Statement of
James Arden Barnett, Jr.
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Legislative Hearing on the Public Safety Broadband Network and H.R. 4829

Before the
Subcommittee on Communications, Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives

June 17, 2010

Good morning Chairman Boucher, Ranking Member Stearns, and Members of the Subcommittee. I appreciate this opportunity to appear before you today on this issue of significant national importance. We must work together to ensure that our law enforcement officers, firefighters, emergency medical personnel and other public safety officials have a nationwide, truly interoperable broadband wireless network, and it is critically important that we do so now. Unfortunately, the costs of not having a nationwide, interoperable public safety network can often be measured in lost American lives. I welcome your input and look forward to working with you and the public safety community to ensure that this system is deployed and operable as quickly as possible so public safety can receive the benefits of state-of-the-art nationwide interoperable broadband communications and the American people may be afforded the safety and security to which they are entitled.

The Navy transferred me to Washington, D.C. in October, 2001, when there was still a gaping hole in the Pentagon. We are facing the ninth anniversary of 9/11, and yet the nation is still plagued by many of the same interoperability problems that hampered emergency responders on that very tragic day. Since then, America has suffered Hurricanes Katrina, Ike and Gustav, as well as other storms where interoperability was a factor in the aftermath of the storm.

Even as the armada of oil approached our shores, it took Herculean effort to link the land mobile radio systems of the Gulf Coast states so that they could coordinate the efforts of their public safety officers. All of these emergencies have highlighted that, despite significant funding in the billions of dollars, and energetic efforts, public safety communications still face significant interoperability challenges, jeopardizing the ability of the public safety personnel to communicate during emergencies. Further, first responders do not have access to the advanced data communications capabilities they require to do their job.

However, for a brief moment in time, a solution is readily within reach. We, as a nation, have the opportunity of a lifetime to ensure that public safety has a nationwide *interoperable* public safety broadband wireless network. But this vital national asset will not become available to future generations, even the next generation, unless we act now. Unless we embark on a comprehensive plan now, including public funding, to construct a 4G broadband network that reaches at least 99% of the population, from the most crowded urban street to the most rural road, catching the technological wave as commercial networks are built, America will not be able to afford a nationwide, interoperable public safety network. There is nothing that is inevitable about having in nationwide, interoperable system. Indeed, the last seventy-five years of public safety communications teaches us that there are no natural or market forces or incentives which create interoperability. To achieve an interoperable network, we must start at this very inception of 4G technology, and we must aggressively pursue a comprehensive, well-reasoned and well-researched plan.

The approach that the FCC recommended in the National Broadband Plan, which was developed with the significant public safety input outlined in Appendix A, provides a realistic, achievable roadmap to successful deployment and operation of this system. I would like to

emphasize to the Sub-Committee that the public safety community has expressed agreement, in most respects, with the National Broadband Plan's comprehensive concept for the public safety broadband network[1]. There is broad agreement on the need for the new LTE technology, on priority access for public safety, on roaming onto commercial networks and other public safety networks, with the recognition that those details have to be worked out. There is general agreement on the need for an emergency response interoperability center, whose main function is to ensure interoperability across the network. Public safety generally agrees with the plan that the FCC should require the development of devices that "see" the relevant bands, and that we should pursue policies and rules that will reinforce the opportunity for public safety to obtain devices at nearly consumer priced electronics costs.

We agree that the public safety network should not be an isolated technological island, but that it continues to evolve and upgrade as commercial technology improvements are made. Public safety agrees that there needs to be public funding for the network to ensure that it is built, that it is hardened, that it works inside buildings and that it extends to rural areas. These are all significant points of agreement with the FCC approach, and reflect the fact that we have listened closely to the public safety community and solicited its information and requirements. The only major point of disagreement by the public safety community of which I am aware is the amount of spectrum that it will take to make the network fully functional. In other words, most of the public safety community would like the 10 MHz of the D Block added to the 24 MHz of

[1] Robert LeGrande II, Association of Public-Safety Communications Officials, Presentation at Federal Communications Commission's Public Safety and Homeland Security Bureau's Technical Panel on a 700 MHz Nationwide Interoperable Public Safety Broadband Network (Mar. 17, 2010). The presentation is available at http://www.fcc.gov/pshs/docs/public-safety-spectrum/031710/LeGrandeAPCO-Open-meeting-Presentation-031710.pdf.

spectrum already dedicated to public safety in the 700 MHz band. (Although, it bears noting, some in the public safety community have spoken in favor of auctioning the D Block.[2])

In addition to broad agreement with public safety, the FCC's recommended approach has been expressly endorsed by the leaders of the former 9/11 Commission, who stated that "the 9/11 Commission on which we served concluded that the absence of interoperable communications capabilities among public safety organizations at the local, state and federal levels was a problem of the highest order. . . . The FCC's plan offers a realistic framework to move forward."[3] This is what we must do if we ever want to solve the 9/11 interoperability problem.

