

SUBJECT TO DEBATE

A NEWSLETTER OF THE POLICE EXECUTIVE RESEARCH FORUM



2010 PERF Annual Meeting

April 15–17, 2010
Ritz Carlton, Philadelphia, Pa.
For details, go to www.policeforum.org

VOL. 24, NO. 3 | MARCH 2010



PERF CONFERENCE ON BROADBAND SPECTRUM

FCC Officials Spar with Public Safety Leaders On Future Wireless Communications Needs

POLICE, FIRE, AND EMS AGENCIES' ABILITY TO FULFILL their most important missions over the coming decades is being threatened by a proposal by the Federal Communications Commission (FCC) regarding the future use of radio spectrum, according to a wide range of public safety officials who gathered in Washington on March 19 for a conference convened by PERF.

At issue is whether a band of broadband spectrum known as the "D Block" should be assigned to public safety agencies, so they can use it for an ever-increasing number of technologies that require wireless communications—such as live video from major crime or disaster scenes, and transmission of information from hundreds of databases that can provide critical real-time information to police officers, firefighters, and medics.

Perhaps the most common current use of broadband in public safety is the widespread use of mobile data terminals in police, fire, and EMS vehicles. Many public safety agencies also have begun using other broadband technologies, such as mobile incident command centers, automated license plate readers, and wireless gunshot detection sensors.

As for the future, it does not take much imagination to think of dozens of possible public safety applications. For example, firefighters talk about being able to tap into and share live video feeds from all of the security cameras inside office buildings, so they can instantly determine where a fire is concentrated before a single firefighter enters a burning building. And public safety agencies will continue to find new ways of using portable video equipment at crime or accident scenes and in other situations.

SPECTRUM CAN BE SHARED, BUT THE ISSUE IS WHO CONTROLS IT

Public safety leaders at the PERF conference said they must have control over the D block so they will be able to reliably transmit video and data that requires broadband spectrum, much as they currently rely on their own narrowband spectrum for voice transmissions via police, fire, and EMS radios.

The FCC, however, on March 16 delivered a sweeping National Broadband Plan to Congress that details its recommendations on a wide

range of spectrum issues, one of which is that the D Block be auctioned to the highest bidder. Under the FCC's recommendation, the winner of the auction—presumably a commercial carrier—could use the D Block for commercial applications, but also would be required to give public safety agencies priority access to the airwaves, particularly when they need it most to facilitate their response to major disasters or terrorism incidents.

However, contracting with commercial carriers is the type of arrangement that public safety agencies currently have for their broadband applications, and public safety officials contend that these systems often fail, both in day-to-day activities and especially in times of crisis, when wireless systems are overloaded by surges in calls by millions of cell phone customers. Promises of "priority access" to airwaves controlled by commercial carriers have proved to be unenforceable, public safety officials said.

Acting under previous laws, the FCC already has assigned to public safety 10 MHz of the spectrum that was made available in 2009 when television broadcasts switched to digital rather than analog transmissions. Public safety agencies in a number of jurisdictions have begun the process of seeking FCC "waivers" or approvals to start building the infrastructure to use that broadband spectrum. But the public safety broadband spectrum is not yet in use. That is why public safety agencies currently rely on commercial carriers for their broadband applications.

PREVIOUS ATTEMPT TO AUCTION D BLOCK FAILED

One final bit of background is required to understand the current situation: The FCC tried once before, in 2008, to auction off the D Block to private carriers. But no one met the reserve price of \$1.3 billion for the spectrum. Potential bidders reportedly were frightened off by the financial implications of requirements that the high bidder would have to make the spectrum available to public safety agencies. The FCC contends that its new plan will provide a better set of rules for those private-public partnerships, which will successfully combine solid guarantees of public safety access with reasonable assurances to commercial bidders that their plans for the spectrum will be feasible financially.

This special issue of Subject to Debate recounts the discussions at PERF's conference, which was undertaken with support from the Motorola Foundation. The discussions included a vigorous debate between public safety officials and two of the top FCC officials who developed the public safety aspects of the National Broadband Plan and who agreed to come to PERF's conference to discuss it: Admiral James Barnett, who serves as chief of the FCC's Public Safety and Homeland Security Bureau, and David Furth, deputy chief of that FCC bureau.

At the PERF conference, police, fire, and EMS agencies contended that it is already clear that the 10 MHz already assigned to public safety will not be enough spectrum to accommodate their needs, and that they will also need the additional 10-MHz D Block.

Admiral Barnett agreed that public safety "will someday need more spectrum than the 10 MHz designated to it by Congress." But he noted that the FCC plan provides a mechanism for public safety agencies to use additional spectrum controlled by commercial carriers.

Admiral Barnett urged public safety officials not to focus exclusively on the D Block issue. Equally important, he said, is the question of how public safety will pay the tens of billions of dollars that will be required to build the radio transmission towers and other

infrastructure for public safety broadband. The FCC plan includes recommendations that Congress provide \$6.5 billion in capital spending over 10 years for this purpose, plus \$6 billion to \$10 billion over 10 years for operating costs.

The public safety establishment's battle for the D Block has now shifted from the FCC to Congress and the White House, which have the final authority to decide the issue. Congressional hearings on the FCC's National Broadband Plan have already begun. Other aspects of the plan having little or nothing to do with public safety also have proved controversial, so Congressional action on the plan will be complicated. However, advocates of the plan are urging Congress to move as quickly as possible.

A wide range of national police, fire, and EMS organizations have called on Congress to assign the D Block to public safety. Additional information is available online here: <http://ld-block.net/>.

