5-2008

A "Successful" Policy for Public Safety Communications

Jon M. Peha
Carnegie Mellon University, peha@andrew.cmu.edu

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC

WT Docket No.06-150
and PS Docket No. 06-229

In the Matter of

Implementing a Broadband Interoperable Public Safety Network in the 700 MHz Band

Service Rules for the 698-746, 747-762 and 777-792 MHz Bands

A "Successful" Policy for Public Safety Communications

Jon M. Peha

Jon M. Peha
Professor of Electrical Engineering and Public Policy
Associate Director, Center for Wireless & Broadband Networking
Carnegie Mellon University

Address: Carnegie Mellon University
Department of EPP
Pittsburgh, PA 15213-3890
Phone: (412) 268-7126
Email: peha@cmu.edu
Web: www.ece.cmu.edu/~peha

May 26, 2008

1 Definition of a "Successful" Policy

No commercial company stepped forward in the recent auction to deploy a nationwide communications system that would serve public safety agencies in the 700 MHz band. Many have mistakenly referred to this outcome as a "failure." Such statements demonstrate an important misconception about what must be accomplished. The lack of a winning bidder should not be seen as failure, and more importantly, the existence of a winning bidder should not be seen as success. "Success" means providing American emergency responders with a communications system that truly meets their needs in a post-9/11 world. "Failure" means allocating this valuable spectrum in any manner that fails to meet public safety and homeland security needs. The lack of a bidder in the last auction or even the next auction is only a delay. Although no delay is welcome, this delay is small compared to the period that has already elapsed since September 11, 2001. No one should use a small delay as the principal excuse to compromise on the final objective.

That final objective remains as important as ever, for reasons that include but go far beyond the oft-cited issue of interoperability. As I have shown elsewhere [1], not only would a nationwide network for all local, state, and federal emergency responders put an end to technology-based interoperability problems, it would also allow public safety to meet its communications needs with perhaps an order of magnitude less spectrum, and it would save many billions of tax-payer dollars. Moreover, by making that nationwide network broadband, public safety agencies would also gain access to many life-saving capabilities that they lack today. A large-scale system can also be designed with the fault tolerance to continue operating in a major disaster, long after today's small-scale systems are largely inoperable. In other words, not only can the US afford a nationwide broadband network, but we pay extra for the failure-prone low-capacity spectrum-inefficient systems of today.

However, to achieve all of these benefits, we would need a nationwide network that is designed to be good enough to eventually replace today's many narrowband municipal systems. We would not achieve the tremendous savings in money and spectrum by maintaining a new nationwide system and thousands of municipal systems indefinitely, nor would doing so be the best long-term solution to interoperability problems, or the many "operability" problems that result from lack of fault tolerance in essential mission-critical components. There must be a significant transition period as public safety agencies decide one by one to use the new network, but we should decide from the beginning that the nationwide network must be capable of serving as the "primary" infrastructure for public safety, which means it should be good enough to support mission-critical communications whenever and wherever first responders need to communicate [2, 3]. As will be explained in this paper, doing so would require important changes in both technology and policy from what was in place before the recent auction of 700 MHz spectrum. This paper will describe a number of these changes. On the other hand, if policymakers disagree and decide that this system is not intended to be of sufficient quality to be the primary communications system for a public safety agency, then this decision should be clearly stated to potential commercial bidders and to the public safety community before another auction occurs.

The FCC deserves praise for its efforts to make the idea of a nationwide broadband public safety network a reality through a "public private partnership." It would be much easier to achieve this goal if the entire federal government was committed to the creation of a nationwide public safety network for all first responders, but unfortunately it is not, and the FCC has been forced to act on its own. In this paper, I will identify a few of the many areas were action from Congress and/or executive-branch agencies such as the Departments of Homeland Security, Commerce (NTIA), and Justice could make an

important difference. Nevertheless, for now, the FCC must act on its own and within its current authority. Until and unless that changes, the only sensible option for the FCC is to begin the challenging process of laying the groundwork for a public-private partnership at 700 MHz that will meet the needs of public safety.

2 The Basic Challenge of a Public-Private Partnership

As discussed in greater length in [2], one could deploy a system that meets public safety needs and will be used only by public safety, or one that will meet the needs of public safety while also serving the general public for a fee. There are important advantages and disadvantages to each of these approaches [2]. The advantage of the latter, which is of course the only option the FCC can consider on its own, is that there are tremendous economies of scope between serving the public and serving public safety. This is primarily because most of the time, the communications needs of first responders are modest,[1] but there are times when their needs are large and of great importance. By sharing infrastructure, and by making much or all of the capacity available to public safety on a priority basis when it is needed, both user groups gain; public safety has access to a great deal of capacity during emergencies, while most of the time, most of the capacity is available for paying customers. The disadvantage of sharing is that public safety agencies have stricter needs than commercial users, and the entire network must be designed to meet those stricter requirements. This increases costs. No one knows for certain whether the advantages outweigh the disadvantages, and some crucial analysis to address this question has not been done, or at minimum, has not been made public. Nevertheless, it is reasonable to pursue the shared approach, and if it does not yield a successful outcome, to try the alterative, as suggested in [2].

