**Motorola Solutions Australia Pty Ltd** A.B.N. 16 004 742 312
10 Wesley Court, Tally Ho Business Park, East Burwood, Victoria 3151
Postal address: Locked Bag 27, Mt Waverley, Victoria 3149

Telephone +61 3 9847 7500
Fax +61 3 9847 7501

# Response to Australian Productivity Commission from Motorola Solutions Australia

# Public Safety Mobile Broadband Issues paper June 2015

## Executive Summary

Public safety organisations in Australia face unprecedented change. From managing daily operations with reduced budgets and resources to dealing with new and emerging threats, times have never been more challenging.

While voice communications will always be essential, data communications are rapidly becoming Mission Critical in public safety.

Intelligent, mobile broadband solutions represent the way forward for agencies to reach new levels of performance and safety for the community and their teams.

Rapid advances in technology can provide revolutionary capabilities for public safety.
To ensure these capabilities have their greatest impact for public safety, they must meet Mission Critical standards and enable agencies to convert the masses of information available today into useful intelligence which can be securely and reliably distributed to the right users in the field.

The benefits of Public Safety Mobile Broadband Solutions (PSMB) include immediate, daily productivity gains as well as enhancing agencies' ability to scale up to manage large scale and extreme events.

PSMB technologies are the key for agencies to move from *responding* to events to analysing data sources to *predict* events before they occur.

Motorola Solutions fully supports the delivery of a PSMB capability by 2020 to ensure Australia's public safety agencies can take full advantage of new and emerging technologies.

We advocate a balanced approach to building a national, standards based PSMB infrastructure in Australia.

Motorola Solutions' recommends adopting a hybrid approach to delivering a national PSMB capability because this is the most effective and economical option.
Our recommendation takes into account Australia's vast geography, population density variations across the country and the need to deliver PSMB in the most economic way for State and Territory governments. To support the delivery of a hybrid model, Motorola advocates that a dedicated allocation of spectrum for use by PSAs is made within popular, harmonised bands (the most desirable of which is band 28 APT 700 MHz).

A hybrid approach allows PSAs to have direct control over their level of operational risk regarding coverage, hardening, security, and performance by allowing selective deployments of purpose built capability utilising dedicated spectrum, enhanced by carrier coverage and infrastructure to provide PSMB over broader state wide jurisdictions.

In delivering this capability, essential, Mission Critical requirements should be maintained including:

- Adequate security levels to enable public safety users to collect and disseminate information, guaranteeing it is only accessed by authorised users
- Resilience to ensure networks operate without compromise in all conditions
- Reliability and sufficient speeds to provide Public Safety with performance exceeding commercial levels
- Dedicated spectrum resources to ensure Public Safety operations are not compromised in sensitive areas or where congestion is likely to occur
- Guaranteed minimum capacity levels for Public Safety that can be dynamically expanded through prioritised access to commercial spectrum when required for any critical incident or event
- Coverage throughout the vast jurisdictional areas that Public Safety agencies protect
- Complete integration of broadband capability with existing and proposed Land Mobile Radio (LMR) systems to extend Mission Critical voice via the broadband environment. (It should be noted that PSAs around Australia are currently making 7-15 year investments in LMR as a mandatory requirement).

Other vital requirements include:

- Agencies having direct, dynamic control of their essential communications
- Capability for Public Safety to integrate and manage new and emerging applications in response to changing operational needs
- The ability to choose combinations of applications, devices and private and public networks
- Flexible consumption models to enable agencies to scale up or down based on incident need
- Networks built on a common set of global Mission Critical standards
- Active, representation of Australia's interests in global standard setting forums to maximise the economic benefits of delivering PSMB locally
- Interoperability between private and public networks, supporting cross border operations and connectivity between both mobile and portable units in emergency and disaster relief situations.

To further support and expedite the delivery of a PSMB capability, Motorola Solutions recommends:

- A Federal, central forum be established to facilitate the setting of standards, policy, user requirements and interoperability needs nationally
- A Federal PSMB Innovation fund is implemented to facilitate State and Territory Governments with a common, standards based approach to the deployment of PSMB.

The responses in our submission are based on Motorola Solutions' experience of working in close partnership with public safety agencies for more than 45 years in Australia and 85 years internationally.

**Consolidated responses from Motorola Solutions Australia to questions from the Australian Productivity Commission**

1. *What is the merit (or otherwise) of the proposed approach to undertaking first principles analysis in this study?*

There have been several reviews into delivering a PSMB capability for Australia's PSAs, the most recent being the July 2013, Parliamentary Joint Committee on Law Enforcement Report on Spectrum for public safety mobile broadband, which recommended:

- *Recommendation 1: The committee recommends that the Minister for Broadband, Communications and the Digital Economy issue a Ministerial Direction to the Australian Communications and Media Authority to allocate 20 MHz of contiguous spectrum in the 700 MHz band for the purposes of a public safety mobile broadband network.*
- *Recommendation 2: The committee recommends that the Minister for Broadband, Communications and the Digital Economy take appropriate measures to secure, for public service agencies, priority access to an additional 10 MHz of spectrum in the 700 MHz band for public safety purposes.*
- *Recommendation 3: If recommendation 1 is not supported by the Australian Government, the committee recommends that the Minister for Broadband, Communications and the Digital Economy issue a Ministerial Direction to the Australian Communications and Media Authority to allocate as a minimum requirement, 20 MHz in the 800 MHz band for the purposes of a public safety mobile broadband network.*

There have been no further developments since July 2013 potentially putting lives and property of Australians at considerable risk with public safety agencies lagging behind their counterparts in the developed world in their ability to deploy the latest technology and communications capabilities.

The scale and frequency of crimes, terrorism events, emergencies, natural disasters, and their effects across Australia are increasing, requiring first responders to work efficiently and in a more effective, coordinated manner to achieve the best possible public safety outcomes. Any delay in providing a PSMB capability is hindering PSAs from realising daily operational benefits as well as their ability to move from reactive to predictive forms of protecting our communities.

Motorola Solutions therefore fully supports the restart of this stalled process with the undertaking of the first principles analysis in this study.

2. *What domestic or international developments, reports or experiences in PSMB (or related matters) are relevant to consider in this study?*

A number of studies around the world have confirmed that providing of Mobile Broadband capability for communications by emergency services would improve public safety services and operations. These include:

**Parliamentary Joint Committee on Law Enforcement – Report on Spectrum for public safety mobile broadband; (ISBN** 978-1-74229-898-6)
http://www.aph.gov.au/~/media/wopapub/senate/committee/le_ctte/completed_inquiries/2010-13/spectrum_mobile_broadband/report/report.ashx

**London School of Economics, "Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the EU: 2x10 MHz in 700 MHz in 10 European Countries" December 2013.**
http://www.lse.ac.uk/businessAndConsultancy/LSEEnterprise/pdf/tetraReport.pdf

**ECC Report 199, "User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks) May 2013".**
http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP199.PDF

**WIK Consult, "Final Full Public Report Study on behalf of the German Federal Ministry of Economics and Technology (BMWi) PPDR Spectrum Harmonisation in Germany, Europe and Globally" December 2010.**
http://www.wik.org/uploads/media/PPDR_Harmonisation_en_public_final_01.pdf