PHILADELPHIA POLICE COMMISSIONER AND PERF PRESIDENT CHARLES RAMSEY: There Is No More Important Issue than This

I can't think of an issue that's more important than what we're going to be talking about here today. This issue is something that already affects us all and will affect us in the decades to come. I was very disappointed to read about the FCC's plan for broadband. We need more spectrum, and we need spectrum more than we need money. We can always work toward getting more money, but we need spectrum to transmit data. I don't think that the public at large has heard our voice on this. They don't understand the implications of what's taking place right now. So this conversation has to go way beyond this room. But it's not too late to turn this around in Congress.



ROB DAVIS, SAN JOSE POLICE CHIEF AND PRESIDENT OF MAJOR CITIES CHIEFS ASSOCIATION: It Should Be Obvious That Public Safety Is More Important Than Text-Messaging Votes for American Idol

We have not defined this issue well enough in the community. When you go out and talk about broadband and spectrum and 700 MHz and D block, people's eyes glaze over. They don't get what it means or how important it is to us.

But make no mistake about it. As we've attended our roundtables three times a year at the Major Cities Chiefs Association and have talked about this issue, it has become clearer and clearer why this is so important to us. We talk about the police officers of the future, and we know that there will be technologies out there that we will not be able to implement if we don't lock down spectrum now.



We're already doing a pilot project in San Jose where we have officers wearing cameras, transmitting information that shows how they're doing their job. To take a car stop as an example, a police officer of the future will get out of his car and won't even have to speak the license plate number, because it will be read through the camera system to check against stolen vehicle reports or outstanding warrants.

We're being told, we'll give you a little bit of spectrum here, a little bit there, that sometime in the future, we'll find it for you. But based on past experience, I'm not going to buy that. What we have now is a window of opportunity for us to lock down that spectrum so we'll know exactly where it is, and our technology developers will know where it is, and it won't matter what company is developing the technology or in what part of the country, it will be right there.

I don't understand why we're being told that we haven't made the case that this is important to public safety. This is a human issue. We are in the public safety business. And we are being told that it is more important for somebody to be able to text message who they want to vote for on *American Idol* than for us to be able to deal with the collapse of a bridge or a hurricane. That's crazy. There's a need for public safety to have control over this spectrum now and in the future for data-sharing, for voice, and to be able to control our responses to emergencies. If that spectrum is given up, we will never have another shot at it. It's now or never.

If this doesn't happen, it will reflect a huge lack of vision on the part of the federal government.

MINNEAPOLIS DEPUTY POLICE CHIEF ROB ALLEN: Why Data Transmission Is Essential in Disaster Response

Rob Allen discussed communications and spectrum issues in the context of the response to the Minneapolis Interstate-35 bridge collapse of 2007:

We had more than 128 public safety agencies involved in the rescue. Police, fire and EMS were all working there. The voice radio system worked fine; it reached capacity but worked. Cell phones were absolutely worthless. There was a Minnesota Twins game going on, and they made an announcement asking people not to use their cell phones, but they didn't explain why. So of course everyone at the Twins game started calling their friends to try to find out what was going on.

Fortunately, just by chance, we were in the process of building a Wi-Fi grid for the entire city of Minneapolis, and the infrastructure was there but it hadn't been turned on and made available to the public. So they turned all that over to us, and we were able to transmit video and data. But if a bridge collapsed today, we'd be competing against Internet porn and Twitter for that bandwidth.

We had over 1,200 first responders. To manage that many people, you need data transmission capabilities. Using voice communications, there's not enough time to communicate all the information you have to share among all those agencies. There's just not enough time in a day; even if you had it all scripted out, you



wouldn't have time to read it over the voice radio. You have to share data.

For example, we had more than a thousand missing person calls in the first 24 hours, and locating people was a challenge. We had to set up data networks with the hospitals to keep track of which patients were at which hospitals. And there was always the threat of secondary collapses of portions of the bridge, so when we had divers in the water, we had to coordinate all the other elements to make sure that something would not be moved that could cause a secondary collapse and hurt the divers.

Transmission of data is the future and is *the* emerging issue in public safety.

MAJOR TOM GROSS, MIAMI-DADE POLICE DEPARTMENT: Commercial Systems Are Not Sturdy Enough To Survive a Hurricane

When we had Hurricane Wilma a couple weeks after Katrina, we lost our cell phone traffic after six hours, and our entire broadband mobile component went down because it relied on a private cellular carrier. The police *voice* radio network stayed up because it was built to mission-critical standards and it is maintained for our priority. If we have to share spectrum down the road and don't control it, how do we know we'll get it when we need it?

And even if a commercial system stays up and running, it doesn't mean we'll have access to it. Take the *272 example [a system in which high-priority subscribers can dial *272 to be given the next available radio connection when cell phone networks are overloaded]. That priority code only gets you priority to the cellular network if you can *hit* the cellular network. It doesn't kick anybody else out of the way. So we still get busy signals. We have to own the spectrum and manage it to ensure that our data will travel on that network when we need it.



PHOENIX FIRE CHIEF BOB KHAN: Coordinating a Major Event Requires Good, Quick Information Through Broadband Systems

After 9/11, we got smarter about our relationships with our colleagues in law enforcement, because we saw the need to communicate on a regular basis. Today we have the Arizona Counter-Terrorism Information Center, which collects information from a wide range of sources. We had the Super Bowl in 2008, and when you have a major event like that, you have to be prepared for multiple scenarios—people with medical problems, a shooting, civil disobedience, a lot of different things that can happen at the same time. And you're coordinating among multiple law enforcement agencies, fire departments, and other entities. The only



way you can do all that is with good, quick information through a broadband communications system.

**PHOENIX DEPUTY FIRE CHIEF KEVIN KALKBRENNER:
To Private Carriers, It's Just Another Dropped Call
When Public Safety Communications Fail**

Our mobile terminals in our fire trucks and police cars in Phoenix use private carriers, and they go down all the time, so we have to fall back to our radio systems.

