Desirable Properties of a National Public Safety Network

Draft Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology

November 21, 2011

Introduction

On June 8, 2011, Aneesh Chopra, the United States Chief Technology Officer (USCTO), requested that the Director of the National Institute of Standards and Technology (NIST) charge the Visiting Committee on Advanced Technology (VCAT) of the NIST with the task of developing a summary of desirable features that could be incorporated into the design of a national public safety network. The subcommittee on Public Safety Networks has met in person and by phone and online and several public meetings on this subject have been held in Philadelphia, Chicago, and elsewhere[1]. NIST also recently issued a request for information and comment on "Desirable Features of a Nationwide Public Safety Broadband Network."[2]

In addition, the USCTO has held coordinating meetings with Federal and other agencies and representatives of public safety and other organizations to further explore the needs of this vital component of protection for the citizens of the United States. The President's Committee of Advisors on Science and Technology (PCAST) has also touched on this topic as it considers the use and allocation of broadcast spectrum. The National Research Council recently published a report on wireless technology and opportunities for its use[3] that highlights the rationale for many of the ideas incorporated into this extended essay on public safety networking.

---

[1] August 10, 2011, w/APCO Meeting, Philadelphia, PA; September 7, 2011, w/SAFECOM meeting, Chicago, IL; VCAT meetings, June 7-8, 2011 and October 17-18, 2011, at Gaithersburg, MD.

[2] "Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Network," *Federal Register*/Vol. 76, No. 176, Monday, September 12, 2011; responses due by October 12, 2011. [Docket No. 110727437-1433-01]

[3] [NRC Wireless] *Wireless Technology, Prospects and Policy Options*, National Academies Press, 2011, ISBN-13: 978-0-309-16398-9, ISBN-10: 0-309-16398-6.

It is also recognized that the diverse participants in public safety include a wide range of private sector organizations and civilian volunteers and that the aggregate also operates, from time to time, in nondomestic emergencies to render aid and assistance. The scope and diversity of demands levied on the public safety fabric strongly influence the nature of the communications infrastructure that is needed to manage and coordinate responses to events that challenge public safety.

This extended essay is intended to provide a summary of features that appear to the VCAT to be relevant to and potentially useful objectives for the design of a national public safety network. This is not a design document, although many of the observations are intended to influence subsequent design or designs for a national public safety network.

1. Observations and Context

1.1 Scope of Public Safety Community

Public safety is an extremely broad term and encompasses law enforcement, response to fire, natural and man-made disasters, medical emergencies, threats to public order and a host of other situations. Moreover, the so-called "first responder" community is, itself, geographically, jurisdictionally and organizationally diverse. Even within the context of the National Incident Management System (NIMS),[4] chains of command and authority can be manifold. In some cases, the usual fire, police, and medical responder cohorts are augmented with National Guard and military units, volunteer efforts, and non-governmental organizations such as the Red Cross, among others. Not to be lost, however, is the observation that most incident responses begin in a local context but may blossom into a much more complex process for a variety of reasons.

It seems worth observing that "national security" and "public safety," while overlapping, are not coincident. The former is generally concerned with external threats that may, of course, also threaten domestic public safety. Public safety includes concerns for natural disasters, accidents and deliberately harmful acts. In many cases, the assets of the military and civilian organizations are drawn together to cope with situations beyond the capacity of either separately. The two regimes function with sometimes significantly different and even conflicting or at least incompatible policies, making the problem of coordination more complex and potentially affecting system designs for interoperability across a broad spectrum of actors.

---

[4] http://www.fema.gov/emergency/nims/

At least one commentator[5] observed that achieving public safety is hard because the effort is fragmented across the country. No single entity is in charge across the entire public safety enterprise, and solutions are expensive. Leadership is needed and costs need to be reduced. The classic “name a Czar” solution is not likely to work, either. Frameworks for cooperation that can build on common planning, standards, technology, budgeting and practices seem to be the most productive avenues for progress.

There are estimated to be 14,000 police departments, 3,000 sheriff’s offices, more than 6,000 911 centers, 65+ Fusion Centers, 1.2 million employees in city, county, state, and Federal law enforcement and 800,000 in private-sector security in the United States. These 2 million people worry about public safety for over 300 million citizens: a ratio of 150:1. Anything we can do to increase the efficiency and effectiveness of our public safety sector will benefit everyone.

1.2 Modern Communications

Coordination requires more than voice communication in this second decade of the 21st Century. It incorporates data, voice, and video communication and in the packet environment of the Internet, these are largely indistinguishable at the packet level. Indeed, it has become helpful if not vital and necessary, to equip emergency responders with access to the contents of the World Wide Web and to specialized and possibly access-controlled sources of information to aid in response to particular emergencies. As devices become part of the growing Internet, emergency responders may well need to have access to and even control over devices for surveillance and remote actuation.

Implicit in these observations is the apparent need for standards that will permit interoperation of communication devices and systems across a broad swath of actors in the public safety landscape. That these standards would benefit from international scope should be apparent, in the interest of facilitating responses to nondomestic emergencies, and taking advantage of larger markets to drive costs down through economies of scale.

1.3 Resilience, Robustness and Recovery

Without question, communications in support of public safety must be reliable, especially under stressed conditions, including, for example, loss of power, loss of infrastructure and lack of operating personnel. It seems appropriate to observe that this objective may be met not only through redundant provisioning but also through rapid deployment of temporary or even permanent infrastructure. Not only will first responders need rugged equipment but they will also need an ability

---

[5] John Gustafson, private communication

to deploy auxiliary or replacement gear quickly, at need. The utility of common standards should be obvious in this context – national, state and local-level caches of common equipment will be far more feasible if standards that permit interoperability can be established, adopted and applied.