**TRPC "Public Protection and Disaster Relief (PPDR) Services and Broadband in Asia and the Pacific: A Study of Value and Opportunity Cost in the Assignment of Radio Spectrum" May 2013**. http://trpc.biz/wp-content/uploads/PPDR-_Report_June-2013_FINAL.pdf -

**US Phoenix Center Policy bulletin No. 26**
www.phoenix-center.org/PolicyBulletin/PCPB26Final.pdf

**Defence Research and Development Canada, "700MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications" February 2011.** -http://cradpdf.drdc-rddc.gc.ca/PDFS/unc122/p535072_A1b.pdf

**CITEL Recommendation on PPDR Spectrum Harmonisation in Americas:**
https://www.citel.oas.org/en/SiteAssets/PCCII/Final-Reports/P2!R-3323r1_i.pdf

**APT Report on "PPDR Applications Using IMT Based Technologies and Networks" April 2012. (APT/AWG/REP-27)** -
http://www.aptsec.org/sites/default/files/Upload-files/AWG/APT-AWG-REP-27_APT_Report_PPDR_IMT_Based_Technologies.doc

**APT Report on "Technical Requirements for Mission Critical Broadband PPDR Communications" September 2013. (APT/AWG/REP-38) -**
http://www.aptsec.org/sites/default/files/Upload-files/AWG/APT-AWG-REP-38-APT_Report_on_PPDR.docx

**White Paper on the Future Architecture of Mission Critical Mobile Broadband PPDR Networks – issued by the Federal Ministry of the Interior Project Group on Public Safety Digital Radio; Federal Coordinating Office Germany (document No. FM49)**
http://www.cept.org/Documents/fm-49/14437/FM49%2813%29-071-Info_White-Paper-on-Mission-Critical-Mobile-Broadband-PPDR-Networks

**Resolution ITU-R 646 (Rev.WRC-12)** – Public protection and disaster relief.
https://www.itu.int/dms_pub/itu-r/oth/0A/06/R0A0600001A0001MSWE.docx

**Report ITU-R M.2033 – Radiocommunication objectives and requirements for public protection and disaster relief, 2003.**
http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2033-2003-PDF-E.pdf

**Public Safety 700 MHz Broadband Statement of Requirements, v0.6, by the National Public Safety Telecommunications Council (NPSTC), USA, 8th November 2007.**
http://www.npstc.org/documents/Public%20Safety%20700MHz%20Broadband%20SoR%20v0.6.pdf

**700 MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications**
http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapi/smse-018-10-public-safety-sub2.pdf/$FILE/smse-018-10-public-safety-sub2.pdf

**US Phoenix center Policy bulletin No. 26**
www.phoenix-center.org/PolicyBulletin/PCPB26Final.pdf

**Motorola Solutions' submission to the Australian Parliamentary Joint Committee on Law Enforcement Inquiry into Spectrum for Public Safety Mobile Broadband.**
http://www.aph.gov.au/DocumentStore.ashx?id=0c073300-95a5-495d-9d96-02c159334384

3. *What are the implications (if any) of the Australian Government's review of the spectrum policy and management framework, and ACMA's ongoing work on spectrum allocation matters, for the delivery of PSMB in Australia?*

The implications as Motorola Solutions sees them are:

- The ACMA's review of the 800 MHz band has raised the possibility of allocating spectrum for PSMB which is currently occupied by LMR systems and would require relocation of those users to free it up for PSMB use. Historically, we have seen the experience of managing this in Australia taking at least three to five years
- There are two sub-bands within the 800 MHz band which are being considered for PSMB use in the ACMA's review. The internationally recognised bands are Band 27 and Band 26. The two sub-bands partially overlap with Band 27 having lower frequency limits than Band 26. Band 27 is adjacent to the APT 700 MHz band (Band 28). The use of Band 27 for LTE may cause interference to LTE systems deployed in the upper part of Band 28 due to a swap in the use of transmit and receive functions at the boundary between the two bands. If PSMB is allocated spectrum in the 800 MHz band this should be provided in Band 26.

4. *Are there any other PSAs that should be considered within scope in this study? To what extent are communications between PSAs and the community relevant to this study?*

5. *How do the organisational and institutional arrangements for PSAs vary between the Australian jurisdictions? What implications (if any) does this have for the way in which PSAs procure, operate and use communications services?*

6. *What is an appropriate definition of 'mission critical' communication systems and capability for the purposes of this study? What metrics should be used to assess whether capability is being delivered to adequate levels during mission critical circumstances? What evidence is there that existing capabilities are satisfactory or unsatisfactory?*

For PSMB systems "mission critical" should follow as closely as possible the definition used for today's public safety LMR narrowband systems. These requirements have been developed over several years in close cooperation with the PSAs.

It is the PSAs who should ultimately define the requirement. The definition is:

**Definition of Mission Critical Communication**[1]

A mobile radio communication system must fulfil four key requirements in order to be usable for mission critical communication:

i. The infrastructure must be resilient, redundant and highly available. (Public Safety networks in Australia are typically required to meet service availability levels of 99.95% availability or greater). This is normally achieved with the help of

[1] http://www.cept.org/Documents/fm-49/14437/FM49%2813%29-071-Info_White-Paper-on-Mission-Critical-Mobile-Broadband-PPDR-Networks

a redundant network architecture, redundant links between network elements and fail-safe network elements. Furthermore, base stations can increase the availability of their cells by operating in a fallback mode and by providing a minimum service when the connection to the infrastructure gets lost and when network wide services cannot temporarily be supported. Furthermore, main network elements need to be physically protected against intrusion and vandalism.

ii. Communication must be reliable. In a mission critical network, communication services have to be accessible and stable, i.e. network capacity has to be available even in case of large scale disaster scenarios. Furthermore, group and individual calls have to be setup in a predefined and extremely fast time, e.g. 500 milliseconds. Even at cell edge, speech packets, short data messages and packet data have to be reliably transferred to the end user.

iii. Communication must be secure. A mission critical network provides security functions in order to protect users from jamming, interception, and spoofing:

- mutual authentication of infrastructure and terminals;
- methods for temporarily and permanently disabling terminals and smart cards;
- functions to detect and compensate for jamming at the air interface;
- air interface encryption of user data and signalling data including addresses;
- end-to-end encryption of voice and data communication.

iv. Point-to-multipoint communication must be supported. Professional users mainly operate in groups. This is why, a mission critical network has to support point-to-multipoint communication, i.e. group calls, group addressed short data messages, and group addressed packet data.

If a mobile radio communication system does not fulfil the above four ‘mission critical’ requirements completely, then it can only be used for business critical communication.

Current narrowband PPDR technologies such as APCO P25 and TETRA comply with the above mentioned four ‘mission critical’ requirements for narrowband and wideband mission critical voice and data.

Although the LTE standard is currently being enhanced to support mission critical communication, it will be some time before mission critical features are developed, standardised and implemented by the LTE equipment manufacturers and operators upgrade their networks to become mission critical.

