Emergency Response Interoperability Center

Public Safety Advisory Committee (PSAC)

Recommended Applications List and Guidelines for Developing Well-Behaved Applications

Applications and User Requirements Workgroup Report

June 2011 – Revised

Acknowledgements

The following individuals contributed to the creation of this report:

Tom Bretthauer
Hugh Clements
John Collins
Michael Coyne
Chuck Dowd and Jim Hassett
Christopher Epps
Raymond Flynn
Mark Hill
Robert Lederman and John Brophy
John Lenihan
Kevin McGinnis
Stephen Meer
Jackie Mines and Brandon Abley
Dick Mirgon
Jonathan Moore
Bill Schrier
Tom Sorley

Table of Contents

1 Executive Summary

1.1 Charter, Goals and Objectives

1. The Applications and User Requirements Work Group of the Public Safety Advisory Committee (PSAC) to the Emergency Response Interoperability Center (ERIC) of the Federal Communications Commission (FCC) will recommend to the PSAC which applications and other user requirements must be supported on the nationwide public safety broadband wireless 700 MHz network (PSWBN) presently under construction in the United States. This document contains revisions to the original report, based upon comments received in the PSAC meeting of May 24, 2011.

2. Goals:

   2.1. Identify a set of principles for use in identifying, creating, deploying and maintaining both nationwide and regional/local applications used on the public safety wireless broadband network.
   2.2. These principles must provide for adaptability and flexibility in the creation and use of these applications, as well as protect the security and reliability of the PSWBN.

3. Long-Term Objectives:

   3.1. Identify and prioritize a key set of nationwide applications which must be available to all responders using the nationwide public safety broadband wireless 700 MHz network.
   3.2. Identify which other applications or functionality must be available ubiquitously on the nationwide public safety broadband wireless 700 MHz network, e.g. VPN to a home network computer-aided dispatch system.
   3.3. Identify and prioritize other user requirements which the on the nationwide public safety broadband wireless 700 MHz network must or should support.
   3.4. Identify guidelines and standards for coding, certification and testing of applications, whether such applications are deployed nationwide or just on local, regional or statewide networks.

4. Shorter-Term Objectives:

   4.1. In order to ensure that the public safety broadband network is interoperable on a nationwide basis, what user applications should each network be required to support?

   4.2. Is there an approach to ensure that over time the regulations governing the public safety broadband network stay current to meet user requirements?

1.2 Background and Purpose

5. The Public Safety Advisory Committee (PSAC) advises the FCC's Emergency Response Interoperability Center (ERIC). The proposed nationwide Public Safety Wireless Broadband Network (PSWBN) will use Long-Term-Evolution (LTE) as a technology. But the PSWBN only

exists to serve as a communications network to bear the applications which first responders in the United States need to protect and serve the public safety. These applications will be developed from many commercial and government sources. Some applications will be national in scope, i.e. available anywhere, anytime, to first responders using the network. Other applications will be unique to certain agencies and jurisdictions, and may be available just to a certain subset of responders.

6. This document details some considerations and recommendations for which applications should be available ubiquitously – nationwide - on the PSWBN, as well as a set of guidelines for "well behaved" applications. The PSWBN will have high speeds and significant capacity. Nevertheless both its speed and capacity are limited. Any application built to run on the network must recognize this restriction and balance functionality versus use of network resources, i.e. the applications must be "well behaved".

1.3 Architectural Background

The Architecture of the PSWBN has a direct affect on how applications will appear on the network and access network resources. In creating this set of application recommendations, the workgroup assumed the following:

7. Local construction. The network will be constructed largely by local jurisdictions. That is, individual cities, counties, regions or states will construct, manage and maintain cell sites and eNodeB equipment at those sites, and will interconnect those sites with backhaul and radio access networks (RAN). There will, however, be a number of central functions or services on the network (see paragraphs 9 and 12 below).

8. Locally hosted applications. Many applications important to local responders will reside on servers and in data centers connected to the local backhaul network. Such applications might include computer-aided dispatch (CAD) systems, local records management systems (RMS) and so forth.

9. Nationwide Archtecture and Business Model. We assume that there is a national architecture and a business model to maintain that national architecture over time.

10. Ubiquitous roaming. Public Safety users will be able to roam freely nationwide on the PSWBN, with no additional charges when roaming on the PSWBN outside their home networks. (Note: this does not apply to roaming onto commercial networks. If a public safety user has a "roaming" indicator on their device, the user is on a commercial network.)