After much written input from public safety and hundreds of meetings, telephone calls, workshops, technical forums and of course, emails, these are the attributes that the public safety broadband network must include:

1. **Nationwide**. The network must provide coverage for public safety to all the locations where Americans live, work, and play, whether rural or urban, with the goal of 99% coverage of the population.
2. **Interoperable.** The network must interoperate across geographies and public safety agencies. We must move away from fragmented public safety networks that currently define the norm.
3. **Capacity and Performance.** The network must have the required capacity and performance to reliably and dependably support public safety on a day-to-day and

[2] *See* Fraternal Order of Police, Press Release, FCC Announcement on D Block (Mar. 1, 2010), *available at* http://www.fop.net/servlet/display/news_article?id=2254&XSL=xsl_pages%2Fpublic_news_individual.xsl&nocache=5549924*; see also* Letter from Harold A. Schaitberger, General President, International Association of Fire Fighters, to Julius Genachowski, Chairman, Federal Communications Commission (Apr. 23, 2010).

[3] Thomas H. Kean and Lee H. Hamilton, 9/11 Commission Chair and Vice Chair, Statement on the Federal Communications Commission's Approach to Interoperable Communications Capabilities for Public Safety (Mar. 18, 2010), *available at* http://blog.broadband.gov/?entryId=297238.

emergency basis, as well as provide contingencies for operations during the worst disasters.

4. **Cost-effective.** The network and its devices must be affordable for the Nation and for public safety to deploy, operate, utilize and upgrade.
5. **Technologically advanced.** The network must utilize the latest technology and have a clear path for technological evolution. We cannot afford for public safety to be trapped in expensive, old technologies that cannot be upgraded without considerable expense and that threaten interoperability.

I would like to take a few minutes to walk you through this vision and plan, which we are actively implementing based on the approach contained in Appendix B.

In order to fully understand the way ahead, it is important that we first focus on the heart of the network, the radio access network. Currently there is 10 MHz of dedicated spectrum in the 700 MHz band available exclusively for public safety broadband communications. This spectrum is available today and, because of its propagation and other technical attributes, it provides a solid platform for deployment of a nationwide, interoperable public safety broadband network. This 10 MHz is the necessary foundation on which to build the public safety network, and it will provide public safety with more than adequate capacity and performance required to support day-to-day and most emergency communications (how the network will handle major emergencies will be discussed below).

The 700 MHz band, where this spectrum is located, is particularly exciting as new commercial 4G technologies, such as LTE, are just beginning to be deployed to support advanced data communications. Public safety, by being able to deploy their networks now and in the near future, can capitalize on these technologies and this commercial deployment, ensuring

a path for technological evolution and reducing costs by leveraging these commercial technologies.

By deploying its network using this core spectrum and capitalizing on synergies created by the contemporaneous deployment schedules of commercial carriers, public safety can enter into incentive-based partnerships with commercial entities to deploy the public safety network using 4G technologies in a way that is significantly less expensive that building a stand-alone system. In other words, public safety will have its own spectrum, its own network, and its own antennas, but in most areas public safety can share infrastructure that already exists or is being supplemented by commercial service providers now. The public safety radio access network can be installed on a commercial tower at the same time that the commercial system is installed, for instance, and use the fiber optic cables or other technology that connect the tower to the network.. In this way, public safety will recognize approximately $9 billion in cost savings for the construction of the network and potentially tens of billions in savings in operating costs. Frankly, I do not see how the Nation, the states, counties, cities or tribes could afford this network if this strategy is not employed. The network simply becomes unaffordable.

As I will discuss a little later, 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 and projected savings for state, local and tribal governments will not be realized because significant cost-efficiencies will be squandered. If this occurs, the mere expense of the network and user devices will make it extremely unlikely that the capability will be nationwide, leaving portions of the country without access to these critical public safety communications services, in essence, leaving these areas behind with the vestiges of legacy, narrowband fragmented networks which encumber our Nation today.

FCC engineers, experts and technical staff have spent hundreds of hours, including late nights and weekends, performing engineering analysis to validate whether the 10 MHz of dedicated spectrum available to public safety will, indeed, provide more than adequate capacity and performance for day-to-day and emergency communications. This analysis, which we released publicly in a White Paper on capacity this week, examines 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 dedicated spectrum supports these critical communications requirements.