Existing Land Mobile Radio Public Safety Agency, mission critical voice systems within Australia and overseas typically include the following features and design capabilities:

- geographically redundant core (control) infrastructure
- multiple intra-site links to each site
- 12 or more hours of backup power for each site
- redundant site controllers at each site

- site base stations installed to provide a specified minimum number of simultaneous calls
- overlapping site coverage
- encrypted calls
- single button call establishment (push-to-talk or PTT)
- call establishment in less than 0.5 seconds
- emergency call prioritisation

Monitored systems can be measured to show whether the designed capabilities are being met. Metrics can be continuously collected and reported to the PSAs on a regular basis.

7. *What applications do PSAs currently use on their LMR networks that are provided for mission critical purposes? Does this differ by jurisdiction?*

Mission critical application data on narrowband, government LMR networks is usually limited to providing information such as:

- radio/ user identification
- status notification (including duress)
- location information (GPS)

Additionally, the following applications are available on *some* LMR networks but not typically used because voice is configured to take priority ahead of data applications.

- database inquiries
- drivers licence checks
- outstanding warrant checks
- patient care information
- despatch information from 000 operators

Due to the mission critical nature of many of these applications a number of agencies are utilising separate dedicated mission critical narrowband data networks to carry this traffic. These are the precursors to PSMB.

The type of data required typically does not vary tremendously from jurisdiction to jurisdiction it does however vary from agency type to agency type.

8. *How often are PSA narrowband networks (such as LMR networks) renewed or upgraded, and to what extent are different jurisdictions at different points in this process? What are the costs involved in maintaining these networks?*

Typically PSA LMR networks have life cycles which include timelines such as:

- 2-3 years for software items
- 3-5 years for computer and server hardware items

- 5-8 years for user radios such as mobiles and handhelds
- 8-10 years for base station infrastructure.

In addition to these items there is a need to provide and maintain the infrastructure needed to support the LMR network. This support infrastructure includes:

- Equipment shelters, huts or rooms
- transmission towers or poles
- inter-site microwave or fibre optic links
- power supply lines
- backup power systems
- site electrical earth systems
- security fencing
- access roads

The life cycle of these items vary considerably and depend greatly on the physical environment in which they are deployed.

9. *How do the different types of events that PSAs deal with affect their demand for communications capabilities? Can you provide examples or evidence to illustrate this?*

Example events include:

Barricades:
As shown in the attached document, "Barricaded Incident Analysis for PS-LTE.pdf", detailed analysis can be conducted on the way that public safety professionals actually respond to a hypothetical scenario where a PSMB system is used. It shows how the response of professionals can place heavy demand on PSMB bandwidth. This particular event shows how a hypothetical SWAT scenario will bring many public safety personnel into a close and dense location.

Major public events:
Events that draw large numbers of people to a central area can cause network congestion. For example, a large number of commercial network users communicating within a city on New Year's Eve could prevent PSAs from being able to upload and download critical communications including video at the very time first responders need it most.

Fires and floods:
These events can affect network resilience should sites be damaged and this will impede the ability for PSAs to issue warnings to the public as well as receive information from the community on the evolving situation. Additionally, this potential for congestion may also inhibit the ability of PSAs to receive management information including predictive fire maps. Network resilience is absolutely essential to the success of PSMB capability.

Routine traffic stops:
Although these events do not typically have higher bandwidth requirements, fully connected environments comprising a combination of devices, applications and sensors that interoperate with each other, often without human intervention, can be programmed to automatically deliver context aware information. This is particularly important at times when a responders personal safety if quickly and unexpectedly put at risk.

10. *How, and to what extent, are PSAs using mobile broadband capability provided over commercial networks, and related products and applications, to support their operational activities? Are there any lessons or insights from these experiences, including the benefits that are being realised?*

11. *How do other large organisations (such as government and corporate organisations with certain requirements which may be similar to those of PSAs) currently use mobile broadband services provided on commercial networks?*

12. *What lessons or insights can be taken from the previous trials of Telstra's LANES model, including during the G20 summit in November 2014?*

13. *Can commercial network solutions that involve dedicated spectrum for PSAs (and prioritised capacity in other spectrum bands during emergency incidents) allow for interoperability between networks operated by other mobile carriers and/or for end user to roam across multiple networks? Are there any technical, institutional or commercial barriers that would prevent this outcome?*

14. *What applications could PSAs use if they had access to PSMB capability? How could this be expected to vary across PSAs?*

    A PSMB network will provide the PSAs with internet-like connectivity, enabling tasks currently completed on a hardwired desktop PC in an office environment to be completed by officers out in the field, so long as the officer is in the coverage area of the PSMB network. This primary benefit of using applications is increased productivity for PSAs by enabling more work to be completed in the field as opposed to returning to the station. An additional, flow on benefit from this is increased visibility of our agencies within the local communities they protect and serve.

    Beyond extending the office environment into the field, PSMB can enable PSAs to operationalise a range of applications to enhance their situational awareness, improve their decision making, increase officer safety and optimise public safety outcomes.

    The way that data is used and the benefits received will differ for each PSA, for example;

- For police, access to higher quality images in all environments will assist with identifying individuals
- For paramedics, better access to databases such as known illicit drug lab or drug taking locations will increase officer safety in dealing with volatile environments
- For fire services, access to social services data including information on community residents whose properties are known fire risks will assist in preparing to combat fires.

Report ITU-R Report ITU-R M.2291 and APT Report 38 provide a number of case studies and examples of applications.

The greater speed and capacity that PSMB enables allows for wider use of higher capacity applications such as image and video as part of routine operations. Video can help to provide a large volume of detail in a very short period, and in a manner that is more insightful and compelling than the use of still images in isolation.

Applied to the PSA environment, video coupled with PSMB can be used for:

- Increasing levels of situational awareness for officers in the field, providing large volumes of contextual information at the time it is needed – improving the response of frontline officers and providing great officer safety.
- Contributing to the common operating picture, ensuring that all stakeholders, including command centre staff, management staff, incident controllers and even media divisions, have visual information during an incident as it unfolds
- Leveraging expertise from remote locations. For example:
    - Police sharing video from the field could enable a forensic specialist to brief other response team members before arriving on scene. This can help to ensure necessary evidence is protected/collected to improve case resolution rates
    - Paramedics sending and receiving video may enable telemedicine support to be provided from hospitals or other surgery environments to the field. Officers applying treatments using this information can help to shorten patients' recovery time and even save lives
    - Fire crews sending video from the field could help to increase the value of the input from remote staff to manage an incident while it is in progress.
- Connecting frontline responders directly or indirectly to a multimedia enabled community, for two-way sharing of content.

Video analytics that can require large computing power to achieve optimum public safety outcomes also require the input of high quality video. PSMB will assist with the delivery of video to the central processing centres. This helps to maximise the use of resources and creates a "force multiplier" effect whereby the actual number of officers in the field is outweighed by their true effectiveness.

As the proliferation of smart devices and sensors expands into PSAs' operational environments, significant amounts of data will be created and made available.
PSMB is required to ensure this information is utilised in real time and mid-incident, to gain its maximum benefit. Applications for PSAs include:

- Medical devices that can provide real time performance and patient information
- Medical equipment to provide status (including location), ensuring operations and locations can be confirmed
- Biometric sensors worn by officers to provide additional safety warnings for frontline officers, even alerting them to the danger before the officer becomes fully aware
- Nuclear or biological and chemical sensors carried in vehicles or worn on individuals, alerting of potential dangers and allowing for faster management responses
- Sensors in vehicles to provide status updates of the vehicle and the occupants
- Additional location information (beyond that available by GPS capability).

