AS PREPARED FOR DELIVERY

James Arden Barnett, Jr., Rear Admiral (Ret.)
Chief, Public Safety & Homeland Security Bureau
Federal Communications Commission

New Mexico
Public Forum
Statewide Public Safety Communications

November 15, 2010
10:00 am-11:00 am

SLIDE #1

Good morning and thank you for the invitation to speak to you today about the opportunities and challenges we face in enhancing and promoting public safety and security. This meeting is a great and timely opportunity to share with you some information on the FCC's plans for advancing public safety and homeland security by improving the communications capabilities of the country's first responders. Much of our effort as of late 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. The issues in the NBP are important issues to New Mexico and in fact every state in the Union. Therefore, they are an important focus of the FCC, specifically the Public Safety and Homeland Security Bureau.

I feel particularly privileged to talk to you about our ongoing work to establish a nationwide interoperable public safety wireless broadband network and other critical areas, including cyber security and promoting next generation and wireless Enhanced 911.

SLIDE #2

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.

While we have made tremendous strides on a number of fronts, the nation is still challenged by many of the same communications interoperability issues that have hampered emergency responders for years. The terrorist attacks on 9/11, and the hurricanes, flooding and ice storms we see every year continue to highlight that, despite expending billions of dollars and substantial man-hours, public safety communications still face significant interoperability challenges that severely jeopardize 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 efficiently and effectively. We know these are issues of concern to New Mexico and in fact the entire country, and we are working daily to close this gap and ensure the availability of and utilization of 4G tools for public safety.

Moving toward a 4G world means that you and I will be able to utilize fast, efficient broadband technologies in even more amazing ways than we’re used to, and many of those technologies will help make our lives easier and safer. Just look at how smart phones, iPads, and other “smart” technologies have already changed our lives. We can now be in touch with anyone virtually anywhere in a matter of seconds whether via voice, text or e-mail. We can send videos and photos from our phones; watch our children via the web as they play in daycare; and monitor our home alarm system, just to name a few. Today, there aren’t many things about which you can’t say “Yes, there’s an app for that!”

In that same vein, broadband technologies can assist public safety entities as they coordinate response efforts—often with other jurisdictions and disciplines—and share mission-critical information. They can assist the public when 9-1-1 calls are made to report crimes in progress or seek help for medical emergencies and can play a tremendous role in improving the way federal, state and local governments use alerting systems to reach the public in times of peril. In each of these areas, broadband technologies can improve communications and, ultimately, save lives.

SLIDE #3

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 recommendations for:

- An administrative system for ensuring that public safety users have sufficient capacity and coverage where they need it and access to commercial technologies at consumer equipment prices;

- 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.

SLIDE #4

After substantial input from public safety, industry, policy leaders and the public, 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. 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 of LTE technology, on the need for priority access for public safety and on the need for roaming onto commercial networks and other public safety networks.

SLIDE #5

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.

Another point of agreement is our shared belief that public safety agencies should be able to reap the full benefits of the spectrum allocated to them for the broadband network. Accordingly, the Plan recommended that public safety agencies have the opportunity to lease their spectrum on a secondary basis to utility companies and perhaps other user groups. My staff and I are in the process of examining the details of this recommendation, including its possible legal implications, but we recognize that this could provide public safety with a promising revenue stream to support the ongoing operation and evolution of their network.

And while we have had a differing opinion as to the amount of spectrum that should be allocated for the network, these areas of agreement form a solid foundation upon which the Commission and the public safety community can build.

SLIDE #6

One example of the work PSHSB is doing to meet the goal of creating a nationwide public safety network is the development of an Emergency Response Interoperability Center or “ERIC” which I mentioned earlier. ERIC was created earlier this year to establish a technical and operational framework that will ensure nationwide operability and interoperability in deployment and operation of the 700 MHz public safety broadband wireless network. ERIC will adopt, implement, and coordinate interoperability regulations, license requirements, grant conditions and technical standards. While the FCC leads ERIC, we are all about teamwork. To that end, the Department of Homeland Security and the National Institute of Standards and Technology will contribute to ERIC's functions. In addition, a Technical Advisory Committee for ERIC is already in place and a Public Safety Advisory Committee is currently being established.

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. As you may be aware, in May, the Commission conditionally granted 21 waiver petitions for early deployment of statewide, countywide and local public safety broadband networks, including in New Mexico. Working closely with ERIC, our Federal partners and the Public Safety Spectrum Trust, these waivers represent an important initial step that will allow public safety to capitalize on 4G deployments. More recently, we placed on public notice the additional waiver requests we have received since May. We received a number of substantive comments on these requests, including from New Mexico, and we are in the process of examining these comments as we determine how to handle this influx of requests.

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. Today we are working on final interoperability rules and we would appreciate your input.

SLIDE #7

Clearly, there will not be a nationwide interoperable public safety network without funding. Therefore, we proposed public funding to ensure public safety's requirements are met. Our leveraged cost model 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 – I don't need to tell you that this is a difficult time to ask Congress for funding. We applaud NTIA for its award of BTOP funding to seven waiver recipients, including the State of New Mexico, although we maintain that a much larger investment is needed to make this nationwide network a reality. 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.