It is also worth observing that operating conditions in emergencies are usually far from optimal, leading to the need for rugged gear that can be operated hands-free or with one hand and with protective gear in place including gloves. It is also important to recognize that not every piece of gear associated with emergency response has to have the same degree of ruggedness. There are in-vehicle devices, command centers and remote information processing sites that may be protected from the worst conditions and therefore able to operate with commercial quality equipment. A key objective, again, is for all equipment and systems to be able to interwork at need.

At least one participant in the public meetings suggested the creation of self-supporting “Regional Resilience Networks” acting as emergency communications utility companies that could be interconnected, possibly through commercial backbones. Such systems in the 25 largest coastal metropolitan areas would cover approximately 100 million of the 330 million U.S. population. In a related observation, the incorporation of private sector facilities, organizations and resources into national scale planning for public safety could lead to cost sharing and increased coherence.

1.4 Security, Authentication and Access Control

Generally speaking, access to emergency communications (including information sources, surveillance devices, remote control systems and so on) has to be managed. This implies that some kind of authentication is needed to validate a participant in emergency or public safety response. As has been suggested in section 1.1, a wide range of potential participants may require validation, and that rapid and reliable means to authorize responding actors will be particularly helpful. A variety of mechanisms may be invoked to achieve this objective, but it seems important to suggest that relying solely on such methods as user names and passwords may be naïve if not seriously risky. Again, the need for broadly applicable standards is clear, as are distributed methods for authentication to avoid the potential clumsiness and latency of overly centralized management. Pre-authorizations may prove useful as well as mechanisms that support and validate inter-organizational trust. It may also be worth considering the notion of identity according to “role” in addition to “person” to aid in pre-configuring communication and authentication system responses to particular kinds of incidents.

Homeland Security Presidential Directive 12 [HSPD12][6] represents a major initiative towards establishing common standards for personal identification within the Federal Government. Many of the ideas contained within this framework are potentially relevant to the problem of authentication in the context of general emergency services and should be taken into consideration.

1.5 Cost

Among the most serious barriers to effective emergency response is the cost of equipment, systems, maintenance and training in support of first responders. While there are many components that contribute to cost, there is a need to balance functionality and cost. Again, the potential value of common standards seems clear because they promote interoperability and competition. The design of the public safety network and the gear needed to exercise it must take into account realistic limits to affordability. Bulk purchases and national-or state-level warehousing may help to drive some costs down through economy of production scale.

It is also worth recognizing that commercial, “smart phone” platforms have produced substantial creative energy for development of useful applications. The notion of a land-mobile radio as a smart platform and designing that notion into the system seems very attractive as a way to facilitate public safety features and applications, many of which may be developed by the public safety community itself.

Use of commercial, off-the-shelf equipment, adapted or augmented perhaps to support specific emergency service needs, is also attractive and the next section explores this avenue briefly.

1.6 Interoperation with Commercially Deployed Systems

The currently apparent vector for a national public safety network acknowledges and builds on the anticipated deployment of the commercial, wireless Long Term Evolution (LTE) broadband standard. It is arguable, however, that a national public safety network will likely have needs that extend beyond deployed commercial system(s) and that, even if augmented with LTE components (cell towers, etc.) that are prioritized for public safety use, a robust and reliable system may need components that extend beyond the LTE operational envelope. For example, the need for peer-to-peer (“talk around”) capability and some form of relay capability might drive such extensions. An assumption in the remainder of this essay is that such extensions are worthy of exploration and may require a

---

[6] http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

combination of research, experimentation and prototype deployment for testing and evaluation.

In addition, it can be imagined that commercial equipment might be applied to serve emergency needs, potentially realizing cost savings. Smart phones could be equipped with applications and augmented to interwork with public safety equipment, especially where the use is in relatively benign environments.

1.7 Role of 911 and Other Online Public Safety Systems

The national public safety system is triggered into action through a variety of signals. Among the most common and important is the 911 telephone system, which has been extended over time to include mobile devices that can be located through proximity to specific base stations and, in many cases, the use of the Global Positioning System (GPS). That a national public safety network design needs to take into account the 911 system seems obvious. However, the 911 concept itself may well evolve as Internet-enabled devices become part of the online landscape. Hazard detectors that “know where they are” and can access the Internet may be able to announce emergencies automatically. Mobile phones may learn their precise location in public places such as hotel rooms from local announcements literally made by the room itself. The Federal Communications Commission (FCC) focus on location accuracy illustrates the richness of potential location-based designs.[7] There are many scenarios that invite creative means for improving the effectiveness and precision of the 911 concepts and a national public safety network design should take advantage of these possibilities. Civilians may become key sources of information in aid of incident response and their inputs need to be accounted for in the design of the information systems supporting public safety systems.

1.8 Frequency Allocations

Current frequency allocations assign 763-768 MHz and 793-798 MHz for base station and mobile unit use, respectively. The so-called “D” block would expand this allocation to include 758-763 MHz and 788-793 MHz to base station and mobile use, respectively. In addition, the public safety net communication requirements are also served with allocations in the 769-775 MHz and 799-805 MHz bands in 12.5 KHz narrowband increments. These latter allocations are primarily used for voice communication. The use of 700 MHz spectrum for public safety applications is attractive because of its propagation and penetration characteristics.

---

[7] http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0713/FCC-11-107A1.pdf

In 2003, the FCC allocated 50 MHz of spectrum (4940-4990 MHz) to public safety[8]. The FCC part 90 Rules governing the use of 4.9 GHz spectrum authorize public safety agencies to license and use the spectrum [472 U.S.C. §90] and the relationship of this band and the 700 MHz band for public safety remains an open question[9]. Any system design should take into account the possibility of devices operating in distinct and even multiple frequency bands, leading to the implication that bridging of frequencies through gateway methods (e.g. RF, IP or application layer conversions) may prove beneficial.