And when we contact the private carrier and try to work through these issues, they say, "Well, we had a big blip on the system." To them it's just another dropped call. They have no idea what a dropped call means to a firefighter or a police officer.

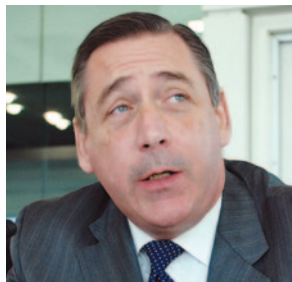
We are judged in the court of public opinion. People are Twittering us at an emergency scene, and CNN is reporting, "We're hearing from bystanders that this and that are happening, but the police and fire officials don't even know what's going on." And that's because the private carrier is down and we aren't receiving the information we need.



**NYPD DEPUTY CHIEF CHUCK DOWD:
We Can't Expect Cops to Use These Systems
If They Are Unreliable**

One of the things that has changed with this issue over the last year or two is that today we have chief executive officers of police and fire agencies who understand how this is going to transform how they do their business.

One of the arguments we've heard is, "Prove your case for a need for 20 MHz of spectrum. In a city like New York, you probably need 20 MHz of spectrum. But in a lot of smaller cities, you probably don't need that." Our argument is that that's simply not the case. Look at the example of the Minneapolis bridge collapse. They had 1,200 first responders at that scene. How do you manage all those responders on a



mission-critical basis on a communications system without sufficient spectrum?

I've heard a lot of comments that "this is the future." And that's true, but it's also true that the future is now. We're doing a lot of this stuff already. Is there anybody in this room who is not carrying a Blackberry right now? That's the kind of capability we're talking about. We're talking about taking that capability and driving it down to the level of the patrol officer and the firefighter. It is cost-prohibitive to do that on commercial networks. And even if we could afford it, we wouldn't want to do it, because as everyone has said in their examples, when we need those systems most, they fail us. We have to have our own proprietary network. We have to have a public safety system that is mission-critical grade, that will survive in these events.

One of the things we looked at first in trying to decide how to build our data communications system is how we built our land mobile radio systems. The principles are exactly the same: Data has to have survivability, redundancy, and coverage capabilities that we build into our voice radio systems. When police and fire key up their radio systems, they have to be able to get in. There can't be a waiting time. They can't get a busy signal. We cannot expect cops and firefighters to use these networks if they don't feel they can rely on them.

We have never in our experience been able to convince any of the commercial carriers to give us the kind of prioritization on their networks that we need. It simply hasn't been the case, and we have no expectation that they would do it. Whenever there is a failure of our communications networks, it almost invariably is tracked back to the commercial components of it.

So while there are some components of the FCC plan that we like, there are fundamental aspects of it that we know fly in the face of how we do our business. It's a question of bandwidth. 10 MHz is simply not going to do it for us. Funding is important, but they can give us all the money in the world, and if we don't have enough spectrum to accomplish our mission, we can't get it done.

**DEPUTY CHIEF JIM VLASSOPOULOS,
DC FIRE AND EMERGENCY SERVICES:
When Emergencies Happen, Our Data Systems Fail**

This is an incredibly important discussion. In Washington we have had the Million Man March, the Pope's visit, Independence Day celebrations every year, Marine Corps Marathons, Interna-

Some Existing and Future Public Safety Technologies That Require Use of Broadband Spectrum

- Real Time Crime Centers
- Mobile Incident Command Centers
- Mobile Crime Scene Units
- Automated License Plate Readers
- Streaming Video Applications
- Mobile Geospatial Information Systems
- Wireless Video Surveillance

- Biometrics and Hazardous Materials Detection Devices
- Photo ID and Facial Recognition Technologies
- Automatic Vehicle Location and Dispatch Systems
- Wireless Gunshot Detection Sensors
- EMS Telemedicine and Patient Tracking
- Mobile Ticket Writer Systems

tional Monetary Fund protests, Presidential Inaugurations; these are just a few of the events that require a lot of coordination of federal, local, and regional entities. And with these planned events, commercial carriers bring in portable towers and increase capacity and they can meet the demand, as long as there's no major incident that occurs.



But when emergencies happen, you lose your cell phone capabilities. DC fire and EMS has about 225 computers in our vehicles connected to the computer-aided dispatch system, and they rely on a broadband commercial wireless carrier. Unfortunately, when your cell phones go down, so do your mission-critical applications. Just forget it if you have to pull down anything that requires a lot of bandwidth.

Years ago, a lot of progressive public safety agencies began using mobile data computers, but they only required a little bit of bandwidth. We were only transmitting little bits and pieces of data. Now we're using high-resolution imagery, live-streaming video, or just emailing a large file—try doing that if your cell phones don't work. Why does this happen? Because we don't have priority. The *272 system doesn't work. We as public safety agencies haven't seen commercial wireless carriers provide the access and assurances to us that when we log onto the network, we will remain on the network because our jobs are mission-critical.

SAN DIEGO POLICE CHIEF WILLIAM LANSDOWNE:

In the Critical Hours Following a Disaster, Local Agencies Are the Only Responders

People talk about “first responders,” but in a major emergency we're not just the first responders; local police and fire departments are the *only* responders. For those first 24 hours, we have to be self-sufficient.



I'll discuss the wildfires that hit San Diego in 2007 as an example of why we need an interoperable communications system for voice and data. We were not caught off-guard; we knew we had been experiencing a drought and that the fires come with the Santa Ana winds, and we were all waiting for the call that we hoped wouldn't come. But we did get the call about 10:30 at night out in the east county near Alpine, about 35 miles from the city of San Diego.