11. Standards for applications.

11.1. Applications on the network must be well-behaved. The workgroup assumes the PSWBN will have governance, and the governing entity will adopt standards and manage which applications are allowed onto the network.

11.2. Supporting protocols. Many of the applications in this document will require specialized protocols and functions to be installed on the PSWBN. These might include IMS (Internet protocol Multimedia Subsystem), "multicast", and SIP (session initiation protocol) as two examples. These protocols may require releases of LTE beyond the current standard.

12. Governance. A Nationwide Governance Entity is an absolute requirement for deploying applications and, in particular, well-behaved applications. The governance entity would cause

testing and certification of applications, as well as a wide variety of network management functions such as priority which are vital to adequate response time for applications on the nationwide network. Other required network management functions including an updating service, patching service, software download service and similar functions.

13. Network Evolution. The PSAC has a Network Evolution Workgroup. This workgroup developed an evolutionary path and roadmap for the technology used in the PSWBN. The Network Evolution report extensively discusses applications. Many of the applications listed below are not supported in by current or immediate near-term future releases of the Long-Term-Evolution (LTE) protocols. See the Network Evolution report for more details about such features.

2 Applications Important to Public Safety

This is list is in approximate priority order, most important first.

2.1 **Emergency Function**.

14. This application would be deployed throughout the PSWBN. It would function similarly to the "emergency button" function available on some land-mobile-radio (LMR) voice system. When activated, the "emergency function" application would send an alert using the highest permissible LTE priority to the local public safety dispatch center. The alert should include AVL/GPS information, user identification and all other possible information which might help the dispatch center understand and respond to the alert. This function would differ from a 911 call, in that the emergency alert would be sent to the public safety dispatch center, which in some cases will be different from the public safety answering point (PSAP) or 911 center.

2.2 Global positioning information.

15. The network will allow GPS applications[1], including GPS location, automated vehicle location (AVL), and so forth. The network will allow GPS information to be transmitted as part of any message or data packet sent by any other authorized application through the network. GPS data shall be exchanged on the PSWBN in a single universal (interoperable?) form/format which provides location information as latitude and longitude in decimal degrees and includes a reference to the Datum used. (example: North American Datum of 1983 (NAD 83)).

2.3 Commercial Mobile Alert System (CMAS-Public Warning).

16. The PSWBN will support CMAS, which is defined by the FCC under Part 10 rules, to handle broadcast of geo-targeted imminent threat to life or property emergency alerts distributed by the federal government though a CMAS aggregation function under the FEMA iPAWS program.

[1] GPS Applications are still subject to assumption II-5 above.

2.4 Incident management tools including data access.

17. Access to incident management tools such as computer-aided dispatch systems (CAD), records management systems (RMS), mobile NIMS administration systems (M-NIMS),and other databases with all manner of information necessary for first responder work on behalf of public safety are the most important applications, other than voice, for the PSWBN. We expect some of these applications could be deployed on a nationwide basis, others with local implementations. In certain cases, nationwide applications may be constrained by local laws. For example, access to criminal history information could be restricted by a local ordinance or state law, even though it is NCIC information. Or local laws may require certain kinds of additional tracking and logging for each such access. In these cases, a local application may have to be used.

    17.1. Nationwide implementation:
        17.1.1. NCIC and other nationally-maintained criminal databases
        17.1.2. Material Safety Data Sheet (MSDS) databases
        17.1.3. EPA information
        17.1.4. Mobile applications that use file sharing from any mobile device to any other mobile device.

        17.1.5. Applications that mobilize NIMS ICS protocols, processes and administration should be national and ubiquitous. This includes NIMS ICS forms, reports and the ability to create and manage event archives. (This is consistent with the FEMA 5-year plan for nationwide NIMS deployment and adoption)
        17.1.6. Many other queries and applications

    17.2. Local implementation:
        17.2.1. Resource status, e.g. "fire company cleared from scene and available for dispatch" or "EMS unit arrived on scene".
        17.2.2. Computer aided dispatch (CAD) systems
        17.2.3. Records management systems (RMS)
        17.2.4. Local criminal databases
        17.2.5. Patient information (local hospitals)
        17.2.6. Ad hoc patient information created each time a patient is encountered by EMS in the field.
        17.2.7. NIMS ICS forms and reports, shared between field operations and EOCs, and able to be printed and distributed on scene.
        17.2.8. Many others

2.5 Welcome or "splash" page.

18. Each device connected to the PSWBN, when leaving its home network and going into another public safety network on the PSWBN, will have access to a welcome, "splash" or "help" web page. This page will likely be simple HTML, and will contain information the roaming user may need when away from the user's home network, e.g. telephone numbers for support/service, the name/contact information for the local builder or local controlling agency of the network, alerts/notices and other information.