Ensuring funding for innovative means to enhance coverage and capacity are also a vital part of the plan. For example, commercial and residential buildings, where a substantial amount of cellular network traffic originates, could be upgraded with pico-cells and femto-cells 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

In addition to the many broadband initiatives we are working on related to public safety, we are also focusing on other public safety related issues such as 9-1-1 and Next Generation 9-1-1. As you are aware, 9-1-1 can be a life-saving tool when someone is in need of assistance. Therefore, 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. This past September the Commission adopted new rules establishing timelines and benchmarks for wireless carriers to provide more granular E9-1-1 location information at either a county-based or PSAP-based geographic level. The Commission also adopted a Further Notice of Proposed Rulemaking and Notice of Inquiry seeking to improve E9-1-1 location accuracy and reliability for existing and new voice communications technologies, including Voice over Internet Protocol and, consistent with the National Broadband Plan, to understand the ways in which voice communications enabled by broadband and next generation 9-1-1 technologies could support enhanced first response.

As more people rely on wireless service as their primary means of communication, it is increasingly important not only that wireless users 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 and on September 23, 2010 a Further Notice of Proposed Rulemaking/Notice of Inquiry was adopted to explore NG 9-1-1's impact on wireless location accuracy requirements.

Another 9-1-1 related proceeding at the Commission concerns the issue of fraudulent and harassing 9-1-1 calls from non-service initialized phones. We are very concerned that harassing and fraudulent 9-1-1 calls from non-service initialized phones continue to be a serious problem for 9-1-1 call centers. These calls disrupt 9-1-1 service and waste precious public safety resources, which should be devoted to true emergencies. The Commission previously issued a

Notice of Inquiry on this matter, and we plan to release a Notice of Proposed Rulemaking in the near future.

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. In the September NPRM, the Commission initiated a Notice of Inquiry to explore how public expectations may evolve as new broadband and IP-based communications, devices, applications and technologies develop, and how deployment of NG 9-1-1 can meet those expectations and accommodate new forms of communications.

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 certain 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 you will be able to take advantage of the benefits of NG9-1-1 in the near future.

SLIDE #9

As we move towards the broadband and IP-based NG9-1-1 architecture I have discussed today, we need to remain wary of the potential cyber-related threats that could severely disrupt public safety communications and impair emergency response. 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.

Since June, we have met with multiple stakeholders to help us understand cyber security risks and identify threats that the FCC should consider. In addition, we are also establishing a two-year plan, including milestones, for the FCC to address these threats. Our goal is to have this plan completed later this year.

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. A Public Notice has been released on this issue. 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 been released on this issue and we welcome your input 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. A Notice of Inquiry for the first of these has already been issued. 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. Please consider giving us your input on this NOI as network preparedness and resilience are extremely important issues for your states and the country as a whole.

SLIDE #10

On another note, when we talk about national security and emergency preparedness, we can't help but think of disaster preparedness and emergency response. The Bureau is very much focused on these issues. For example, this year for Hurricanes Alex and Earl the Bureau deployed its spectrum mapping Roll Call team to help FEMA identify whether key public safety communications facilities remained operational after the storms passed. The Roll Call team conducted spectrum surveys before the storms hit and compared the data collected with the information on stations operating after the storms made landfall. On a full-time basis, we station two Roll Call units and operators in Florida and Texas, and we keep two other units on alert status at FCC Headquarters for deployment to other parts of the country.

The Bureau is also engaged in Federal interagency response and recovery program called Emergency Support Function # 2—Communications, which falls under the auspices of DHS FEMA and the National Communications System. Under ESF # 2, the FCC deploys skilled personnel to FEMA field installations to assist with recovery and restoration efforts for critical communications infrastructure. Working closely with the communications sector, we identify needs and requirements such as fuel, security, access, and we work with the communications industry to get service restored as quickly and efficiently as possible.

During emergencies, at Commission Headquarters, we stand up an Incident Management Team comprising several FCC Bureaus and Offices responsible for licensing, consumer and disabilities issues, spectrum coordination, and public safety matters just to name a few. This Team is capable of operating on a 24-hour basis and is able to reach out to the all FCC Bureaus and Offices for additional resources. We have found that this approach leads to rapid operational and policy decision making, which, in turn, lead to more effective and efficient recovery and restoration in the field.