We were faced with doing an evacuation of a half-million people at 4 o'clock in the morning, when people are asleep, they're not up watching TV or listening to the radio and getting the news, and you have elderly, disabled, and people on medication who need special attention. You've got to get them out of the house, and the only way to do that is to go door to door, go to each house and make sure you get each individual person out of there safely. And you can't do that effectively and really manage the situation unless you have a communications system.

We got everybody out, but it was challenging because we had 16 jurisdictions involved. Each of them opened up their Emergency Operations Centers, but we were all aware that none of us could talk to each other. We should not have a system in which you have to waste valuable resources, sending your officers to other agencies just so they can bring them a hand pack so we can talk to each other. We were relying on phone calls back and forth from center to center, but the fires were eating up some of the cell phone towers, so the cell phone system started going down real quick.

On an average day I have 300 officers on the streets of the city of San Diego. But when the fire came at us, we went to 1,500 officers, and we did not have the spectrum to handle the volume of information. You need real-time information when a disaster is coming at you, and you can't share information among that many people via word of mouth, with phones. You need to transmit other kinds of data, which can take up a lot of spectrum. We can downstream video from our helicopters, which is absolutely essential in managing these disasters effectively. The video tells you which way the fires are going so you can plan your evacuations and move your resources to where they're needed.

When it was over, we were debriefed and I was asked by the Department of Homeland Security, “What is it you need? More money? More people?” And my response was, “I need a communications system that works on a national basis, so if we go to someone else's jurisdiction, we can get real-time information.”

Especially in a tough economy, if we're going to be effective at doing our job and saving lives, we've got to work closely with each other, and the only way we can do that is if we can share information with each other quickly and effectively. We are video-streaming information and the technology is getting better, but we don't have enough spectrum

FORMER FEMA DIRECTOR DAVE PAULISON:

Katrina Catastrophe Resulted in Some Reforms

Dave Paulison, former fire chief in Miami-Dade, Florida, was named Director of the Federal Emergency Management Agency (FEMA) in September 2005. Mr. Paulison replaced the embattled Michael Brown, who resigned in the wake of the disastrous response to Hurricane Katrina, in which at least 1,300 people, and perhaps far more under various other estimates, were killed.



Communication really boils down to situational awareness, and I can talk about what happens when you don't have situational awareness, with Hurricane Katrina. The city of New Orleans was not ready to deal with it, we had a catastrophe going on, and we didn't have a clue as to what was really happening.

We ended up evacuating a million people to almost every state in this country, but did not have the capability of tracking where they went. We were not able to track buses and when they were supposed to show up to evacuate people.

We didn't have the capability of doing any video streaming ourselves, so were getting our information from CNN. But

sometimes we didn't realize that CNN was running video from days earlier and we thought it was live, which caused us to move a lot of food and equipment to places where it wasn't needed.

We didn't have any automated vehicle locating systems on trucks, so supplies were getting lost. I went to one place in Louisiana where a mayor was screaming that he needed food and water and ice, and we found out later that the supply trucks were on the other side of a building a block away, and nobody knew they were there.

We did not have the capability to set up a unified command system. We had no way to hook up the state, the city, the federal government, and even the federal agencies themselves were not working in a unified command center.

Once we convinced the President that we needed a national response plan and a unified command system, we went out and bought equipment and convinced all the Cabinet members that they had to play ball. For example, FEMA now has the ability to put 48 governors on video screens at one time if we have a national catastrophe. That eats up a tremendous amount of bandwidth, but it served us extremely well with Hurricanes Ike and Gustav in 2008.

This country embarrassed itself with how it handled Katrina. We can't stop damage from happening; we couldn't help that the levees broke. But with better communications we could have saved lives. We would not have had people left in nursing homes to die; we would not have had people on the rooftops.

CHARLOTTESVILLE, VA FIRE CHIEF CHARLES WERNER: Today's Decisions on Spectrum Will Impact Tomorrow's Fire, Police, and EMS Agencies

In every major catastrophe, communications are always an issue. We're looking not only at what we have today, but what we'll be doing in the future. We can see the exponential growth in critical applications—chemical monitors, road temperature gauges, multiple streams of video that actually capture what is going on inside a burning building, building floor plans and cameras on firefighters so we can see the movement of the firefighters on those floorplans, and we can know where they are located, so if something happens to them, we can know about it immediately and prevent line-of-duty deaths.



At some point we'd like to tap into security cameras in buildings, to actually see inside the building on multiple floors simultaneously, for the incident commander to understand the magnitude of the fire. One day I see us having cameras on every police officer, every firefighter, every medic. You'll be able to see what they see, so when police officers are going into a building where there's an active shooter, the commanders will be able to see what they are dealing with and make better decisions about how to manage the situation.

But it's only going to be as successful as the network that we operate on. With these decisions about spectrum that we are making today, we are deciding not only what we'll be able to do today, but also what will happen to those who come after us.

ARLINGTON COUNTY, VA FIRE CHIEF JAMES SCHWARTZ: The Federal Government Relies on Local Agencies To Respond to the Disasters Which Will Undoubtedly Happen

The federal government is finally realizing that they are dependent on state and local agencies to provide the services in the middle of a crisis. The federal government has no resources to respond to the kinds of incidents that we deal with. The federal government needs a national capacity to respond, but we're not being given the tools necessary to support that capability.



We know that disasters are going to happen. Whether or not we can prevent terrorism is a big question. But we *know* we can't prevent hurricanes, tornadoes, and earthquakes. So the question becomes, how do we build a more resilient society? One aspect of resilience that is absolutely critical is our communications systems.