19. Typically the user might receive a text welcome message with a link to the "splash" page when first connecting to a jurisdiction's public safety network.

20. This function implies some manner of a common "connection" or "talk/data group" which is available throughout the nation. See also paragraph 10 above for assumptions about roaming – that when a user device receives a "roaming indicator", that device is on a commercial network – there is no "roaming" in the traditional sense between regional portions of the PSWBN.

2.6 Internet Access.

21. Access to the Internet must be available ubiquitously within the footprint of the PSWBN to all authorized users of the network.

22. Ideally, each local, city, county, regional or statewide network will have direct connections to the Internet, as opposed to having only a few nationwide Internet access points. This architecture should provide faster and more robust Internet connections for local responders.

23. Many local and state agencies, however, restrict Internet access for their users. Local ordinances and state laws may restrict the access, and the long-standing policies of some agencies may further prohibit or restrict such access.

24. Therefore the ability of individual users to connect to the Internet must be controlled and managed on a policy basis by the agency which authorizes their connection to the PSWBN. This implies some users may directly connection to the Internet no matter where they roam on the PSWBN. Other users, however, might be restricted by their agency so their Internet access must be routed through the backhaul of the PSWBN to their home agency, where appropriate firewalls, filters and policy restrictions can be applied to their use.
    - 24.1. Priority access to transmission bandwidth should be selectable from the user device level, as authorized by the agency, based on exigencies.
    - 24.2. High QoS for emergency video/audio streams, documents and other critical data or media files requiring priority access and distribution should be made available without file transfer limitations, to the full extent of available bandwidth.

2.7 Virtual private networking (VPN).

25. Every user of the PSWBN will be allowed free and unfettered access via VPN to their home networks to access files and applications.

26. The PSWBN will allow VPN, and will also allow any "standard" VPN software to be used, as long as such software complies with security standards established by the nationwide governing entity.

27. Network security schemes should be designed to facilitate secure client-server communication without inhibiting the operability of mobile applications.

2.8 Text messaging.

28. The network will allow text messages to/from any device on the PSWBN to any other device on the PSWBN or any device on any commercial network which is capable of receiving or sending text messages. While the short-message-service (SMS) is commonly used on many networks today, it lacks a number of characteristics which are important to public safety, e.g. embedded location information. A text messaging service using the features of LTE would better serve public safety's needs.

2.9 Video.

29. A primary reason for building the PSWBN is to transmit real-time video to/from field units. Such video can be mobile-to-mobile, mobile to fixed sites (e.g. EMS Medic Units to hospital emergency rooms), fixed sites to mobile units (e.g. video surveillance cameras to police vehicles) and to/from aerial units.

30. Video applications must have user-selectable variable frame rates and priorities (QOS). This allows standard video on the network at low frame rates and quality. This allows, for example, surveillance video to transmit in lower quality, but then to be rapidly increased to higher quality, higher frame rates and higher priority when an incident occurs.

31. As a matter of course, most video should be recorded to semi-permanent media close to the source. For example, video from cameras mounted in police vehicles would be recorded to hard drives inside the vehicle. During an incident or urgent situation, it can also be broadcast across the PSWBN.

32. The network must support non-real-time video (e.g. video taken by a citizen's smartphone, then sent via NG 911 services to 911 centers and then relayed to field units. This video would be handled as file transfer (see below). Note: This functionality isn't currently supported in commercial networks. (Carriers have yet to implement SMS to 9-1-1.)

33. Certain kinds of video will receive high network priority and quality of service (QOS), user-selectable from device-native applications,whenever it is placed on the network, e.g. medical quality video transmitted from dispatched EMS units to hospital emergency rooms.

2.10 File Transfer.

34. The entire PSWBN should allow the transmission and download of static maps, mug shots, and other kinds of static images or files from any authorized source using standard FTP protocols.