When analyzing capacity, an important point to keep in mind is that spectrum does not equal capacity. Making a decision on network design by considering spectrum alone or even principally would be an erroneous decision. Network capacity and performance are affected by spectrum, as the White Paper states, 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. Further, based on the past evolutionary trends of commercial technologies, if the public safety network is deployed utilizing non-proprietary commercial technologies, capacity and performance of the network are likely to improve in the same amount of spectrum. We must escape the mindset of evaluating the promise of new technologies based upon the limitations of old technologies. We cannot design a public safety 4G broadband network using concepts, and spectrum, from decades old narrowband land mobile radios concepts. The capacity White Paper quotes a recent study of public safety communications in the greater Los Angeles area. The study indicated moving from

today's LMR technology to the type of cellular technology that will be used (LTE or even pre-LTE) could increase capacity per megahertz by a factor of 16. To state this more starkly, as shown in Appendices C and D, the study demonstrated that 10 megahertz of capacity on a cellular network would be the equivalent of 160 megahertz on an LMR-type network![4] 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 may challenge the public safety spectrum, and the National Broadband Plan developed a smart, innovative approach. Every public safety agency must have immediate, agile additional capacity for use when needed, such as when their network is at capacity or otherwise unavailable. To that end, as shown in Appendix E, the FCC will initiate a rulemaking proceeding, planned for this summer, that will examine 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 will have access to 60 MHz or more of additional spectrum – far more then the 10 MHz of spectrum available in the D block. Further, unlike the case of just reallocating the D block, roaming and priority access will provide public safety with access to redundant networks in case their network is rendered unavailable. Public safety networks occasionally suffer outages, sometimes during catastrophes and sometimes just on a daily basis. The District of Columbia public safety communications systems suffered such an outage for several hours back in March of this year. If the FCC concept is employed, police, fire and emergency medical communications could simply roam over onto one or more commercial networks, with priority, and still continue their public

[4] J.M. Peha, "How America's Fragmented Approach to Public Safety Wastes Money and Spectrum," *Telecommunications Policy*, Vol. 31, No. 10-11, 2007, p. 605-618.

safety work. This level of resiliency and redundancy has important benefits not only for public safety, but also for homeland security. Simply reallocating spectrum does not provide this level of resiliency.

Still, there are additional pieces to ensure adequate capacity and performance. We developed an in-depth cost model for this network, and I have not seen any cost model for any alternative plan that will ensure nationwide coverage at an affordable, sustainable price. First, our cost model recognizes and captures the need for deployable caches of communications equipments, such as cell towers on wheels, to ensure that the public safety community is able to supplement its network during the worst emergencies. Second, we have also recommended that states and localities should include in their building codes requirements for the installation of in-building transmitters. This will ensure that communications is extended to deep within buildings.

Finally, we are planning to seek comment on a letter filed by the Sandy Spring, Georgia Police Department asking about the possibility of public safety obtaining additional flexibility for broadband communications in the adjacent 700 MHz public safety narrowband spectrum. We recognize that this spectrum supports critical public safety voice communications that must be protected and promoted to increase voice interoperability. But at the same time, we look forward to building a record based on the suggestions of our colleagues in the public safety community, such as Sandy Spring, Georgia, exploring whether flexibility could be given to public safety to utilize this spectrum on a non-interfering basis for broadband communications. We recognize that this is part of the draft discussion legislation and we look forward to further discussions with Committee staff on this important issue.

Another 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 we established the

Emergency Response Interoperability Center or ERIC. 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. We are planning to shortly announce the formation of a technical advisory committee to ERIC made up of a diverse group of state and local public safety officials from around the country. This advisory committee will be 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. Just last month, we granted 21 waiver petitions for early deployments of this network.[5] In these initial grants, the FCC adopted stringent 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. 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.