In this essay, it is assumed that solutions to public safety communication needs might be augmented through the use of unlicensed spectrum in the 2.4 GHz and 5 GHz ranges, Television White Space and even through use of 60-100 GHz allocations that might also be treated as unlicensed spectrum or, perhaps, shared for public safety and commercial purposes. These super-high-frequency bands have the potential for extremely high speed and broad bandwidth, although their propagation characteristics would likely require some forms of relay to achieve coverage, either owing to signal dissipation or inability to penetrate structures. Recently reported results[10] show that these super-high-frequency signals need not be strictly line-of-sight. The potential for multiple small antennas to improve received signal-to-noise ratio is attractive.

The Wireless Innovation Forum conducted two analyses of the role of software-defined radio and cognitive radio technology in the concept of a shared public-private 700 MHz network during the initial D-Block auction.[11]

1.9 The Role of Wired Communication

While much attention is often placed on the wireless elements of public safety communication, it would be a mistake to ignore or downplay the importance of

---

[8] http://transition.fcc.gov/Bureaus/Wireless/News_Releases/2002/nrwl0202.html

[9] Federal Communications Commission, 3rd Report & Order and 4th Notice of Proposed Rulemaking Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band (FCC 11-6), 26 January 2011.

[10] Marconi Society annual symposium on communications, UC San Diego, September 8, 2011.

[11] Considerations and Recommendations for Software Defined Radio Technologies for the 700 MHz Public/Private Partnership, 7 December 2007 [http://groups.winnforum.org/d/do/1579]; and Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership, 18 June 2008 [http://groups.winnforum.org/d/do/1564].

backhaul and national scale broadband wired networks that bind the wireless systems into a national and even a global fabric. The possibilities of shared and variable capacity facilities used by commercial and incident responders should not be overlooked. Expansion of shared or sharable capacity may prove to be more cost-effective than separate build-outs for public safety and commercial systems as long as the priority of public safety needs can be assured. It has been observed that backhaul capacity for commercial mobile systems such as 2G, 3G, 4G and LTE may be significantly under-provisioned and investment in this capacity may prove critical to the success of the national public safety network.

2.0 Desirable Features of a Public Safety Network Design and System

2.1 Flexible System Architecture

Among the problems encountered in interjurisdictional public safety response deployments is the failure of many devices to interoperate. Even those that purport to implement the P25 standards[12] do not always interwork. Given that there is a serious desire and need to support voice, video and data exchanges in public safety contexts, it may be instructive to consider how the Internet architecture supports mixed media and bridges otherwise incompatible physical and logical transmission mechanisms.

An important feature of the public safety network architecture should be its ability to evolve. It should be able to take advantage of commercial technology and services but not be limited by them. Integration of multiple radios or software-defined radios into the system may permit introduction of new functionality while retaining compatibility with earlier components.

One can also imagine the use of packet encapsulation and encryption methods to extend the reach of a secured public safety network across commercial backbones to increase the scope and resilience of the system.

2.1.1 Use of Internet Protocols

From the NRC report on wireless technology, we read:

“Technological capabilities are also driving the introduction of new radio system architectures, including a *shift away from centralized systems to more localized*

---

[12] PSCR Compliance Assessment Program: http://www.pscr.gov/projects/lmr/p25_cap/p25_cap.php

transmission in distributed systems that use very small cells (the smallest of those being deployed today are called femtocells) or mesh networks, and a shift from centralized switching to more distributed, often Internet-Protocol-based networks."[13]

In the Internet, a key protocol layer is the so-called Internet Protocol (IP) layer. This layer carries formatted "packets" of information from an addressed source to an addressed destination. There are also notions such as "multi-cast" and "broadcast" incorporated into the architecture. Internet packets are not aware of how they are carried. Consequenly, the routers that forward traffic from a source to a destination through intermediate relays may shift from one medium to another with impunity. An Internet packet may flow over a coaxial cable, a satellite link, a ground mobile radio link, and hard-wired optical fiber or Digital Subscriber Loop. The routers of the Internet take care of relaying packets on various media through the use of "convergence layer" software that adapts packet transmission to the next medium of transport.

In addition, the packets of the Internet are unaware of their contents. They carry "bags of bits" from source to destination where the bits are then received and interpreted by software at the destination. The Internet is, essentially, application unaware and a result of this is that new applications can be added to the system without having to change the network. This is not exactly correct, since some applications would not work unless the underlying network had sufficient capacity (e.g. streaming video), but such bandwidth is not application specific and all applications potentially benefit from an increase in the bearing capacity of the underlying Internet.

This leads to the idea that a public safety network based on the transport of Internet packets might prove to be more flexible and able to bridge more underlying transport technologies than the present designs. Even where radios are not compatible, if they can be made to carry Internet packets, then an intermediate routing and switching device could use classical store-and-forward methods to receive an Internet packet on one radio transport method and transport in another. Such overlay methods actually animate some of the commercial mobile systems today and have been demonstrated in military tactical communication as well.[14] The Internet itself makes use of the feature to

---

[13] [NRC Wireless] Op. cit. page 1

[14] The Defense Advanced Research Projects Agency (DARPA) has developed a system called MAINGATE that has features of this kind. In addition, DARPA has tested ideas arising from Delay and Disruption Tolerant Networking to achieve robust communication in hostile, interruption-prone environments.

allow satellite, fiber, coaxial cable, DSL and mobile communication systems to interwork at the IP layer.

On the demonstrable presumption that IP packets can carry voice, audio, video, and data and can be used in highly interactive modes, a public safety network design based on overlay transport of IP packets seems worthy of serious consideration. There are two formats for IP packets called IPv4 and IPv6, respectively. The former was standardized in 1978 and the latter in 1996. Both need to be supported because the IPv6 format, supporting many orders of magnitude more addresses, has not yet been fully deployed.