Examples of some applications that could be utilised by PSAs on PSMB:

- Command and Control applications
    - Location (including in field views of assets)
    - Dispatch
    - Video streaming
    - Frontline Incident management
    - Dynamic Navigation
- Video applications and associated analytics
    - In vehicle capture and streaming
    - Telepresence
    - Telemedicine
    - Body worn video
    - UAV based
- Database queries (records access)
    - Person, place/guns/patient history/building plans/ city services/ Hazmat, etc
- Facial recognition software
- Automatic number plate recognition and real time database updates
- Resource mapping applications
- Collaboration tools to enhance operations
    - Providing common operation pictures and Interoperability
    - Virtual whiteboards within workgroups
- Various tools to support in field mobility
    - In field reports
    - E –citations
    - Running sheets

    - Patient observation assessment and clinical cafe
- Control room solutions
- Wearable technology (used within the broader applications ecosystem) and developed specifically for public safety users including:
    - Body worn camera
    - Biometric monitors
    - Contextual sensors
- Social media access for officers in the field

15. *To what extent could these applications replace or supplement the capability and systems currently used by PSAs on their narrowband networks?*

    Virtually all of the application listed above will not operate efficiently or effectively on a narrowband network.

    Only a broadband network with sufficient speed, quality of service and capacity allows data rich application to transform PSA operations.

    In the US, FirstNet has been described to all PSAs as a PSMB system that augments (or supplements) current narrowband voice systems, *not* a replacement for the narrowband system. FirstNet sees the PSMB system as a broadband data pipe that provides additional and new functionality that narrowband voice systems cannot provide.

16. *How important are communications between PSAs and the community during emergency incidents?*

    This is becoming increasingly important for providing warnings to the public about major events as well for PSAs receiving information from the community to provide real time updates about evolving incidents and events.
    Interaction between public safety agencies, government and the community on social media is growing and has reached peaks during major events and natural disasters including the Queensland cyclone of February 2015 and December 2014 Sydney hostage crisis.

17. *What PSMB capability characteristics should be considered in this study?*

    At the most fundamental level, PSMB's overall capability should support the ability of PSAs to protect the community and their teams.

    Other essential field capabilities include:

    - Providing solutions that help to convert the masses of data available today into usable intelligence and securely disseminating it to officers in the field

- Providing information that is relevant to the tasks team members are managing at any given time
- Receiving easy to consume information for one or multiple users
- Ensuring the right information goes to the right public safety users in a manner that reflects their operational roles.

18. *How should 'national interoperability' be interpreted in this study? Does it include interoperability between networks, devices and applications used by PSA in different jurisdictions? Does it extend to integrating communications services between different local PSAs (for example, police, fire, ambulance and other responders)?*

National interoperability can certainly be interpreted to include interoperability between networks, devices and applications.
It can also be interpreted as an operational, non-technical requirement, such as communications between the various local PSAs.
Both technical and non-technical interoperability issues contribute to situations where State and Territory, cross border PSA operations such as large bush fires, floods and severe weather events have highlighted communications difficulties.

There are many operational circumstances where multiple PSAs are in attendance at a single or widespread incident. In each of these circumstances communications within and between PSA groups is essential to the outcomes of the situation. Interoperability in all of the scenarios outlined in the question should be available to the teams on the ground.

The definition of national interoperability needs to be defined by the PSAs themselves since they are the groups that either require it or not. There are many ways to solve interoperability challenges. When technology is standardised, it solves only one aspect of interoperability.

It should be noted however, that one of the biggest barriers to achieving interoperability has not been technical requirements, but the provision of efficient, cross-agency policies.

19. *Does delivering a PSMB capability raise any new opportunities for achieving national interoperability?*

The use of a consistent and harmonised spectrum regime will provide a consistent, interoperable environment nationally.

20. *Would the benefits, costs and risks of achieving national interoperability vary under different deployment options? If so, how?*

Motorola Solutions believes the delivery of PSMB under a hybrid model provides the best opportunity for national interoperability in an economically sustainable manner.

21. *What progress has been made in putting in place arrangements to better coordinate emergency communications within and across PSAs and jurisdictions?*

22. *What level of network coverage do the existing networks used by PSAs (for narrowband voice and low speed data capability) currently provide? How does this vary across jurisdictions?*

Narrowband networks provide greater coverage than commercial cellular networks do today. For PSMB to be fully Mission Critical it will require similar network coverage levels to narrowband networks.

23. *What level of mobile broadband network coverage do PSAs require across metropolitan and regional Australia? Does this vary for different PSAs?*

PSAs will need to define what level of mobile broadband coverage and capacity is acceptable to their own operations.

Currently, PSA narrowband voice systems typically require 95-98% area coverage and often include in-building coverage. Coverage is directly linked to voice quality and typical specifications for Public Safety voice quality are measured as Delivered Audio Quality (DAC).

The Public safety requirement is DAC3.4 or above where speech is easily understandable with little noise or distortion. Generally speaking, and with consideration of the cost of a PSMB system, PSAs would usually require a good level of in-building coverage in metropolitan areas, and coverage in rural areas with narrowband systems for voice communications. The coverage and capacity does not vary significantly across different PSAs, but this can change over time as the PSAs discover new applications that they can add onto the PSMB system.

24. *What is the most appropriate measure of network coverage for use in this study?*

Wireless broadband system design is driven by both coverage, capacity and throughput expectations. Coverage, capacity and throughput are interrelated and cannot be analysed independently. The first step to network coverage design is to identify the required operational coverage area and to define the traffic profile (capacity and throughput) of the users at each site. Based on the traffic profile, coverage tools can then be used to perform a coverage simulation to determine the number sites required to support both the coverage and traffic requirements.

25. *What options are there for extending the mobile coverage of commercial networks?*

26. *Would the benefits, costs and risks associated with achieving an acceptable level of network coverage for PSAs vary under different deployment options? If so, how? And with what operational consequences?*

27. *How could voice services — traditionally carried on narrowband networks be integrated into a mobile broadband network capability? What challenges and risks need to be accounted for? Are the challenges at the local level (due to legacy factors) greater than those at the national level?*

In the digital world today, voice is now treated as data (voice is digitised into packets and then transmitted as data packets on the network) and therefore it can be transported across a mobile broadband data network easily.

The real challenge for voice on a mobile broadband network is ensuring that voice packets are not delayed and are given a high enough priority so that they can be sent and reassembled at the receiving end without causing latency for verbal communications.

Unlike other types of data, like accessing a web page or doing a database query, voice packets require a constant stream of data packets to be received at the other end so that it can be reassembled and vocoded into an audible voice stream for the listener.

If the voice packets take too long, or arrive at random intervals, the voice will be presented to the listener with “audio holes” or “drop-outs”. The challenges of transmitting the voice packets in a consistent stream multiply greatly when there are multiple receivers, as in the case of two-way radio style users.