35. The entire PSWBN should facilitate prioritized transfer and sharing of forms and media files that are user-selectable from the device level.

36. No bandwidth limitations should be placed on any high priority transmissions.

2.11 Bio-telemetry, telemetry and sensor data.

37. Many agencies or jurisdictions will purchase equipment and applications which will allow these functions. We assume the vendors of the equipment will write applications which can reside on mobile devices and equipment, and transmit data over the PSWBN. These applications will need to be certified as "well behaved" before being deployed by local jurisdictions. Much of this data will be low priority. Some of it, e.g. human bio-signs for public safety officers, will be very high priority on the network.

38. Transmit sensor data from multiple sources, including in-building sensor systems, municipally deployed sensors, chem/bio/nuc sensors, etc.

39. Low-bandwidth data such as electrical or water meter reading, weather info, etc.

40. Patient Multi-Vital Signs Monitoring. The ability to attach one or more micro-monitors to a patient to wirelessly receive and transmit electrocardiograph, capnography, blood pressure, and other vital signs packaged for display in a database. One project, by the Johns Hopkins Applied Physics Lab, suggested that simple multi-vital signs transmission require 76 kbps per sending unit and demonstrated a system that could monitor twenty wireless patient sending units per receiver at a time in a mass casualty situation.

41. Responder Multi-Vital Signs Monitoring: Similar to the Patient Multi-Vital Sign Monitoring, but intended for use by EMS responders monitoring fire, police and other responders in hazardous circumstances (e.g. firefighters inside a burning building; SWAT team members inside a building in a hostage taking scenario). This could also be used to detect chemicals, gases, radioactivity and other hazards being encountered by monitored responders.

42. Stand Off Vital Signs Monitoring: The ability to wirelessly detect, receive and wirelessly transmit multiple vital signs to a database without physically touching the patient.

2.12 Voice.

43. Voice applications are always the most important applications for use in any public safety network. However public safety requirements for voice networking are somewhat unique, e.g. talkaround (device-to-device voice communications without the need for an intervening cell tower/eNodeB or evolved packet core) and mission-critical voice dispatch. We know that 3GPP and ATIS specifications and standards are developing. We believe voice applications will gradually become available on LTE networks, and, over time, will be usable and adaptable for mission-critical public safety purposes. This evolution might include:
    43.1. Side-by-side functionality, where LTE is used for data network connectivity and a different technology in the same device (e.g. 3G circuit-switched technology) is used for voice calls.
    43.2. VoIP functionality over LTE data networks.
    43.3. LMR gateway - This function would allow an authorized user with a cell/smart phone on the PSWBN to link to an LMR gateway for voice/push-to-talk functions back to their home LMR network.
    43.4. Cellular telephony functionality directly over LTE networks, using LTE's inherent QOS and priority capabilities. Such capability should be available on commercial networks as soon as 2013.
    43.5. One-to-many broadcast capabilities, using the MBMS services of LTE.
    43.6. One-to-many dispatch capabilities using specifications to be incorporated in future releases of LTE.
    43.7. Mission-critical reliable voice dispatch and push-to-talk, one-to-many.
    43.8. Direct-connection from one PSWBN-connected device to another without need to relay through a cell tower/site, perhaps using non-LTE technology emplaced into devices. This is sometimes called "talk around" or " simplex".

3 Application Attributes

44. Further work must be done to define the attributes and characteristics for each such specific application. This work might be done by NIST or NPSTC or the national governing entity. These characteristics might include:

44.1. Priority on the network
44.2. Quality of Service
44.3. Pre-Emption
44.4. Security

4 User Requirements, Device and Location Support

45. It will be important for public safety to define the user requirements for subscriber units and end user equipment. We feel such definition is beyond the scope of this workgroup, given the time constraints for our work, but could include the following:
45.1. Handheld devices, e.g. "smartphones"
45.2. Tablet or slate computers
45.3. Robotic-mounted devices (short range, low to the ground)
45.4. Vehicle-mounted (mobile) devices
45.5. Aerial platform-mounted devices
45.6. Waterborne devices (e.g. on boats, ships)
45.7. Semi-fixed, devices, e.g. cameras deployed on tripods and set up around incident scenes.
45.8. Fixed location devices (on poles, buildings, etc.)

