# Progress on P25: Furthering Interoperability and Competition for Public Safety Radio Equipment

Statement by:

Tom Sorley
Deputy Director Radio Communications Technology
City of Houston

before the

Subcommittee on Technology and Innovation, House Committee on Science and Technology

September 23, 2010

Hello, my name is Tom Sorley. I am the Deputy Director of Radio Communication Services for the City of Houston. I also serve as the Chair of the Technology Committee for the National Public-Safety Telecommunications Council and as Vice-Chair of the Governing Board for the Department of Homeland Security Project 25 Compliance Assessment Program.

I am leading the City of Houston's efforts to implement one of the largest P25 radio systems in the Country. Once completed, the system will be one of the first to implement the newest version of the P25 standard known as Phase 2. This newest version of the standard was created to operate with double the frequency efficiency of the currently deployed Phase 1 systems. This efficiency is paramount for large metropolitan areas such as Houston which suffer from severe spectrum shortages.

Designing, building, and operating a P25 radio system can be a big challenge. The standard is actually a suite of standards that has hundreds of sub-elements. Most people that are writing specifications to buy a new system do not know enough about the P25 suite of standards to even properly document their requirements. In fact, most just specify that the technology must be P25 compliant. They fail to specify individual elements that must be complaint and the result is that systems are sold as P25 complaint when many parts of the system that could be standards-based remain proprietary.

The City of Houston has more resources than most agencies in the country and therefore we were able to employ one of the largest consulting firms in the public safety communications industry. However, even with our expertise and the assistance of our consultant, there were still items that we missed related to the P25 standard. Imagine the challenges facing small rural public safety entities. I believe this is due to the complexity of the standard and the ever changing elements that make up the standard.

The P25 standards development process has been going on for more than 20 years. As mentioned previously, there are many elements to the standard and several interfaces that all must be fully defined. While this work is being done, technology continues to change. In fact as the years pass, the rate of technology change is increasing. Further complicating the process are regulatory changes, such as frequency efficiency rules, that must be addressed in the standards development process. While it is true that technology standards must be constantly updated, some better way of delineating the P25 standard must be developed.

It would be very helpful if the P25 process created versions that could be easily summarized. (example P25 version 3) This version number would allow agencies to know what is included as part of the P25 standard and more importantly what is not included. This is done in other technology standards such as IEEE 802.11 which is a widely accepted standard for wireless local area networks. The 802.11 standard has many versions delineated by different letters of the alphabet. Although consumers don't necessarily understand the difference between 802.11a and 802.11n, they can easily understand that a product is compliant to one version or the other. The bottom line is that P25 has so many moving parts comprised of many different standards within the suite of standards that the lay person would have no real way of determining if the products they are buying really conform.

The three key aspects of Project 25 that make it particularly important for improved communications interoperability:

- 1. The initiative was begun and is driven by public safety agencies and organizations.
- 2. It proceeds with both a vision of forthcoming technological change and the need for graceful migration between technologies used by public safety.
- 3. Competition founded on open standards would produce the best technology, at the best prices for pubic safety agencies.

#### **Driven by Public Safety Agencies and Organizations**

Over the years, public safety involvement in the P25 standards development process has become harder and harder to maintain. Some key public safety representatives have been involved virtually from the beginning of the process. However, the number is small and the involvement of others is limited at best. Vendor representatives vastly outnumber public safety. Most of the major vendors have several people that dedicate a substantial portion of their work time to participate in P25. In reality, this means that the standard is being driven by the active participants – vendors.

The P25 standard development process is set up to encourage consistent participation from both vendors and public safety officials. While this seems like a valid approach, travel restrictions on local public safety representatives often leave them unable to consistently attend making them ineligible to vote on key items. Also, the P25 Steering Committee only has two of the initial public safety representatives who have never been rotated, leaving the impression that they have become more partial to the vendors' perspectives on key issues.

The process could be improved by providing more public safety representation on the Steering Committee and by creating limited, staggered terms for those representatives.