One of the interesting features of the Internet Protocol is that it works on a peer-to-peer basis. It is not necessary to pass through a router for two devices to exchange IP traffic assuming the devices are compatible at the layer below IP. This suggests that Internet-enabled public safety network radios should be able to exchange IP packets directly or even serve to relay such packets among edge devices that serve the triple role of source, sink and relay of Internet traffic. In the public safety network work, this is sometimes called “bypass” or “talk around,” although in the Internet case, virtually any class of traffic (voice, data, video) could be, in theory, directly exchanged or relayed.

2.1.2 Backward Compatibility

Introduction of a system that cannot interoperate with previously deployed equipment creates potentially serious barriers to effective operation. If backward compatibility requires the use of software-defined radios (SDRs), however, this could inflate cost. Alternatively, multiple radios within each edge device might actually prove to be more cost-effective. Adding compatibility modes of operation increases complexity, but this, too, might be ameliorated if automatic detection and adaptation can be achieved. A somewhat less attractive alternative is to make configuration relatively easier by maintaining common databases that associate particular edge equipment with particular emergency service/first responder organizations so that compatibility is achieved by configuring the edge equipment at time of deployment to take into account compatibility requirements.

Ideally, it is attractive to have the ability to fall back to simple voice broadcast without disabling the ability to use, concurrently, more sophisticated IP-oriented traffic exchanges. That this might involve the use of multiple radios needs to be considered and taken into account. Project 25-compatibility may be attractive, although it has been noted that not all “P25” devices appear to interoperate directly and may require gateways to assist.

2.1.3 Mesh or Mobile Ad Hoc Networking

Even if the baseline assumption is that public safety network elements will take advantage of commercial LTE technology, and even if dedicated to public safety

purposes, it is arguable that mesh networking could increase the flexibility of communication by allowing edge devices to serve as packet relays in a dynamic, mobile, mesh network design. The military has had considerable experience using these methods for tactical communication in hostile conditions. Moreover, these techniques may allow the use of much higher frequency and higher bandwidth capacities. There are commercial systems that make use of this technology such as the ArchRock sensor network,[15] though at modest data rates. The limitation of battery power is an important constraint on the design of mesh network protocols since every transmission draws down on the battery. Power-aware protocols may need to be developed to optimize battery life.

When combined with the ability of an Internet Protocol system to route traffic on alternative paths, a mesh network can be made part of a much larger, much more flexible, multimedia communication network. So-called “Interior Gateway Protocols” and “Exterior Gateway Protocols” allow for the formation of meshed subnets that are linked to each other through more global, internetwork protocols. The ability to interlink networks, to mesh adjacent, radio-compatible devices, and to combine them into a common network is one of the strengths of the Internet model and it may apply to the public safety network as well.

The introduction of dynamically deployed elements such as aerostat platforms to maintain wider-area connectivity to augment land-mobile communication fits well with a mesh kind of architecture with multilevel routing in which many networks are interlinked, as in the internet. The same may be said for multi-radio routers that can re-connect otherwise incompatible land mobile networks.

The potentially self-organizing character of mesh networks also fits well with cacheing or preplacement of equipment so that rapid deployment can augment, repair or replace damaged, broken or destroyed assets needed to support operational communication requirements.

The Wireless Innovation Forum Public Safety Special Interest Group (PSSIG) has conducted several studies that have addressed these ideas. Two of the studies were detailed analyses of public safety response scenarios - one actual (the bombing of the London underground on 7 July 2005) and one hypothetical (an explosion/fire at a chemical plant). In each case, the PSSIG reviewed the sequence of activities and postulated the impact of reconfigurable and cognitive radio technology on the response. For example, they identified the potential value of mesh-type technology in the London bombing scenario in which responders in the underground had no connectivity with the above-ground

---

[15] ArchRock was recently acquired by Cisco Systems; see also Moog Crossbow [http://www.moog.com/]

infrastructure and resorted to running to the closest stations to relay messages. These reports can be found at the Wireless Innovation Forum website.[16]

2.1.4 Robustness and Recovery

A national public safety network must be robust and reliable on a daily basis. Its design must take into account power failures and loss of critical components (e.g. relays, cell towers, routing and switching equipment). Moreover, it must be possible to reconstitute the system quickly either by rapid deployment of replacement equipment or temporary deployment of equipment to augment the network operation. For example, one might imagine use of aerostats[17] or balloon-based relays, repeaters, gateways and routers to provide connectivity.

Under this rubric, it should also be an objective to make the equipment used in incident response as instantly available as possible. When a device is turned on, it should be immediately operational or as nearly so as possible. “Instant on” should be part of the evaluation criteria for system and device design evaluation.

During the discussions leading to the preparation of this essay, it was observed that scenarios for varying levels of infrastructure loss should be developed to assess the ability of the public safety network to recover from and respond to impairments. Included in this assessment would be malicious physical and logical attacks, jamming and other pernicious actions intended to interfere with the successful operation of the public safety system.

2.2 Security and Authentication

Public safety communications, while potentially benefiting from access to and use of commercial technology, equipment and services, also have a general requirement that use of the system and information it contains is limited to authorized parties. This observation does not rule out the importance of providing for public access information about dangers, necessary actions, evacuation points, shelters, emergency procedures and so on. To assure that systems intended for emergency responders are used only by authorized personnel,

---

[16] *Use Cases for Cognitive Applications in Public Safety Communications Systems* – Volume 1: Review of the 7 July Bombing of the London Underground, 8 November 2007 [http://groups.winnforum.org/d/do/1565]; and *Use Cases for Cognitive Applications in Public Safety Communications Systems* – Volume 2: Chemical Plant Explosion Scenario, 10 February 2010 [http://groups.winnforum.org/d/do/2325]

[17] See http://www.fcc.gov/document/fcc-hold-open-commission-meeting-thursday-september-22-2011

some form of authentication is needed not only for personal authentication but also to assure that the equipment tied into the system is also authorized. This is a nontrivial problem to solve because security and authorization can often end up creating unintended denial-of-service to the very parties who need access to respond to the emergency.