Next, I want to focus on the nationwide aspect of the network. There are two requirements that must be met if the public safety broadband network is to be truly nationwide. First, public safety must be able to leverage commercial technologies and infrastructure to capture cost efficiencies through economies of scale and shared resources. If this does not occur, it is

[5] These include the City of Boston; the City and County of San Francisco, City of Oakland, City of San Jose CA; State of New Jersey; City of New York; City of San Antonio TX on behalf of the San Antonio Urban Area Security Initiative Region; City of Chesapeake, VA; State of New Mexico; City of Charlotte, NC; State of New York; District of Colombia; County of Maui, County of Hawaii, County of Kauai, City and County of Honolulu, and the State of Hawaii; City of Seattle, WA; Adams County, CO Communications Center; City of Pembroke Pines, FL; Los Angeles Regional Interoperable Communications System; Iowa Statewide Interop. Comms. System Bd.; Calumet, Outagamie and Winnibago Counties, WI; Mississippi Wireless Communications Commission; City of Mesa AZ and the TOPAZ Regional Wireless Cooperative; State of Oregon; and State of Alabama.

exceedingly likely that deployment of the network will be extended indefinitely and will be too costly for many jurisdictions to pursue. As I will discuss shortly, if D block is reallocated, it is likely that the costs of the equipment to support the public safety broadband network will increase dramatically, threatening nationwide deployment.

Second, it is critical that funding be provided by Congress to support the network's capital and operating expenses. To this end, I was heartened when the Department of Commerce's National Telecommunications and Information Administration re-opened its Broadband Technology Opportunities Program (BTOP) filing window recently to allow the waiver recipients to apply for BTOP funding for capital expenses. However, this is only the tip of the iceberg. Our cost model demonstrates under an incentive-based partnership approach, which is able to fully leverage commercial technologies and infrastructure with 99% of the U.S. population covered by the network, capital expenses for a fully hardened network will cost approximately $6.5 billion over 10 years. Operating expenses for this network will cost for the same ten-year period between $6 and $10 billion. With this funding and based on the roadmap we are pursuing, the citizens of our country can be certain that we will have a nationwide, interoperable public safety broadband network.

However, all of this is at risk if the D block is reallocated to public safety. First, 10 MHz of additional spectrum allocated to public safety cannot provide public safety with the capacity it may require in the worst emergencies. Ten megahertz of additional spectrum also fails to provide the redundancy and dependability of roaming and priority access on multiple commercial networks across the commercial 700 MHz bands. Further, our study demonstrates that except for the very worst emergencies, most of this spectrum will go unused or it will be significantly under-utilized. This would be the equivalent of building a separate four-lane

highway for emergency vehicles when all that is required for clear access are a public safety "HOV" lane and flashing lights and a siren.

Further, one thing that is certain is that additional spectrum will not ensure interoperability. In fact, D block reallocation may endanger interoperability. D Block re-allocation would remove a key advantage of the FCC's plan that would have a commercial operator develop devices for public safety use with commercial-level economies of scale. The D Block and public safety broadband allocations are in the same LTE band class, so "off-the-shelf" devices created for D Block customers would be available to public safety users at consumer-electronic prices, as could radio network equipment. Reallocation will eliminate the commercial market for off-the-shelf devices in this band class, relegating public safety to the same position they are in now, with quickly-outmoded devices that cost thousands of dollars. At the very least, a licensee in the D Block could provide another potential partner for public safety agencies seeking to construct and operate their network.

Without this basis for public safety to be able to capture traditional commercial economies of scale, the cost of the public safety network would skyrocket. The cost can easily rise for capital and operating expenses from approximately $6.5 billion for construction costs and approximately $8-10 billion in operating costs to an estimated combined total of $35-$48 billion over ten years, a three to four times increase. Similarly, as depicted in the Appendix F, D block reallocation, because of its impact on cost and equipment availability is likely to significantly retard network deployment. Instead of a ten year deployment it is more likely that the deployment will take at least 20 to 25 years, or perhaps never occur.

Further, there is no evidence that reallocating the D block will provide public safety with the funding from the lease of excess capacity to deploy and operate a nationwide interoperable

public safety broadband network. There has been no showing presented that demonstrates that the amount, if any, of projected income from this opportunity and how that would meet capital and operating expenses of the network. To the contrary, at least some leaders in the public safety community have admitted that in rural areas this opportunity will not be available and instead public safety would have to build fewer towers in those areas as a cost savings method. This concerns me because limiting infrastructure has a very real impact on capacity and performance.

Our mission is to ensure that public safety agencies in **all** areas of the country have the best chance of successfully gaining access to an advanced, wireless broadband network. Our holistic approach fulfills this mission. We have a singular opportunity to ensure that public safety has a nationwide interoperable broadband network. Our plan takes advantage of this opportunity by offering a sustainable, long-term, cost-efficient model that provides first responders with the state-of-the-art, affordable, and interoperable broadband communications networks they deserve. We can provide the public and the public safety community with a nationwide, interoperable broadband network that is robust, which can evolve with commercial technological gains, and which is affordable, truly a national asset. But we must act quickly and decisively, based on a comprehensive plan using the best technology and scientific analysis. We must not commit to a plan that perceives the future based upon the limitation of old technologies. We can solve the 9/11 interoperability problem.