SLIDE #11

We are also working on some other public safety communications issues in which FCC involvement may not be as obvious or intuitive. One of those major issues is contraband cell phone use in our nation’s prisons and it is a significant problem. I appreciate that some prison administrators desire to use cell jammers as a means to combat the serious problems they face with prisoners using cell phones to conduct criminal activities, including threatening government officials and the public, and even to carry out serious offenses including murder. However, simply stated, today, cell phone jammers are illegal in the United States. It is illegal to manufacture, import, sell, offer for sale, operate or use devices designed to prevent, jam or interfere with the operation of cell phones. The Communications Act of 1934, as amended, and the FCC’s rules prohibit the manufacture, importation, marketing, sale or operation of these devices within the United States. The legal citations are Section 302(b) of the Communications Act, and Section 2.803(a) of the FCC's rules. In addition, under Section 333 of the Act, it is unlawful for any person to willfully or maliciously interfere with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government. Further, Section 301 of the Act requires persons operating or using radio transmitters to be licensed or authorized under the Commission's rules.

Parties violating the provisions of the Communications Act and/or FCC rules mentioned above may be subject to the penalties set forth in 47 U.S.C. §§ 501-510. Monetary forfeitures for a first offense can be as much as $11,000 a day for each violation and could subject the offender to criminal prosecution. Equipment may also be seized by the United States Marshals and forfeited to the U.S. Government. So while on its face, cell jamming technology seems like a simple, logical answer to a very complicated question, it is not. We have been working closely with two states, Maryland and Mississippi, the Federal Bureau of Prisons and the National Telecommunications and Information Administration (NTIA) and the National Institute of Justice (NIJ) as they work to develop creative solutions to this problem.

In 2009, the United States Senate passed a bill that would permit a correctional facility to operate a system to prevent, jam, or otherwise interfere with unauthorized wireless communications by prisoners. Later in 2009, Congress tasked NTIA, in coordination with the Federal Communications Commission, the Federal Bureau of Prisons (FBOP), and NIJ, with developing a plan to investigate and evaluate how wireless jamming, detection, and other technologies might be used for law enforcement and corrections applications in Federal and state prison facilities. Congress asked that the plan consider the adverse effects that these technologies impose on commercial wireless and public safety communications services in areas surrounding the prisons. Congress is showing true leadership in this area, and I am pleased that we can build upon our strong and collaborative relationship with NTIA by consulting further on this matter.

The newest product of this collaboration is NTIA's recent Notice of Inquiry on preventing contraband cell phone use in prisons, which was drafted in response to this legislation. This was another great opportunity for the FCC to work with NTIA, FBOP, and NIJ in developing this document, and I believe that the NOI serves as an excellent platform for not only accomplishing Congress's goals, but for leading the way for a collaborative federal effort to resolve the difficult and serious problem associated with contraband cell phone use in prisons. I support the approach of the NOI to explore three categories of cell phone intervention – managed network access, detection, and cell jamming.

This approach permits a straight-forward way to compare and contrast the effectiveness and potential drawbacks of each technology category. There are many intricate and interdependent issues involved, including technical efficacy and adaptability, legal considerations, relative costs, interference concerns, preserving legitimate consumer, public safety, and 911 wireless communications, and avoiding unintended and harmful consequences. The NOI evoked a rich public dialogue, with comments submitted by managers of correctional institutions, manufacturers, prison employees, and interested members of the public, to name a few. I look forward to our continued work with NTIA, NIJ and the Federal Bureau of Prisons as we evaluate the comments and develop the plan Congress requested.

We are looking at the technologies currently available to combat this problem including cell-jamming and another technology known as managed-access. We believe we have a straight-forward way to compare and contrast the effectiveness and potential drawbacks of each technology category. There are many intricate and interdependent issues involved, including technical efficacy and adaptability, legal considerations, relative costs, interference concerns, preserving legitimate consumer, public safety, and 911 wireless communications, and avoiding unintended and harmful consequences.

We still don't know the right answer or combination of answers. In the meantime, know that we understand the issues and the urgency and that we are working with all interested parties to find a workable solution.

SLIDE #12

One last issue I'd like to mention because the deadline is quickly approaching is VHF/UHF Narrowbanding. Narrowbanding is the migration of certain VHF and UHF channels to narrower bandwidths by January 1, 2013 to increase spectrum efficiency and to free additional channel capacity within these bands. These deadlines have been in place since 2004 and have been consistently supported by public safety organizations because of the need to obtain additional channel capacity for first responders in the Private Land Mobile Radio (PLMR) bands.

The Commission recently adopted two orders that will simplify the narrowbanding process. In March 2010, the FCC eased the requirements for licensees who narrowband their systems to avoid costs and administrative burden of unnecessary frequency coordination. In June 2010, the Commission allowed PLMR licensees to continue to obtain wideband-capable equipment for their existing systems until January 1, 2013, making it easier to manage the transition. These orders further promote spectrum efficiency so that more public safety and non-public safety users may utilize these frequencies.

If you are currently in the narrowbanding process (or if you need to be but haven’t started yet) I encourage you to continue moving forward. The 2013 deadline is very important, and the Commission will be looking at any waiver applications with a very strict eye. With that said we are here to help you with any issues that arise, so if you have problems or concerns in this area, please contact our bureau soon. We will do all we can to assist you and answer any questions you have.

SLIDE #13

I have covered a lot of ground here today, and I hope you know how much I appreciate your attention and interest in these very important matters. I am happy to take any questions you may have.