2.2.1 Strong Authentication

Since the revelation that asymmetric cryptography is not only imaginable but also implementable, public key cryptography has had a growing role to play in securing communications, effecting symmetric key distribution, assuring the integrity of information with digital signatures and implementing strong authentication of individuals and devices in networked environments. The use of user names and passwords, as prevalent as this has been for many decades, is now recognized as a risky practice subject to easy penetration in many cases.

It is desirable to be able to configure emergency communication and information systems to validate the devices that access or form the networks and servers and also to validate users and their authorization to use these systems. Not all information needs to be nor should be accessible to everyone. It should be possible to form closed user groups for communication and information access, if only to limit resource demands and protect privacy and confidentiality. What is desired, however, is the ability to quickly and flexibly assign and restructure such groups as the need arises. It should be possible to predefine groups of users/responders who should be able to communicate. A desirable outcome is that communication between any pair of responders should be technically possible and only barred by administrative decision, not by technical incompatibility.

So-called “two-factor” authentication is attractive, if it can be made to work easily and transparently. Colloquially, this is sometimes referred to as “something you know and something you have.” Occasionally, it becomes “something you are and something you have.” The idea is that access to the public safety network and systems is mediated by strong cryptographic authentication. For example, a device that the first responder carries may contain cryptographic information that can be “activated” through use of a personal identification number (PIN), voice authentication, iris scan, or thumb print. Once activated, the device becomes the means by which the first responder can be remotely authenticated into the public safety system. The mechanics of this process can vary. One possibility is a “challenge/response” method in which the first responder identifies himself or herself with a user name and the system responds by requesting that the activated edge device decrypt a random numeric challenge encrypted in the public key of the edge device (or first responder). This random number is then re-encrypted in the public key of the destination server and validated upon receipt.

Methods such as this can be used to strongly authenticate devices and users as they enter into the public safety network. Potentially replicated and distributed databases can be used to confirm authorizations, exclude invalid users, and admit new devices into the network, etc.

It is not the purpose of this essay to make specific technical recommendations, but such scenarios, applied both to the users, information and the equipment in the public safety systems, can improve its robustness and resistance to abuse.

One can imagine devices authenticating themselves to local mesh network systems in order to join in radio contact and users authenticating their privileges through strong identification and validation of their identities. Mesh networks can use these methods to validate the entry of new equipment, access devices and servers into the system. It is important to note that pairs of devices may need to validate directly, possibly without reference to a third party, under some conditions.

These ideas are not new. Some of them can be found in the U.S. Unified Community Anchor Network effort.[18]

2.2.2 Distributed Authentication

Because first response may involve parties from many different organizations, it may be important to establish the ability to validate first responders through their organizations, rather than attempting to maintain a centralized database of all valid users. Federation of the authentication system seems called for, so that a first responder joining a response team can be validated by reference to his or her “home” organization. Plainly, a trust model is needed that will accommodate many institutions in the same way that we trust the motor vehicle departments of each state in the Union to validate the holders of drivers’ licenses and accept this validation across the United States. There are many technical means through which to accomplish this federated validation and these should be investigated for applicability to the public safety network design.

In emergencies, the ability to qualify responders quickly to access and use public safety communication and information resources and to group them as needed for broadcast or multicast applications should be considered a highly desirable property.

---

[18] http://www.usucan.org/

An example of effort in this dimension is found in the InCommon Federation for nongovernmental organizations whose work might be made to interwork in some federated way with governmental authentication.[19]

2.3 Standards Application and/or Development

In the Smart Grid program, the National Institute of Standards and Technology (NIST) instituted the creation of the Smart Grid Interoperability Panel (SGIP) that was populated with representatives from 22 sectors at interest in the Smart Grid. A Governing Board was elected from among the 1700+ participates and 656 companies. SGIP is *not* a government advisory body. It is a distinct non-governmental and non-profit organization devoted to facilitation of the development of standards in aid of Smart Grid development and deployment.

One could imagine a similar Public Safety Interoperability Panel operating in a similar fashion to coordinate the efforts and interests of the many stakeholders in the public safety arena. Its purpose would be to facilitate standards development and adoption through recognized Standards Development Organizations. While the SGIP effort is still a work in progress, it has been an effective mechanism for serious work on the elaboration of standards and requirements and identification of useful specifications for Smart Grid devices. There exist organizations with charters related to this idea such as the National Public Safety Telecommunications Council[20] and the Federal Partnership for Interoperable Communications.[21]

There can be little debate that standards will be a determining factor in the success of a national public safety network on the grounds that compatibility among the network elements and between and among the edge devices can only be usefully achieved through adoption of common standards and practices. Just as important as standards are tests that can verify and validate the conformance of fielded systems to standards. This was a crucial element in the Smart Grid program, and a focused working group was created to assure that this idea received persistent attention. The public safety network, as conceived in this report, is vitally dependent on consistent interoperability of all components.

It is also relevant to note the remarkable effect of standardized,or at least publicly available Application Programming Interfaces (APIs) for smart phones. The large and growing “app stores” for mobiles have leveraged these specifications by

---

[19] http://www.incommonfederation.org/

[20] http://www.npstc.org/

[21] http://www.dhs.gov/files/committees/gc_1176496203797.shtm

allowing virtually anyone to create and make available new applications for smart phone platforms. A similar standardization for public safety systems could unlock substantial innovation from the first responder community itself. A similar experience can be seen in the use of information system APIs for geographic presentations services such as Google Earth, Microsoft Bing Maps, etc. These systems allow users to present their information to users and are often used in emergency situations to illustrate the boundaries of fires, the locations of emergency evacuation centers, before/after imagery in earthquakes and tsunamis, and so on. The application space appears to be unlimited and the use of APIs allows even the general public to contribute content. Plainly, validation of public content is important to avoid deliberate misrepresentations. It is interesting to note how quickly the use of mobile images and video uploaded to the YouTube system have been used in emergency communications by the public news broadcasters.