In a public-private partnership, the pervasive challenge for the FCC is to make sure that the commercial provider can keep costs low enough to make a profit, while making sure that public safety needs are met, which requires a careful balance. Significant policy changes will be needed, or neither of these objectives will be met. For the short term, this means establishing technical and pricing requirements that serve both sides, as discussed in Sections 3 and 4. For the long term, this means establishing institutional arrangements that can protect both sides, as discussed in Sections 5 and 6.

This innovative approach to meeting public safety needs is in some sense experimental. No one should be surprised that fine tuning is needed, as the FCC must now do in the wake of the first auction. The cost of auction rules that yield no bidders is small; there are more serious outcomes to avoid as a result of the inherent tradeoff described above. One danger is giving up on a nationwide network for public safety before all of the options with a reasonable chance of success have been tried. Another is to choose an easy-to-achieve failure over a hard-to-achieve success. It is inevitable that commercial providers who are considering a bid on this spectrum will try to minimize requirements to well below those needed by public safety, as this maximizes profits. If policymakers allow these arguments to succeed, then the resulting network will be of limited use to public safety. Either of these results would ensure that the 700 MHz spectrum, which is the most valuable resource ever to be allocated to public safety at one time, will be squandered at precisely the time in US history when public safety and homeland security needs may be the greatest.

[1] As will be discussed in Section 8, this applies to communications among people involved in emergency response, but it may not apply to new public safety devices that operate whether there is an emergency or not, such as stationary cameras that transmit video 24 hours per day.

3 Policy Should Change to Serve Commercial Companies Who May Bid

No well-run company would ever commit funds in a spectrum auction without a good idea of what it is bidding on. In this case, the value of the spectrum is highly dependent on the auction-winner's obligations to public safety, including technical build-out requirements, quality of service requirements, price constraints, license renewal policies, and more. None of this was known before the auction, as it was to be determined through negotiation with the Public Safety Broadband Licensee (PSBL) at a later time. This fact alone, combined with a requirement for the auction-winner to pay a penalty for failure to reach an agreement in negotiations, was enough to deter companies from bidding. Requirements must be worked out in detail before an auction, or there may never be a bidder.

It is understandable why the FCC would want such issues to be worked out through bilateral negotiation, rather than a typical FCC procedure such as a Notice of Proposed Rule Making (NPRM). The NPRM process was designed to be effective for other purposes, but it is a slow and cumbersome way of developing complex technical requirements. If other federal agencies were working with the FCC, there would be more options, but this is not the case. The FCC has little choice but to establish many of the requirements in advance of any auction.

Some will argue that the lack of high bids for the Block D spectrum band shows that those requirements on auction-winners that were specified before the auction were too strict. Such arguments are without merit. Regardless of how strict or lax those stated requirements were, the uncertainty over requirements would have deterred bidders, so the results of the first auction reveal nothing on this point.

It is also worth lowering the minimum bid, although doing this without addressing the more fundamental issues above will accomplish little. If the goal is to meet public safety needs and address a serious weakness in US homeland security rather to raise money, a large minimum bid is counterproductive. Indeed, as I have proposed elsewhere [4], it would make sense to choose a minimum bid below 0. If the winning bid is above 0, this is the amount that the auction-winner must pay. If the winning bid is below 0, then the US government would pay a subsidy to the winner in return for guaranteeing that public safety needs would be met. However, once again, this is not possible without action from other federal agencies, and probably from Congress.

Moreover, if it is agreed that the objective is serving public safety rather than raising money, a bid in the auction might reflect something other than money. For example, each bid might reflect the percentage of the country that will be served at standards suitable for public safety. As the next section will show, this is a serious concern.

4 Policy Should Change to Meet the Near-Term Needs of Public Safety

The FCC delegated much of the responsibility for ensuring the public safety needs would be met to the Public Safety Spectrum Trust (PSST), the organization which received the license to 10MHz of spectrum intended for public safety. Unfortunately, this approach did not succeed. The new nationwide system must offer public safety agencies new capabilities that most of them lack today such

as broadband, new levels of dependability and security, and a solution to many interoperability problems. Presumably, this new system should at minimum exceed the capabilities of today's jumble of public safety communications systems, so local public safety agencies always gain by switching to the new system. Unfortunately, had there been a winner in the recent Block D auction, it appears likely that the requirements on that winner would not have been sufficient to achieve this.

As discussed in the preceding section, most of the actual requirements were to be established during post-auction negotiations between the auction winner and the Public Safety Broadband Licensee (PSBL), which turned out to be the PSST. However, the FCC did state some requirements, and the PSST established some initial specifications, which would "form the basis of its negotiation" [5]. These specifications could be changed during negotiations, presumably in response to requests from the commercial provider to make them even weaker. These initial specifications were below what one would expect for public safety, in a number of ways.

First, consider the coverage area requirement. The FCC [6] requires "signal coverage" of 99.3% of the population by the end of 10 years, where the precise definition of signal coverage was left to subsequent actions. 99.3% of population sounds impressive, but analysis shows that this modest requirement will leave many communities with no service. PSST estimates [7] that 63% of the US and 73.5% of the continental US would be covered under this requirement. The map in Figure 1 shows the areas in the continental US that they believe will be covered with terrestrial wireless. As I expect to discuss in a future submission, a requirement to serve 99.3% of the population could lead to geographic coverage that is considerably lower than the 63% and 73.5% figures that the PSST has released. However, for the moment, let us accept the PSST figures. Clearly, coverage is good in the east, but many western states will have problems. Of course, there are areas in the US where people do not live, and infrastructure is not worth the cost even today, but this is not the case in 37% of the US.

