is the amount of spectrum that it will take to make the network fully functional – namely, the allocation to public safety of an additional 10 MHz of spectrum in the 700 MHz band known as the D Block.

Slide 6 – Public Safety Network & Solutions

Currently, 10 MHz of spectrum in the 700 MHz band is available exclusively for public safety broadband communications and provides a solid platform upon which to deploy a nationwide, interoperable public safety broadband network. In fact, the FCC's study has shown that it will provide public safety with more than adequate capacity and performance required to support day-to-day and most emergency communications.

The D Block has been slated by Congress for commercial sale through an auction. The FCC believes that, by auctioning this spectrum and encouraging flexible, incentive-based partnerships between public safety and the network provider of its choice, we can reduce costs on the part of commercial operators while providing public safety users the ability to roam on, as well as priority access to, commercial networks within the 700 MHz band.

The groups within the public safety sector arguing that Congress should reallocate the D Block to public safety believe that 10 MHz of spectrum will not be enough to accommodate the needs of public safety's day-to-day operations, particularly in the event of a national catastrophe.

If the D block is reallocated and combined with the current public safety broadband spectrum, equipment costs will skyrocket no matter whom public safety selects as a partner. Additionally, projected savings for state, local and tribal governments will not be realized because significant cost-efficiencies will have been squandered. If this occurs, the mere expense of the network and user devices will make it extremely unlikely network will ever reach rural or even suburban areas. These areas will again be left behind.

FCC engineers, experts, and technical staff have spent countless hours performing engineering analyses to validate whether the 10 MHz of dedicated public safety spectrum will, indeed, provide more than adequate capacity and performance. Last month, we released a White Paper detailing this analysis, examining two real-life, large-scale emergencies and empirical data collected and analyzed by FCC staff. It demonstrates that allowing public safety to build out their broadband network on the 10 MHz of currently dedicated spectrum sufficiently supports these critical communications requirements.

When analyzing capacity, an important point to keep in mind is that spectrum does not equal capacity. Network capacity and performance are affected by spectrum, but other important "factors include the type of architecture employed, the number of cell sites in operation, the number of sectors per cell, sound network and spectrum management, and the specific technology that the network utilizes." By deploying advanced, 4G wireless technologies and cellular network architecture, public safety can achieve much greater capacity than they have achieved in the past. To state this more starkly, a study conducted by the FCC's Chief Technologist demonstrated that 10 megahertz of capacity on a cellular network would be the equivalent of 160 megahertz on a narrowband, Land Mobile Radio-type network. We must escape the mindset of evaluating the promise of new technologies based upon the limitations of old technologies. Our plan ensures that adequate capacity is afforded public safety and that scarce, valuable spectrum will be used efficiently.

However, we must plan for the major disasters and emergencies that will surely come and that will challenge the public safety spectrum. The National Broadband Plan recommended a smart, innovative approach: requiring commercial operators across the 700 MHz band, and possibly other bands, to provide public safety with roaming and priority access for public safety on their networks at reasonable rates in those times of critical need. This means that public safety would have access to 60 MHz or more of additional spectrum – far more then the 10 MHz of spectrum available in the D block.

Slide 7 – Funding

As I mentioned earlier, spectrum is not the only issue at stake. Make no mistake - there will not be a nationwide interoperable public safety network without funding. We believe the most economically and physically efficient way of rolling out new technology would be to capitalize on the efforts of commercial carriers, who are already deploying upgrades to their own infrastructures. It would save nearly $9 billion for the construction of the network, and potentially tens of billions in savings in operating costs. The network simply becomes unaffordable if we do not seize this leveraging opportunity now.

We know that reliance on basic commercial networks will not meet public safety's specific needs for network reliability, resiliency, and coverage in remote areas where commercial providers are unlikely to build. Therefore, we propose specific public funding to ensure public safety's requirements are met. Our plan includes:

- Approximately $6.5 billion for capital expenditures over ten years, to be funded through direct federal grants to public safety, which would support hardening of the network to public safety standards.

- $6-10 billion over ten years for operating costs, which ramp up as the network expands to a peak of $1.3 billion per year.

Of course, this element of our plan requires action by Congress – and I understand that many of you at the county level are concerned with securing Congressional resources to support broadband grant and loan funding, specifically bills that could reduce funding in the Broadband Technology Opportunities Program (BTOP) and the Broadband Initiatives Program (BIP). I don't need to tell you that this is a difficult time to ask Congress for funding. But right now we have a unique opportunity to catch a technological wave that actually reduces the public cost of this network over the long run. Missing this window could increase construction and operating costs to a combined $35-$48 billion over ten years, and deployment could be prolonged from a projected 10 years to 20-25 years – or perhaps never occur.