2.4 Ruggedization

While not all devices employed in the conduct of public safety service need to be ruggedized, some most definitely need this feature. A key difference between an inexpensive cell phone and a public safety radio is that there are serious consequences if the public safety device is dropped, submerged in water or otherwise rendered inoperable. For a policeman in a life-threatening situation or a fireman battling a fire in a wet, smoky environment, the consequences of mechanical or other failure can be deadly. Two conclusions may be drawn from this observation:

1) ruggedized units and more conventional devices need to share architectural and technical characteristics that allow them to interoperate, and

2) ruggedization will have an impact on affordability, battery life, weight/size, utility while wearing protective clothing, including gloves, etc.

A balance has to be struck in designing in ruggedness to assure utility and reasonable cost without loss of reliability.

2.5 Sensor and Location Systems

Sensors are getting smaller and proliferating and they can be effectively outfitted with the ability to become part of a network. That the information from such devices can be essential to effective incident response must be acknowledged and accounted for in a system designed to bring relevant data to the attention of responders. In essence, responders should be in a position to draw upon a wide range of accumulated and real-time sensor data, preferably with convenient and reasonably uniform user interfaces.

It is vital to know where responders are, and a number of options could be incorporated into the design including the use GPS coordinates, and relative locations based on radio triangulation, among others. Commercial use of WiFi locations information might well prove useful in incident response to augment other methods, for example. Incorporation of an accurate “terrestrial GPS” capability in the public safety network design to better support indoor and underground positioning information would be very beneficial. The safety of the responders would be enhanced, as would the ability to locate survivors found by first responders, even when satellite GPS is not available.

2.6 High Density Radio Operation

One of the classic problems that can be encountered during emergencies is congestion of publicly accessible wireless services, including commercial consumer mobile services, citizen’s band radios and, potentially, frequencies dedicated to public safety communications. The use of LTE, even if in frequencies dedicated to emergency services, might encounter congestion and the need for prioritization. This is equally true of packet switched systems operating in broadcast mode. Any successful architecture will need to deal with the possibility of self-interference owing to heavy concentration of emergency service actors in a localized region.

2.7 Next Generation 911 Emergency Services IP Networks[22]

The 911 system, based on conventional telephone services, is due for a serious upgrade to take advantage of new communications and information technology. The need for standardization in such a system should be obvious. Because so many new platforms have the ability to interact with both the existing public switched telephone network (including wireless) and the public Internet, it seems clear that effort is needed to incorporate the advanced thinking about emergency services communication into the general fabric of the national public safety network design. There are remarkable opportunities to make an advanced 911 system far more effective. Internet-capable devices can know exactly where they are, and some concepts include interior positions. For example, a hotel room could literally tell a mobile or laptop exactly what room it is in so that the emergency responders have far more than an address to go to. One can even imagine mobile devices that can deliver information about the condition of the person in need of emergency assistance thanks to various kinds of monitoring that is increasingly possible with smart phones and assistive devices.

Several IP-based networks have been or are being developed to link Public Safety Access Points but it is not clear how coordinated these efforts have been

---

[22] http://en.wikipedia.org/wiki/Next_Generation_9-1-1

with regard to technical interfaces, if any, such as to the public Internet and to each other. This is an area well worth examining.

3.0 Prototyping, Collaboration and Testing

The current public safety system in the United States is a diverse conglomeration of institutions, organizations, groups, equipment, systems, radio frequencies and communication protocols. Communications technology, software and systems continue to evolve at a rapid pace in the commercial sector as well as in the military and in specialized public safety sectors. Achieving long-term resilience, robustness, reliability and interoperability in a secure context that is flexible and adaptable to changing needs is a major challenge. It is a thesis of this essay that a purely top-down design approach is unlikely to result in a system with the quality and features desired and needed. Rather, serious prototyping and testing under realistic conditions and with the full range of public safety practitioners is necessary to accommodate iterative designs and maintain interoperability.

There are numerous test beds that have been organized to improve the quality of design and feedback for complex communications and information systems. Among these is the Network Integration Evaluation (NIE) effort organized at Ft. Bliss by the U.S. Army in cooperation with the Defense Advanced Research Projects Agency (DARPA).[23] Strongly supported by the Vice Chief of Staff of the Army, GEN Peter Chiarelli, this is a good example of the use of realistic testbeds to inform and drive design, innovation and validation of systems. NIST operates a test bed in its Boulder, CO, facility in which many first responder participants are evaluating equipment and systems for their interoperability and serviceability.

It seems important to establish a framework in which implementations of first response support systems can be validated in realistic settings, including ability to support desired applications, and ability to interoperate and accommodate the many different organizations that have to come together to preserve public safety. Municipal, state and Federal cooperation should be accommodated. Nor can this be a one-time activity. Rather, this should become the normal practice for the evolution of new and improved first response systems and technologies.

As the public safety system evolves, and it must evolve, the testbeds will be vital for exploration of new technology, methods, ideas and architectural enhancements. It would be a major mistake to imagine that the design of a public safety system is a one-time event. It will be part of a continuing evolution of telecommunication and information technology and will play a key role in facilitating that evolution.

---

[23] http://www.bctmod.army.mil/news/agility.html

4.0 Multiple Stakeholders

There are many stakeholders in the public safety arena (cf: section 1.1). Their interests and established positions vary although all of them are, to first order, aligned in the interest of public safety. There are many public safety organizations, institutions, operators, regulatory agencies, private-sector suppliers, volunteers, legislators with budgetary responsibility and beneficiaries of public safety activities. Navigating through the potential thicket of competing interests will not be easy. The technical community can contribute strongly through formulation of designs and architectures that maximize the flexibility of the public safety network system to ingest and use new technology, spectrum, platforms and systems. Leadership is needed to achieve that objective and to take advantage of the strengths of commercial sector capability while escaping any limitations that would inhibit the ability of the public safety actors to carry out their work.