To assess this, we have conducted an analysis of the amount of the US covered today by public safety communications systems. We collected information on the precise location, frequency, and technical characteristics of thousands of antennas operating under public safety licenses, and calculated their combined coverage area.[2] (A forthcoming paper will describe the analysis more fully.) We found that in 83.2% of the US and 96.0% of the continental US, it is currently possible to establish bidirectional communications with one or more public safety transmitters. Figure 2 shows th**e** area served in the continental US. Thus, roughly 22.5% of the continental US has built out infrastructure to serve public safety, and will have to maintain these aging systems because the new "nationwide" network will not be available to them.[3] While it is conceivable that this problem could be rectified at some time in the future, perhaps with assistance and funding from other federal agencies, there is no stated expectation that this is required, and no mechanism in place to ensure that it happens. As will be discussed further in Section 5, institutional arrangements must be established for such things now, in order to provide adequate protection for both public safety and the commercial provider.

[2] My thanks to Sumedha Swamy and Ryan Hallahan, two outstanding graduate students at Carnegie Mellon University, who performed this analysis.

[3] Communities in these areas also have the option of switching to satellite, but this will probably increase costs, and as discussed in Section 8, will yield a quality of service that is below that of terrestrial systems and seriously problematic for mission-critical voice communications.

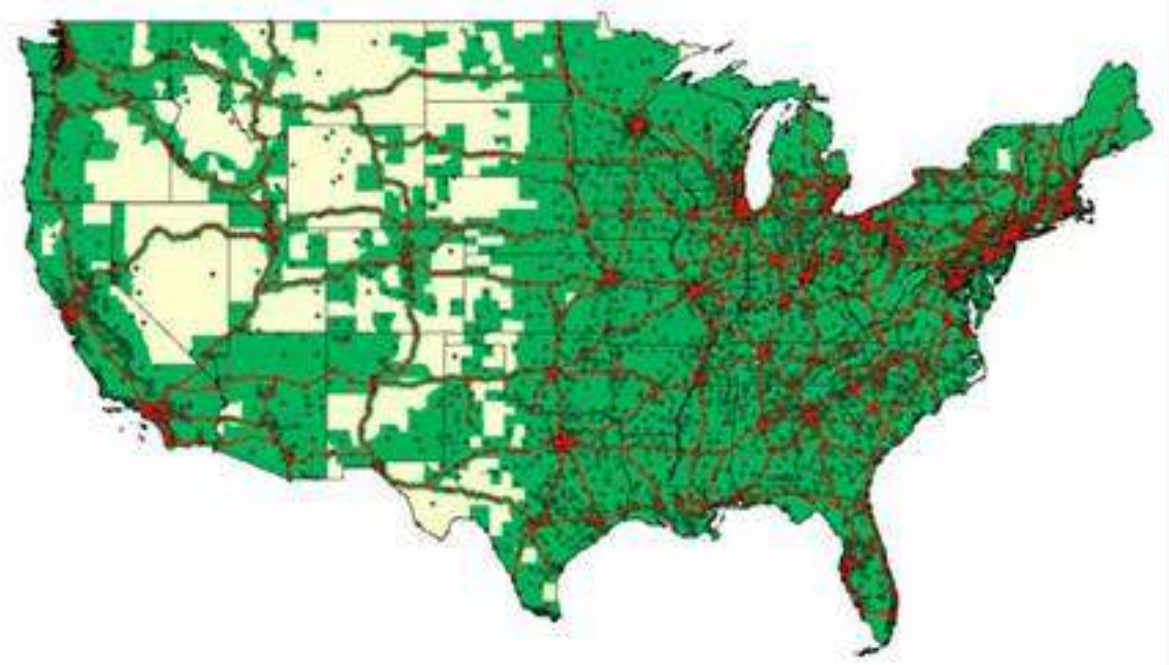

Figure 1: PSST estimates that the green area will have terrestrial coverage by 2019 from the new public safety communications system operating in the 700 MHz band. Figure taken from [7]

Figure 2: We calculate that the green area had terrestrial coverage in Feb. 2008 from one or more public safety communications systems

Perhaps an even bigger problem is that under the technical specifications proposed by the PSST [5], much of the area that is supposedly covered for public safety is not covered with adequate signal reliability. All cell phone users are familiar with the frustration of not getting an adequate signal for a call. Users of commercial systems are willing to tolerate this in return for lower prices, but first responders have more reasons to demand high signal reliability. This need is not reflected in the stated system requirements. The PSST has proposed that the in-building penetration margin should be the same for buildings in what they call "rural" areas as it is for open highways: 6 dB. 6 dB is fine for a highway, but it is simply not enough of a margin to penetrate the walls of many buildings. Moreover, the PSST defines rural such that 92.3% of the area served will be rural. Thus, if the auction winner meets but does not exceed the stated requirements, there would not be adequate in-door coverage in many buildings throughout 92.3% of the area "covered." Such requirements may be adequate if public safety agencies only intend to use the nationwide network from their cars, or if there are plans to deploy millions of repeaters throughout the country – an option that implies both technical challenges and a significant pricetag. But there is nothing in the public debate to indicate that either of these results is expected. (This is one of many areas where additional work is needed to analyze tradeoffs and set requirements appropriately.)