In this case, many high-quality data paths must be set up to each and every receiver. The complexity grows significantly as the network grows larger, from a local site to a region, state or a national level.

Another fundamental challenge to the integration of mission critical voice with PSMB is the speed in which talk group (all informed) communications are established. In today’s narrowband LMR systems any talk group member can initiate a group call via a single button press and the call is establish in less than half a second.

A range of “Over The Top Push To Talk” services are available in the market today that offer best effort services for the provision of group-based PTT capabilities over broadband. These services provide integration to a range of traditional narrowband services. Integration is achieved either through radio links or via direct wireline connections to digital, P25 narrowband systems.

These solutions are not standards based and work is currently occurring on defining standards from multiple bodies (OMA & 3GPP) to support Mission critical services on

broadband including group based voice (GCSE - Group Communication System Enablers & MCPTT Mission Critical PTT).

As the Standards evolve and features are deployed (including the use of real time broadcast capabilities (eMBMS) and dynamic user priority) these best effort services will evolve to become more of a mission critical solution.

It should be noted however that there are some services such as off network capabilities (ProSe – Proximity Services or Direct Mode) that are key public safety requirements that will require purpose built high powered devices and separate spectrum.

28. *What challenges or opportunities arise (from a technical, institutional and/or commercial perspective) from such integration, and would the benefits, costs and risks vary under different options for PSMB? If so, how?*

29. *The Commission understands that there is currently work underway to develop voice applications for 4G/LTE networks for use in mission critical circumstances. When are these applications likely to become available?*

In the future, LTE will have voice capabilities that will be valuable to public safety. However, networks will not initially be able to provide the Mission Critical level of voice service and dependability needed by public safety – this level of capability may not be able to be provided this for several years.

The proposed mobile broadband capability is intended to provide urgently needed broadband data access for public safety and is not initially being designed to replace current LMR, Mission Critical public safety voice systems. One key element lacking in the LTE technology is that it does not currently provide the “off network” capability levels that are critical for public safety. This means that when the broadband network is not available or not reachable there will be no communications. This would not be simply unacceptable for public safety users.

The US Public Safety Communications Research (PSCR), The Korean Ministry of Science, ICT and Future Planning and many other agencies around the world are working with the LTE standards body (3GPP), on the addition of a specification to the 3GPP LTE standard to support Mission-Critical Voice (MCV) over LTE, and to come up with a standard for off-network voice and data communications (simplex, tactical, peer-to-peer communications). But the Public Safety community has agreed that the most important function of the new LTE network would be to provide access to data and video and that voice over LTE (VoLTE) would be added at some point. They also agreed that LMR voice systems, which are the lifeline of the emergency responders, would be around for a long time to come.

It is currently estimated that the 3GPP will add mission-critical voice PTT to the LTE standards by 2018 through progressive updates in Releases 13, 14 and beyond. However, the addition of Mission critical voice is more than just a single application or

feature. This will be dependent on a range of capabilities that are being defined in the standards including security and console interfaces. It will be many years before mission critical voice becomes a reality in the public safety environment. Public safety voice communications must consider the following items.

- Mission-critical voice communications are the first and last lifeline for Public Safety users and must work reliably at all times. If Mission Critical voice is not made available on the LTE network, compatible users' devices must be provisioned which means extensive testing and verification is required before any devices are deemed ready for full-scale deployment
- To provide mission-critical voice, the Public Safety or PPDR network must provide the same or better coverage as the existing Land Mobile Radio (LMR) systems do today
- Mission-critical voice must provide a fallback mode in case of network failure. Today LTE has no fallback mode. If a cell site or a group of cell sites are out of service, the LTE user devices cannot communicate. With today's LMR systems there is at least one fallback mode—simplex or device-to-device communications—and many LMR networks offer several levels of fallback
- There must be a common standard. Today, Push-To-Talk (PTT) over LTE is available from network operators and a score of other players that offer cross-network PTT services. Some of these systems work pretty well and are being used today for non-mission-critical PTT. Further, many of these PTT solutions are being deployed with an IP bridge between the commercial network and LMR systems in order to provide communications to and from some LMR systems. However, no one standard has emerged and, in fact, many of the solutions are not compatible with PTT services offered by others. It would create severe interoperability issues if mission-critical PTT were permitted before there is a fully defined, approved, and well tested industry standard for PTT. This is what the 3GPP is working
- Mission-critical LTE voice must be able to support true despatch capability, in many cases, with multiple zones to mimic the LMR systems in major cities which are broken into zones or districts, usually with one of more citywide voice capabilities. Today this is accomplished using different LMR channels or with different talk groups in an LMR trunked radio system but this capability needs to be built into any LTE mission-critical voice system
- Other capabilities that must be provided for include talk groups that can be predefined or defined on the fly and the ability to combine multiple talk groups into a single group when needed. Finally, off-network voice, which is critical for Public Safety, must be robust, easy-to-use, and capable of being used while units are still within network coverage as well as when they are outside the LTE coverage area
- There are more capabilities that are required but the final test for any PTT technology or system is how quickly a user can talk on the system after pushing a PTT button, and how soon the others listening to that "channel" receive that transmission. A simple test for a PTT system is still the same as has been using for years—push the button and say, "Don't shoot," and make sure the first word is not lost due to system setup timing
- PTT must be a one-handed operation. Today on many of the commercial carrier networks equipped with PTT, smartphone users have to hold the phone in one

hand and “push” a button on the touch screen. This is unacceptable for certain roles and circumstances affecting public safety users.

30. *What factors are important in ensuring the integrity and security of communications for PSAs? To what extent does this differ for different types of PSAs?*

The integrity of communications for PSAs is critical since reliable and secure communications form the basis of PSAs’ responses in both crisis environments and for daily operations. PSAs, governments, and the general public demand the systems remain operational in the worst of conditions so that the first responders can come to the aid of the victims.

In terms of security of communications for PSAs, many PSAs may, in the course of executing their duties, transmit and convey information that may be protected by privacy laws. As such, having a secure communications channel is very important to comply with relevant laws and regulations. Some PSAs may require a secure communications channel in order to carry out their duties to enforce the law, such as surveillance, drug interdiction, etc.

Integrity and security can vary from across each PSA and every agency has its own policies to determine the level of need. For example, if one PSA has a bad crime problem, then a secure communications system may be required for use. Another PSA may have almost no crime and therefore wouldn't need a secure communications system. All PSAs require integrity of communications.

To that end, the factors that are most important to PSAs for ensuring integrity and security are: coverage for all areas they need to operate in, capacity so that they can get a channel when they need it most, the ability to encrypt their voice and data when required, redundancy and resilience in the infrastructure, fast service in case of a failure, trusted end-to-end encryption schemes and architecture, capability to deliver Mission Critical communications.

In addition, the integrity and security of the communication service itself, rather than the information that is transported by it, is also vital. As governments and PSAs consolidate and share communications solutions, these solutions become greater targets for attack and as such, measures must be taken to protect against the risk of both physical security and cyber security (firewalls, intrusion detection, antivirus, etc.).

