21 May 2012

From: Rex A Buddenberg
2151 Trapani Circle
Monterey, Ca 93940

Subject: Comments on RFI:
Docket No: 120509050-1050-01
RIN: 0660-XC001
Development of the State and Local Implementation Grant Program for the Nationwide Public Safety Broadband Network

I wish to comment on three subject areas in your RFI:

- interoperability
- requirements
- business model

The three interrelate; the business model is easily the most important. But the other two categories affect it so they must be treated first[1].

Interoperability.

Paragraph 4 (page 6) contains:
c. Can these existing governance structures be used for the PSBN, and if so, how might they need to change or evolve to handle issues associated with broadband access through the Long Term Evolution (LTE) technology platform?

And page 8:
11. Are there best practices used in other telecommunications or public safety grant programs to ensure investments in rural areas that could be used in the State and Local Implementation grant program?

In LMR, interoperability is usually defined as a common frequency. And ability to roam into a foreign jurisdiction.

In broadband, including LTE, both the definition of interoperability and attainment of interoperability are much different. You cannot successfully view broadband interoperability through the LMR experience. Different that it is, interoperability is critically important because the components of the next generation communications system will not come from a single source.

LTE is a routable network technology – it can be viewed as a means of extending the internet to mobile platforms. Recognizing the internet (ARPANET) character gives rise to a division of 'interoperability' into two parts[2]:

- interoperability of applications that use the internet infrastructure[3] and

1 Comments are mine personally, not those of my employer or other entity.
2 Applications are indicated by a port number – a value included in the IP datagram. Other than that, the infrastructure is indifferent to what the application is or what the bits carried represent. This modularity is the key that decouples applications (hundreds of them) from infrastructure (one).
3 Information system interoperability.

– interoperability of the infrastructure itself[4].

This is a fundamental modularization in the internet – we have one infrastructure and a multitude of applications.

Application interoperability. Applications such as voice, asset tracking / common operational picture, weather advisory, etc. must be both operable over an internetwork and interoperable between themselves. It is inconceivable that such applications would be from a single source, so interoperability must be specified: data, process, procedure, ... are interoperability categories that must be included. And interoperability must be tested.

Interoperability among multiple realizations of an application is commonly accomplished within the Internet Engineering Task Force, and open source software community, especially that clustered around open source operating system distributions. For example, there are many Voice over IP implementations and most are interoperable with each other. There is a role for a federal-level testing here, but it's a dual role: both requirements and interoperability.

Communications interoperability must be approached in two tiers. The first is internetworkability so that any network segment makes up a building block of a larger internetwork. This requirement applies to the

– terrestrial network[5],
– the radio-WAN (the niche to be filled by LTE technology) and
– in-vehicle LANs (such as one in an ambulance).

This is 'layer three' interoperability and can be tested by placing the network segment under test between a lab-full of routers. If it interconnects the routers, it's a routable network.

The second tier can be characterized as a 'layer 2' test which consists of cross-vendor interoperability – can a subscriber station built by Vendor A operate with a base station built by Vendor B? This is a somewhat more complex problem and is usually a subject of independent industry testing and certification. One example is that within the WiMAX industry association for IEEE 802.16 profiles; another is the University of New Hampshire's interoperability testing program. A single vendor claiming compliance without independent testing is unlikely to yield layer 2 interoperability; a 'neutral ground' testing ground is necessary. This kind of testing or supervision of testing is also unlikely to be within the capability of a state or more local entity.

The good news here is the inherent modularity of the internet. This infrastructure interoperability can be tested and certified entirely independently from the application problem. This is a fundamental difference between the internet and older communications systems where there is no modular separation between infrastructure and application.

The short answer is no, the existing governance structures will not suffice.

4 Communications system interoperability.
5 Deprecatingly called the backhaul, but it's not an afterthought, it's foundation.

Requirements.

Paragraph 1, page 4:
… This section enumerates several areas for consultation, including: (i) construction of a core network and any radio access network build-out; (ii) placement of towers; (iii) coverage areas of the network, whether at the regional, State, tribal, or local level; (iv) adequacy of hardening, security, reliability, and resiliency requirements; (v) assignment of priority to local users; (vi) assignment of priority and selection of entities seeking access to or use of the nationwide public safety interoperable broadband network; and (vii) training needs of local users. …

A good share of this RFI seems to tacitly assume that FirstNet will erect an infrastructure entirely segregated from the commercial Internet. For instance i and ii above. This is a very suspect assumption which should be consciously examined, not tacitly accepted. Especially with the demise of Integrated Wireless Network (IWN) within DoJ and DHS. Periodically there have been proposals for the federal government to own internetwork infrastructure. Given the record, NTIA would be well-advised to derive lessons learned from IWN and various other 'gov.net' false starts before trying another one.

We should also recall the telephone system of, perhaps, fifty years ago. We used it for emergency services communications, and gained the required emergency services characteristics by adding robustness to the telephone system. Because of the monopolistic position of AT&T at the time, the emergency services requirements were levied against the company, mostly by FCC. AT&T, in turn passed the costs on to the public in the form of PUC-approved surcharges. The tools that assume single-vendor are no longer usable, but the lesson that we plussed-up the commercial network rather than try and build another is.

Emergency services does not need -- and cannot afford -- a segregated infrastructure to meet its critical needs.

The two primary infrastructure differences between general-purpose internetwork and what emergency services needs are two:

- Higher availability.
- Greater geographic coverage.