#### **Technology Change and Graceful Migration**

As previously discussed, the pace of the standards development process is slow. The rapid pace of technology change further slows the completion of this complicated suite of standards. Also, in some cases, it is in the best interest of the vendor community to have parts of the standard lag as this creates an unmet need that must be filled with a proprietary option. For example: The P25 standard has provisions that allow vendors to offer proprietary features/functions provided there is not an equivalent feature/function mandated by the standard. This serves as a motivator to slow the process down.

#### **P25** Competition

Competition is hampered by a lack of understanding by public safety agencies. The only consistent P25 education effort is conducted by the P25 Technology Interest Group (PTIG). This group is made up of vendors and public safety representatives that are charged to promote the success of Project 25 and educate interested parties on the benefits that the standard offers. As indicated in their purpose statement, this group is focused on the success of the standard. I

believe that a group needs to be established that is focused solely on the education and success of public safety agencies using or contemplating the use of P25 equipment.

This public safety education effort should be focused around helping local, state, and federal agencies understand the standard by creating outreach materials, draft requirements language, draft purchasing language, and draft contract language. It would seem that the existing partnership between DHS and OEC in the P25 CAP could be expanded to include this new role. However, to be effective this effort must be undertaken seriously and appropriately funded.

Competition is not encouraged by manufacturers. P25 manufacturers often try to sell proprietary features that reside on top of the basic P25 operation of the radios in order to force future sales of their products. Some examples include very simple encryption algorithms that are proprietary and appear to solve a problem for local agencies by providing a cost-effective alternative to standards-based encryption that typically costs several hundred dollars more. However, new entrants into that system, or existing agencies on that system that need radios, are forced to remain with that particular vendor to maintain interoperability with the existing radios that utilize the proprietary encryption. Radios on systems are rarely replaced in mass. Therefore, an initial decision on proprietary options has far-reaching impact for years to come.

Another example of this practice is making accessories that are dependent on particular radios and/or other related items. Years ago, siren controls in police cars were integrated into mobile radios to make the user experience easier. However, compatibility ultimately became an issue as a result most public safety agencies de-coupled siren controls and radios in the late 1980's. Recently, our vendor proposed that we consider using a new integrated control head for our radios. The users were very interested in the device as the functionality and ease of use met most of their needs. However, the control head would only operate that particular vendor's siren control package. This would have forced us into a proprietary relationship with radios and related sirens limiting our future buying options. We chose to pass on the option.

#### **P25 Compliance Assessment Program**

The DHS CAP is a relatively new program that endeavors to ensure that products marketed and sold to public safety as P25 actually adhere to the standard. Years ago, the P25 participants produced a paper on compliance assessment that established three types of tests to prove compliance:

- 1. Performance This test ensures the device performs to the specifications.
- 2. Conformance This test ensures the device adheres to the P25 standard.
- 3. Interoperability This test ensures the device seamlessly interacts with similar devices.

The P25 Compliance Assessment Process and Procedures Task Group (CAPPTG) drafts Recommended Compliance Assessment Tests (RCAT). These RCATs are used as input documents into the DHS CAP program. The National Institute of Standards and Technology (NIST) participates in P25 and provides input to the CAPPTG to consider in the development of RCATs. However, like public safety representatives, NIST is outnumbered by vendors on this

task group. In the past two years, several critical votes have been divided down the line of vendors versus public safety. Each of these votes was decided in favor of the vendor position.

The DHS CAP program created and published the first Compliance Assessment Bulletin that was based substantially (but not completely) on the RCAT from the CAPPTG. Subsequently, the CAPPTG changed its stance and said that Conformance testing was no longer needed. Instead, they advocated replacing conformance testing with enhanced Interoperability testing. The CAP Governing Board and several leading public safety agencies objected to this change. Eventually, the manufacturers acquiesced on this in regard to the Inter Subsystem Interface (ISSI). In fact, some of them testified earlier this year at this sub-committee stressing that they were committed to the CAP program and would continue to participate even if conformance testing were required.

Over the last several months, those same vendors are reverting back to their previous stance on Conformance testing. They have asserted that the testing is too complicated, expensive and burdensome. This is their position even though NIST has created a test and developed a test tool that is easily adopted. In meetings earlier in the year, one vendor stated that they already run ALL the conformance tests during development making the need to repeat them unnecessary. None of the other vendors in attendance at that meeting raised an issue with that statement. If the vendors already run ALL the conformance tests during development and NIST has develop a test while publishing all the applicable test code, why is it that conformance testing is still too complicated, expensive, and burdensome? If developing a test tool to perform conformance tests is too onerous for the vendors, DHS should charge NIST to expand their support of the CAP program by developing the tests and making them available to the test laboratories.