The public safety groups which advocate reallocation claim that they would be able to generate the funding by subleasing the excess capacity on the D Block to non-public safety entities, but no business model has been presented supporting this plan, particularly for rural areas. If the D block is reallocated, the public safety network likely will not reach rural America or smaller cities that cannot afford to build a broadband network.

Furthermore, ten megahertz of additional spectrum allocated to public safety cannot provide public safety with the capacity it may require in the very worst emergencies. We believe that there are other ways to increase capacity, for example, by building supplemental infrastructure to expand available capacity. Commercial and residential buildings, where a substantial amount of cellular network traffic originates, could be upgraded with picocells and femtocells to improve coverage and offload traffic from external cell towers. Similarly, capacity can be further expanded by using deployable communications systems, such as next generation cell sites on wheels and vehicular relays, as is frequently done with today's wireless technologies during disasters and major incidents or events. In fact, the NBP recommends deployment of these technologies for public safety broadband use, through a program that would help fund caches of equipment throughout the country that can be rapidly deployed to the site of any major disaster. These approaches decrease strains on the available cell site infrastructure.

Slide 8 - ERIC

A critical requirement for this network is to ensure that it is interoperable. In April of this year we took a dramatic step forward to ensure interoperability when the FCC established the Emergency Response Interoperability Center or ERIC within the Bureau. ERIC's mission is to develop technical requirements to ensure that the 700 MHz public safety broadband wireless network will be fully operable and interoperable on a nationwide basis, both day-to-day as well as during times of emergency. In May, we established a technical advisory committee to ERIC made up of a diverse group of state and local public safety officials from around the country. This committee is instrumental in working with ERIC to develop an effective interoperability regime for the public safety broadband network.

The impact of ERIC is already being seen as we move forward to ensure the expeditious deployment of this critical network on an interoperable basis. In May, the Commission conditionally granted 21 waiver petitions for early deployment of statewide, countywide and local public safety broadband networks. Working closely with ERIC, our Federal partners, and the Public Safety Spectrum Trust, these waivers represent an important and timely initial step that will allow public safety to capitalize on 4G deployments. In these initial grants, the FCC adopted baseline requirements as a first step towards to ensure day-one interoperability of the public safety broadband network wherever it is deployed. ERIC will be responsible for evaluating the interoperability showings required of the waiver recipients, which will then be instrumental as the FCC adopts its final technical rules.

While we still have work to do, we believe these systems will jumpstart the Commission’s broadband and interoperability goals.

As the establishment of ERIC and our recent actions on the waiver petitions demonstrate, the FCC is committed to ensuring that as deployment begins on this network, interoperability is fully achieved.

Slide 9 – E911 and Next Generation Services

On another very important public safety note, one of the FCC's goals is ensuring that all Americans can access 9-1-1, regardless of the technology they use to place the call. In the coming months we will be examining our rules as they relate to the geographic area over which wireless carriers should comply with the Commission's location accuracy requirements. As more people rely on wireless service as their primary means of communication, it is increasingly important that wireless users not only have access to 9-1-1, but also that first responders receive automatic and accurate information to identify the caller's location. There is certainly an expectation among the public that a 9-1-1 call taker should have a good idea of the location of a 9-1-1 caller so that first responders can be directed to the correct place. In light of today's technological advances, this is a reasonable expectation and one we take very seriously. Related to that is deterring fraudulent and harassing 9-1-1 calls made from nonservice initialized phones. These calls disrupt 9-1-1 service and waste precious public safety resources, which should be devoted to true emergencies, and we are examining technical and legal remedies to this problem.

Now I want to turn to some exciting recommendations concerning Next Generation 9-1-1 from the National Broadband Plan. The nation's 9-1-1 system is evolving toward supporting NG9-1-1, an IP-based platform integrating the core functions and capabilities of E9-1-1 while adding new 9-1-1 capabilities, such as texting, photos, video, and e-mail. The FCC's National Broadband Plan includes specific recommendations on how to encourage the timely deployment of NG9-1-1. The plan recognized that we need to analyze the costs involved for deploying NG9-1-1 across the nation and recommended that the National Highway Traffic Safety Administration (NHTSA) prepare a report to identify them, including a technical analysis and cost study of different delivery platforms, and an assessment of the characteristics, feasibility and limitations of NG9-1-1 delivery. Further, the NBP recommended that the report address the current state of NG9-1-1 readiness among PSAPs and how differences in PSAPs' access to broadband across the country may affect costs. This report could serve as a resource for

Congress as it considers creating a coordinated, long-term funding mechanism for NG9-1-1 deployment and operation.

The NBP also recognized that federal and state regulations that focus on legacy 9-1-1 systems have hampered NG9-1-1 deployment, such as existing laws, regulations, and tariffs that reference older technologies, which could be interpreted to prohibit the implementation or funding of IP-based 9-1-1 systems. The plan recommended the enactment of a federal NG9-1-1 regulatory framework to remove jurisdictional barriers and inconsistent legacy regulations. Without such a comprehensive framework, it is unlikely that your counties will be able to take advantage of the benefits of NG9-1-1 in the near future.