Availability. The typical default internet laydown is single threaded – a component failure represents system failure. System failure is an annoyance in an office-automation situation but it is a critical problem when it happens in emergency services. Internet technology, by itself, does not solve these availability problems, but internet technology is highly amenable to building highly available and survivable communications systems.

Most of the high availability communications solutions deal in backup communications routes and backup power – the material of multiple-threading. Neither of which require a departure from quite ordinary internet technology or segregation of the system away from the general Internet.

Coverage. Obviously some of the areas that emergency services need coverage are areas where commercial internet services providers will find uneconomical. This also does not justify departure from either commercial technology or commercial infrastructure, rather some subsidized extension of it.

One of the realities of LTE in the envisioned frequencies is that the footprints per base station will be much smaller than in existing LMR. For instance in the county where I live in there are currently eleven LMR base stations. In an LTE structure with equipment using less than a watt, the number of required base stations can be expected to increase by about an order of magnitude. This requires a much denser terrestrial internet to reach all these POPs than what we are used to. That density exists … in the commercial internet[6]. But it is not practical to envision an emergency services owned/operated terrestrial internet that duplicates that population of POPs[7].

Emergency services properly commands the most stringent requirements in these areas; but attainment of them benefits all, not just emergency services.

Business model.

In the Background section, page 3:

> The Act establishes the First Responder Network Authority (FirstNet) as an independent authority within NTIA and authorizes it to take all actions necessary to ensure the design, construction, and operation of a nationwide public safety broadband network (PSBN), based on a single, national network architecture ...

While the language does not quite charge FirstNet with being an infrastructure owning and operating Internet Services Provider, it comes pretty close[8]. This is a very suspect assumption:

- DoJ and DHS' experience with IWN should prove cautionary. I have not read the grant proposals you have received, but suspect that many fall into the category where a state or county tacitly assumes that it will be the owner and operator. After all, that's the way we built LMR systems. I know of several jurisdictions that have unthinkingly gone down this road only to find that there's no completion, life cycle maintenance, and upgrade budget.
- It is not sufficient to simply avoid competing with commercial Internet Service Providers, rather it is important to leverage them and get those commercial ISPs to meet emergency services availability and coverage needs. There is also value in leveraging non-emergency service internet infrastructures such as that in the school system.

6 In the county where I live, the school system alone potentially provides this density in the urban/suburban parts of the county.
7 The number of schools in the county comes close to equaling the number of POPs needed.
8 The term 'architecture' is particularly ambiguous. There seem to be 101 definitions of the term.

As FirstNet is created, we should note that several federal agencies are already dealing with communications grants. Including emergency services grants. And they are dispensing grant guidance. Some of it is contradictory and apparently little to none is coordinated:

- FCC has an entire chapter on emergency communications in the National Broadband Plan. And many emergency-services related points appear throughout the Plan.
- DHS and DoJ have coordinated but contradictory guidance on their web pages (see SAFECOM). It has major divergences from the National Broadband Plan.
- NIST has facilities and a claim to the interoperability function.
- NTIA shares the BTOP grant kitty with USDA. While most of the grants are not for overtly emergency services communications, any grant proposal that extends the internet to more citizens benefits emergency services.

Will FirstNet be yet another cacophanous voice in the chorus?

If FirstNet leverages commercial ISPs then the provisioning problem is to add the infrastructure necessary to meet the high availability and coverage requirements. A marginal cost.

If FirstNet is to build a segregated infrastructure then this requires a robust multiple-threaded infrastructure that must be capitalized and operated from scratch. A full-freight cost.

The latter approach will either result in unmet requirements or will cost a great deal more than the former approach.

Recommendations.

Business model. The FirstNet business model should be constructed to foster upgrades of the commercial internet to meet emergency services needs. I would expressly recommend approaching some internet service providers for input.

Equally, the grant criteria should foster this upgrade strategy rather than create government-owned and operated infrastructures.

Architecture. Since FirstNet is charged to formulate a "single, national network architecture " FirstNet should define 'architecture' as a modularization model. So that infrastructure is 'building block' interoperable regardless of vendor, owner or operator. The necessary modularization model is actually quite simple:

- All communications (terrestrial-WAN, radio-WAN, LAN) comes in the form of routable networks.
- Applications live in end systems (such as a handset or computer); all end systems attach to LANs. The corollary to this principle is these end systems only put protected data onto the network.

This modularization model should ring consistently through all federal agencies' grant guidance and program investments. If FirstNet is to be the coordinating agency, fine.

Availability. The grant criteria for emergency-services specific programs should include availability requirements statements and strategy for meeting them.

Similarly, the grant criteria for non-emergency-services programs should also include

the expected availability criteria and the 'design for' criteria in case of upgrade later. A lot of high availability internet didn't start out that way but certainly became that over time.

Interoperability. NTIA should focus on interoperability of emergency services:

- A certain small set of applications (such as VOIP implementations) should be tested, certified and supported to meet end-to-end security, multicast, and manageability needs that typical non-emergency services users do not demand. The testing and certification must cover both requirements attainment and application interoperability.
- All infrastructure to go into the emergency services internetwork needs to have interoperability testing and certification. Intereoperability is critical regardless of sourcing and ownership. This includes both internetworkability (layer 3) and multi-vendor interoperability at lower layers. In many cases, this does not need to be done from the whole cloth, but can be accomplished by leveraging existing bodies.

Since both of these interoperability issues have to do with interoperability across multiple jurisdictions, it doesn't make much sense to attempt this at governmental lower than national level. And since the standardization and certification bodies themselves work at the national an international level, it makes little sense for a state or county governmental entity to work in this area.

Thank you for the opportunity to comment.

Buddenberg