The DHS CAP work plan has been largely driven by the availability of RCATs from the CAPPTG. This is based on the assumption that the P25 process contained the largest collection of P25 experts making it the logical place for test requirements development. Again, NIST and public safety representatives are involved in that process. However, development of RCATs can be delayed based on any number of factors. As an example, P25 trunked radios have been sold in the market place for more than 10 years but there is not one RCAT available that includes conformance tests for trunking functionality. The CAP governing board would like to develop and release Compliance Assessment Bulletins establishing the testing of P25 features prior to or in concert with those features entering the market place. We have a great deal of catching up to do, but it clear to us that we may have to develop an alternate process that is not dependent upon the P25 CAPPTG developed RCATs.

Most major public safety associations have publically advocated for retaining all three types of tests: performance, conformance, and interoperability as each play a key role in determining if a product is compliant. First responders must be able to predict with certainty what the device they use will perform as expected. It is imperative that each type of test be performed to make sure.

One complicating factor in the DHS CAP is the fact that it is voluntary. No vendor is forced to participate. To date, most vendors do participate, but during the disagreement over conformance testing of the ISSI several vendors informally indicated that if conformance testing was pursued, they would simply not participate. If all the vendors chose to opt out of the process, the process

dies. DHS has included a requirement in the Federal Grant Guidance that requires any P25 equipment purchased with grant funds must have a Suppliers Declaration of Compliance (SDOC) on file on the Responder Knowledge Base (RKB) website. However, there are creative ways to get around this requirement. For instance, I heard a story last month that a vendor was willing to give away certain features as "add-ons" to avoid the SDOC requirement. I am not sure if making P25 CAP a mandatory requirement is practical, but it should be investigated.

#### Why not just use Cell Phones?

Recently, Reuven Carlyle a State Representative from the Seattle, Washington area posted an entry into his blog entitled, "Want Government Reform? Idea #3: A new public safety communication strategy." (Attachment A). In this blog post, Representative Carlyle asserted (among other things) that P25 radios are too expensive and public safety would be better served using cell phones. He asserts that US public safety agencies pay many times more for their equipment than do their counterparts in other countries. While some points in the blog on the surface appear to be true, they are not presented in context.

Several days after Rep. Carlyle's blog, Bill Schrier, CIO of the City of Seattle drafted his own blog entry in response. (Attachment B). In Mr. Schrier's post, he points out many of the flaws in the original post by Rep. Carlyle. I agree with all of Mr. Schrier's points. Simply put, public safety has several requirements that can't possibly be met by cellular devices. Network priority, reliability, availability during disasters or weather events, talk-around mode, and ruggedness are several of the requirements that public safety radios need and cellular devices and systems can't provide.

I have the responsibility of buying these devices for the City of Houston. I would love to be able to purchase a cellular phone that met the needs of public safety. However, one does not exist and it is quite unlikely that one will exist in the foreseeable future.

I would like to thank Chairman Wu for inviting me to testify today. On behalf of public safety and the City of Houston, I would like to commend the work of the sub-committee as it relates to public safety communications and encourage you to continue to weigh in on this important topic.

### **Attachment A**



## Want government reform? Idea #3: A new public safety communication strategy

By Reuven Carlyle September 6, 2010



Have you ever noticed how police officers carry both a cellular phone and a hand-held radio? It might surprise you to learn that you are paying hundreds of times more for the radio than the cell phone. And you're about to pay millions more unless we have the courage to change course. Even the New York Times is <u>starting to agitate</u>.

When I joined McCaw Cellular Communications in the early 1990s—one of the world's most entrepreneurial companies—less than 10 million Americans had mobile phones. They were big, clunky and had no data capability. Today there are as many mobile phones as people, prices have fallen and consumers have benefitted from innovation that led to iPhones, Windows Mobile, Droid and other robust platforms. The change has been technically disruptive and positive. In that same time, the nation's public safety community—law enforcement, fire, EMS—has also spent billions of public tax dollars on new infrastructure and yet the quality, cost and functionality of their expensive, proprietary, two-way radios has not materially improved since the 1970s.