What of the areas that are not adequately served? This includes the 37% of the US that still lacks infrastructure as of 2019, and the areas that are supposedly served but where signal reliability is too low. The PSST suggests satellite service [5]. I have strongly supported the use of satellite as a *secondary* system [3] to supplement a primary system, because satellites can serve many areas that terrestrial wireless cannot, and because satellite systems are likely to be more immune from natural disasters and terrorist attacks. However, satellite is not a true substitute for terrestrial wireless communications. It takes a quarter of a second to bounce a signal off of a geosynchronous satellite, and no amount of clever engineering can change that. As a result, satellite communications will always be vastly inferior to terrestrial alternatives for mission-critical voice communications and highly interactive data communications. Other disadvantages include pragmatic limits on capacity, larger handsets to carry around, and greater problems with respect to indoor coverage.

The proposal to use satellite as a primary rather than a secondary system is the logical consequence of a procedural problem. If we explicitly state that the new nationwide system must be good enough that a public safety agency could (after a transition period) choose to use the new system in place of the old system, and if we state the quality-of-service requirements that this implies, then satellite would be precluded as a primary system in most of the US. Quality-of-service requirements would include constraints on latency, and satellite service could not meet those constraints. However, no such quality-of-service requirements have yet been stated. (This is another area where more work is required.)

Another obvious concern for public safety is dependability. One of many important aspects of dependability is the ability to operate after a power outage. Presumably, public safety's need for backup power meets or exceeds the needs of the typical commercial cell phone user, but this is also not reflected in PSST specifications. The FCC has concluded that all commercial cellular providers with at least 500 thousand customers should be required to provide at least 8 hours of backup power at every cell site [8]. The PSST proposes not to require this of the new network that is supposedly intended for public safety, because they say the "cellular-like network architecture obviates the need for economically non-viable reliability and availability measures such as any requirement for extended power and redundant backhaul at every site." As discussed further in Section 8, there are many ways to

meet dependability requirements that deserve consideration, and some would lessen the need for battery backup. Nevertheless, it is unclear why a cellular-like architecture would entirely obviate this need in a network used by public safety, and not in today's cellular systems. At minimum, this assertion deserves open debate. Nor is it obvious why the added cost of backup power would be "economically non-viable" in the former and not the latter. Moreover, a representative of public safety must consider what public safety actually needs, in addition to the economic impact on the commercial provider.

5 Policy Should Change to Meet the Long-Term Needs of Public Safety

Although the task will take time and effort, it is clearly possible to spell out in detail what public safety agencies demand from their communications infrastructure over the next five years. It is not possible to know what they will demand in 15 years, as both communications technology and the demands on public safety agencies will change over time. As I have discussed elsewhere [2, 4, 9], the most difficult challenge in the public-private-partnership approach is establishing the institutions and procedures that will guarantee that the interests of public safety agencies are protected in the long term, without threatening the profitability of the commercial provider and the financial sustainability of the approach.

Consider this issue from the perspective of an individual municipal public safety agency. Using the new nationwide system requires an investment of both time and funding. New equipment must be purchased. New procedures must be adopted. Staff must be trained. A wise Police Chief or Fire Chief would hesitate to make this investment for a system that may not be useful in five years. Even if the coverage, capacity, signal reliability, power backup, quality of service, availability and security are sufficient today, what guarantee is there that they will remain so? Even if the monthly fees that the agency must pay the new provider are reasonable today, will they remain so? Moreover, a wise Police Chief or Fire Chief would not even consider giving up the current system unless there is a very high degree of certainty that the new system will be useful in five years and far beyond. Once the old system is gone, the Chief will have no option but to stay with the new system, even if it is vastly inferior. Negotiation is difficult, because if public safety agencies can no longer stop using the new system, they have little negotiating power. Thus, without adequate protection in advance, public safety agencies will not make significant use of the new public-private partnership, and the policy will fail.

On the other hand, consider the issue from the perspective of the commercial provider. If a representative of public safety can impose arbitrary technical requirements that increase costs, or arbitrary price constraints that limit revenues, then this provider faces a perpetual threat that outside forces will force it into bankruptcy. What if operating costs go up, and public safety refuses to increase their payments? What if public safety insists on making much greater use of video, and this strains the capacity of the system? It is unlikely that a commercial provider would enter into an arrangement without adequate protection from such demands.

Thus, an effective policy must serve both public safety and the commercial provider. I have proposed one possible approach [9], which has been used in other contexts. For example, during wartime, the Department of Defense relies heavily on commercial munitions suppliers, just as public safety agencies may someday depend heavily on a public-private partnership to protect the nation. One way to ensure the availability of new goods without creating a permanent unregulated monopoly is to

issue long-term contracts for service; if that contract is not renewed, the provider must surrender its production lines to the winner of the follow-on contract. Similarly, as proposed in [9], the commercial provider and a representative of public safety could negotiate new technical and pricing requirements that will apply after the license i renewed. If public safety and the provider are unable to reach an agreement that meets the needs of both, then the spectrum and the infrastructure can be transferred to a new provider, who is selected though a new auction. (Perhaps in the interim, the infrastructure is transferred to the PSBL.) To ensure that the provider can derive enough profit from this arrangement even if its license is not renewed, it may be necessary to select a license duration greater than 10 years. Moreover, the renewal decisions must be reached well before the license actually expires to ensure a safe transition.