31. *Would the costs and risks associated with ensuring the integrity and security of communications differ depending on how a PSMB capability is delivered? If so, how?*

From a security perspective encryption needs to be implemented that gives control directly to the respective PSAs.
The costs associated with this are unlikely to vary significantly depending on how PSMB is implemented. Data pertaining to the configuration of users such as provisioning, access and configuration data, may be required to be separated or

isolated and as such may dictate the need for separate database system components which may impact costs depending on the model implemented. A separate dedicated network provides the highest level of isolation however also costs the most.

32. *What methods or metrics could be used to define and/or measure the level of security provided over a network that delivers mobile broadband capability?*

33. *What additional security needs do PSAs have compared to other sectors with high security requirements for their communications?*

Many PSAs (especially police) have specified the need for mission critical applications (apply to both voice and data) to be end-to-end encrypted to achieve the highest level of security compared to commercial sectors.

In line with current digital LMR networks the UE device must support a software/hardware based encryption module that is FIPS 140-2 level 3 compliant. This means that the keys stored on the encryption module are tamper protected. For stolen device or any unauthorised attempt to access these keys in the device, the crypto module will be “zerorised” thus rendering the device unusable, thus protecting the confidentiality of further communications and information.

PSAs need the ability to control the encryption of devices and workgroups in a dynamic manner, with the ability to regularly change the encryption key.

Security is one of the key design considerations in any PS LTE solution architecture. The security solution needs to provide an extensive defence-in-depth security posture, with multiple layers of protection to ensure information confidentiality, integrity and user privacy. The security solution should minimally include the following:

- LTE Core Security
- In-transit Data Security
- Authentication
- Over-The-Air Security
- Device Security

34. *How should PSA demand for mobile broadband capability be estimated in this study, including their expected demand requirements into the future?*

Please refer to our response to question 2 that provides links to multiple reports on this subject.

With respect to future demand we are seeing exponential growth in data capability in the general community and predictions of growth in this segment may be of value in estimating PSA demand in the future.
It is worth noting however that PSA are starting form a lower base as compared to commercial users and as such, their acceleration may be greater once a PSMB capability is established.

35. *What methods or metrics could be used to define and/or measure the level of service capacity provided to PSAs?*

36. *What level of capacity will PSAs need for a PSMB capability, and how will this differ between business as usual activities and large scale emergency incidents?*

A number of studies mentioned in the response to question 2 (above) include methodology of estimating the PSA demand for mobile broadband capability. In particular:

- **The ECC Report 199,** http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP199.PDF - concludes that an amount of spectrum in the range of 2x10 MHz is needed for future European broadband PPDR Wide Area Networks (WAN) and there could be additional spectrum requirements on a national basis to cater for Direct Mode Operations (DMO), Air-Ground-Air (AGA), ad-hoc networks and voice communications over the WAN

- **The WIK Consult study** http://www.wik.org/uploads/media/PPDR_Harmonisation_en_public_final_01.pdf - concludes that the main driver for the PSA demand for mobile broadband is real-time video while other data applications (e.g. database/internet access) are less demanding, because some latency/contention is permissible. The Report estimate that based on realistic user requirements the data bit rates is 1.2 Mbps downlink and 1.9 Mbps downlink and concludes that PPDR broadband systems require 10 MHz for the uplink and 15 MHz for the downlink

- **The Canadian Defence Research and Development Canada,** - http://cradpdf.drdc-rddc.gc.ca/PDFS/unc122/p535072_A1b.pdf - estimates that the tactical video will play an increasingly important role to enhance situational awareness and by limiting public safety to 10 MHz (5+5 MHz) will require significant reduction in public safety broadband requirements, including a 50% reduction in video data rate and quality, and limiting simultaneous data users to 1 in 20 instead of 1 in 4. Even 20 MHz (10+10 MHz) is insufficient bandwidth to support the needs of public safety in the 10-15 year horizon

37. *How might the demand for PSMB capability differ between types of PSAs? How could competing demands amongst PSAs be managed? Should particular uses be prioritised?*

Demand for PSMB capability will differ between PSAs but also within a PSA.

By their nature, different incidents will require different levels of response from different agencies. The level of response required is not static either so resourcing and management needs may change as an incident unfolds.

It is also worth noting that while a particular incident may be underway, "normal" day to day activity that has the potential of life and death consequences still continues.

Subsequently there is a need for PSMB to support the ability for PSAs to not just statically prioritise but to dynamically prioritise users and applications, and even to "pre-empt" other users by removing them from the network when capacity is limited.

The U.S. National Public Safety Telecommunications Council concluded in April 2012 that Public Safety has unique QoS (Quality of Service) requirements including the need for Dynamic / Real Time, pre-emptive and discrete control of the priority of users on PSMB.

This dynamic prioritisation should not be simply limited to a user but rather, based on application type, user roles, agencies, incident types, mutual aid, quick action, and jurisdiction. For example;

- **Agency Priority** – The systems needs to moderate priority and QoS requests from different agencies to ensure each agency or user is given equitable QoS. This capability needs to be configurable on a per agency basis
- **User Role Priority** – An agency needs to prioritise network resources based on user roles. For example, an incident commander can be prioritized over a first responder
- **Application Priority** – An agency needs to prioritize any agency or regional application on the network. For example, a voice telephony call can be prioritized over a data session
- **Jurisdictional Priority** – Agencies need to prioritize their resources based on home or visiting jurisdiction. This prevents a responder who is not within their home jurisdiction from consuming critical resources needed by the local agency. For example, a responder's communications can be prioritized when they are within their home geographic area, and have lower priority when the responder is outside their home geographic area
- **Agency-Level Configuration** – Agency administrators need to be able to locally define their own set of users, roles, and the details of their own applications, including traffic type and relative priority. This allows each agency to make timely, customised updates to their QoS policy.

The management of competing demands will need to be agreed amongst PSAs and the necessary policies put in place.

*38. How would the benefits, costs and risks of ensuring sufficient capacity vary under different deployment options?*

Comparisons across these different deployment options are as follows:

1. **Dedicated Network (a full customer controlled dedicated private network)**

   The major benefits of a dedicated approach are that it provides the customer with maximum control over their level of risk in making decisions about coverage, hardening, security, and performance. These factors need to be carefully balanced against available funding resources.

   Capacity of a dedicated network will be guaranteed and provide user control of network access and priority but capacity and coverage will be limited to the dedicated PPDR spectrum allocated and actually deployed by the customer.

2. **Carrier network deployment**

   The major benefit of a carrier approach is that it gives PSAs access to carrier spectrum assets and coverage at commercial pricing arrangements.

   However, the carrier option provides PSAs with minimum direct control over their level of risk regarding coverage, hardening, security and performance. In addition, carrier networks do not provide direct PSA dynamic control of user access and priorities. These factors need to be carefully balanced against the operational benefits of PSMB to the PSAs.

   Carrier networks are not usually built and deployed to the levels of hardening and security that many PSAs demand. A careful assessment of carrier services should be considered to ensure the network operations and end-to-end application and data security meet the PSMB demands of public safety.