Now, the taxpayers of Seattle, King County and Washington State are being asked to spend up to hundreds of millions more for a brand new radio system for police, fire, EMS and other emergency workers.

In Seattle and King County alone my gut check is that the cost will be in the \$50 million to \$250 million range. Since I'm not on the inside I don't know if this is close or far from the truth, but my gut is that it's uncomfortably in that range. And that says nothing of our friends in Pierce, Snohomish and other

communities who are struggling through a similar journey. And Oregon is much further down the same pathway and is now politically panicking in the face of a \$600 million bill.

It's time for courageous honesty: In my personal view, the decision is the wrong direction technically, politically, and financially.

The uncomfortable truth is that for city, county and state governments public safety radio equipment costs between 10x and 100x more than it does in most other countries, despite the U.S. leadership position for wireless technologies such as smartphones, WiFi, WiMax and more. Even Seattle, in many ways the hometown of the consumer wireless industry, will pay tens of millions for a proprietary new police radio system.

The reason is that the nation's public safety communications market does not enjoy healthy, vibrant, market-based competition in any way comparable to consumer mobile services

First of all, it is important to acknowledge that we must ensure our police, fire and EMS officials have access to high quality emergency communication systems. Unfortunately, we must upgrade the hardware-based system because the current vendor for the Seattle and King County system, Motorola, has made a business decision to end support for the current network.

In fairness, they told us long ago they would eventually turn off our system, and we needed to buy their next generation system (or conceptually their competitor's system). Unlike in the consumer market, we may have purchased the equipment, but the company retains the right to determine how long our system is supported. It's not much of an exaggeration to say that it's sort of like Verizon asking consumers to directly fund new cell towers and network and then forcing everyone to buy new mobile phones because the company wants to upgrade their internal network capabilities.

Second, our nation's first responders and 9-1-1 dispatchers aggressively moved to establish an industry standard for first responders called "P25" to get better radios at lower prices, to break the monopoly of the current structure. Unfortunately, more than 25 years later, P25 is still not available, still not implemented and even the Chairman of the FCC recently jolted Members of Congress by acknowledging "...[P25] has taken more than 20 years to develop and is still not complete" and "the protracted development of P25 has allowed vendors to take advantage of selling proprietary solutions."

The industry knows that P25 isn't, in fact, truly standards-based and has resulted in even more expensive radios, not the other way around. If our state's march toward P25 continues, it will be more business as usual – and first responder radios will still cost \$5,000 each. (Did you catch that? Just one P25 radio for one police officer costs \$5,000 and yet it has less processing power and functionality than an iPhone, Windows Mobile or Droid phone).

Yet with few exceptions that is exactly where our current 'group think' in Seattle and King County is leading.

Third, some local Seattle and King County officials have recently applied for the Obama Administration's plans for broadband across the nation utilizing "4G" or "LTE" technology on 700 MHz... for the Seattle area. Their position is inspired in part because the broadband system would help first responders. And yet The National Broadband Plan, as written, doesn't help with voice communications—the most essential element for police, fire and EMS officials.

This isn't a modest technical decision, it's a major policy choice facing King County Executive Dow Constantine and the county council as well as Mayor Michael McGinn and the city council.

Here's a picture of where Seattle and King County are headed if we don't change direction: The first 4G or LTE system built in the U.S. for first responders is already underway, in the San Francisco Bay Area – a geography and population similar to our own. The federal government is fronting the \$50 million it will

cost, and the result is that 300 public safety vehicles will be equipped with 4G data modems. That is \$167,000 per police car and fire truck, for video to and from the scene.

At the same time the consumer marketplace—AT&T, Verizon, Sprint and T-Mobile—provides virtually the same mobile service at a fraction of the cost at equal or higher service quality levels in many cases. Public safety is building their own mirror system to commercial services. A mirror system that is on track to be proprietary, closed, and expensive like our existing first responder radio systems.

Of course consumer cellular phones are not perfect nor always a technically viable alternative, and they are by no means a simple alternative, but philosophically they demonstrate the profound value of market-based competition.