This is just one possible approach. It is probably better for a greenfield deployment, i.e. where a provider builds out an entirely new network in the 700 MHz band. Other approaches may be preferable if the Block D licensee already has a large infrastructure operating in other bands. It is my hope that both public safety representatives and potential bidders will begin proposing their own solutions to this challenging issue.

6 Policy Should Change to Establish an Entity That Can Represent Public Safety

Under current FCC policy [6], a Public Safety Broadband Licensee (PSBL) must be selected. Depending on its role, the PSBL should presumably represent either public safety, or the broader public interest. (The two goals are often but not always the same.) Either way, this organization must always serve the public, and always appear to serve the public, as even the appearance of inappropriate actions can be problematic. Policies are not yet in place to ensure this.

As I have commented elsewhere [10], one essential requirement is transparency. How can any organization truly represent public safety if the leaders of public safety agencies across the country cannot find out what decisions the organization has made, and why? Public safety agencies will wonder whether their interests are being protected. Equipment manufacturers and commercial service providers will wonder how they can participate in this multibillion dollar endeavor, and whether there is a sufficiently level playing field for them to try. Tax-payers will wonder whether their money is well spent. None of this is possible without serious transparency requirements. Even if all of the PSBL's decisions are appropriate, they may appear inappropriate without such requirements. Thus, where the FCC lists requirements that an organization must have to be considered to be a PSBL, requirements related to transparency should be added to the list. The current PSBL, the PSST, would not meet such requirements, and would therefore be ineligible.

Beyond mere transparency, the PSBL must be accountable to public safety agencies. (It may also be accountable to other organizations whose goal is to advance the broader public interest, such as the FCC.) Organizations are in part accountable to their board, and the FCC has rightfully considered who would serve on the PSBL's board. However, organizations are also accountable to those who fund them. The PSST was funded by Cyren Call, a for-profit company [11]. This relationship makes it unclear who the PSST serves, the organizations represented on its board or the source of all its funding. At minimum, this is likely to create the appearance at times that the organization is not serving public safety. Moreover, the PSST has probably lost the option of choosing a new advisor if it is ever unhappy with the

current one (and it is clear that Cyren Call's role goes well beyond merely offering advice). The FCC's latest NPRM [12] asks whether the PSBL should not be allowed to accept funds from for-profit companies. This is a useful restriction, but not a sufficient restriction. For example, the Cellular Telecommunications Industry Association (CTIA) is a non-profit organization, but because of their mission, it would still be problematic if they funded the PSBL. The funding should come from a source whose unambiguous objective is either to serve the public interest, or to serve public safety.

It is entirely understandable that this did not occur. The PSST had few options. This is another unfortunate result of the fact that the FCC is the only part of the federal government that is trying to address this national need. One obvious source of funding is the federal government, and the amount of money required to support a PSBL until negotiations with the winner of the spectrum auction are complete would be negligible compared to what either the Department of Homeland Security (DHS) or the National Telecommunications and Information Administration (NTIA) has spent on related matters in recent years, but such matters are beyond the control of the FCC acting alone. Another obvious source of funding is from organizations representing public safety agencies, many of which are already represented on the PSST board. Indeed, such funding might encourage these organizations to play a greater role in oversight, and to contribute more actively in the definition of requirements, which would be helpful. However, there are many practical challenges to making this happen.

The PSST is not the only organization whose credibility is adversely affected by the current financial arrangement. Any PSBL will need the ability to hire for-profit entities for anything from janitorial services to accounting services. However, any for-profit company that is in the role of advisor must be free of conflicts of interest, so it can offer advice that advances the PSBL's objectives rather than its own. For example, it would clearly be inappropriate if the Block D licensee were an advisor of the PSBL. It is similarly inappropriate for an organization who loans money to the PSBL to be an advisor. Once the money has been loaned, this organization has a great deal to lose if the PSBL is unable to reach an agreement with a commercial provider, as the loan will never be repaid. On the other hand, the organization has nothing to lose if the PSBL reaches an agreement that fails to meet the needs of a single public safety agency, and is therefore the very definition of monumental failure, as discussed in Section 1. Would this advisor serve public safety or itself? I know of no reason why Cyren Call should be faulted for loaning money to the PSST. The PSST needed money from somewhere, and unfortunately there was no other obvious funding arrangement in place. However, the instant Cyren Call made this loan, they faced a fundamental conflict of interest.

In part because of the lack of transparency, it is difficult to know precisely what the PSST and Cyren Call were trying to achieve, or why they made the decisions they did, or what was done by PSST versus what was done by Cyren Call. Even if all decisions were fully appropriate, the issues above can create at least the appearance that some decisions might have been motivated by profit. Hypothetically, if a PSBL were motivated entirely by profit rather than the needs of public safety, such an entity would make some of the same decisions that the PSST and Cyren Call have made. A profit-maximizing PSBL would try to maximize revenues from the Block D licensee, in part by asking for large payments in negotiations with the auction winner, and perhaps in return by establishing low standards for public safety requirements to make the Block D license more valuable to a commercial provider. Cyren Call did inform potential bidders that they would pay a fee to the PSST, and the figure of $50 million per year was suggested as a possible amount [11, 13]. Moreover, as discussed in Section 4, the initial requirements on the commercial provider were below what one might expect for public safety in some important respects. A profit-maximizing PSBL might also try to maximize revenues derived from public safety agencies. Cyren Call has suggested that the PSST would be the sole entity that acts as a

retailer to public safety agencies. While such an arrangement does not necessarily mean that excessive revenues would flow to the PSBL, a profit-maximizing PSBL could use this arrangement effectively to that end. Such a policy should not be adopted or considered without adequate oversight, transparency, and accountability.