Slide 10 – Cyber Security

Advanced broadband communications technologies have dramatically changed the lives of Americans and others around the globe by enriching the way they communicate and receive information. As we move towards the broadband and IP-based NG9-1-1 architecture I have outlined today, we need to remain wary of the potential cyber-related threats that could impact communications from the public to PSAPs, the PSAPs themselves, and Next Generation 9-1-1 networks. The impact of such cyber breaches could cripple county operations; accordingly, the National Broadband Plan recommended a number of steps to help advance cyber security.

Our first recommendation is for the FCC, in coordination with the Executive Branch, to identify and develop a roadmap for confronting our nation's five most pressing cyber security threats to the communications infrastructure and its users. The roadmap should establish a two-year plan, with milestones for the FCC to address each threat.

The Plan also recommends that the Commission examine extending the FCC's current outage reporting requirements to broadband Internet Service Providers and interconnected VoIP providers, in order to improve our understanding of broadband service outages, how to respond to them when they occur, and how to prevent them in the future. In addition, the Plan also recommends establishing a voluntary cyber security certification program that would create market incentives for communications service providers to implement a full range of cyber security best practices. A Notice of Inquiry has already been released on this issue, and we look forward to the responses we will receive on this very important topic.

On critical infrastructure survivability, the plan recommends two inquiry proceedings, one to address network preparedness and resilience, the other to address standards for reliability and resiliency of broadband communications. The Plan also recommends the creation of a priority network access and routing system for broadband communications of a national security and emergency preparedness nature.

Slide 11 – Alerting

Finally, it is absolutely critical that the public has access to timely and accurate emergency alerts and warnings about impending disasters and other emergencies. The public relies on a multitude of communications technologies in their daily lives, from radio and television to cell phones and other wireless devices, and increasingly, the Internet and other broadband technologies. A comprehensive alerting system that utilizes these multiple communications technologies will have the ability to reach more people more quickly and effectively than ever before.

One system with which I'm sure you are familiar is the Emergency Alert System (EAS), the national public warning system that requires broadcasters, cable television systems and others to allow the President to address the American public during a national emergency. As you are aware, the system is also used by state and local authorities to deliver important local emergency information, such as AMBER alerts and weather information targeted to specific areas. Federal and state governments thus share an interest in ensuring that the EAS infrastructure functions correctly, and fully utilizes the resources of our modern, digital communications technologies. Accordingly, over the next few months, the Commission, along with FEMA, will initiate an outreach effort to coordinate the “first-ever” national test of the EAS. As our outreach plan unfolds, we will be reaching out to you as a partner.

Another system with which you probably are not as familiar is the Commercial Mobile Alerting System (CMAS), the first iteration of a next generation alerting platform making use of the new Common Alerting Protocol, or CAP. CAP is an alerting standard that will allow authorized federal, state and local officials to distribute alerts over an ever-increasing variety of networks, provide greater flexibility with regard to content, and allow for greater precision in targeting messages to specific geographic areas. Consumers will not have to sign-up for these alerts, they will automatically receive them so that they are aware of a regional or large-scale event or situation that could potentially impact them.

The CMAS will supplement the EAS by allowing wireless service providers to send emergency alerts to their subscribers. FEMA will accept and aggregate CMAS alerts from the President of the United States, the National Weather Service, and state and local emergency operations centers, and then send the alerts over a secure interface to participating wireless providers, who in turn will distribute text alerts to their subscribers. In December, 2009, the FCC initiated the 28-month period during which participating Commercial Mobile Service providers must develop, test and, by April 7, 2012, deploy the CMAS. We are very excited about the possibilities and the lives we know will be saved because of this technology.

Broadband has the potential to greatly expand the capabilities of these and future warning systems' capabilities, and the Commission is taking two important steps to facilitate the development of a broadband-based "Next Generation" alert and warning system. First, FEMA will be adopting CAP as part of its Integrated Public Alert and Warning System (IPAWS), and the Commission is seeking comment on how the introduction of CAP will affect our current EAS rules. Second, the Commission will be initiating a Notice of Inquiry on the development of a next generation, broadband-based alerting system. We welcome your input on both of these important issues.

Slide 12 – Closing Remarks/Questions

In closing, let me say that you are witnessing a very exciting year for public safety. The public safety elements of the National Broadband Plan, and the proceedings and FCC actions to follow, will lead to great strides in improving counties' ability to save lives and property. We appreciate all that you do and look forward to working with NACo and other public safety partners in the years to come. Again, thank you for having me here today. I am very happy to take any questions you may have.