MILWAUKEE POLICE CHIEF ED FLYNN: Police Are "First Preventers," Not Just First Responders

Police departments are "first preventers," not just first responders. And preventing crime and terrorism absolutely depends upon the quality and quantity of information that can be communicated rapidly. Every year, I'm amazed at how much more is available to us, in terms of video streaming, data transmissions, photographs, automated license plate readers, the fact that we can not only microphone our officers but have them on camera. Every day the capabilities at our disposal expand exponentially, making us more effective at crime control and by extension preventing acts of terrorism. The availability of spectrum for data transmissions is as vital to us in our "first preventer" responsibilities as our ability to be interoperable is to our first responder responsibilities.



HARLIN MCEWEN, CHAIRMAN, PUBLIC SAFETY SPECTRUM TRUST: Bad Spectrum Decisions of the Past Caused Our Interoperability Problems Today

Harlin McEwen is chairman of the Public Safety Spectrum Trust, the entity created by Congress to manage the 10 MHz of broadband spectrum already allocated to public safety.



For 32 years I've been the chairman of the Communications and Technology Committee of the IACP. Over more than three decades of fighting for spectrum for public safety, I can tell you that this is not something new. This is an old story. The FCC has always given us a little spectrum here, and then they get to the next band and give us a little

spectrum there. But they never have had the vision to look to the future. The FCC generally are fine people who have never walked in our shoes. They don't understand our needs and they are pushed by many different people.

This is the most important effort that we have ever undertaken, because this really means the future for many many years. We are looking at 4th generation technology that we need desperately, and all of the experts are telling us that in order to have a 4th Generation Long-Term Evolution technology network, which is what we're supporting, you can't really do it with 10 MHz of spectrum. You've got to have 20 MHz to be efficient and to have the robust network that we need.

The problem is that everybody here understands that we need the spectrum and we can't let it go. But we're being told by the FCC, "We'll give you more money to do this, but we're not going to give you the spectrum." But if we lose the spectrum now, it's gone forever. They tell us that later we can get additional spectrum in another band, but this is exactly what they've done to us for years and years and years. They say, "Here's a little, and if you need more, come back later."

But that's the reason we have interoperability problems, because these different bands don't talk to each other. You can't buy equipment cheaply that works on multiple bands.

**CHIEF PHIL MORSE, U.S. CAPITOL POLICE:
The Government Itself Is at Risk**

My agency protects the legislative branch of government, and we have events like the State of the Union address and Presidential Inaugurations, where the leaders of all three branches of government are under one roof. Many law enforcement, fire, and other public safety agencies come together to plan these events. That requires sharing of a great deal of sensitive information. And we need to share the information immediately; we can't wait in line to do it. We need to be prepared for the next attempted acts of terrorism in Washington. If communications is a piece of the puzzle that's missing, we need to fix it now.



**ALAN HOFFMAN, DEPUTY CHIEF OF STAFF
TO VICE PRESIDENT JOSEPH R. BIDEN:
The White House Knows How Important This Issue Is**

We understand how important this issue is, and it is an issue that I've been working on since I was at the Justice Department in the 1990s. I think there are certain things we can all agree on, such as the scope and magnitude of the challenges that are ahead in terms of interoperability and the costs that are associated with communications, and the need to make certain that we are listening to law enforcement and are doing as much as we can do to take



care of the concerns of law enforcement. The President and Vice President understand the importance of this issue. We have met on this in the White House numerous times.

We expect to have some information for you in the near future and we promise we will work with you to get to the place where you think you need to be.

**ORANGE COUNTY, CA FIRE CHIEF KEITH RICHTER:
We Could Fill 10 MHz Today With Existing Applications**

We have 1.4 million people to protect in Orange County, and we have about 850 firefighters. We have a pretty robust communications system. We have automatic vehicle locators in all our units, mobile computers in our units, computer-aided dispatch so we can see where all of our units are in real time and recommend the closest units to respond. As Chuck Dowd said, we're trying to get the same types of information you can get on your Blackberry pushed down to the lowest level in our organizations. We could fill up 10 MHz today if we had the technology in all of our police and fire vehicles. And we've just scratched the surface in terms of transmitting all of the information that needs to be down at the field level. For example, with wildfires, we need to know the geographic information, the terrain, what is the population in each area, and which way is the fire moving, so we can work with police and get people out of the way of the fires and move our equipment to where it's needed.



**SAN JOSE DEPUTY POLICE CHIEF CHRIS MOORE:
Commercial Networks Are Not Built to Serve All Locations**

I'd like to thank Admiral Barnett and David Furth of the FCC for being here. A lot of what is in the FCC plan came from public safety, so they have been listening to us. But it comes down to this issue of our ability to get bandwidth when we need it, where we need it.



We keep hearing about capacity, but let's look at where we build our networks. We have to build them everywhere we operate, not just in the high-density population centers. We don't know where an emergency is going to be, so we build so we can operate anywhere. Commercial networks don't do that; they build where they're going to make the most money. They do not provide mission-critical service; they never have.

We know what our needs are, because we use it every day. The key is that public safety has to have control of that network, because even if we are promised "guaranteed" access to a commercial network, frankly, we don't believe it. All of our experience tells us that hasn't happened in the past, and it likely won't happen in the future. Even if the FCC comes down in an enforcement capacity and says, "We're going to fine commercial carriers if they fail to provide the service to public safety," to them it's a business decision. When we need it, it's not there.

**ADMIRAL JAMES BARNETT,
CHIEF, FCC PUBLIC SAFETY AND
HOMELAND SECURITY BUREAU:
Public Safety Must Join Private Carriers
In Building Out the Broadband System Now**

These really are critical issues, and they have been my primary focus at the FCC since I arrived in July 2009. My first job was in the U.S. Navy aboard a destroyer as a communications officer, so I learned early on as a young man in uniform about the criticality of voice and data communications and what it means. It means life or death. It means mission failure or success.