A recent inquiry found no impropriety in the actions of the PSST and Cyren Call discussed above [13]. I am not disputing this. The most important issue is not impropriety, but whether we have the policies in place to establish an organization to credibly represent public safety now and for many years to come. From all of the above, it is apparent that the PSST in its current form is not suitable for this purpose, nor is it suitable in current form to be licensed as the PSBL. The FCC should adopt additional requirements for the PSBL, including requirements related to transparency and funding, and should continue to provide ongoing oversight as well.

7 Current Federal Policy Makes the FCC's Job Unnecessarily Difficult

As discussed in Section 1, the FCC is limited in some ways because it is acting alone. For any readers in Congress, the Department of Homeland Security, and elsewhere, it is worth summarizing just a few of the reasons cited in this paper why this is problematic.

Most obviously, while there are many possible ways to achieve a nationwide system that would meet the needs of public safety [2], options other than the "public private partnership" fall outside the authority of the FCC acting alone. Thus, while this approach has many merits, the question of whether it is the best approach is currently academic.

As discussed above, to attract bidders to the auction, the FCC must specify many technical parameters and price constraints. This requires extensive knowledge of current *and future* public safety needs, and of the current and future technology that could meet those needs. This is a complex undertaking, for which the FCC's NPRM and NOI processes are not well suited. This will yield a much slower process than might have been possible had other government and non-government organizations played larger roles.

The statutory eligibility requirements for a license-holder in the band designated for public safety may be problematic. First, although it is essential that an organization be established that can represent the needs and interests of public safety, this organization could serve the public interest even if it is not the actual licensee. There are advantages to making it the licensee, but there are also disadvantages, including the greater need for transparency and protection from conflict of interest discussed in Section 6. In theory, the spectrum could be licensed to a commercial provider that is serving public safety rather than to a public safety agency, and the FCC could interact more directly with that provider, but this may violate existing statute.

Another potential eligibility problem is that the definition of "public safety services" covers "state or local government entities" but not federal. Including federal users on the same network will alleviate interoperability problems when local and federal entities cooperate, and it will save money. There may be ways to include federal users under existing statute, but this restriction is not helpful.

Another obvious constraint is that the FCC cannot allocate funds, and those agencies who could allocate and then manage funds are not involved. Funding for the PSBL would have greatly helped in dealing with the problems described in Section 6. Section 3 raised the possibility of setting an initial bid for Block D that is less than 0, which would be possible with funding, as proposed in [4]. Federal funding could also be used in many ways to help local agencies make the transition to the new nationwide system, such as grants to support the replacement of handsets using the old technology. Not only would this increase the number of public safety agencies that make use of the nationwide network in the coming years, but if such programs are established before the auction, this could also generate greater interest among potential bidders by increasing their revenue projections.

Other agencies and organizations could also provide resources beyond funding, such as standards-setting, or certification programs that identify whether products meet established public safety requirements. In addition, many public safety agencies would welcome a trusted source of advice on technical and organizational changes needed to make the best use of the new system. Large agencies may keep their own technology experts on staff, but this is harder for small agencies, and 88.5% of public safety agencies support fewer than 100 users [14].

Given the limitations of the FCC authority on these and other issues, the rate of progress might be slower than we would all prefer.

8 Technical Requirements for Public Safety

As discussed in Section 3, the FCC now faces the difficult task of setting detailed requirements on the future licensee. This section will briefly address some of the outstanding issues. If time permits, I hope to comment in more depth on some of these technical issues in a future filing.

As described in Section 2, one of the primary advantages of the public-private partnership is derived from the ability of a network provider to allocate a large amount of capacity to public safety in those unusual instances when it is needed, and a large amount of capacity to the general public the rest of the time [2]. Thus, it is helpful to make all 20 MHz of the spectrum and all of the capacity that public safety is not using at any given time and location available to the commercial provider. Moreover, the commercial provider should not compensate public safety agencies for not using all of the spectrum or capacity they can, as this creates a disincentive to use the new network.

The public interest is best served with a consistent technical architecture throughout the US. This will substantially reduce costs, and alleviate all of the interoperability problems that result from dissimilar technical choices in different regions. A nationwide license may be the simplest way to achieve a consistent nationwide architecture, although it is not the only way. If the FCC considers regional licenses, it should take great care examining mechanisms that would ensure technical consistency.

Whether there is a single nationwide licensee or not, open standards can be of great benefit [10]. Common standards are one way to improve technical consistency, and adopting open rather than proprietary standards can increase competition among equipment providers and thereby decrease costs. Neither FCC nor PSST requirements to date have actively endorsed open standards.