   To guarantee that PSAs have operational access to carrier capacity, carriers will be required to be both technically and commercially capable of offering prioritized, carrier network access and traffic priority. Without these technical and commercial arrangements in place, PSAs may not be guaranteed access to PSMB resources at times of heavy network demand (e.g. New Year's Eve, major sporting events and major, local incidents)

3. **Hybrid network**

Motorola Solutions believes an advanced hybrid approach that uses advanced LTE technology provides the most economically feasible solution for PSAs to gain access to the capacity they need to maximise their PSMB opportunities. This is a solution that can work effectively regardless of the location of an incident or event. The hybrid approach also provides all the benefits of a dedicated network as well as potentially guaranteeing access for PSAs to commercial carrier spectrum and coverage when they need it. This solution can also be provided under contracted SLAs if required.

A hybrid approach allows PSAs to have direct control over their level of operational risk regarding coverage, hardening, security, and performance by allowing selective deployments of purpose built capability utilising dedicated spectrum, enhanced by carrier coverage and infrastructure to provide PSMB over broader state wide jurisdictions.

Networks with capabilities such as dynamic user and application prioritisation with automatic load balancing can guarantee PSA users access and traffic priority on commercial spectrum should the PPDR and commercial spectrum become congested.

39. *What level of resilience do PSA narrowband networks usually provide and how does this differ from commercial mobile broadband networks?*

It is essential for PSAs to determine the minimum levels of resilience that they require for their own communications.

The following table summarises the key differences between the dedicated and commercial model of deployment of PSMB:

| PARAMETER | COMMERCIAL OPTION | DEDICATED PSMB OPTION |
|---|---|---|
| **BUSINESS OBJECTIVE** | **Revenue growth** | **Protect life and property** |
| **CAPACITY DESIGN** | **For "typical day"** | **For "worst day"** |
| **COVERAGE DESIGN** | **Based on population density** | **Based on full geographic coverage** |

| | | |
|---|---|---|
| **COMMUNICATIONS DESIGN** | **One-to-one communications** | **One-to-many and Off-network communications** |
| **BROADBAND DATA NEED** | **Centralised Internet Access and Heavy Download** | **Distributed Access (Traffic is Locally Generated, Logged and Consumed with Heavy Upload)** |
| **NETWORK RESILIENCY** | **Commercial Grade** | **Mission Critical Hardening** |
| **SERVICE PRIORITY DIFFERENTIATION** | **Device or application only** | **Dynamic Priority based on Incident Type and User Role** |
| **SECURITY CONSIDERATIONS** | **Carrier Controlled Device Authentication Only** | **Federated Agency-Based Identity Mgt. Used-based Authentication** |

Existing PSA, Mission Critical voice systems within Australia and overseas typically include the following features and design capabilities:

- Geographically redundant core (control) infrastructure
- Multiple intra-site links to each site
- Site operation without links
- Backup power for 12 or more hours for each site
- Redundant site controllers at each site
- Site operation without controllers
- Site base stations installed to provide a specified minimum number of simultaneous calls
- Continued operation with reduced capacity in the event of base station failure(s) overlapping site coverage.

Unlike typically commercial carrier services PSA narrowband networks or services are usually contracted to meet a set of stringent SLAs including availability, performance, response and restoration times. Transparency in reporting of service performance and coverage is also key.

40. *What methods or metrics could be used to define and/or measure the level of resilience provided by the networks used to deliver PSMB?*

Typically, the metrics used are based on a combination of availability of a particular service or capability within the network, and restoration time for failures (which can different from failures of a redundant portion of the network where the outage does not impact the service).

Traditionally, core voice services have been designed for the highest availability and have the more stringent SLA's compared to some other services such as configuration and reporting services.

41. *What priority should be given to the capacity to stand up a replacement service within a specified timeframe in the event of a physical or network based disruption?*

42. *Are there any barriers (for example, institutional, informational and/or technological) to, or challenges associated with, delivering a resilient PSMB capability? How might this differ between different deployment options?*

43. *How could future developments in technology, or growth in demand for mobile broadband services and capacity, affect the sustainability of PSMB capability under different deployment options?*

44. *How will the convergence of voice and data services affect the sustainability of PSMB capability under different deployment options?*

45. *What challenges are involved with delivering a mobile broadband capability to PSAs by 2020? Do these differ under alternative deployment options?*

Successfully delivery of mobile broadband capabilities to PSAs by 2020 requires;

- The allocation of suitable spectrum
- The clearance of the allocated spectrum in encumbered (this could be a number of years based on previous band clearing excercises)
- The development of suitable product both infrastructure and devices suitable for operation in the allocated bands
- The construction of a suitable network to meet PSA requirements. The time to achieve coverage will vary greatly depending on the deployment chosen.
  - Carrier services already provide baseline coverage but are not PSA grade.
  - Dedicated networks will by their nature be the longest to implement as they will require the securing sites or constructing new sites and necessary linking infrastructure to achieve coverage
  - A hybrid approach would provide the ability to leverage existing coverage and harden and augment with purpose built capacity and coverage where required.
- The time required to securing funding will impact the ability to delivery PSMB capability by 2020. This may be impacted by the quantum of funding required by the different deployment models.
- The establishment of linkages to existing LMR for both migration and long term interoperability
- Finalisation of necessary standards.
- The establishment of the appropriate governance bodies and agreement achieved with respect to items such as control, ownership, interoperability, prioritisation, SLAs etc.

46. *What potential obstacles exist to a mobile broadband network being fully compatible with a range of end-user devices? Does this depend on the network deployment option?*

There are several variables that may limit or prevent a PSMB from being able to use a full-range of end-user devices.

One is the PSMB spectrum. If manufacturers do not wish to make product for a particular spectrum, this can greatly reduce the range of devices. Manufacturers will make devices for the spectrum that will bring them the greatest return on their product development investments. Another area that may limit the range is software compatibility.

Generally, the device software must be able to work with the infrastructure software in order to enable certain types of functions. If the feature or function is absent in the device or in the infrastructure, this will limit full use of the function and/or the devices themselves.

To be fully compatible with a wide range of devices, the network must be thoroughly tested with each and every model of the subscriber that will be allowed on the

network. A test setup and lab will be required. This brings up another potential obstacle - cost to run such a testing lab. In the public carrier world, it is common practice to test each new device for functionality before deployment to consumers.

However, it's almost impossible to test for every function.

It is also important to note that it's not just about network-subscriber compatibility; it's also about "subscriber-to-subscriber" communications too. In a PSMB, a direct mode of operation is a mandatory requirement for all subscriber devices. Testing of the subscriber devices is a mandatory function that needs to be done to ensure a common baseline can be met.

Finally, the network deployment model can affect full interoperability with a wide range of devices.

In environments where PSAs do not have any control over system software updates, and these software updates occur frequently, there is potential to cause incompatibilities between the subscribers and the infrastructure. In a privately-owned model, the PSAs have total control over what is upgraded and when, and overall functionality of the system.

This model makes it very easy to control the release of software, thereby allowing the PSA to control any incompatibilities, and to manage the entire functionality of the system to match it with the devices. In general, the greater the control of the network, the better one is able to manage all the variables to ensure that you can minimise incompatibilities and bugs creeping into the system.