Thank you for your time and attention. I am very happy to take any questions you may have.

Appendix A

FCC and PSHSB have proactively reached out to the Public Safety Community on the Public Safety Broadband Network for Input and Recommendations

A continuing, open dialogue on promoting public safety broadband communications including speaking engagements across the country

- Hundreds of pages of comments and dozens of ex parte presentations from public safety groups on the National Broadband Plan (GN Docket No. 09-51) and on the development of a nationwide interoperable public safety broadband network (PS Docket No. 06-229).
- Hundreds and hundreds of email exchanges, conference calls and telephone calls with public safety officials, state and local officials and key trade associations including APCO, NENA, the Major Chiefs, among others.
- National Broadband Plan workshops on public safety and homeland security (Aug. 25, 2009) and cybersecurity (Sept. 30, 2009), and a field hearing at Georgetown University Medical Center (Nov. 12, 2009) on public safety communications and emergency response.
- A forum on creation of the Emergency Response Interoperability Center (Mar. 2, 2010)
- A symposium on the public safety and homeland security aspects of the National Broadband Plan (Mar. 31, 2010)
- Meetings in Las Vegas (Mar. 9, 2010) and Washington, D.C. (Mar. 15, 2010) to discuss the FCC's cost model for the public safety broadband network
- Multiple conference calls to discuss key policy matters such as roaming and priority access
- Public notices soliciting comment on such matters as the technical aspects of interoperability and a follow up call on interoperability issues
- Regular attendance at NPSTC meetings and NPSTC Broadband Task Force meetings
- Participation in the PSCR Shareholder Meeting (April 20-21, 2010) in Boulder, CO
- Meetings with representatives from the U.S. Conference of Mayors
- Briefing of the DOJ Tribal Working Group (May 27, 2010) on ERIC and the public safety broadband network
- 9-1-1 Gala (Mar. 16, 2010)
- Police Executive Research Forum (Mar. 19, 2010)
- National Governors Association (Apr. 1, 2010)
- SAFECOM Executive Committee conference call (May 12, 2010)
- NENA Conference (June 8, 2010)
- Meetings with the National Governors Association and the United States Conference with Mayors

Appendix B

Components of Public Safety Broadband Network

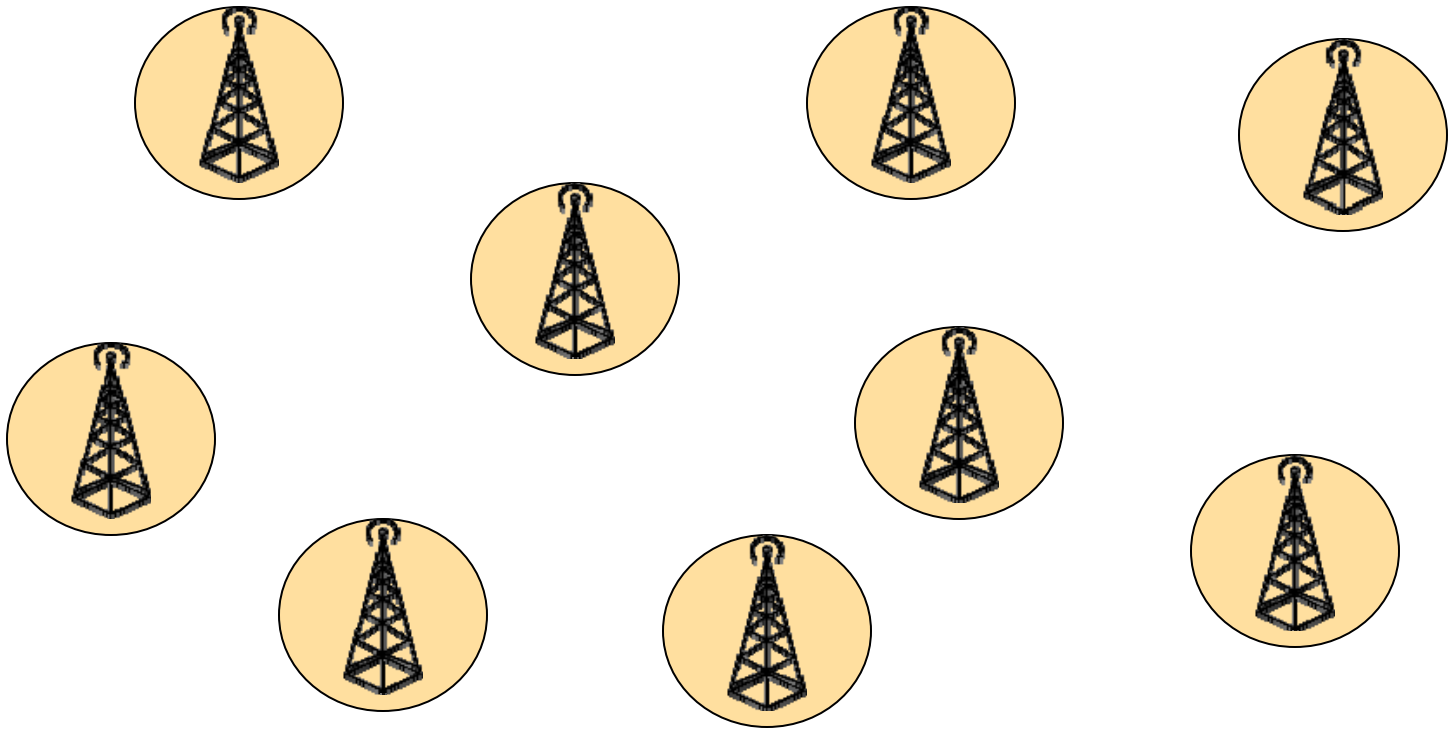
Nationwide, 99% population coverage from dense cities to rural counties