Among the considerations derivable from the multi-stakeholder aspect of public safety is the observation that the stakeholders are often on different funding cycles and amounts. Of necessity, decisions are frequently made independently among the stakeholders without regard to interoperability and interconnection. Steps to improve the ability of stakeholders to increase the likelihood of compatible operation would be highly beneficial.

5.0 Programmatic Considerations

5.1 Public Safety Network Interoperability Panel (PSIP)

With reference to sections 2.3 and 4.0, it may be very helpful and effective to establish a Public Safety Interoperability Panel to help facilitate the evolution of standards that can help to achieve the goals suggested in this essay. NIST acted very effectively in the creation of the Smart Grid Interoperability Panel as a private-sector entity, and it seems worth considering a similar entity for the benefit of standards for public safety systems, equipment and applications. Mechanisms for preparing configuration profiles and for managing identifier and other resources will also be needed and might be created through the PSIP.

It is clear that a rich and diverse stakeholder representation would be required to make useful and effective such a panel. A business model and institutional framework (e.g. NGO? Non-Profit? Government-sponsored entity?) will be needed to assure sustained operation of the PSIP.

5.2 Coordinated Research, Development and Testing

Without doubt, DARPA, the National Science Foundation, NIST and others are already engaged in the development or testing of technology and systems that can be of benefit to the first responder community. A coordinated program of

research, development and testing to include private-sector, commercial activities could be an effective way to harness innovative energy. A steering/coordinating activity engaging OSTP, NSTC, NIST, DARPA, NSF, DHS, NIJ[24]along with state and local agencies and private sector public safety entities may provide a platform for review of research and development activities. Funding for this work could derive from spectrum auctions, as currently provided for in legislation under consideration[25]. An estimated $300 million has been identified for the multiyear development and test effort needed to perfect the design of a national scale public safety system.

Coordinated use of test beds to assess, validate and refine technologies, prototype systems and applications could be established. Exercises involving public safety actors across the spectrum might also be undertaken in this test bed context. There exists an extensive test bed available and already in use for this purpose at the NIST Boulder, Colo., facility. In addition, there are Defense Department facilities such as Ft. Huachuca and Ft. Bliss that offer potential sites for interoperability testing between military and civilian mobile communication systems.

The creation of a private or quasi-public entity to manage the design and development of an evolvable public safety network might provide a framework for progress.

Areas for research and development could include:

Dynamic spectrum management

Policy management

Mobile, ad hoc networks and protocols

Introduction of broadcast and multi-cast facilities into the wireless and wired Internet (may require new protocol developments)

Peer-to-Peer use of LTE

Strong authentication technology and systems

Platforms for public safety applications development

---

[24] National Institute of Justice that acts as the R&D arm of the Department of Justice [http://nij.gov/]

[25] http://www.politico.com/news/stories/1011/65644.html

Certification regimes and practices to validate safety and utility of devices and systems

Support for multimedia application and integrations

Tools for collaborative display, databases and geo-spatial information

Open Source Software Development[26]

It is clear that there is a great deal of opportunity for advanced research, tool development, testing regimes and coordinating activities to make a major difference in the development of advanced public safety systems.

5.3 National Incident Management System (NIMS)[27]

NIMS "provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location or complexity."[28] NIMS provides a consistent set of policies and procedures for multiple agencies to collaborate in preparing for and responding to an incident. These policies and procedures have implications for the kinds of communication support needed for resource management and command in an incident response. The design of the national public safety network should take into account the referenced polices and procedures found in the NIMS framework.

5.4 Training and Evaluation Program

Any successful effort to create a national-scale public safety communication infrastructure and framework will also need to incorporate a training and evaluation program to assure that the diverse actors dependent on the system have adequate training, facilities, equipment and documentation as well as operational qualifications sufficient to assure success.

---

[26] http://sahanafoundation.org/ by way of example.

[27] http://www.fema.gov/emergency/nims/AboutNIMS.shtm

[28] Department of Homeland Security, "National Incident Management System," December 2008, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

5.5 Institutional Framework

In addition to the Association of Public-Safety Communications Officials (APCO) and its spectrum management arm (AFC), the Public Spectrum Safety Trust (PSST),[29] and the 3rd Generation Partnership Program (3GPP),[30] there are many other existing domestic and international bodies that have an interest in the design and operation of public safety communication systems and technologies. It is an open question whether an existing body or federation could be tasked with orchestrating the development of a U.S. new domestic public safety communication system, but it is clear that the process will need management, steering and oversight. A primary challenge in realizing the aspirations outlined in this essay will be the formation or adoption of an agent that can lead, manage and execute a program leading to the desired result.

6. Conclusions and Recommendations

1. **A Public Safety Capability organization should be selected or created to orchestrate the detailed design, development and coordinated operation of a new, national public safety communication system. It should include a Public Safety Interoperability Panel and resource management capability.**
2. **The architecture of the new public safety network should:**
    a. **Incorporate commercial technology where appropriate.**
    b. **Extend commercial technology to achieve robustness.**
    c. **Provide for backward compatibility or interoperability through standards adoption and/or development where feasible. including interoperation with existing and new 911 systems**
    d. **Give high priority to cost-effectiveness and affordability.**
    e. **Take advantage of Internet and other packet-based technologies to support multi-media communication and mobile ad hoc network formation.**
    f. **Incorporate assigned public safety spectrum and other data communication spectrum assignments and include opportunity for sharing where feasible.**
    g. **Incorporate strong, federated authentication and other security technology to positively identify and authorize personnel and equipment permitted in the system.**
    h. **Incorporate advanced position location capabilities, including indoor and underground location.**