47. *How does the method of ensuring interoperability impact on the cost of the system to PSAs?*

48. *What detailed options should be evaluated in this study? What underlying assumptions and key parameters would be associated with each option?*

49. *What (if any) assumptions or parameters should be 'common' across all options?*

50. *What are the sources of costs relevant to this study?*

51. *In what ways could delivering a PSMB capability affect non PSA users? How would these effects differ across deployment options? What methods could be used to estimate these effects?*

52. *Is it appropriate to consider option values as part of the cost benefit analysis in this study? If so, how? What information or data is relevant?*

53. *Are the network cost elements identified in box 4 relevant for this study? What specific cost items would fall within these categories? What other network costs*

*should be considered? What is the nature and materiality of these (and other relevant) costs under alternative PSMB options?*

Yes, they are relevant. The specific cost items that should be considered are as follows:

Capital Costs (Capex)

- Site acquisition & construction (RAN tower, shelter, generator)
- Hardening costs (existing and new sites)
- Public safety deployable equipment and development
- Site equipment (eNBs, antenna, installation, etc)
- Core network equipment and installation (LTE core, IP core, NOC, data centres, HSS costs, spares, EF&I other one time service costs)
- Billing Platform
- Backhaul transmission capacity (Backhaul build, MW backhaul )
- Devices, handsets and terminals

Operating Costs (Opex)

- Network related costs
    - Site rentals, Leases
    - Backhaul
    - LTE Core
    - IP Core
    - NOC, data centres
    - HSS
    - Spares
    - EF&I
- Roaming charges
- Business function costs (utilities, customer acquisition, support, marketing and administration costs, etc)
- Equipment, facilities and depreciation

Studies have demonstrated that a dedicated PSMB network would require at least 2.5 times more capital costs than a shared network model. (OBI Technical Paper No.2, FCC 2010). The FCC study also demonstrated that overall, a partnership model as compared to a stand-alone network build, reduces opex and capex by at least 10% over a 10 year horizon.

This is largely because a shared model assumes leverage on the commercial assets of carriers, which would have large economies of scale by serving existing subscribers across Australia. One such example is billing platform. Under a dedicated system, site acquisitions and hardening costs, and eNBs are other major capital cost drivers. Additional sites tend to be higher for Greenfield site and one needs to consider incremental marginal costs for additional coverage outside current network coverage and adding new RAN for public safety to any existing site which has backhaul to a core network particularly in remote areas across Australia.

54. *What method(s) should be used to estimate the network costs of different deployment options for delivering PSMB? What studies should inform the Commission's thinking in this area?*

55. *What network cost components are interdependent with other costs, or other parameters (such as assumptions about the amount of spectrum allocated)? What is the nature of these interdependencies?*

There are several parameters and cost components with interdependencies which need to be considered and balanced against each other in order to deliver a PSMB system that meets PSAs' needs:

**Spectrum**: The quantum of spectrum used will impact the magnitude of network costs. A larger bandwidth may be required for the system (a 10 +10 MHz spectrum vs. 5+5 MHz spectrum) to support the traffic load. With a larger spectrum, the eNodeB site will require a larger backhaul leased line transmission bandwidth back to the EPC, thereby affecting the backhaul transmission capacity capital costs, The lack of sufficient bandwidth however will require an increase in the number of sites to achieve the same network performance characteristics.

Some countries charge PSAs for their own spectrum. This cost has a large impact on coverage and capacity design affordability, as the cost of spectrum is offset against capability due to the limited financial resources of PSAs. If using PSA-dedicated spectrum, there is assurance of non-interference and required capacity for emergency communications. The choice of spectrum has a large impact on the availability of base stations (eNodeB's) and user devices. If the spectrum allocated for PSMB is unique in the world, then there will be very few manufacturers supplying into that market. This, in turn, drives up the cost of equipment. Unique spectrum arrangements, like the use of carrier aggregation to increase bandwidth, will also drive unique product design, which increases costs. Keeping spectrum use simple and consistent with other major international markets will minimise device design and thereby lower overall network costs.

**Coverage**: The amount of coverage will drive a significant cost of the system as this determines how many sites will need to be deployed. A sub-dependency for the cost of coverage is sites, which includes the "buy or rent" decision, towered or on buildings, in-building coverage vs. street level coverage, urban vs. suburban vs. rural coverage, Greenfield vs. use existing sites only decision, etc.

**Capacity and throughput (or Traffic)**: The number of users and the amount of expected voice and data applications traffic will determine the bandwidth required. This will drive the design of the backhaul and amount of site capacity. Spectrum is highly linked to this as well because spectrum determines the amount of bandwidth per site. This will impact speed and performance; having too little spectrum will slow the performance of the system down.

**Capability**: The required features and functionality of the system are critical in a PSMB system. One common PSA feature is end-to-end encryption. Depending on the

architecture of the system and the deployment model, this feature can be relatively easier to implement for privately-owned or relatively more difficult for carrier model, thereby impacting core network capability cost.

56. *What data sources could be used to estimate expected PSMB traffic requirements, and the network infrastructure elements required to deliver PSMB capability under different deployment options?*

Each manufacturer will have their own ways to calculate coverage and capacity requirements. Capacity and coverage go hand-in-hand with PSMB systems. The architecture of the system will also affect the coverage and capacity, so it's important to understand how the system will be architected.

The recommended approach is to always work with a reputable partner that can do all of the coverage and capacity design work. While there are many LTE component manufacturers in the world, PSMB system design requires unique knowledge of the PSA environment and performance demands of the system. This affects the system design, which ultimately impacts coverage and capacity.

The selection of the right network elements becomes critical in the architecture and the design work. The different deployment options will also affect the coverage and capacity design. The multitude of variables that must be managed in the proper design of a PSMB system is quite large and requires experienced system designers to evaluate every element of the design to insure that it will perform optimally for the PSA.

57. *What data sources could be used to estimate the cost of the infrastructure, equipment and operation in delivering PSMB capability under different deployment options?*

58. *What is the appropriate approach (or approaches) to model the opportunity costs of spectrum under different deployment options? What issues does 'spectrum sharing' raise for estimating these opportunity costs, and how might they be addressed?*

59. *What data sources could be used to estimate the opportunity costs of spectrum under different deployment options for PSMB?*

60. *What is the appropriate discount rate, or range of discount rates, to use in this study?*

61. *How far into the future should costs and benefits be measured?*

62. *What are the sources of benefits relevant to this study?*

63. *How can the potential benefits of PSMB capability (in terms of PSA outcomes) be estimated? Is scenario analysis useful? How should scenarios be constructed to reflect an appropriate range of situations faced by PSAs?*

64. *Can you identify any trials or pilot programs of PSMB capability? Are there any insights to draw from these experiences about potential benefits (or costs)?*

    There have been and continue to be numerous PSMB trials that have been undertaken globally. More importantly a number of PSAs and government bodies have let contracts for the deployment of PSMB solutions. Two of these are Harris county Texas, which currently has deployed approximately half of its 30 contracted EnodeB sites and the Los Angeles Regional Interoperable Communications System (LA-RICS) which is deploying 82 EnodeB sites. http://www.la-rics.org/

65. *Can you identify evidence or examples that illustrate the effects of PSMB capability on PSA outcomes?*

66. *What method(s) should be used to value the effects of PSMB capability on PSA outcomes?*

67. *Is there research that considers how the costs of responding to natural disasters, crime or other events could be affected if PSAs had access to mobile broadband?*