5 DRAFT Guidelines for Well-Behaved Applications

5.1 Background and Purpose

46. The Public Safety Advisory Committee (PSAC) advises the FCC's Emergency Response Interoperability Center (ERIC) related to the pending Public Safety Wireless Broadband Network (PSWBN). The PSWBN is planned to serve as a Long-Term-Evolution (LTE) based communications network to bear the applications, including ultimately voice, which first responders in the United States need to protect and serve the public safety. These applications will be developed from many commercial and government sources. Some applications will be national in scope, i.e. available anywhere, anytime, to first responders using any portion of the network. Other applications will be unique to certain agencies, jurisdictions, or locations and may be available just to a certain subset of responders.

47. The Applications and User Requirements Workgroup prepared a list of applications which it recommends should be available nationwide on the PSWBN (see Section 2 above). Such applications will include splash or welcome page, voice applications, video applications, text messaging and so forth.

48. The PSWBN will have high speeds and significant capacity. Nevertheless both its speed and capacity are limited. This system will be supporting a multitude of devices ranging from small handheld telephone like devices through laptop computers and any applications built to run on these devices and network must recognize this restriction and balance functionality versus use of network resources. This document recommends what sorts of rules and guidelines are necessary in developing such "well-behaved" applications.

5.2 Why Guidelines are Required

49. Equipment manufacturers and telecommunications carriers have been building commercial cellular mobile networks for almost 30 years. While the initial networks were voice-only, recent networks have supported smart phones and hundreds of thousands of applications which transfer and display large amounts of data. The carriers have learned a number of lessons – sometimes through the unfortunate experiences of running out of capacity and network outages – about both network and applications design.

50. Individual commercial cell sites need to support hundreds of simultaneous users. The spectrum available at each site is constrained as well is the backhaul capacity from individual sites to the overall system, which in-turn constrains user capacity. Poorly designed applications can consume large amounts of capacity, thereby denying use of the network to many users. Applications must be designed to appropriately balance functionality with frugal use of these constrained network resources. Likewise, carrier constraints on bandwidth can impede the capability and operability of mobile field applications. A balance must be maintained, and care must be taken to avoid technical constraints that discourage innovation by increasing its cost.

51. The PSWBN will be funded ultimately by public funds as so directed by elected officials and government agencies. It will be expensive to build, secure and maintain. Many elected and public safety officials have high – perhaps unrealistic – expectations for the capabilities of the PSWBN. These high expectations underscore the need for efficient, well-designed applications which make the network as usable as possible for first responders.

52. In addition, "technology marches on". Equipment manufacturers are constantly developing new devices with ever increasing capabilities supporting ever-more-complicated applications. Originally cellular networks only supported voice handsets. Newer subscriber devices supported text messaging. With the development of smart phones and tablet computers, a great leap occurred in the capability of the devices and their ability to drain network resources. As the mix of the devices on the network shifts to a higher percentage of more capable units, each with even more need for capacity and speed, attention to device and application resource performance becomes more critical. In addition "MiFi" and similar aggregation devices, where a single device connects to the network but rebroadcasts the signal to a small area in which many devices can connect will be more extensively used causing additional concentrated network impact. Agencies must have the ability, from the software level, to determine network access priority and to allocate available bandwidth to media and data transfers that are most critical at that time. It is recognized that this will vary by event and circumstance.

53. This evolution of devices undoubtedly will continue, driving the need for faster networks and well-behaved applications frugal in using network resources. Ultimately applications must be both network aware and network savvy to provide the highest levels of user efficiency.

54. Testing of Applications to help insure they are "well behaved" and are frugal with network resources is absolutely essential. This would be a primary purpose of the governing entity mentioned above.

6 Public Safety Application Guidelines and Standards

It is essential that the governing entity for the network will need to adopt guidelines, standards and a testing and certification protocol for applications. This section outlines what kinds of guidelines and standards should be adopted.