Public Safety Spectrum	700MHz Commercial Networks	Distributed Antenna System and Microcells	Deployable Equipment
Core of the Public Safety Network Using Public Safety Dedicated Spectrum 10 MHz	Priority access and roaming Up to 60 MHz	In-building and underground coverage Improves localized performance	Cellular on Wheels and Externally Mounted Antennas on Public Safety Vehicles Boosts capacity for the worst emergencies and in rural areas
Provides nationwide interoperable coverage for day to day operations and most emergencies, guaranteed access, and hardened against disasters and power outages	Provides access to additional capacity during major emergencies, and increased network resiliency and redundancy if the public safety system goes down or is not available	Coverage inside buildings and capacity for high pedestrian density can be provided by in-building solutions	For exceptional times and places when Public Safety and commercial infrastructure is insufficient

Appendix C

The Old Current Technology and Architecture: Narrowband Land Mobile Radio (LMR)

LMR is “noise limited”, tall towers, high power, large spaces in between

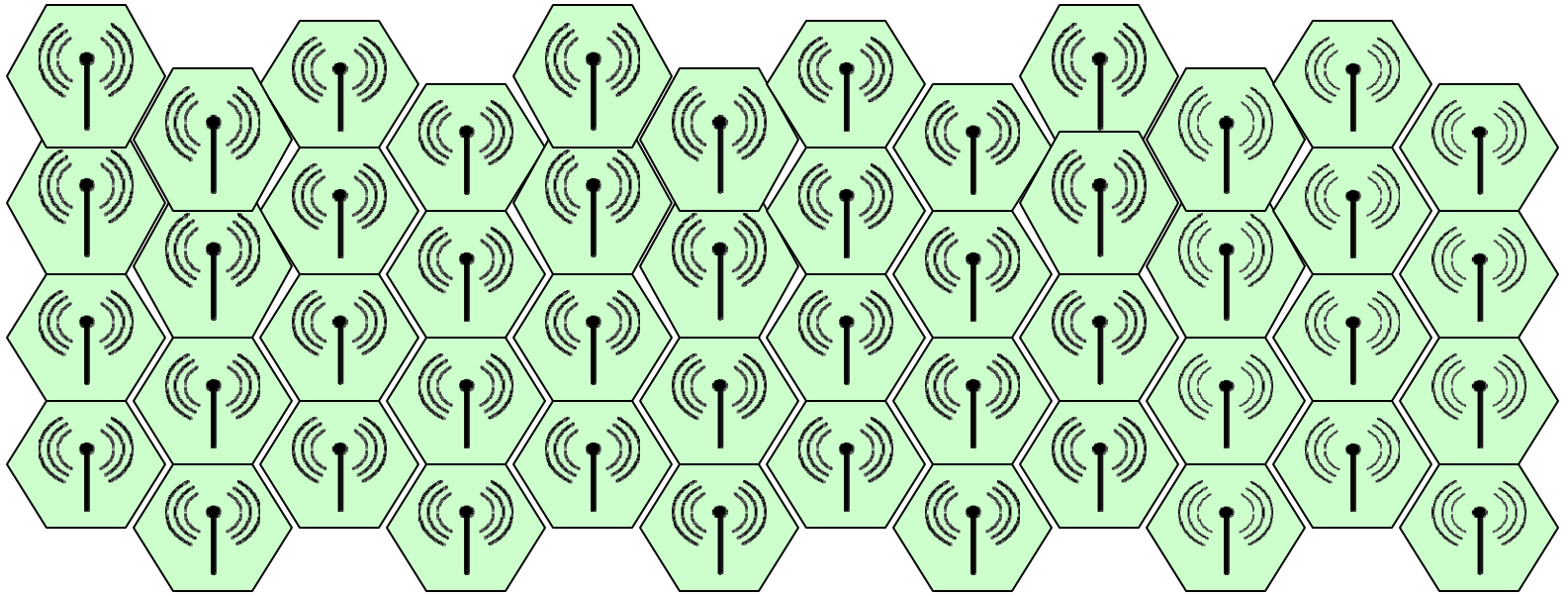


Inefficient use of spectrum, limits capacity, but saves money on fewer towers

Appendix D

The New Technology and Architecture: Broadband and Cellular

Cellular architecture is only “interference limited”, many towers, lower to the ground, each covering a small space, no spaces in between

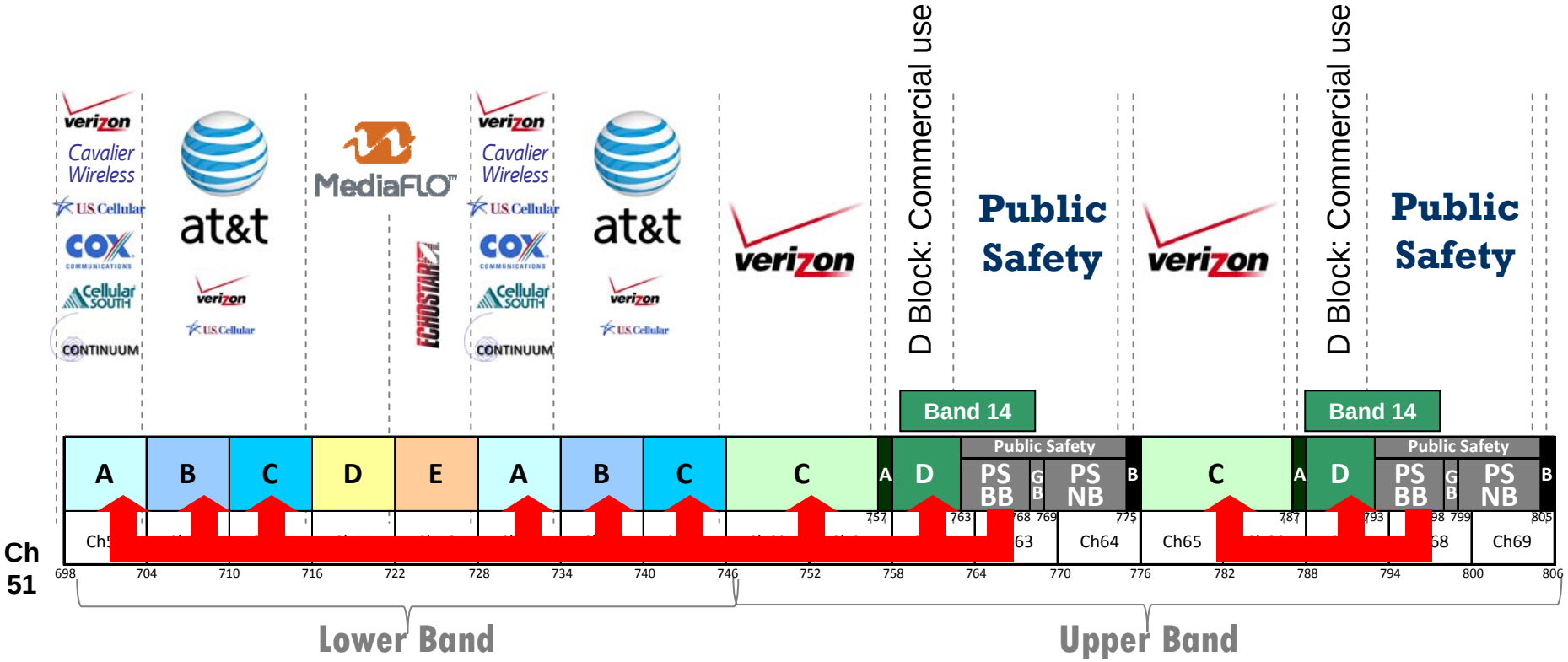


Efficiently reuses same spectrum in each cell, vastly boosting capacity, but requires more towers