I am willing to bet a private tour of the State Capitol building that if you ask 20 police, fire and EMS officials to choose between their cellular phones and their two way radios, the majority will choose to hold onto the former. Their mobile phones are easier, more flexible, equally as reliable in most cases and now support data.

Without question it's important to acknowledge that technically cell phones do have limitations – in basements, rural and other "out of coverage" areas they won't provide essential voice communications for first responders. But the very important and dirty little secret is that neither do the P25 radio systems, or the 4G/LTE systems. Our first responders need handsets that utilize the high feature / low cost advantages of open market cell phone systems, but also work in basements "peer to peer" when out of range of the system. And that solution still shouldn't cost \$5,000 for each and every single radio.

While it is true public safety radios need to be heavy duty, it doesn't inherently mean they should cost 10 times as much as commercial systems that have more processing power, more technical flexibility and more application functionality.

Yes this is a bit technical and wonky but the financial implications are stunning in scale – as Oregon is experiencing, approaching \$1 billion when the costs of all local agencies are included with the first \$600 million buildout.

Is it too late? There is a way forward if we have the courageous honesty to tackle old assumptions and myths.

- 1. We should stop buying P25 radios at literally \$5,000 per radio and start buying TETRA radios. TETRA is similar to P25, but it is truly open standard radio used by police and fire departments in Europe and Asia . They offer more features and are tested around the globe... and cost less than \$500 each. They are essentially "Nextel-like" in their capability but are a fraction of the cost of the non-open standard P25.
- 2. We should absolutely back a national broadband plan but not this one. Not until it is legally bound to an open, public standard that enables true, free market participation from any and all vendors. Not a penny of federal or state funding should go towards any proprietary 4G/LTE solutions, and Seattle and King County public safety leaders should insist on an open standard before launching any 4G/LTE 700 MHz construction in Washington.
- 3. Let's ask line officers and regular firefighters what they need to do their jobs. They are the users and yet we rarely ask them firsthand what they need to succeed.
- 4. Investigate the real-deal of the \$50 million pilot project in San Francisco, which puts the proprietary 4G/LTE technology in the lead for another 20-year monopoly. Let's understand the implications before Seattle goes down the same expensive route—but likely without the pot of federal money provided to San Francisco.
- 5. We're not the only ones with this issue. We should ask other regions and states to join us in asking for a market that gives our first responders what they really need, at a price that we can afford.

6. We should have the courage to explore a stronger partnership with commercial mobile operators in underserved areas. We could subsidize the expansion of their networks and provide cell tower sites, for example, in exchange for more sophisticated 'priority access' for public safety—and improved service level agreements—and pricing breaks.

Perhaps a stronger partnership with Oregon could save us both hundreds of millions of dollars or more. We can no longer afford a world where each state, each county, each city 'goes it alone' in the delivery of 'utility' services such as communications. Imagine our buying power united by a technical vision and strategy?

Unfortunately, at the end of the day, we acknowledge we have to buy a new radio system for our faithful and hard-working police, firefighters, and EMTs in the Seattle and King County area.

We as a city, county and state are more innovative, entrepreneurial and technically sophisticated than this. If we believe in government reform and want to display to the public that we have the courageous honesty to seize the opportunity of this crisis, we need to change course even in sacred areas like public safety. We have to question old assumptions, challenge monopolies inside and outside of government, and demand that when taxpayers are paying the bill, there is value for our dollar.

It's the right thing for the public who are served by our courageous law enforcement, firefighters and EMS officials. And it's right for taxpayers.

Your partner in service,

Reuven.

## **Attachment B**

#### Why Don't Cops and Firefighters Just Use Cell Phones?

By Bill Schrier, bill.schrier@seattle.gov Chief Technology Officer, City of Seattle September 10, 2010



Police officers and firefighters carry \$5000 radios. Local and state governments spend hundreds of millions of dollars to build public safety radio networks. Yet, today, cell phone networks seem to be everywhere, most people carry a mobile phone and many of us think paying \$199 for an iPhone is expensive.