Requirements must be established for the prices that public safety will pay. Clearly, no public safety agency will purchase equipment to use a system unless it can be certain that the monthly fees will be reasonable for the life of that equipment, if not indefinitely. Customers of commercial cellular services can count on competition for protection, but the public-private partnership will generally have no competitors for public safety customers. At the same time, commercial providers need to understand their potential revenues. How will prices be established? Will the D Block licensee or the PSBL be able to change them at will? What will the prices be initially? Note that it is impossible to separate the pricing issues from a number of technical issues. How does price depend on the number of active devices from a given agency? How does price depend on which applications those devices run? Surely those who require high-definition TV will pay more than those who want only text messaging. How does price depend on the quality of service that is needed?

Many technical requirements must be stated for the wireless system. A few examples of these such as coverage area, signal reliability, latency, and power backup were discussed in Section 4 (although the FCC requires more detail on all of these). As a general guideline, I would recommend technology-neutral requirements where possible. For example, instead of specifying that each cell site needs a diesel generator with a given amount of fuel, the requirement might state that coverage and capacity must be maintained even without AC power for at least 5 days. The licensee then has the flexibility to choose the technical method of meeting this requirement.

One particularly challenging area for technical requirements is in the capacity needs of public safety. It is impossible to build a network with enough capacity to serve public safety without knowing how much capacity public safety needs. Moreover, how much traffic generated by public safety will be given preemptive priority over commercial traffic? How much traffic will be carried at prices that are capped for public safety? I have yet to see any analysis that comes close to providing sufficient guidance on what public safety needs, whether it is achievable, or at what cost. One cannot address this without agreeing on who is served under the public safety umbrella. Are there 100 thousand people? 1 million? 10 million? It depends on how broadly one defines public safety.

The most difficult part of this problem will be defining what applications are used and how, in part because there is not yet agreement in the public safety community on this. Video is particularly important, because of its relatively high and constant data rate. This includes mobile cameras that reside in ambulances or on the helmets of firefighters, as well as fixed cameras that may sit around critical infrastructure or in high-crime areas. If a public safety agency is free to deploy as many fixed cameras as it wishes and the carrier must accommodate the traffic at one fixed price, then the carrier may soon see its capacity completely overwhelmed by video traffic. Such an arrangement is not viable. Given that there are other wireless and wired technologies that can be used to support fixed cameras, it may make sense not to give public safety the same price guarantees for fixed video that they get for mobile applications. However, even mobile video is a potential problem. If every first responder begins carrying a mobile camera while on active duty, this could also exceed a network's capacity. Agreement must be reached on such complex issues regarding capacity.

Even if one understands precisely what capacity public safety will need to respond to a given emergency, which is certainly not the case today, there are difficult tradeoffs to make. Do we design for the level of emergency that occurs about once per year? Once per 10 years? Once per 100 years? (I hope to have more to say on capacity requirements in a future paper.)

Similar to capacity requirements, many quality-of-service requirements depend on the applications that will be used, and this is not well defined. If there is video, must the quality of service be good enough for interactive videoconferencing, or is it sufficient to meet the easier requirements of unidirectional streaming video? This also affects costs and design strategies.

Issues of dependability and security will also be challenging. The transmitters in a system designed for public safety are more likely to become the target of deliberate attack from criminals or terrorists than a typical commercial cellular system. What steps are needed to provide adequate protection, and what do they cost? Moreover, no degree of hardening can protect a transmitter if it sits in the path of a tornado. One important advantage of a nationwide system [2] is that a cellular architecture can be designed to withstand the loss of some transmitters with limited reduction in capacity and/or coverage, but such a fault-tolerant design increases cost. Public safety requirements for fault tolerance may exceed those of commercial users, but there is no agreement on this. To what extent should a commercial provider be required to adopt such techniques? Designers can take steps to reduce the chances that any device will fail, and they can take steps to tolerate the failure of more devices. How should these be balanced? At this time, there is no consensus on these and other dependability requirements.

It is often stated that the new network must employ state-of-the-art technology for security, but it is not clear what is meant by this. Is it merely encryption? Are there authentication requirements? Or other security issues?

Location capabilities are likely to be important for public safety applications. For example, when a firefighter is not responding to calls, his life may depend on whether others can determine his location with sufficient speed and precision. The FCC has imposed some requirements on cellular providers to locate handsets. Should those same requirements apply in this network? Are public safety requirements with respect to location different from those of cell phone users?

While much of the attention has rightfully been focused on the wireless portion of the nationwide network, there are also reasons to establish requirements for a nationwide broadband backbone, without which the wireless system is of limited use. This network should interconnect all wireless transmitters, as well as important sources of data for public safety organizations, e.g. criminal records, medical information, etc. This backbone must also connect to a wide variety of legacy systems. How these systems are interconnected, and with what quality of service, will have important implications for interoperability. There may be complicated technical tradeoffs that have yet to be addressed.

Each of the complex issues above would affect the cost of deploying a network, so commercial companies will be looking for guidance before they risk money in an auction. Clearly, much work remains in the definition of public safety requirements.

9 Conclusions

The US needs a nationwide broadband network to serve local, state, and federal emergency responders. This will save spectrum, save tax-payer dollars, and save lives. Consequently, the FCC should continue its pursuit of a viable "public private partnership" by refining their previously stated policy [6]. We can hope that Congress and federal agencies other than the FCC will eventually participate in this effort, as doing so would both make it easier to achieve a successful public private partnership, and make other options possible as well, but there are currently no signs that this will occur. For now, as Chairman Martin, Commissioner Copps, and others have correctly stated, this policy is the "last best hope" for public safety.