---

[29] http://www.psst.org/index.jsp

[30] http://www.3gpp.org/

   i. **Make extensive use of open national or international standards and, where appropriate, open source software.**
3. **The development program should include substantial opportunity for coordinated development and testing of protocols, systems, devices and practices among a wide range of actors including traditional emergency responders, national homeland security elements, military, state militia, municipal, private sector public safety organizations and research agencies and institutions. Nontraditional players, including a wide range of private sector networked information industry elements, should be included.**
4. **Persistent and sustainable testbeds should be incorporated into the program in support of long-term evolution of public safety communication standards and technologies.**
5. **Above all, the system must be flexible and adaptable to new requirements and incorporation of new technologies and capabilities.**

7. Acknowledgements

Visiting Committee on Advanced Technology (VCAT)**:**

Thomas Baer, Vint Cerf, Sujeet Chand, Uma Chowdhry, Paul Fleury, Tony Haymet, Karen Kerr, Shaygan Kheradpir, Pradeep Khosla, Michael McRobbie, Roberto Padovani, Alton Romig, Darlene Solomon, Alan Taub

VCAT acknowledges with gratitude the following individuals and organizations:

Members of the President's Committee on Science and Technology (PCAST): Mark Gorenberg, Craig Mundie, William Press, Maxine Savitz, Eric Schmidt

OSTP contributor: Aneesh Chopra

NIST and PSCR contributors and participants: George Arnold, David Atkinson [PSCR], Jason Boehm, Jeff Bratcher [PSCR], David Cypher, Donna Dodson, Cita Furlani, Patrick Gallagher, Katharine Gebbie, Ajit Jillavenkatesa, Suzanne Lightman, Doug Montgomery, Emil Olbrich [PSCR], Dereck Orr [PSCR], Alan Pentz [PSCR], Jim Schufrieder, Chuck Romine, Mark Stolorow

DARPA contributors: Kaigham Gabriel, Larry Stotts

Public sector contributors: David Boyd [DHS], Keith Bryars [FBI], Ralph Burnett [DHS], Andrew Clegg, Jeff Dulin [Charlotte NC Fire Dept.], Emily Early [DHS], Chris Essid [DHS], Anna Gomez [NTIA], Terry Hall [APCO], Regina Harrison [NTIA], Jim Hassett [NYPD], Joe Heaps [DOJ], Farnam Jahanian [NSF], Lance Johnson [NTIA], Rick Kaplan, John Leibovitz, Peter Levin, Tim Lowenstein [National Association of Counties], Cuong Luu [DHS], Gary McCarraher [Franklin

MA Fire Dept.], Harlan McEwen, John Melvin [Grant County Sheriff], Dick Mirgon [APCO], Chris Moore [San Jose Police Dept.], Jon Olson [Wake County EMS], Craig Peters, Dusty Rhodes [DHS], Allan Sadowski [NC State Highway Patrol], Bill Schrier [City of Seattle], Robert Schneider, Henning Schulzrinne [FCC], Doug Sicker [NTIA], Tom Sorley [City of Houston], Lawrence Strickling [NTIA], Steven VanRoekel [OMB]

Private sector contributors: Doug Aiken [NPSTC], Coleman Bazelon, Stacy Black [AT&T], Vanu Bose [Vanu Inc], Don Brittingham [Verizon Wireless], Jim Bugel [AT&T], Michael Calabrese, Ken Carlberg, Robin Chase, John Cracolici [Cisco], Fred Frantz [L3 Communications], Kevin Gifford [Univ. Colorado], John Gustafson, Christopher Guttman-McCabe, Philip Harris, Dale Hatfield, Ajit Kahaduwe [Nokia Siemens], Brian Kassa [Nokia Siemens], Michael Katz, Paul Kolodzy, William Lehr, David Liddle , Bill Manke [Qualcomm], Michael Marcus, Preston Marshall [USC-ISI], Dennis Martinez [Harris], Mark McHenry, Milo Medin [Google], Sascha Meinrath [New America Foundation], Joseph Mitola, Michael Nelson [Georgetown University], Stagg Newman, Eli Noam [Columbia University], John Powell [NPSTC], Justin Ratner [Microsoft], Dan Reed, David P. Reed [MIT], Jeffrey Reed, Corey Reynolds [Corner Alliance], Dennis Roberson, Brian Rosen, Gregory Rosston, Andy Seybold, Bill Smith [PayPal], Darlene Solomon [Agilent], Saul Steinberg [Motorola], Marilyn Ward [NPSTC], Tony Werner, Diane Wesche [Verizon Wireless], Tony Wheeler

References

[MAINGATE] http://www.afcea.org/signal/articles/anmviewer.asp?a=2102

[NFPSBBN] National Forum on Public Safety Broadband Needs
http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=601

[NRC Wireless] *Wireless Technology Prospects and Policy Options*,
National Research Council, 2011, National Academies Press,
ISBN-13: 978-0-309-16398-9, ISBN-10: 0-309-16398-6 [more stuff goes here]

Glossary

3GPP: 3rd Generation Partnership Program [http://www.3gpp.org/]

AFC: APCO Spectrum Management [http://www.apco911.org/frequency/]

APCO: Association of Public Safety Officials [http://www.apco911.org/]

COPS: Community Oriented Policing Services [http://www.cops.usdoj.gov/]

IP: Internet Protocol

LTE: Long Term Evolution [refers to long term generations of commercial mobile radio]

NIMS: National Incident Management System

NPSTC: National Public Safety Telecommunications Council
[http://www.npstc.org/]

PSCR: Public Safety Communications Research (NTIA/NIST)
[http://www.pscr.gov/]

PSIP: Public Safety Interoperability Panel [an idea introduced in this essay]

PSST: Public Safety Spectrum Trust [http://www.psst.org/index.jsp]