Why can't cops and firefighters and emergency medical technicians (EMT) use cell phones like everyone else? A Washington State legislator from Seattle <u>recently public argued for this approach in his blog.</u> And, at first, this appears to be a simple way for governments to save a lot of taxpayer dollars.

Here are a few reasons public safety officers need their own dedicated networks:

- Priority. Cellular networks do not prioritize their users or traffic. A teenager's cell phone has the same priority as a cell phone used by a police officer or, for that matter, the BlackBerry used by President Obama. We've all experienced "no circuits available" or "network busy" when using a cell phone. When I'm being assaulted or have been injured in an automobile accident or even have had my house burglarized, the last thing I want is to have the network be "busy" so a police officer or EMT couldn't be dispatched. Public safety needs dedicated frequencies where police officers and firefighters have priority and even, perhaps, exclusive rights to for use, without calls being clogged by the public.
- Reliability. Seattle's public safety radio network, part of the larger King County-wide 800 megahertz public safety radio network, handles more than 60,000 police, fire and emergency medical calls every day. It operated last year with 99.9994% reliability that's about 189 seconds of downtime out of more the than 31 million seconds which composed the year 2009. On the average, only about five out of the 60,000 calls were delayed for any reason, and even then the average delay was about two seconds. What cell phone network has that kind of reliability? How many times have you experienced "no service" or "call dropped" with your cell phone? Do we want firefighters who are reviving a heart attack victim and talking to the emergency room on the radio to all-of-a-sudden have their call dropped? Or should police officers lose service when drunk drivers clog the roads and bars are closing at 2:00 AM because a cell phone company decides to do maintenance because "no one uses the network then"?
- <u>Disasters</u>. Even small disasters cause cell phone networks to collapse. In Seattle, we've had swat team actions or car accidents which have shut down a freeway. Suddenly cell phone service abruptly ceases in that area because EVERYONE is on their phone. A few years ago a rifleman was loose and <u>shooting people in Tacoma Mall</u>. Responding police and EMTs had communications because they had dedicated networks and frequencies, but again cell phone networks were overloaded and down. In a larger disaster such as an earthquake or hurricane (with associated evacuation of large cities), commercial networks will be overloaded or jammed for days by people trying to escape the affected areas. Do we want police and fire departments or even transportation, electric utilities and public works departments to be trying to use those same networks while they are responding to the disaster? I don't think so.
- <u>Talk-around</u>. A key feature of most government-operated networks is something called <u>talk-around or simplex or "walkie-talkie" mode</u>. In this mode, individual radios talk directly to each other, without using a radio or cell tower. This is very important at incident scenes -

firefighters commonly use it at the scene of a fire, because the radios will operate at the scene even if there isn't a tower nearby. But this NEVER a feature of cellular phone networks. If the cell tower is down or out of range, that cell phone in your hands is a useless lump of plastic. But the radios of public safety officers still work and will talk to each other even without the tower.

 Ruggedness. No firefighter in his/her right mind would fight a fire using a cell phone for communications. The heat, water and ruggedness of the environment would quickly destroy the device. Yet most public safety radios will survive being dropped repeatedly on the ground or being immersed in water for 30 minutes or more. No standard cell phone can survive the rigorous work of firefighting or policing.

Are there problems with the current dedicated public safety networks? Absolutely.. The use proprietary technologies, for example "Project 25". Theoretically all "Project 25" radios work on any "Project 25" radio system. But only a few of those are deployed around the nation. These proprietary technologies are one reason the radios cost up to \$5,000 each.

Representative Carlyle, in his blog, proposes that we deploy "Tetra" radios for public safety. While Tetra is common in some parts of the world, it is not used at all in the United States. This is a dangerous proposal, because it means Tetra networks we buy would not work with the equipment used by any other government or telecommunications carrier anywhere in the United States. If called to respond to a disaster overseas, we could talk to firefighters in Hong Kong or the police in Ireland, however.

Another problem we face is the small market - the total market for public safety is perhaps 10,000,000 radios which are replaced, say, once every 10 years. On the other hand, the cell phone market is huge - 260 million cell phones replaced every two years in the United States alone. The economies of scale means consumers will have a lot more choice, and their cell phones will be relatively cheap.

So is there some way to reduce the sky-high cost of these dedicated public safety networks while at the same time not endangering cops, firefighters, EMTs and the public in general?