A bit of history: The FCC spent a number of years seeking to establish a nationwide interoperable public safety broadband network. The first step was reclaiming some spectrum. Part of that spectrum was dedicated without cost to public safety. An adjacent block, the D Block, was slated by Congress for commercial sale through an auction. The initial approach would have created a mandatory public-private partnership between the auction winner of the D Block and the national public safety licensee of the adjacent public safety spectrum.

As we all know, that didn't work. There was too much uncertainty regarding the requirements that would be placed on the potential D Block winner, which called into question whether such a venture would be commercially viable. So nobody bid on the minimum requirement for the D Block. The D Block remains as Congress designated for commercial use, and the FCC is mandated by law to auction it for commercial use.

We are determined that we are going to succeed this time, and the first thing we're doing is learning the lessons from the recent past. Last summer, I charged our public safety team to start from scratch and review all available options for creating a nationwide interoperable public safety network. Our investigation had to be fact-based and data-driven. Recommendations had to be based on reasons, logic, facts, data, or models. The process was very open; we've had workshops, forums, field hearings, and scores of meetings and conferences with public safety officials, including many of you in this room, to ensure that we had public safety input and that we understood your requirements.

**NATIONWIDE COVERAGE, INTEROPERABILITY,
TECHNICAL AND COMMERCIAL VIABILITY**

From the outset, I emphasized that any option we chose must meet certain basic requirements. Number one, I told them that it has to be truly nationwide; it needs to cover the densest population centers and the most rural areas. Number two, it must have true nationwide interoperability. Number three, it must meet public safety's unique needs for coverage and mission-

critical reliability in emergency situations. Number four, it must be technically viable—in other words, it has to work—and also that it's commercially viable, so it will not be cost-prohibitive to public safety agencies that have limited resources. Number five, that it leapfrogs public safety to advanced 4G broadband technologies and that it keeps pace with evolving technological developments, so that public safety doesn't get isolated on a technological island. Number six, that it captures economies of scale in equipment and service costs, and number seven, that it captures the way that commercial broadband develops in order to save significant money. The commercial broadband networks are about to take off. If we don't get the public safety network going with them, it will cost significantly more, perhaps as much as 50 percent more. And we also know that we need to design a public safety network that is secure; it has to have proper authentication and access restrictions, that it can survive physical forces such as storms or earthquakes, and that communication networks are properly encrypted.

I understand that our recommendation on the D block has disappointed you, and I have not shied away from this discussion, nor have I discouraged anyone in public safety from vying for the D Block. In fact, I think you should continue any plans you have for making your arguments to Congress, which holds the ultimate sway in this.

PUBLIC SAFETY WILL NEED MORE THAN 10 MHz

I think we can also agree that public safety will someday need more spectrum than the 10 MHz designated to it by Congress. But the record of information filed by public safety on the need for more spectrum *now* was sparse; really it was only New York City [that filed a brief]. And that brief was insufficient from an engineering standpoint. It did not meet fact-based, data-driven requirements.

I'm convinced that we've come up with a plan that not only meets our objectives, and also provides the best and most achievable path for doing so, a path that that does not require the D block, but provides more resiliency, redundancy, and access to capacity than the D block would alone.

Our plan establishes a 3-prong approach for creating the network. First, it includes an administrative system that will enable public safety users to effectively use the public safety broadband spectrum, and also provides access to additional capacity on a day-to-day and emergency basis.

Two, we will establish an Emergency Response Interoperability Center, or ERIC, to ensure nationwide interoperability, and operability of the network.

And third, there has to be a program for public funding, to provide needed funding for deployment and ongoing costs of the network.

Let me address your concern that the public safety community cannot rely on roaming and priority access to commercial networks. I don't agree. I do agree that we need to work together with public safety to make sure that roaming and priority access work effectively. But I am convinced that through a system of license conditions, grant conditions, standards, and

regulatory requirements, we can ensure that. These discussions are already starting and we will continue to make sure that we get this right.

Without adequate funding, there will not be a nationwide interoperable public safety network. We have completed a detailed cost model on how this can work. The D block alone will not produce the nationwide and perhaps not the interoperable network, and no one that I've seen yet has produced a real-cost model and business plan for how that would work.

Under our plan, you will still own your own spectrum, and you will get to use commercial spectrum as well. We know that reliance on commercial networks alone will not meet public safety's specific needs for network reliability, resiliency, and coverage in remote areas where commercial providers are unlikely to deal. Therefore, we propose public funding to ensure that all of these requirements are met. In essence, what we propose is \$6.5 billion in capital expenditures over a 10-year period to be funded through direct federal grants to public safety, and another \$6 billion to \$10 billion over 10 years for operating costs, which will ramp up as the network expands to a peak of \$1.3 billion a year.

I'm not going to claim to you that this is perfect. But it is workable and it should be funded.

Of course, this funding requires action by Congress, and this is where your voices need to be heard. 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 the technological wave that will actually reduce the costs of this network in the long run. So I have a request for you and a prediction. You have friends in Washington who are poised to move forward on funding for a national public safety broadband network. They see the potential. They are willing to risk political capital

to find the funding. All that is needed to move these friends of yours forward is to hear from public safety that this plan is workable and that public safety wants it funded. It is now in your hands whether that goes forward or not. But right now the only message that is getting through to our political leaders is public safety's dissatisfaction and that it only wants the D block. So my fervent personal request of each of you is that you suspend any distrust that I understand that you have, and that you change the message to one that public safety thinks this plan can work. You can also ask for the D block, but if that is the first and only thing that is said, or if the concerns about the roaming and access are the only thing that is heard, then I also have a prediction for you. Public safety could miss this brief once-in-a-lifetime opportunity afforded by the delivery of the FCC's national broadband plan, not get the funding, and not get the D block. Public safety must change its message, and that must come within days, if not hours.