Appendix E

700 MHz Band Plan

with Priority Access and Roaming



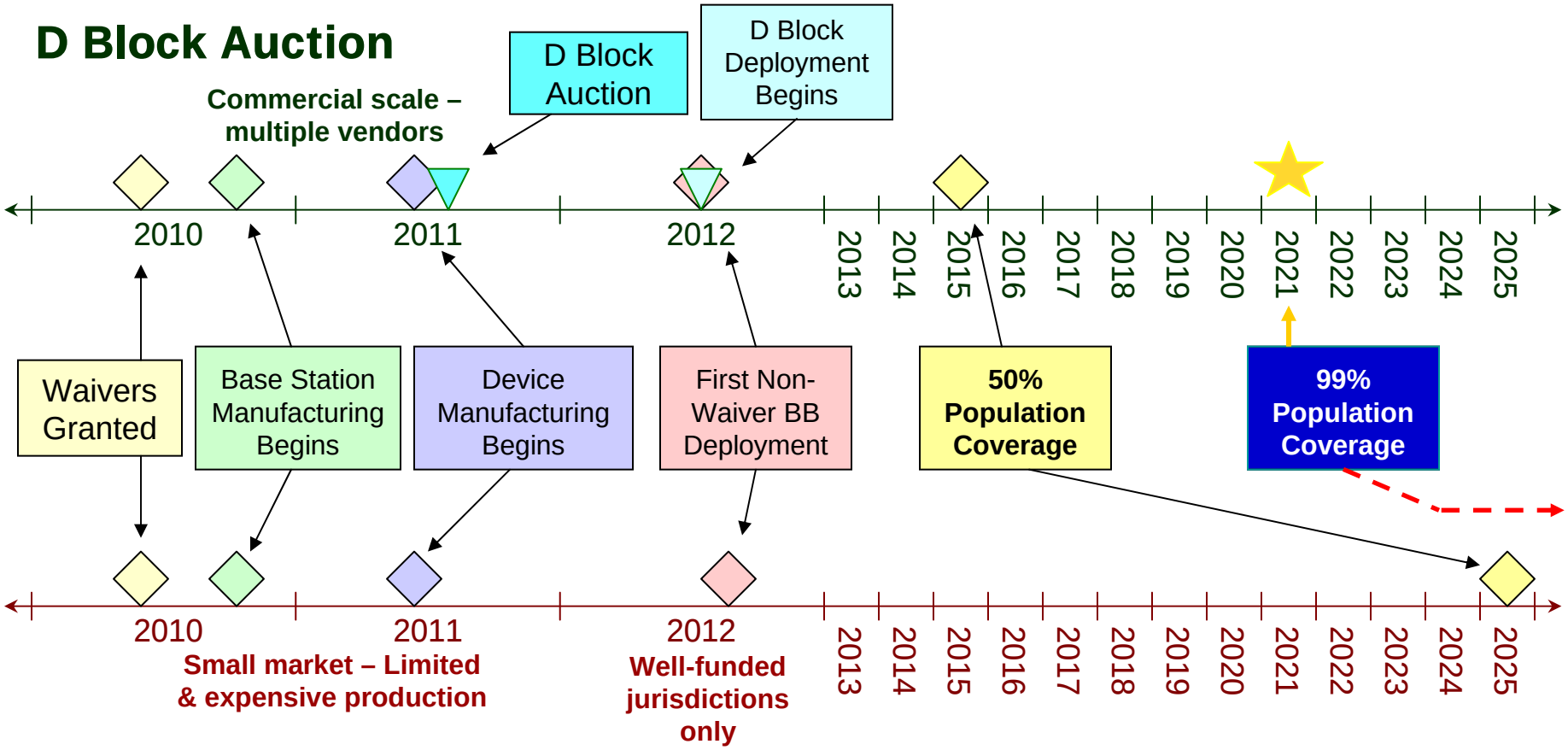
- **Priority Access and Roaming provides far more capacity for major emergencies than reallocating the D Block alone, plus the resiliency of back up networks**

- **Reallocating D Block isolates Public Safety from reasonably priced devices and equipment, and from commercial technology advances**

Appendix F

Timeline Comparison: D Block Auction vs Reallocation

Delay Equals Added Cost, Less Coverage and Threatens to Nationwide Interoperability



D Block Reallocation

D Block reallocation undermines the market for reasonably priced devices and equipment, vastly increases the expense, and defeats nationwide coverage.