The FCC should firmly and loudly declare that it defines success as the creation of a nationwide network of sufficient quality to meet the needs of public safety agencies, including as a replacement for the narrowband municipal systems they have today, and that the FCC defines failure as the allocation of the 700 MHz spectrum in any way that does not achieve this objective. Lack of a bidder in any particular auction is therefore neither failure nor success; it is a delay.

To achieve this goal, the FCC must go much further than it has so far to establish the technical and nontechnical requirements that will be imposed on the winner of the next auction, or there will be no bidders. The requirements established must be sufficient to meet public safety needs over the coming years. Moreover, there must be some institutional arrangement that will ensure that the needs of public safety are met in the future, even as needs and technology changes. This arrangement does not yet exist. One obvious step in defining such an arrangement is establishing an organization to represent public safety that is transparent to all, accountable (at least in part) to public safety organizations, and lacks even the appearance of a conflict of interest. Beyond that, either this organization or the FCC or both need sufficient leverage to protect the evolving needs of public safety. At the same time, the long-term arrangement must provide adequate protection for the licensee. The arrangement is only sustainable if the licensee can expect profits.

Potential bidders will naturally request that the already-lax requirements be reduced further, as this reduces their costs. Some will use the result of the first auction as an excuse for this, although the result can easily be explained for reasons other than these requirements. The FCC must continue to insist that any future license-holder meet the actual requirements of public safety, whatever those turn out to be. If the requirements established before the auction are stricter than public safety actually needs, then this risks delaying a successful outcome, but it does not risk failure. On the other hand, accepting requirements that are not strict enough to meet public safety requirements and that cannot easily be changed later does not merely risk failure; it guarantees failure.

A substantial amount of work remains to define all of the requirements discussed above. The public safety community must endorse the requirements, and unfortunately there is no consensus opinion from that community on many of these issues at present. While we would all like to see a successful resolution of this effort as early as possible, the FCC must take care with this extraordinary opportunity. It is not clear when, if ever, another block of spectrum like this will become available for public safety. Thus, I hope the FCC will place more emphasis on moving in the right direction than on moving quickly.

10 References

[1] J. M. Peha, "How America's Fragmented Approach to Public Safety Wastes Spectrum and Funding," *Proc. Telecommunications Policy Research Conference,* Sept. 2005. www.ece.cmu.edu/~peha/safety.html

[2] J. M. Peha, "Fundamental Reform in Public Safety Communications Policy," *Federal Communications Bar Journal,* Vol. 59, No. 2, March 2007, pp 517-46. www.ece.cmu.edu/~peha/safety.html

[3] J. M. Peha, "A Secondary Broadband Provider for Public Safety," white paper, July 2007. www.ece.cmu.edu/~peha/safety.html

[4] J. M. Peha, Testimony for the House Subcommittee on Telecommunications and the Internet, Hearing on Innovations in Interoperability, March 2007. www.ece.cmu.edu/~peha/safety.html

[5] Public Safety Spectrum Trust, *Public/Private Partnership Bidder Information Document, Version 2.0,* Nov. 30, 2007. www.psst.org/documents/BID2_0.pdf

[6] Federal Communications Commission, Second Report and Order, in the Matter of Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150, August 10, 2007. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-132A1.pdf

[7] Public Safety Spectrum Trust, "Will Public Safety Promises Be Kept? Building a Nationwide Public Safety Broadband Network," *International Wireless Communications Exposition,* Feb. 27, 2008. www.psst.org/documents/PSSTIWCE022708.pdf

[8] Federal Communications Commission, Order, in the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, EB Docket No. 06-119 and WC Docket No. 06-63, June 8, 2007.

[9] J. M. Peha, *A New Proposal for a Commercially-Run Nationwide Broadband System Serving Public Safety*, Comments in Federal Communications Commission PS Docket No. 06-229 and WT Docket No. 96-86, Feb. 7, 2007. www.ece.cmu.edu/~peha/safety.html

[10] J. M. Peha, "Requirements for Mission-Critical Communications and Governance," Comments in the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Federal Communications Commission PS Docket No. 06-229 and WT Docket No. 96-86, July 24, 2007.

[11] M. E. O'Brien, House Energy and Commerce, Subcommittee on Telecommunications and the Internet, Hearing on Oversight of the Federal Communications Commission – the 700 MHz Auction, April 15, 2008. http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.041508.700mHz.shtml

[12] Federal Communications Commission, Second Further Notice of Proposed Rulemaking, in the Matter of Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, and the Matter of Implementing a Nationwide Broadband Interoperable Public Safety Network in the 700 MHz Band, WT Docket No. 06-150 and PS Docket No. 06-229, May 14, 2008.

[13] Office of Inspector General Report, D Block Investigation, April 25, 2008. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281791A1.pdf

[14] Booz, Allen & Hamilton, *Cost Study Data Characterization Report*, The Public Safety Wireless Network (PSWN) Program, Feb. 1999. www.safecomprogram.gov/NR/rdonlyres/5EBE930C-47D9-49E1-A16E-27B1183798B2/0/Cost_Study_Data_Characterization_Report.pdf