I don't agree that if public safety gets the D block but not the money, then it's OK. If you don't have the money right now, you're going to miss the technological end of it because the 4G networks are poised to take off. If you don't build out the public safety network with them, your costs go up exponentially, and how many jurisdictions will be able to afford that?

PERF Executive Director Chuck Wexler: What makes you think private carriers will bid on the D block this time when they didn't last time?

Admiral Barnett: The last time, it was an open-ended thing. There were so many requirements on it that they just couldn't see commercial viability. It looked to them like an open checkbook. That's why our team worked to make sure that our plan is viable both for public safety and for the commercial entities, so they won't walk away from it.

SAN JOSE POLICE CHIEF ROB DAVIS:
**We Are the Ones Who Know What We Need,
Because We Have Been at the Center of It**


We know what we need. We're the ones who are doing this work. We have been in the middle of these disasters. We're the ones who have been struggling to get our communications systems going. We have been in the trenches. We've seen the failures that have occurred; when we pick up the cell phone, it doesn't work. We know what technology currently exists out there and what will be coming down the road. We know what we're trying to do with our national fusion centers. We know about the relationships we are trying to develop with our federal and state partners to share information not just in response to a disaster, but in terms of sharing data to prevent crime and terrorism from happening.

We know where we're going; we know what we need; and we know that we need to lock this spectrum down. If we can't get that spectrum, all this discussion about money that *might* come in the future is irrelevant. We've got to get our foot on the real estate now.

SAN DIEGO CHIEF BILL LANSDOWNE:
**This Is a Chance to Do Something
For the Future of Public Safety**

Admiral, first let me thank you for your great service to this country and for all the work you've done. The United States is the longest-lasting democracy the world has ever seen, and I think there are two great entities that protect it—the military, and public safety.

There's a unique happening in this room that I haven't seen in 40 years, and that is we've got police and fire in one place with one request: Give us the tools that we need. Police and fire departments don't always get along this well, but on this issue we are absolutely unified. My read on this is that our voice is getting louder, and we have an opportunity of a lifetime to fix something for the future, for the next generations of chiefs, both fire and police.

Next year, I'm probably going to have wildfires coming at us again in San Diego, and I'm going to have to mobilize and communicate with a lot of people, and I will have exactly the same problem I've had before—I can't communicate with fire, I can't communicate with medical services, I can't talk to the military that comes in. Admiral, I thank you for everything you said, I know you've got a difficult job, but quite frankly, I don't agree with you. I think we need this spectrum. 

Congressional Committees With Jurisdiction Over Broadband Issues

House Committee on Energy and Commerce

Democrats

Henry A. Waxman, CA, Chair
John D. Dingell, MI, Chair Emeritus
Edward J. Markey, MA
Rick Boucher, VA
Frank Pallone, Jr., NJ
Bart Gordon, TN
Bobby L. Rush, IL
Anna G. Eshoo, CA
Bart Stupak, MI
Eliot L. Engel, NY
Gene Green, TX
Diana DeGette, CO
Lois Capps, CA
Mike Doyle, PA
Jane Harman, CA
Jan Schakowsky, IL
Charles A. Gonzalez, TX

Jay Inslee, WA
Tammy Baldwin, WI
Mike Ross, AR
Anthony D. Weiner, NY
Jim Matheson, UT
G.K. Butterfield, NC
Charlie Melancon, LA
John Barrow, GA
Baron P. Hill, IN
Doris O. Matsui, CA
Donna M. Christensen, VI
Kathy Castor, FL
John P. Sarbanes, MD
Christopher S. Murphy, CT
Zachary T. Space, OH
Jerry McNerney, CA
Betty Sutton, OH
Bruce L. Braley, IA
Peter Welch, VT

Republicans

Joe Barton, TX, Ranking Republican Member
Ralph M. Hall, TX
Fred Upton, MI
Cliff Stearns, FL
Nathan Deal, GA
Ed Whitfield, KY
John Shimkus, IL
John B. Shadegg, AZ
Roy Blunt, MO
Steve Buyer, IN
George Radanovich, CA
Joseph R. Pitts, PA
Mary Bono Mack, CA
Lee Terry, NE
Mike Rogers, MI
Sue Wilkins Myrick, NC
John Sullivan, OK
Tim Murphy, PA

Michael C. Burgess, TX
Marsha Blackburn, TN
Phil Gingrey, GA
Steve Scalise, LA
Parker Griffith, AL

Senate Committee on Commerce, Science, and Transportation

Democrats

John D. Rockefeller IV, Chairman, WV
Daniel K. Inouye, HI
John F. Kerry, MA
Byron L. Dorgan, ND
Barbara Boxer, CA
Bill Nelson, FL
Maria Cantwell, WA

Frank R. Lautenberg, NJ
Mark Pryor, AR
Claire McCaskill, MO
Amy Klobuchar, MN
Tom Udall, NM
Mark Warner, VA
Mark Begich, AK

Republicans

Kay Bailey Hutchison, TX, Ranking Republican Member
Olympia Snowe, ME
John Ensign, NV
Jim DeMint, SC
John Thune, SD

Roger Wicker, MS
George S. LeMieux, FL
Johnny Isakson, GA
David Vitter, LA
Sam Brownback, KS
Mike Johanns, NE



NYPD White Paper Addresses the Question: How Much Spectrum Does Public Safety Need?

Debate over the future of public safety broadband communication inevitably comes down to one question: How much spectrum does public safety really need? New York City attempted to find out.