6.1 Outline for Application Guidelines and Standards

55. General characteristics
    - 55.1. Device operating system(s)
    - 55.2. Audio, video and multimedia codec recommendations
    - 55.3. Standards recommendations for use with application by type
    - 55.4. General device and user security and authentication recommendations

56. Impacts on control plane
    - 56.1. Device Centric
        - 56.1.1. Registration and location updating standards
        - 56.1.2. Remote management, testing, validation and security
        - 56.1.3. Over-the-air updating of device OS, security, applications and local data stores
        - 56.1.4. Machine to Machine (M2M) implications
        - 56.1.5. Peer-to-peer operation
        - 56.1.6. Ability to simultaneously operate on-network and in local simplex or talk-around mode
    - 56.2. Application level requirements
        - 56.2.1. User permissions beyond device authentication
        - 56.2.2. Status, both of the device and its user
        - 56.2.3. Presence, i.e. is the user online and available for any of a number of interactions including voice call, interactive data and/or push data, etc.
        - 56.2.4. Frequency of updates for push and polled data by application, user type, current user involvement and data type as well as within context of current system situation
        - 56.2.5. Email
        - 56.2.6. Other agency based public safety applications such as CAD and RMS
        - 56.2.7. Other agency administrative uses such as duty rosters, time accounting, etc
        - 56.2.8. M2M application guidelines such as for automated sensing and alarming devices

57. Impacts on traffic plane (video and voice)
    - 57.1. Video application guidelines
        - 57.1.1. Bandwidth aware and adjustable at the software level
        - 57.1.2. Downlink streaming
        - 57.1.3. Uplink streaming
        - 57.1.4. Chat and video conference
        - 57.1.5. Standards to assure interoperation
        - 57.1.6. Dynamic and adjustable bandwidth requirements
    - 57.2. Voice application guidelines
        - 57.2.1. Standards derived from commercial cellular VoIP
        - 57.2.2. Changes which are unique for public safety applications such as push-to-talk, talk-around, and simultaneous network/local operation
        - 57.2.3. Guidelines for behavior in mixed commercial and public safety wireless networks
            - 57.2.3.1. Normal case
            - 57.2.3.2. Public safety emergency case

57.2.3.3. System impaired case

58. Impacts on traffic plane (non-video, voice)
    58.1. Application guidelines by category (other than video)
        58.1.1. Social networking applications
        58.1.2. Messaging applications
        58.1.3. Browsing
        58.1.4. Database access applications
        58.1.5. Virtualization and thin client remote access

6.2 Some Proposed Guidelines - Details

59. Operating system. It is anticipated that a number of subscriber terminal operating systems will vie for a place within this environment. Given this reality, it is important to recognize and effectively manage development and testing to assure that system-wide interoperability and security is not compromised, and to ensure that innovation is not discouraged by technical or commercial constraints unique to each operating environment. There may be good reason to limit the number of authorized operating systems to help efficiently manage system evolution and application development cost effectiveness. It is also noted that Open Source operating systems, historically not considered for public safety system use, are likely reasonable options for consideration in this situation, provided that they promote and support independent application development through the provision of development tools and testing applications.

60. Legacy applications. As this system becomes available for public safety use there will be pressure to support legacy applications. These legacy applications should be subject to the same guidelines regarding network impact and performance as any new applications. This is especially critical for in-car computer and laptop based applications due to the dramatically larger network impact that this class of devices my represent.

61. Multiple layer system impact. Advanced wireless networks incorporate multiple operating planes or levels (control, traffic, etc) that support overall system operation. Applications must be designed and implemented with attention to their impact to each of these planes. Special attention should be given to minimize impact on the control plane given the overall impact to the system.

62. Use of maps, building diagrams and similar spatial or design documents. Applications using or displaying this sort of data or utilizing transfer of any large amounts of data should be designed to minimize their impact on the network. Strategies to eliminate or limit retransmission of static information should be utilized in favor of transmission of change information only. To the extent possible information such as base maps and diagrams should be stored on the device and updated with changes only as necessary. In addition to conserving critical system resources users will enjoy faster response time, and the network will not be over-burdened during an emergent incident. For "near real-time" information displays only dynamic information should be updated during the update cycle, not a complete refresh of the display. Displays of this nature should also consider an application design that pre-loads the device with static under layers with transmission of dynamic data only.
63. File transfer creates unique system performance impacts. While it is tempting to place hard limits and priorities on file transfer as is commonly done with commercial 3g networks today, it is recommended that a mechanism be implemented to allow high priority large transfers in unique situations with appropriate authorization. It is appropriate to establish default file transfer

characteristics that put this traffic at low priority and with total size constraints, provided that doing so does not defeat the utility or purpose of mobile applications designed to support critical response functions.