Yes, there is.. The FCC, in its <u>national broadband plan</u>, and the federal Department of Commerce, with its <u>forward-thinking grant program for broadband</u>, are lighting the way for a new public safety network which will be more robust, national in scope, and interoperable. By "interoperable" I mean the new public safety equipment will probably operate almost anywhere in the nation, whether on a dedicated government network or on a commercial cell phone network. Here are some features of the new networks:

- The FCC and major public safety organizations have called for the new public safety networks to be built using a fourth generation (4G) technology called LTE long-term evolution. Not coincidently, this is the same technology which will be used by the major cell phone companies Verizon and AT&T when they construct their 4G networks. The commercial networks will operate on different frequencies than the public safety networks, but they will all be built in same general area of the wireless spectrum the 700 megahertz (MHz) band.
- Because they are all using the same technology (LTE) and are in a similar slice of radio spectrum (700 MHz) potentially they will all interoperate. That means that public safety officers will use the government networks and frequencies when they are within range, but could "roam" to a commercial network if necessary. So cops and firefighters will have the best of both worlds coverage from dedicated government networks and coverage from multiple private carriers. The FCC is even considering rules which would require the commercial companies to give public safety priority on the commercial LTE networks.

- Because everyone consumers, cops, firefighters and even general government workers such as transportation and utilities - are all using LTE, constructing the networks can be much cheaper. Commercial telecommunications carriers could put government antennas and equipment at their cell sites, and vice-versa. Perhaps the network equipment at the cell site, or even the central switches could be shared as well. Public safety will still be using its own frequencies and have priority, but could share many other network elements.
- And the radios used by individual public safety officers or placed in police vehicles and
  fire trucks can be much cheaper as well. Because manufacturers are all making
  equipment for the same technology LTE it could cost just a few hundred dollars. Again,
  there will be specialized and ruggedized devices for firefighters and others working in
  punishing environments, but the "innards" the electronics will be much less expensive.
- Next, we have to get all first and second responders to use the same or common networks. Here in Washington State, for example, we have multiple overlapping and duplicate networks. City and County police and fire in the region have one network, each electric utility (e.g. Seattle City Light) have another network. Transportation departments have their own networks (e.g. Seattle Transportation and Washington State Transportation each have their own separate network). The Washington State Patrol has its own separate network. The State Department of Natural Resources has its own network. Fish and Wildlife has its own network. And federal government agencies (FBI, customs and immigration) have their own networks. This is patently stupid and expensive. As we build these new fourth generation LTE networks, we need to build a single network with lots of sites and a lot of redundancy and hardening to withstand disasters. And everyone first and second responders from all agencies should use it.
- Finally, and perhaps most importantly, all the networks will be nationally interoperable. The lack of communications interoperability was a major finding of the <u>Commission which investigated the September 11th</u> World Trade Center attack. But with these new networks, a Seattle police officer's 4th generation LTE device will also work on New York City's LTE network or New Mexico's :LTE network or on any Verizon or AT&T network anywhere in the nation. As disasters happen anywhere in the United States, and first and second responders are rushed to the scene of the disaster, they can take their communications gear with them and it will work.

The City of Seattle is one of a handful (about 20) forward-thinking governments leading the way to deploy these new networks. Seattle's public safety LTE network, <a href="https://hopefully.launched.with.a.">hopefully.launched.with.a.</a> federal stimulus grant, will eventually expand throughout the Puget Sound region and across the State of Washington. The State of Oregon also has authority and a grant request to build an <a href="https://linearchy.li

Is all of this a pipe dream? I don't think so. A number of public and private companies, governments and telecommunciations carriers and equipment manufacturers <u>are working together</u> to realize it. Many of them are in the Public Safety Alliance. In the Federal government, the FCC is working with the <u>National Institute of Standards</u> and the Departments of Commerce and Homeland security are providing <u>grant funding</u>. It will take a lot of work and many years to realize this network.

But when it is finished, we'll have public safety networks which work to keep us safe, and consumer networks which work to keep us productive and linked to our friends and families. These networks will be separate yet connected. They will be built from common technologies. And they will be less expensive for taxpayers than the networks we have today.