In November 2009, the FCC issued a public notice seeking comment on public safety, homeland security, and cybersecurity elements of the National Broadband Plan. New York City submitted comments in response, outlining the needs of the public safety community over time for mobile wireless broadband networks and applications, both for normal operations and in case of a major emergency. An excerpt of these comments was later reproduced in a white paper submitted to the FCC by the New York City Police Department in February 2010, entitled “700 MHz Broadband Public Safety Applications and Spectrum Requirements.”

The City of New York already had extensive experience with the challenges and demands of a public safety broadband network. In 2009, the city finished deploying the New York City Wireless Network (NYCWIN), a high-speed mobile broadband network for public safety and government agencies.

Using data from the build-out and operation of that system, the city was able to determine the data demands of different public safety applications, and to estimate the total bandwidth needs for the public safety community of a major city, using a secure network on 700 MHz spectrum.

Bandwidth needs are not the same in all situations. New York City projected what would be needed for day-to-day operations, both today and over the next 12 years; what would be needed to respond to a major emergency; and how taxed the city’s public safety bandwidth capacity would be both with and without access to the D Block.

Normal Day-To-Day Operations: Without D Block, Problems Surface in 6 Years

When projecting the day-to-day needs, the city said it used models “similar in structure to those models used by commercial broadband providers in analysis of their capacity needs, but adapted with assumptions appropriate for public safety usage.”

The model assumed as a starting point that there would be 1,000 vehicle-installed mobile data terminals in NYPD cruisers, 40 license-plate-recognition units, 100 mobile video assets, and 1,000 mobile handheld device users.

The model predicts that public safety usage will increase on an “s-curve” over a 12-year period: building slowly over the first few years, then increasingly quickly, and tailing off in the final years. By the end of 12 years, the model predicts a final count of 10,000 vehicle-installed mobile data terminals, 1,200 license plate recognition units, 2,000 video assets, and 25,000 mobile

handheld users. In addition, the model predicts that each mobile data terminal and mobile handheld unit will use 5 percent more broadband each year, to account for increased usage and new applications.

The city said that these are all conservative projections, and that “these estimates may be low as secure broadband data access becomes an integral part of everyday operations.”

According to this model, if public safety does not have access to the D-Block and therefore has only 10 MHz of dedicated spectrum for their broadband needs, demand for uplink (sending out data) would reach 75 percent of capacity in year 5 and 100 percent in year 6; and demand for downlink (receiving data) would be at 75 percent in year 7, and 100 percent in year 9.

But with the additional 10 MHz of the D Block, the model paints a more favorable picture. With a total of 20 MHz at public safety’s disposal, uplink demand reaches 75 percent of capacity in year 8 and never reaches 100 percent over the 12-year period. The downlink demand never reaches as high as 75 percent over the entire 12 years.

Dirty-Bomb Emergency Response Scenario: 10 MHz of Spectrum “Falls Considerably Short”

A public safety broadband network cannot be functional only in everyday operations; it must also provide mission-critical support in the event of a catastrophe, natural or man-made, during which time public safety demand for broadband would drastically spike.

Not only would local agencies need more broadband, but a major incident would also bring in first responders and support personnel from other agencies, who would all be using the network upon arrival. The city notes that “the number of active users could increase by approximately 75 percent if a large response is required.” This would be the true test of a public safety broadband network.

In its comments to the FCC, New York City attempted to determine how much spectrum is required to meet the needs of first responder emergency operations. The city’s model was based on a theoretical “dirty bomb” terrorist attack at Pennsylvania Station in Midtown Manhattan. This would trigger a coordinated response from many agencies, including New York City police, fire, and emergency medical services and the Office of Emergency Management Services, each with unique broadband needs.

The city’s conclusion: “For the incident scenario presented and the associated site density, 10 MHz of spectrum will fall considerably short of the required bandwidth demand. 20 MHz of spectrum is barely sufficient.”

The NYPD analysis, *700 MHz Broadband Public Safety Applications and Spectrum Requirements*, is available online here: http://d-block.net/assets/pdf/NYC_Spectrum_Requirements.pdf.



POLICE EXECUTIVE
RESEARCH FORUM

SUBJECT TO DEBATE
1120 Connecticut Avenue, NW
Suite 930
Washington, DC 20036

Pre-Sorted
First Class
U.S. Postage
PAID
Permit No. 4889
Suburban, MD



POLICE EXECUTIVE
RESEARCH FORUM

BOARD OF DIRECTORS

PRESIDENT

Charles Ramsey | Commissioner,
Philadelphia Police Department

VICE PRESIDENT

Charlie T. Deane | Chief, Prince
William County, Va., Police Department

TREASURER

William M. Lansdowne | Chief,
San Diego Police Department

SECRETARY

Rick Myers | Chief, Colorado Springs
Police Department

AT-LARGE MEMBERS

Edward Flynn | Chief, Milwaukee
Police Department

William Blair | Chief, Toronto Police
Service

EX OFFICIO MEMBER

Sir Hugh Orde | President, Association
of Chief Police Officers (UK)

EXECUTIVE DIRECTOR:

Chuck Wexler

EDITOR:

Craig Fischer

The Police Executive Research Forum is a nonprofit association of progressive police professionals dedicated to improving services to all our communities. ■ *Subject to Debate*, published by the Police Executive Research Forum, welcomes input from PERF members and other interested parties. Please submit articles, ideas and suggestions to Craig Fischer, PERF, 1120 Connecticut Ave., NW, Suite 930, Washington, D.C. 20036. Phone: (202) 454-8332; fax: (202) 466-7826; e-mail: cfischer@policeforum.org. ■ Contributors' opinions and statements do not necessarily reflect the policies or positions of the Police Executive Research Forum. ISSN 1084-7316. ■ Subscription price: \$35/year.