64. Web browsing. Any public safety or similar websites which are commonly used by first responders over the PSWBN must have a version which is optimized for mobile use, both to be frugal in bandwidth but also to recognize the smaller screen sizes and often lack of full keyboards associated with smart phones and slate/tablet computers. Application awareness of the capabilities of the user terminal device should ideally be utilized to modify application use accordingly.
65. Codecs and Protocols. A key goal of this initiative is to assure overall interoperable communications. In support of this, public safety applications slated for use in this environment should be standardized around a limited number of standard codecs and protocols. This has the further positive impact of minimizing the complexity of the devices and strain on the network while enhancing overall system performance.

66. Codecs can be implemented in hardware or software. In general, devices that utilize hardware based codecs operate more efficiently and enjoy longer battery life than similar implementations based on software codecs. Software based codecs are more easily able to be upgraded or enhanced over the life of a device and as new algorithms are introduced, provide enhanced functionality. It is recommended that the standardized codecs be implemented in hardware on all devices and applications should be implemented using the chipset codec, not a software codec, unless there is a clearly documented rationale to do so. Alternatively, applications could be designed to predominantly use the hardware-based codec for most uses and switch to a software codec only when mandatory to meet an operational need or to facilitate use during periods of adoption of new standardized codecs.

67. Cellular networks are asymmetrical, with uplink speeds significantly lower than downlink speeds. This has potential impacts on high-bandwidth interactive applications such as video chat and should be considered in the design and implementation of every interactive application.

68. Video streams from static sites (e.g. surveillance) or mobile locations (e.g. vehicles or handheld devices at incident scenes) should not be streamed live on the network until an incident or triggering situation occurs. Agencies must be able to determine file transfer priorities at the local level, and be able to upgrade or downgrade transmission priorities from the device software level.

69. Video should be streamed at a relatively low frame rate and quality until such time as higher frame rates and quality, up to HD, are required for the specific public safety incident in progress, consistent with paragraph 65 above

6.3 Additional Notes

70. The guidelines suggested in this document will need to be developed more completely in the near future by public safety, telecommunications, and other appropriate standards bodies

71. As the use of the network, the number of users, and the number of applications grow, the PSWBN will almost certainly reach saturation. This is not the only network available for use by public safety and careful consideration must be given to each proposed application to determine if this network, or one of the other wired or wireless options, is most appropriate for the intended use.

72. The PSAC's Applications and User Requirements Workgroup should, as a next step, consider how to build applications on top of standardized network services (e.g. IMS) and, perhaps, with standardized user interfaces.

73. Additional work also needs to address standards for push-to-talk and mission-critical public safety voice over LTE. That may be the domain of the PSAC, but is probably better informed by the work of the standards bodies (ATIS and 3GPP) and NPSTC.

7 Conclusion

74. This set of recommendations encompasses both a set of recommended applications, and a set of guidelines for developing, testing and deploying those applications so they are "well-behaved" and frugal with network resources. Considerable additional work must be done to further vet and create both the applications list and the guidelines.

8 References

- GPS standards information can be found at http://www.fema.gov/about/programs/disastermanagement/standards/dev.shtm, and is largely steered by http://www.opengeospatial.org/

- Significant portions of the applications lists and applications characteristics information was developed by the National Public Safety Telecommunications Council (NPSTC) and specifically its Broadband Task Force (BBTF).

9 List of Acronyms

3G	3rd Generation
3GPP	3rd Generation Partnership Project
CALEA	Communications Assistance for Law Enforcement Act
COPS	Community Oriented Policing Services
E911	Enhanced 911
eMBMS	evolved Multimedia Broadcast Multicast Service
EPC	Evolved Packet Core
ERIC	Emergency Response Interoperability Center
eUTRAN	evolved UMTS Terrestrial Access Network
FCC	Federal Communications Commission
Gbps	Gigabits per second

GPS	Global Positioning System
ICS	Incident Command System
IMS	IP Multimedia Subsystem
IP	Internet Protocol
kbps	kilobits per second
LMR	Land Mobile Radio
LTE	Long Term Evolution
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MMS	Multimedia Messaging Service
NPSTC	National Public Safety Telecommunications Council
OFDMA	Orthogonal Frequency Division Multiple Access
P25	Project 25
PDA	Personal Digital Assistant
PSAC	Public Safety Advisory Committee
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RF	Radio Frequency
SMS	Short Message Service
UASI	Urban Areas Security Initiative
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network